ARTIKEL 29-DATENSCHUTZGRUPPE

10557/02/DE/endg.
WP 54

FÜNFTER 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 2000

TEIL II

Angenommen am 6. März 2002

FÜNFTER 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 2000

TEIL II

Angenommen am 6. März 2002

Inhalt

EINFÜHRUNG ZU TEIL II

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten[1], im Folgenden als die Artikel 29-Datenschutzgruppe bezeichnet, legt ihren fünften Jahresbericht für das Jahr 2000 vor. Der Bericht richtet sich an die Kommission, das Europäische Parlament und den Rat ebenso wie an die breite Öffentlichkeit. Die Artikel 29-Datenschutzgruppe ist das unabhängige Beratungsgremium der Europäischen Union zum Thema Datenschutz und Schutz der Privatsphäre[2]. Ihr Jahresbericht soll einen Überblick über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern[3] geben.

Die so genannte 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 Umsetzung galt eine Frist von längstens drei Jahren ab dem Annahmedatum (d. h. bis zum 24. Oktober 1998)[4]. 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 Artikel 29-Datenschutzgruppe und enthielt die wichtigsten Fakten, die 1996 im Bereich des Datenschutzes zu beobachten waren. Der zweite Bericht für das Jahr 1997 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 Europarates. Des Weiteren ging der Bericht auf die wichtigsten Entwicklungen in Drittländern und weitere Entwicklungen auf internationaler Ebene ein. Im vierten Bericht wurden die Aktivitäten der Artikel 29-Datenschutzgruppe in einem gesonderten Kapitel ausführlicher dargestellt und Fragen im Zusammenhang mit der Europäischen Union wurde mehr Platz eingeräumt.

Der fünfte Bericht wird nun erstmals in Form einer Broschüre in publikumswirksamer Aufmachung veröffentlicht. Aus diesem Anlass werden im ersten Teil des Berichts die Mitglieder der Artikel 29-Datenschutzgruppe und deren Sekretariat seit ihrer Einsetzung bis zum Jahr 2000 vorgestellt. Darüber hinaus erläutert Teil I den Auftrag der Artikel 29-Datenschutzgruppe und ihre Geschäftsordnung und vermittelt einen

---

1 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. Siehe Teil I, Seite 24.

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

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

4 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 EG-Vertrag).

Überblick über die wichtigsten Themenbereiche ihrer Tätigkeit im Jahr 2000. Das neu eingeführte Stichwortverzeichnis am Ende von Teil I erleichtert dem Leser das Auffinden von Informationen in den angenommenen Papieren.

Die wichtigsten Themen auf der Ebene der Gemeinschaft waren im Jahr 2000 die Übermittlung personenbezogener Daten in Drittländer, insbesondere die Vereinigten Staaten von Amerika im Rahmen der Vereinbarung über den „sicheren Hafen", sowie Fragen im Kontext von Internet, Telekommunikation und elektronischem Geschäftsverkehr und nicht zuletzt die Umsetzung der Richtlinie 95/46/EG.

Die Artikel 29-Datenschutzgruppe trat 2000 sechsmal zusammen. Sie befasste sich mit 53 Tagesordnungspunkten und erörterte im Zuge der Vorbereitung ihrer Stellungnahmen, Empfehlungen und Arbeitsunterlagen rund 66 Papiere.

Die Stellungnahmen und Empfehlungen der Artikel 29-Datenschutzgruppe 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.

Das Sekretariat der Artikel 29-Datenschutzgruppe stellt die

Europäische Kommission
Generaldirektion Binnenmarkt
Referat „Datenschutz"

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

http://europa.eu.int/comm/privacy

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

1.1. Richtlinie 95/46/EG

1.1.1. Umsetzung in nationales Recht

Österreich

Das Datenschutzgesetz 2000, BGBl. I Nr. 165/1999 zur Umsetzung der Datenschutzrichtlinie 95/46/EG wurde 1999 erlassen und trat am 1. Januar 2000 in Kraft. Da Österreich ein Bundesstaat ist, kann auf Grund der Aufteilung der Verantwortlichkeiten zwischen Bund und Ländern die Richtlinie auf Bundesebene nur auf denjenigen Gebieten umgesetzt werden, für die der Bund Gesetzgebungskompetenz besitzt, was aber jedenfalls im gesamten Bereich der automationsunterstützten Datenverarbeitung der Fall ist. Datenschutz bei manuell-strukturierter Datenverwendung fällt, soweit Daten für Zwecke der Länder verarbeitet werden, in den Zuständigkeitsbereich der Länder; diesbezüglich haben die Länder die Richtlinie umzusetzen. Tatsächlich sind auch bereits 7 von 9 Ländern über Verpflichtung durch Erlassung von Landes-Datenschutzgesetzen nachgekommen.

Im Berichtsjahr wurde in Umsetzung des Datenschutzgesetzes 2000 (und damit auch der Richtlinie 95/46/EG) die so genannte „Standard- und Musterverordnung“ erlassen, die mit 1. Juli 2000 in Kraft trat. In dieser Verordnung wurden einige „alltägliche“ Datenanwendungen - deren Maximalinhalt in der Verordnung genauestens festgelegt wird - von der Meldepflicht an das bei der Datenschutzkommission geführte Datenverarbeitungsregister ausgenommen (so genannte „Standardanwendungen“) und für bestimmte andere Datenanwendungen eine vereinfachte Meldepflicht vorgesehen (so genannte „Musteranwendungen“).

Belgien

Das Durchführungsgesetz ist am 1. September 2001 in Kraft getreten (Belgisches Gesetz vom 8. Dezember 1992 über den Schutz der Privatsphäre in bezug auf die Verarbeitung personenbezogener Daten, geändert durch das Gesetz vom 11. Dezember 1998 zur Durchführung der Richtlinie 95/46/EG).
http://www.law.kuleuven.ac.be/icri/papers/legislation/privacy/engels/

Nach der öffentlichen Anhörung im Dezember 1999 folgte im Verlaufe des Jahres 2000 die Ausarbeitung des königlichen Erlasses zur Durchführung des Gesetzes. Der am 13. Februar 2001 angenommene königliche Erlass (Amtsblatt von 13. März 2001) schreibt das Inkrafttreten des Gesetzes im sechsten Monat nach Veröffentlichung des Durchführungserlasses im Amtsblatt vor, d. h. am 1. September 2001.

Dänemark

Das Gesetz über die Verarbeitung personenbezogener Daten (Gesetz Nr. 429 vom 31. Mai 2000) wurde am 31. Mai 2000 angenommen und trat am 1. Juli 2000 in Kraft. Mit dem Gesetz wird die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umgesetzt. http://www.datatilsynet.dk/eng/index.html.

Das Gesetz löst das Gesetz über behördliche Verzeichnisse und das Gesetz über private Verzeichnisse ab.

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 in Finnland mit dem Gesetz über personenbezogene Daten (523/1999) umgesetzt, das am 1. Juni 1999 in Kraft trat. http://www.tietosuoja.fi

Am 1. Dezember 2000 wurde das Gesetz geändert. Dabei wurden Bestimmungen über die Verfahrensweise der Datenschutzkommission bei Entscheidungen und über die bindende Kraft der Entscheidungen in bezug auf die Übermittlung personenbezogener Daten in Drittländer gemäß der Datenschutzrichtlinie in das Gesetz aufgenommen.

Der Schutz der Privatsphäre ist in Finnland bereits seit dem 1. August 1995 ein Grundrecht. Gemäß der finnischen Verfassung ist der Schutz personenbezogener Daten in einem eigenen Gesetz geregelt.

Frankreich

Im Frühjahr 2000 ersuchte die französische Regierung die Datenschutzbehörde *(Commission Nationale de l'Informatique et des Libertés - CNIL)* und den Beratenden Ausschuss für Menschenrechtsfragen (Commission Consultative des Droits de l'Homme) um eine Stellungnahme zu dem vorläufigen Gesetzentwurf betreffend den Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten und zur Änderung des Gesetzes Nr. 78-17 vom 6. Januar 1978 über Datenverarbeitung, Archive und Grundfreiheiten. Der Gesetzentwurf wurde am 18. Juli 2001 vom Ministerrat angenommen und an die Nationalversammlung weitergeleitet. Die Lesung des Gesetzentwurfes in der Nationalversammlung wurde für Anfang Januar 2002 angesetzt. (http://www.assemblee-nat.fr/dossiers/cnil.asp)

Deutschland

Im Laufe der Modernisierung des deutschen Datenschutzgesetzes verfolgt die Bundesregierung ein Vorgehen in zwei Stufen :

Am 14. Juni 2000 beschloß das Bundeskabinett den Gesetzentwurf zur Änderung des BDSG. Der Bundesrat nahm zu dem Gesetzesvorhaben am 29. September 2000 Stellung, wobei er eine Reihe von Änderungswünschen formulierte. Am 13. Oktober 2000 wurde der Entwurf eines Gesetzes zur Änderung des des Bundesdatenschutzgesetzes und anderer Gesetze von der Bundesregierung im Deutschen Bundestag eingebracht (BT-Drs. 14/4329). Die Beratungen in den Ausschüssen des Bundestages begannen in 2000 und wurden mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 22. Mai 2001 (Bundesgesetz Gazette Vol. I, S. 904).

Im Nachzug zu dieser Novellierung, hat die zweite Stufe, die schon im Anlauf ist, eine grundlegende Reform des Datenschutzgesetzes zum Ziel. Ein wichtiger Schritt in diese Richtung war die Übergabe des Expertenberichts über die Modernisierung des Datenschutzrechts an das Bundesinnenministerium am 12. November 2001.
http://www.bfd.bund.de/information/bdsg_hinweis.html

Griechenland

Das Datenschutzgesetz wurde mit dem Gesetz 2472 über den Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten umgesetzt. Das Gesetz wurde am 10. April 1997 angenommen und trat am selben Tag in Kraft. Das Gesetz kann in englischer Sprache abgerufen werden unter http://www.dpa.gr/Documents/Eng/2472engl_all.doc

Irland

Derzeitiger Stand: Der Regierung wurde im Juli 1998 ein Entwurf für eine Rohfassung eines Gesetzentwurfs vorgelegt.

Weiterer Ablauf: Es wurde ein Gesetzentwurf erarbeitet, der von der Regierung angenommen und anschließend dem Parlament vorgelegt werden muss. Entsprechend dem Legistlativprogramm der Regierung ist von einer Veröffentlichung im Frühjahr 2002 auszugehen.

Italien

Die Richtlinie 95/46/EG wurde mit dem Gesetz Nr. 675 vom 31.12.1996, dem Datenschutzgesetz, in italienisches Recht umgesetzt.

Die Maßnahmen zur Angleichung der nationalen Rechtsvorschriften an die in dem Gesetz Nr. 675/1996 festgesetzten Grundsätze dauerten das ganze Jahr 2000 über an. Ausgehend von den Erfahrungen der zurückliegenden Jahre bei der Umsetzung des Gesetzes wurde insbesondere auf die Prüfung von Vollständigkeit und Wirksamkeit der im Datenschutzgesetz vorgesehenen Regulierungsmaßnahmen Wert gelegt und dabei diejenigen Bereiche ermittelt, in denen vermehrt ins Detail gehende, spezifische Bestimmungen notwendig erschienen. Durch diese eingehende Analyse verschob sich der Zeitpunkt der Annahme der Gesetzgebungsmaßnahmen, mit denen der ordnungspolitische Bezugsrahmen für die Verarbeitung personenbezogener Daten

fertig gestellt werden sollte, durch die Regierung auf den 31. September 2001. Auf das im März 2001 verabschiedete entsprechende Gesetz wird im nächsten Jahresbericht näher einzugehen sein.

Das erwähnte Gesetz sieht unter anderem vor, dass alle Bestimmungen, die den Schutz von natürlichen Personen und anderen Personen bei der Verarbeitung personenbezogener Daten sowie alle damit zusammenhängenden Maßnahmen bis Ende 2002 in einem konsolidierten Text zusammengefasst werden, um die Konsultation und die Koordination bei der Anwendung zu erleichtern.

Besondere Aufmerksamkeit sollte auf die Regulierungsmaßnahmen der Garante im Jahr 2000 gerichtet werden, da die Garante in diesem Jahr die von der Datenschutzbehörde vorgegebenen atypischen rechtlichen Instrumente zur Festlegung der Bedingungen, unter denen die Verarbeitung personenbezogener Daten für historische und statistische Zwecke rechtmäßig ist, einsetzte. Die Maßnahmen wurden 2001 unter Mitwirkung der maßgeblichen Interessenvertreter abgeschlossen. Für die genannten Bereiche wurden Verhaltensregeln und Leitlinien für die berufliche Praxis formuliert und angenommen.

Luxemburg

Der Gesetzentwurf für die Umsetzung der Richtlinie 95/46/EG in luxemburgisches Recht wurde dem Parlament am 7. Dezember 2000 vorgelegt.

Das Papier kann im Internet abgerufen werden unter www.chd.lu unter *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche avancée, Dossier Parlementaire n° 4735*.

Bislang liegen vier Stellungnahmen von folgenden Organen vor:

- Verband der Beamten und Angehörigen des öffentlichen Dienstes (*Chambre des Fonctionnaires et Employés Publics*)
- Staatsanwaltschaft (*Procureur Général d'Etat*)
- Arbeitskammer (*Chambre de Travail*)
- Verband der Beschäftigten in der Privatwirtschaft (*Chambre des Employés Privés*)

Niederlande

Als wichtigstes Instrument wurde in diesem Jahr das neue niederländische Datenschutzgesetz angenommen. Das Gesetz zur Umsetzung der Richtlinie 95/46/EG in niederländisches Recht wurde am 6. Juli 2000[5] angenommen.

[5] Wet van 6 juli 2001, houdende regels inzake de bescherming van persoonsgegevens (Wet Bescherming Persoonsgegevens), Staatsblad 2000 302. Eine nicht-amtliche englische Übersetzung des Gesetzes kann auf der Website der niederländischen Datenschutzbehörde www.cbpweb.nl. abgerufen werden.

Das neue Gesetz löst das Gesetz vom 28. Dezember 1988 ab, das allerdings in weiten Teilen übernommen wurde. Die wichtigsten Neuerungen:

- Der Geltungsbereich ist jetzt genauso definiert wie in der Europäischen Richtlinie. Während sich das bisherige Gesetz auf die sogenannte „Registrierung von Personen“ bezog, wobei der Schwerpunkt im wesentlichen auf der Aufbewahrung von Archiven über mehrere Personen lag, wird im neuen Gesetz konkret die in Artikel 2 der Richtlinie definierte „Verarbeitung“ angesprochen.
- Das neue Gesetz unterscheidet bei Verarbeitungsvorgängen nicht generell zwischen öffentlichem Sektor und privatem Sektor.
- Transparenz ist der zentrale Begriff des neuen Gesetzes. Insbesondere verweist das Gesetz auf die Notwendigkeit, den Betroffenen angemessene und aktuelle Informationen zur Verfügung zu stellen, damit sie anhand dieser Informationen über die sie betreffenden Daten entscheiden können.
- Es wurde ein entsprechend der Richtlinie formuliertes neues Widerspruchsrecht aufgenommen.
- Das neue Gesetz widmet ein ganzes Kapitel dem Thema internationale Datenübermittlungen in Länder außerhalb der Europäischen Union. Grundsätzlich dürfen Daten nur in Länder mit einem angemessenen Schutzniveau oder aber in den in dem Gesetz genannten Ausnahmefällen übermittelt werden. Das Justizministerium kann nach entsprechender Beratung durch die Datenschutzbehörde die Genehmigung für eine spezifische Übermittlung oder mehrere Übermittlungen erteilen, wenn der für die Verarbeitung der Daten Verantwortliche ausreichende Sicherheiten bietet. Dies kann insbesondere im Wege von vertraglichen Vereinbarungen geschehen.
- Nach dem neuen Gesetz wird die niederländische Datenschutzbehörde (bisheriger Bezeichnung: Registratiekamer) umbenannt in *College Bescherming Persoonsgegevens* und erhält verschiedene zusätzliche Kompetenzen. Hier ist insbesondere und zusätzlich zu den in dem Gesetz enthaltenen Strafbestimmungen die Ausstattung der Datenschutzbehörde mit neuen Vollmachten in bezug auf Sanktionen und die Verhängung von Geldstrafen oder behördlichen Zwangsmaßnahmen zu nennen. Die niederländische Datenschutzbehörde verfügt über keinerlei Kompetenzen in bezug auf Informationsfreiheiten.

Portugal

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

Die portugiesische Datenschutzbehörde gab 2000 Stellungnahmen zu Angelegenheiten mit direktem Bezug zu den Aktivitäten der Europäischen Union ab, so u. a. zur Angemessenheit der Datenschutzbestimmungen von Gesetzen Ungarns und der Schweiz sowie zu den Grundsätzen des „sicheren Hafens“, einer gemeinsamen Geschäftsstelle für die Kontrollinstanzen von Europol, Schengen und Zollbehörden sowie zur Verarbeitung personenbezogener Daten durch die

Einrichtungen und Organe der Gemeinschaft und das Recht auf freien Verkehr für diese Daten.

Schweden

Die EG-Richtlinie 95/46 wurde am 24. Oktober 1998 mit der Annahme des Gesetzes über personenbezogene Daten (1998:204) in schwedisches Recht umgesetzt. http://www.datainspektionen.se/in_english/default.asp?content=/in_english/legislation/data.shtml

Eine sekundäre Rechtsvorschrift, die Verordnung über personenbezogene Daten (1998:1191), trat mit demselben Tag in Kraft. Das vorherige schwedische Datenschutzgesetz, das Datengesetz (1973:289), behielt für Verarbeitungsvorgänge, die vor dem 24. Oktober 1998 eingeleitet wurden, vorläufig weiter Gültigkeit. Seit dem 1. Oktober 2001 sind die neuen Rechtsvorschriften nun allerdings in vollem Umfang auf die automatisierte Verarbeitung personenbezogener Daten anwendbar. Für die gesamte manuelle Verarbeitung gelten ab dem 1. Oktober 2007 die neuen Rechtsvorschriften.

Grundsätzlich ist das Gesetz zum Schutz personenbezogener Daten auf die Verarbeitung personenbezogener Daten in allen Sektoren anwendbar. Eine Ausnahme stellt allerdings die Verarbeitung personenbezogener Daten insoweit dar, als diese Verarbeitung spezifisch in einem anderen Gesetz oder Erlass geregelt ist. Spezielle Gesetze wurden für die Verarbeitung personenbezogener Daten im polizeilichen sowie im medizinischen und Gesundheitssektor erlassen (z. B. Gesetz über Aufzeichnungen medizinischer Daten (1998:543), Gesetz über Aufzeichnungen im Gesundheitswesen (1998:544), Gesetz über Aufzeichnungen über verurteilte Personen (1998:620), Gesetz über Aufzeichnungen über verdächtige Personen (1998:621), Gesetz über polizeiliche Daten (1998:622)).

Spanien

Wichtigstes Ereignis war das Inkrafttreten des Organgesetzes Nr. 15/1999 über den Schutz personenbezogener Daten am 14. Januar 2000.
(https://www.agenciaprotecciondatos.org/datd1.htm)

Vereinigtes Königreich

Im Jahr 2000 trat das Datenschutzgesetz (Data Protection Act) 1998 in Kraft. http://www.hmso.gov.uk/acts/acts1998/19980029.htm
Durch diese Rechtsvorschrift ist gewährleistet, dass das Vereinigte Königreich die Bestimmungen der Richtlinie 95/46/EG umgesetzt hat. Durch die Umsetzung wurde der Rahmen an Rechten und Verantwortlichkeiten gegenüber dem Datenschutzgesetz 1984 erweitert. Sekundäre Rechtsvorschriften, durch welche die Bestimmungen des Gesetzes wirksam werden, wurden ebenfalls eingeführt.

1.1.2. Vertragsverletzungsverfahren

Die Europäische Kommission entschied im Dezember 1999, Frankreich, Luxemburg, die Niederlande, Deutschland und Irland wegen der Nichteinhaltung der Pflicht zur Notifizierung aller zur Umsetzung der Richtlinie 95/46/EG erforderlichen Maßnahmen beim Europäischen Gerichtshof zu verklagen. Dieser Schritt stellt die dritte formale Stufe des formalen Verletzungsverfahrens gemäß Artikel 226 EG-Vertrag dar. Die Niederlande und Deutschland führten die Notifizierung 2001 durch, daher entschied die Kommission, die Klageanträge gegen diese beiden Mitgliedstaaten einzustellen.

1.2. Richtlinie 97/66/EG

1.2.1. Umsetzung in nationales Recht

Österreich

Die Richtlinie 97/66/EG wurde in Österreich mit dem Telekommunikationsgesetz, BGBl. I Nr. 100/1997, bereits im Jahre 1997 umgesetzt.

Belgien

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

Die Artikel 78 und 79 des Verbraucherschutzgesetzes vom 14.07.91 wurden abgeändert und enthalten jetzt auch Bestimmungen für unerbetene kommerzielle Kommunikationen. Die neuen Bestimmungen traten am 01.10.99 (*Moniteur Belge* (im Folgenden M.B.) 23.06.99) in Kraft. Artikel 9 des königlichen Erlasses 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 (M.B. 01.09.99) in Kraft. Ein königlicher Erlass für Telefonverzeichnisse wurde am 14.09.99 angenommen und trat am 18.09.99 in Kraft (M.B. 18.09.99). Dieser Erlass legt die Bedingungen für die Veröffentlichung personenbezogener Daten in Telefonverzeichnissen fest.

Artikel 105 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 Änderung trat am 21. Dezember 1999 (M.B. 21.12.99) in Kraft.

Dänemark

Die Richtlinie wurde in Dänemark mit dem Gesetz über Wettbewerbsbedingungen und Verbraucherinteressen im Telekommunikationsmarkt (Gesetz Nr. 418 vom 31. Mai 2000), durch die Rechtsverordnung über Datenbanken mit numerischen Daten (Verordnung Nr. 665 vom 6. Juli 2000) und durch die Rechtsverordnung über die Bereitstellung von Telekommunikationsnetzen und Telekommunikationsdiensten (Verordnung Nr. 569 vom 22. Juni 2000, jetzt Nr. 1169 vom 15. Dezember 2000) in nationales Recht umgesetzt.

Finnland

Die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurde in Finnland mit dem Inkrafttreten des Gesetzes zum Schutz der Privatsphäre und zur Datensicherheit im Bereich der Telekommunikation (565/1999) am 1. Juli 1999 rechtswirksam.

Als die Europäische Union eine Überarbeitung der Richtlinie einleitete, wurden gleichzeitig auch in Finnland Maßnahmen eingeleitet, um zu beurteilen, ob eine Revision der nationalen Rechtsvorschriften erforderlich sei.

Frankreich

Die französische Regierung unterrichtete die CNIL im Januar 2000 und nochmals im Juni 2000 über einen vorläufigen Gesetzentwurf und ihren Verordnungsentwurf zur Ergänzung der nationalen Rechtsvorschriften. Die Legislativmaßnahmen wurden am 25. Juli 2001 mit der Verordnung Nr. 2001-670 angenommen. Dieser Rechtstext nennt als Voraussetzung für die Zulässigkeit von Direktmarketing durch automatische Anrufsysteme oder Fax die vorherige Einwilligung der betroffenen Personen.

Deutschland

Telekommunikationsdatenschutzverordnung (TDSV).vom 18. Dezember 2000 (in Kraft seit 21. Dezember 2001)

Griechenland

Die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurde in Griechenland mit dem Gesetz zum Schutz personenbezogener Daten im Bereich der Telekommunikation (2670/98) umgesetzt.

Irland

Im Jahr 2000 erfolgte keine Umsetzung der Richtlinie in irisches Recht, allerdings wird mit der Umsetzung Anfang 2002 gerechnet.

Italien

Die Richtlinie 97/66/EG wurde durch die Gesetzesverordnung Nr. 171/1998 in nationales Recht umgesetzt.
Um die Verordnung voll mit der Richtlinie in Einklang zu bringen, müssen noch einige Änderungen vorgenommen werden, insbesondere mit Blick auf Notrufe und alternative Abrechnungsmodalitäten, die Gegenstand eines gegen Italien eingeleiteten Vertragsverletzungsverfahrens waren. Die Änderungen werden im Wege der auf der Grundlage des bereits erwähnten Gesetzes erlassenen Bestimmungen vorgenommen.

Luxemburg

Bislang wurde noch keine Vorlage für die Umsetzung der Richtlinie ausgearbeitet.

Niederlande

Die maßgebliche Rechtsvorschrift mit sektorspezifischen Vorschriften zu diesem Bereich ist das Telekommunikationsgesetz vom 19. Oktober 1998[6]. Mit diesem Gesetz werden Teile der Richtlinie 97/66/EG in niederländisches Recht umgesetzt, für weitere Aspekte müssen allerdings noch sekundäre Rechtsvorschriften erlassen werden.

Portugal

Die Richtlinie wurde 1998 mit dem Gesetz zum Schutz personenbezogener Daten und zum Schutz der Privatsphäre im Bereich der Telekommunikation – Gesetz 69/98 vom 28. Oktober 1998 - in nationales Recht umgesetzt.

Artikel 9 der Richtlinie: Die Datenschutzbehörde äußerte sich unter Würdigung der Gegebenheiten hinsichtlich Angemessenheit, Notwendigkeit und Verhältnismäßigkeit zu der Situation bei den nach dem nationalen Gesetz vorgesehenen Ausnahmen bezüglich der Unterdrückung der Rufnummernanzeige. Es wurde gefordert, dass in Fällen, in denen der Angerufene bei böswilligen Anrufen die Anwendung der Ausnahme geltend macht, der Betreiber des Telekommunikationsdienstes die Rechte des Anrufers und die Rechte des Angerufenen gegeneinander abwägt und hierfür z. B. weitere Informationen über Häufigkeit und Art der Anrufe anfordert. Ein einfacher

6 Wet van 19 oktober 1998, houdende regels inzake de telecommunicatie (Telecommunicatiewet), Staatsblad 1998 610.

Fragebogen würde es ermöglichen, über Angemessenheit und Verhältnismäßigkeit der Anzeige der Rufnummer des Anrufenden zu entscheiden.

Die portugiesische Datenschutzbehörde veranstaltete im November 2000 ein Kolloquium zum Thema „Schutz der Privatsphäre und elektronischer Geschäftsverkehr", an dem neben zahlreichen Unternehmen aus diesem Bereich sowie Studenten auch die französische Datenschutzbehörde (CNIL) teilnahm.

Unter großer Anteilnahme der Presse wurden auf diesem Kolloquium wissenschaftliche Studien und Praxiserfahrungen über den Stand des elektronischen Geschäftsverkehrs in Portugal und die von den in diesem Bereich tätigen Unternehmen angewendeten Online-Maßnahmen zum Schutz der Privatsphäre vorgestellt. Außerdem wurden unter anderem Ausführungen über die Grundsätze des Datenschutzes und des Einschreitens der Aufsichtsbehörden sowie die Rolle der Internet-Diensteanbieter für die Sicherheit der im Internet kursierenden Informationen, die digitale Signatur und die Verbraucherrechte von den Teilnehmern mit großem Interesse verfolgt und diskutiert.

Spanien

Wichtigstes Ereignis war das Inkrafttreten des Organgesetzes Nr. 15/1999 über den Schutz personenbezogener Daten am 14. Januar 2000.

Schweden

Die Richtlinie 97/66/EG wurde 1998 in der Hauptsache durch Änderungen des Telekommunikationsgesetzes (1993:597) und der Telekommunikationsverordnung (1997:399) umgesetzt. Die Änderungen traten am 1. Juli 1999 in Kraft. Die Umsetzung von Artikel 4 Absatz 1 der Richtlinie bezüglich Sicherheitsmaßnahmen erfolgte im Abschnitt 31 des Gesetzes über personenbezogene Daten, der am 24. Oktober 1998 in Kraft trat. Die Vertraulichkeit von Kommunikationen (Artikel 5 der Richtlinie) wird zusätzlich zu den Bestimmungen des Telekommunikationsgesetzes auch in Kapitel 4 Abschnitt 8 des Strafgesetzbuchs (1962:700) geregelt. Artikel 12 über unerbetene kommerzielle Kommunikationen wurde durch eine entsprechende Änderung des Gesetzes über Marketingpraktiken (1995:450) umgesetzt, die am 1. Mai 2000 in Kraft trat.

Vereinigtes Königreich

Die Telekommunikationsverordnungen (Datenschutz und Schutz der Privatsphäre) 1999 traten am 1. März 2000 in Kraft. Mit diesen Verordnungen ist die Richtlinie 97/66/EG (mit Ausnahme der Bestimmungen von Artikel 5) umgesetzt. Die Verordnungen bilden den Rechtsrahmen für die Telefon- und Telefax-Präferenzdienste im Vereinigten Königreich.

1.2.2. Vertragsverletzungsverfahren

Mit Ausnahme von drei Mitgliedstaaten haben zwischenzeitlich alle Mitgliedstaaten Maßnahmen zur Umsetzung der spezifischen Datenschutzrichtlinie (97/66/EG) notifiziert. Die Verfahren gegen Belgien, Dänemark, Griechenland und das Vereinigte Königreich wurden 2000 eingestellt. Die Kommission prüft derzeit die Maßnahmen, über die sie unterrichtet wurde. Im Juli 2000 entschied sich die Kommission allerdings für die Überweisung ihrer Klage gegen Irland wegen Nichteinhaltung der Pflicht zur Notifizierung aller zur Umsetzung der Richtlinie eingeleiteten Maßnahmen an den Gerichtshof. Die gleiche Entscheidung war bereits 1999 gegenüber Frankreich und Luxemburg getroffen worden. Der Generalanwalt trug seine Schlussausführungen in der Sache gegen Frankreich (C-151/00) am 26. Oktober vor. Bezüglich Artikel 5 der Richtlinie, für den als Frist für die Umsetzung der 24. Oktober 2000 festgesetzt worden war, wurden Frankreich, Irland, Italien, Luxemburg und dem Vereinigten Königreich mit Gründen versehene Stellungnahmen wegen der Nichteinhaltung der Pflicht zur Notifizierung der Kommission über alle zur Umsetzung der Richtlinie eingeleiteten Maßnahmen zugestellt. Bis Ende 2000 hatten elf Mitgliedstaaten Umsetzungsmaßnahmen notifiziert.

1.3. Von der Artikel 29-Datenschutzgruppe erörterte Themen

1.3.1. Übermittlung von Daten in Drittländer – USA: Die Grundsätze des „sicheren Hafens“

Die Artikel 29-Datenschutzgruppe gab 2000 ihre abschließende Stellungnahme zu diesem Themenbereich ab[7]. In ihren letzten Stellungnahmen hierzu erklärte die Gruppe, sie sei sich der wirtschaftlichen Bedeutung der Vereinbarung bewusst, doch sprach sie verschiedene Punkte an, in denen sie Bedenken hinsichtlich der Grundsätze hat.

Die fraglichen Punkte betreffen die Notwendigkeit klarzustellen, dass die Grundsätze des sicheren Hafens die Rechtsvorschriften der Mitgliedstaaten nicht ersetzen, die Möglichkeit für Unternehmen zum Beitritt zum sicheren Hafen, ohne den gesetzlichen Befugnissen der FTC oder einer vergleichbaren Instanz zu unterliegen, die Bandbreite der Ausnahmen von den „Safe-Harbor-Standards“, die Frage der Weitergabe von Daten an Dritte in den USA, die sich nicht auf die Grundsätze des sicheren Hafens verpflichtet haben, und nicht zuletzt die Schwachpunkte der vorgeschlagenen Durchsetzungsmechanismen. Die Artikel 29-Datenschutzgruppe dringt auf Verbesserungen in den genannten Bereichen, denn sie ist der Meinung, dass ein besseres Datenschutzniveau erzielt werden kann.

---

7 WP 31 (5019/00) Stellungnahme 3/2000 zum Dialog EU/USA betreffend die Vereinbarung über den sicheren Hafen, angenommen am 16.3.2000.
WP 32 (CA07/434/00/DE) Stellungnahme 4/2000 über das Datenschutzniveau, das die Grundsätze des sicheren Hafens bieten, angenommen am 16.5.2000.
Siehe auch Kapitel 3.3 Vereinigte Staaten von Amerika, Seite 68.

1.3.2. Standardvertragsklauseln

Zwar wird das Jahr 2000 vor allem als das Jahr der Diskussion mit den USA über den „sicheren Hafen“ in Erinnerung bleiben, doch legte die Artikel 29-Datenschutzgruppe in diesem Jahr auch die Grundlagen für die Genehmigung der Standardvertragsklauseln durch die Kommission im folgenden Jahr.

Musterverträge waren bereits zuvor ein Diskussionsthema gewesen, insbesondere, nachdem die Internationale Handelskammer und der britische Industrieverband (CBI) zwei Entwürfe für Musterverträge vorgelegt hatten. Aus der Diskussion wurde deutlich, dass zum einen die Vorschläge der Industrie weit hinter den Erwartungen der Artikel 29-Datenschutzgruppe zurückblieben, und dass zum anderen die Industrie offenkundig nicht bereit war, der Mehrzahl der geäußerten Bedenken Rechnung zu tragen. In der Folge wurden keine neuen Entwürfe vorgelegt und somit die Gespräche über beide Initiativen nicht fortgesetzt.

In dieser Situation machten die Gespräche über den „sicheren Hafen“ deutlich, dass eine Vertragslösung vor allem für diejenigen Wirtschaftszweige, die voraussichtlich nicht unter den Anwendungsbereich des Entwurfs für einen Beschluss der Kommission über die Angemessenheit der Grundsätze des sicheren Hafens fallen werden (US-Finanz- und –Telekommunikationssektor), dringend benötigt wird. In ihrer abschließenden Stellungnahme zu diesem Themenbereich bringt die Artikel 29-Datenschutzgruppe in ihrem Fazit diese Bedenken deutlich zum Ausdruck.

Die Dienststellen der Kommission übermittelten der Artikel 29-Datenschutzgruppe daher im Juli einen ersten Entwurf für einen Beschluss der Kommission über Standardvertragsklauseln. In der Sitzung im September erteilte das Plenum der Untergruppe „Standardvertragsklauseln“ den Auftrag, diese neue Initiative mit der Kommission zu erörtern. Die Untergruppe traf daraufhin mehrmals mit der Kommission in Form einer Art Entwurfsgruppe zusammen [8], die den Weg für die Aussprache im Plenum ebnet. Die Gespräche fanden im Oktober und im Rahmen einer Sondersitzung im November statt, die der Kommissionspräsident eigens zur Aussprache über das Papier einberufen hatte. Am Ende der Aktivitäten der Artikel 29-Datenschutzgruppe zu diesem Thema im Jahr 2000 steht ein Schreiben des Vorsitzenden an die Mitglieder des Ausschusses nach Artikel 31[9] mit einer Zusammenfassung des vorläufigen Fazits der Gespräche.

Der Beitrag der Artikel 29-Datenschutzgruppe zu dem Entwurf für einen Beschluss der Kommission über Standardvertragsklauseln muss besonders hervorgehoben werden. Dabei konnten die Mitglieder der Artikel 29-Datenschutzgruppe auf ihre

---

[8] An diesen Zusammenkünften nahmen die Vertreter der österreichischen, britischen, niederländischen, französischen und spanischen Mitglieder der Artikel 29-Datenschutzgruppe teil. Die Entwürfe wurden der Europäischen Kommission mit Blick auf eine Entscheidung im Sinne von Artikel 26 Absatz 4 der Richtlinie 95/46/EG vorgelegt. Die Kommission konsultierte die Artikel 29-Datenschutzgruppe. Die Artikel 29-Datenschutzgruppe bildete eine Untergruppe „Standardvertragsklauseln“ für die Vorbereitung der Aussprache im Plenum und die Ausarbeitung der Ergebnisse.

[9] Der Ausschuss, dem Vertreter der Mitgliedstaaten angehören, wurde gemäß Artikel 31 der Richtlinie 95/46/EG eingesetzt.

praktischen Erfahrungen mit Musterverträgen auf nationaler Ebene zurückgreifen, was von der Kommission für außerordentlich hilfreich erachtet wurde und entscheidend zu der einstimmigen Annahme des Beschlusses 2001/497/EG der Kommission durch den Ausschuss nach Artikel 31 beitrug.

1.3.3. Internet, Telekommunikation und elektronischer Geschäftsverkehr

A. Internet

Die Artikel 29-Datenschutzgruppe erstellte 2000 ein umfangreiches Papier[10] zum Themenkomplex des Schutzes der Privatsphäre im Internet, das neben einer Analyse der für diesen Bereich geltenden Richtlinien die bereits von der Artikel 29-Datenschutzgruppe angenommenen Stellungnahmen enthält. Das Papier ist das Ergebnis intensiver Vorbereitungsarbeiten der von der Artikel 29-Datenschutzgruppe 1999 gebildeten Taskforce „Internet" (ITF).

Mit dem Papier werden mehrere Ziele verfolgt. Hauptziel ist es, das Bewusstsein für die Gefahren für die Privatsphäre bei der Nutzung des Internet zu schärfen und gleichzeitig einen Leitfaden für die Auslegung der beiden einschlägigen Richtlinien[11] für diesen Bereich zu bieten. Darüber hinaus wird die Erwartung zum Ausdruck gebracht, dass das Papier neue Fragen anspricht, die nach entsprechender Ausarbeitung zu einem späteren Zeitpunkt erörtert werden könnten.

Da das Internet von Anfang an als ein offenes Netzwerk konzipiert wurde, über das riesige Mengen personenbezogener Daten verarbeitet werden, weisen viele seiner Merkmale – eher aufgrund von Nebeneffekten als von absichtlichen Entscheidungen – Aspekte auf, die das Eindringen in die Privatsphäre der Internet-Nutzer möglich machen. Durch die Verwendung von Browsermeldungen, Cookies und Hyperlinks kann unerkannt ein Profil jedes einzelnen Internet-Nutzers erstellt werden.

Das Arbeitspapier verweist darauf, dass die Untersuchung der Verarbeitung personenbezogener Daten im Internet von den Texten der Richtlinie 95/46/EG und im Einzelfall auch der Richtlinie 97/66/EG ausgehen muss.

In dem Papier werden die technischen Merkmale von elektronischer Post (E-Mail) und die damit zusammenhängenden Gefahren für die Privatsphäre erläutert. Angesprochen werden dabei u. a. die Speicherung von „gelöschten" E-Mail-Mitteilungen, Probleme in Zusammenhang mit der Nutzung von Webmail-Konten und die Möglichkeiten, die sich kommerziellen Betreibern durch „Sniffing" (Überwachung) und „Spamming" (unerbetene E-Mails) bieten. Das Papier gibt auch Auskunft über die Rechtmäßigkeit derartiger Aktivitäten gemäß den Richtlinien, wobei eindeutig darauf verwiesen wird, dass das Recht auf Geheimhaltung und Anonymität der Korrespondenz für elektronische Post genauso Gültigkeit haben muss wie für die herkömmliche Post.

---

10 WP 37 (5063/00) Arbeitspapier „Privatsphäre im Internet – Ein integrierter EU-Ansatz zum Online-Datenschutz", angenommen am 21.11.2000.

11 Richtlinie 95/46/EG und Richtlinie 97/66/EG.

Bezüglich der „Spamming“-Problematik spricht die Artikel 29-Datenschutzgruppe konkrete Empfehlungen aus, wie der Betroffene geschützt werden sollte – ausgehend von der Tatsache, dass auf Grundlage der geltenden EU-Rechtsvorschriften die Mitgliedstaaten die Wahlmöglichkeit zwischen einem „Opt-in“- und einem „Opt-out“-Verfahren haben. Zugleich spricht sich die Artikel 29-Datenschutzgruppe eindeutig für den Vorschlag der Kommission aus, durch die Einführung eines „Opt-in“-Systems eine Harmonisierung der Situation herbeizuführen.

Mit Blick auf das Surfen im Internet stellt das Papier ausführlich dar, welche personenbezogenen Daten bei den mit der Nutzung des Internet verbundenen technischen Abläufen gesammelt werden. Es verdeutlicht die „unsichtbaren“ Gefahren für die Privatsphäre, die bei der Nutzung des Internet zum einen durch das Speichern von E-Mail-Adressen und zum anderen durch die Analyse des „Online-Verhaltens“ der Nutzer bestehen. Darüber hinaus wird die durch neue Software gegebene Möglichkeit zur Erstellung umfangreicher Datenbestände über Internet.Nutzer geschildert.

Durch die Anwendung der Datenschutzgrundsätze auf den Internet-Prozess wird eine Reihe von Problemfelder deutlich gemacht – die Notwendigkeit nicht zu langer und klar strukturierter Datenschutzhinweise in eindeutiger und verständlicher Sprache auf jeder Website, der Anonymisierung von Daten, die nicht umgehend wieder gelöscht werden, der Gewährleistung der Zweckentsprechung der Verarbeitung und der Absicherung dahingehend, dass die Schnelligkeit der Datenströme im Internet nicht dazu führt, dass Datenschutzvorschriften vernachlässigt werden. Die Artikel 29-Datenschutzgruppe spricht sich konkret dafür aus, dass Daten über das „Surf-Verhalten“ den gleichen Schutz wie Inhalte genießen sollten.

Erörtert wird auch die Anwendbarkeit der Datenschutzgrundsätze auf Daten, die im Internet veröffentlicht werden (z. B. in Chatrooms, Verzeichnissen). Hierzu vertritt die Artikel 29-Datenschutzgruppe den Standpunkt, dass die Datenschutzvorschriften auch auf öffentlich zugänglich gemachte Daten anwendbar sind.

Ein weiteres Kapitel befasst sich mit der Rolle der Datenschutzvorschriften im elektronischen Geschäftsverkehr. Es wird dargestellt, dass für die Durchführung einer Online-Transaktion unter Umständen eine Vielzahl personenbezogener Daten zwischen zahlreichen Akteuren ausgetauscht werden muss. Hinzu kommt, dass die Aktivitäten der Verbraucher bei einer Transaktion im elektronischen Geschäftsverkehr in einem Maße detailliert überwacht werden können, wie es in der realen Welt nicht möglich wäre. Durch die Anwendung der Datenschutzvorschriften könnten die Akteure im elektronischen Geschäftsverkehr entsprechende Gefahren allerdings beträchtlich verringern.

Gemäß Artikel 7 Buchstabe b der Datenschutzrichtlinie ist die Verarbeitung personenbezogener Daten zulässig, wenn sie für die Durchführung eines Geschäftsvorgangs erforderlich ist. Hieraus leiten Internet-Händler den Anspruch ab, personenbezogene Daten ohne ausdrückliche Einwilligung der Betroffenen verarbeiten zu dürfen. Die Artikel 29-Datenschutzgruppe weist in diesem Zusammenhang allerdings darauf hin, dass die Verarbeitung von Daten über das für die Durchführung eines Geschäftsvorgangs erforderliche Maß hinaus oder für andere

Zwecke als die Durchführung eines Geschäftsvorgangs nicht rechtmäßig ist, wenn sie allein mit dieser Bestimmung begründet wird.

Abschließend empfiehlt die Artikel 29-Datenschutzgruppe die Anwendung von Technologien für einen bessern Schutz der Privatsphäre (Privacy Enhancing Technologies - PET) als einer technischen Lösung, mit der viele Datenschutzprobleme auf diesem Gebiet vermieden werden können. Diese Technik gewährleistet die Wahrung von Anonymität oder „Pseudo-Identitäten" und verhindert, dass Daten für andere Zwecke genutzt werden als diejenigen, für die sie ursprünglich erhoben wurden, und wahrt somit den Grundsatz der Zweckentsprechung. Außerdem spricht sich die Gruppe für die Einführung eines europäischen Standards für Datenschutzkennzeichen aus, um die Verlässlichkeit derartiger Kennzeichen zu gewährleisten.

In ihrer Schlussfolgerung spricht die Artikel 29-Datenschutzgruppe einige allgemeine Empfehlungen zu diesem Themenkomplex aus. Sie weist darauf hin, dass sowohl der öffentliche als auch der private Sektor in der Pflicht stehen, die Verbraucher auf die Gefahr der Verletzung ihrer Privatsphäre durch den Online-Verkehr und auch auf ihre Möglichkeiten, dies zu verhindern, aufmerksam zu machen. Sie fordert die Mitgliedstaaten dringend zu einer einheitlichen Anwendung der Datenschutzvorschriften auf und lädt die an der Entwicklung von Software Beteiligten dazu ein, bei der Konzeption ihrer Produkte den Datenschutz zu berücksichtigen.

B. Telekommunikation

Anfang des Jahres 2000 begrüßte die Artikel 29-Datenschutzgruppe den Vorschlag für eine Überarbeitung der Richtlinie 97/66/EG[12], zugleich brachte sie ihren Wunsche zum Ausdruck, an der Neugestaltung des Rechtsrahmens beteiligt zu werden. Sie verwies darauf, dass jede neue Richtlinie mit den Bestimmungen der allgemeinen Datenschutzrichtlinie 95/46/EG in Einklang stehen müsse, und befürwortete die geplante terminologische Überarbeitung der Richtlinie 97/66/EG. Nach Ansicht der Gruppe muss die wachsende Bedeutung der Software in der Telekommunikationstechnik bei der Änderung der Richtlinie berücksichtigt werden.

Gegen Ende des Jahres gab die Artikel 29-Datenschutzgruppe eine ausführliche Stellungnahme zum Vorschlag für eine Änderung der Richtlinie ab[13]. Die Gruppe begrüßte die Bemühungen um die Klärung der in der Richtlinie verwendeten Terminologie, forderte allerdings auch eine Klarstellung bestimmter Punkte und eine Erklärung für einzelne Änderungen.

Hinsichtlich des Inhalts des neuen Richtlinienentwurfs erinnert die Gruppe erneut daran, dass die Vertraulichkeit der Kommunikation die Regel sein müsse, von der es einige wenige Ausnahmen gebe. Weiter empfiehlt die Gruppe eine eingehende Überprüfung der Bestimmungen zu Verkehrsdaten und Standortdaten und stellt klar,

---

12 WP 29 (5009/00) Stellungnahme 2/2000 zur allgemeinen Neugestaltung des Rechtsrahmens für den Telekommunikationssektor, angenommen am 3.2.2000.

13 WP 36 (5042/00) Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, angenommen am 2.11.2000.

dass der von der ursprünglichen Richtlinie gewährte Schutz beibehalten, wenn nicht gar verbessert werden müsse. Mit Bezug auf die in der Richtlinie vorgesehenen Ausnahmen warnt die Gruppe vor einer Ausweitung gegenüber den bereits in der Richtlinie 95/46/EG enthaltenen Ausnahmen.

Weiter empfiehlt die Artikel 29-Datenschutzgruppe die Aufnahme eines spezifischen Hinweises in die Richtlinie, mit der die Industrie verpflichtet wird, bei der Entwicklung von Soft- und Hardware von Beginn an die Datenschutzgrundsätze zu berücksichtigen.

C. Elektronischer Geschäftsverkehr

Auch im Jahr 2000 befasste sich die Artikel 29-Datenschutzgruppe mit neuen Datenschutzfragen, die durch Entwicklungen im Bereich des elektronischen Geschäftsverkehrs entstanden. Dabei setzte sie sich eingehend mit dem Phänomen des „Spamming", also dem Versand von unerbetenen E-Mails[14], und elektronischen öffentlichen Verzeichnissen[15] auseinander. Die Artikel 29-Datenschutzgruppe verwies dabei auf die Probleme, die den Betroffenen durch diese neuen Technologien entstehen können. Im Fall der unerbetenen E-Mails die Sammlung von E-Mail-Adressen ohne Einwilligung und die Kosten für die Verbindungszeit, die diese E-Mails in Anspruch nehmen, und im Fall der elektronischen Verzeichnisse die Möglichkeiten des Eindringens in die Privatsphäre, die durch die Verfügbarkeit von inversen Verzeichnissen entstehen.

Die Artikel 29-Datenschutzgruppe verweist nochmals auf die Tatsache, dass das Datenschutzrecht auch auf den elektronischen Geschäftsverkehr Anwendung findet, und bringt ihre Auffassung zum Ausdruck, dass mit der Einführung der vorgeschlagenen Richtlinie über den elektronischen Geschäftsverkehr die Rechtslage in bezug auf die Datenschutzgrundsätze nicht verändert sondern vielmehr ergänzt wird.

In bezug auf das „Spamming" unterscheidet die Gruppe deutlich zwischen dem Fall, in dem ein Unternehmen eine E-Mail-Adresse direkt von der betroffenen Person erhebt und dem Fall, in dem E-Mail-Adressen ohne Kenntnis der Betroffenen in einem öffentlichen Bereich des Internet erhoben werden, und erläutert, wie die maßgeblichen Richtlinien[16] in beiden Fällen zum Schutz der Betroffenen angewandt werden können.

In bezug auf elektronische Verzeichnisse vertritt die Artikel 29-Datenschutzgruppe den Standpunkt, dass inverse Suchdienste nützlich sind und nicht grundsätzlich verboten werden sollten. Allerdings müssten die mit der Verarbeitung Beauftragten die Betroffenen über die neue Zweckbestimmung unterrichten, für die ihre Daten genutzt werden könnten, nachdem sie in die Verzeichnisse eingearbeitet wurden, und die Einwilligung der Betroffenen einholen. In dieser Frage befürwortet die Artikel 29-Datenschutzgruppe daher den Vorschlag der Europäischen Kommission für den

---

14 WP 28 (5007/00) Stellungnahme 1/2000 zu bestimmten Datenschutzaspekten des elektronischen Geschäftsverkehrs, angenommen am 3.2.2000.

15 WP 33 (5058/00) Opinion 5/2000 on the Use of Public Directories for Reverse or Multi-criteria Searching Services, angenommen am 13.7.2000.

16 Richtlinie 95/46/EG und Richtlinienentwurf über den elektronischen Geschäftsverkehr.

Entwurf einer Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation, der den verschiedenen Verwendungsmöglichkeiten insbesondere von elektronischen öffentlichen Verzeichnissen Rechnung trägt.

1.3.4. Umsetzung der Richtlinie 95/46/EG

Die Artikel 29-Datenschutzgruppe hält fest, dass eine große Zahl von Mitgliedstaaten noch immer nicht die entsprechenden Vorschriften zur Umsetzung der Richtlinie erlassen hat und verweist auf die negativen Folgen dieser Verzögerung[17]. Die Artikel 29-Datenschutzgruppe unterstützt die in der Folge von der Kommission als Hüterin der EG-Verträge eingeleiteten Vertragsverletzungsverfahren. Wenn Mitgliedstaaten die Richtlinie nicht umsetzen, fehlt der rechtliche Rahmen, auf den die nach Artikel 28 der Richtlinie eingesetzten nationalen Kontrollstellen ihre Entscheidungen stützen können und auf deren Grundlage sie ihre Beratungsfunktion entwickeln können. Benachteiligt sind letztlich die Bürger der betreffenden Mitgliedstaaten. Darüber hinaus besteht für die Wirtschaft Rechtsunsicherheit und die Vorteile des Binnenmarktes können nicht ausgeschöpft werden.

1.3.5. Genetische Informationen

Am 26. Juni 2000 gaben der Präsident der Vereinigten Staaten von Amerika und der Premierminister des Vereinigten Königreichs in einer gemeinsamen öffentlichen Präsentation bekannt, dass die Entschlüsselung des DNS-Bauplans durch ein Gemeinschaftsprojekt öffentlicher und privater Forschungseinrichtungen abgeschlossen wurde. Diese Bekanntgabe fand ein breites Echo in den Medien.

In einer am 13. Juli angenommenen kurzen Stellungnahme[18] begrüßt die Artikel 29-Datenschutzgruppe diese wissenschaftliche Errungenschaft, erinnert allerdings daran, dass die Gefahr eines Missbrauchs des genetischen Wissens berechtigte Sorgen weckt, was den Schutz der Privatsphäre angeht.

1.3.6. Verhaltensregeln

1) FEDMA

Die Untergruppe „FEDMA“ der Artikel 29-Datenschutzgruppe führte 2000 ihre Gespräche mit Vertretern der FEDMA fort und erstattete dem Plenum im Februar und im Oktober Bericht; zeitgleich wurden der Artikel 29-Datenschutzgruppe von der FEDMA Neufassungen der Verhaltensregeln vorgelegt. Es sind beträchtliche Fortschritte zu verzeichnen, und über eine ganze Anzahl technischer und inhaltlicher Fragen bezüglich der Verfahrensregeln konnte Einigkeit erzielt werden.

---

17 WP 30 (5139/99) Empfehlung 1/2000 zur Umsetzung der Richtlinie 95/46/EG, angenommen am 3.2.2000.

18 WP 34 (5062/00) Stellungnahme 6/2000 zur Genomproblematik, angenommen am 13.7.2000.

Ein schwieriges Thema war die Frage der Rechtmäßigkeit der Verarbeitung sensibler Daten zu Direktmarketingzwecken, in der auch innerhalb der Artikel 29-Datenschutzgruppe die Meinungen auseinander gingen. Die FEDMA ersuchte um eine offizielle Stellungnahme zu dieser Frage, die von Artikel 29-Datenschutzgruppe einstimmig angenommen und gegen Jahresende in einem Schreiben an die FEDMA übermittelt wurde.

2) IATA

Die Arbeiten zu dem Papier „Empfohlene Praktik 1774 – Schutz der Privatsphäre und grenzüberschreitende Flüsse personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden“ (RP 1774) des Internationalen Luftverkehrsverbandes (IATA) wurden 2000 fortgeführt. Im Verlauf mehrerer Zusammenkünfte zwischen der Untergruppe der Artikel 29-Datenschutzgruppe und der IATA wurde deutlich, dass diese empfohlene Praktik eine andere Zielsetzung hat als die gemeinschaftlichen Verhaltensregeln im Sinne von Artikel 27 der Richtlinie 95/46/EG. Allerdings bemühte sich die IATA um eine möglichst weitgehende Übernahme der von der Artikel 29-Datenschutzgruppe gemachten Vorschläge, um die RP 1774 mit der Richtlinie ein Einklang zu bringen und den Schutz der Privatsphäre und personenbezogener Daten im internationalen Luftverkehr zu verbessern. Im Dezember 2000 nahm die IATA die überarbeitete Fassung der RP 1774 an, zu der die Artikel 29-Datenschutzgruppe einen abschließenden Standpunkt formulierte[19].

1.3.7. Charta der Grundrechte der Europäischen Union

In ihrer Empfehlung 4/99 über die Aufnahme des Grundrechtes auf Datenschutz in den Europäischen Grundrechtekatalog unterstützt die Artikel 29-Datenschutzgruppe die Initiative des Europäischen Rates zur Ausarbeitung einer EU-Charta der Grundrechte und empfiehlt die Verankerung des Grundrechtes auf Achtung der Privatsphäre und auf Datenschutz in der Charta. Die Artikel 29-Datenschutzgruppe erklärte sich außerdem zur Mitarbeit bei der Ausarbeitung der Charta bereit. Dieses Angebot wurde mit der Ernennung des Vorsitzenden der Artikel 29-Datenschutzgruppe, Prof. Rodotá, zum Mitglied des Konvents zur Ausarbeitung der Charta wahrgenommen[20].

---

19 WP 49 (5032/01) Arbeitspapier über die empfohlene Praktik 1774 der IATA „Schutz der Privatsphäre und grenzüberschreitende Flüsse personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden“, angenommen am 13.09.2001.

20 Auf seiner Tagung am 15. und 16. Oktober 1999 in Tampere, Finnland, legte der Europäische Rat im Einzelnen fest, wie die Ausarbeitung der Charta der Grundrechte der Europäischen Union vonstatten gehen sollte.
Der Europäische Rat übertrug diese Aufgabe einem als „Konvent“ bezeichneten Ad-hoc-Organ aus Vertretern der Staats- und Regierungschefs, dem Präsidenten der Europäischen Kommission, Mitgliedern des Europäischen Parlaments und Abgeordneten der Parlamente der Mitgliedstaaten. Den Vorsitz des Konvents führte der ehemalige Bundespräsident der Bundesrepublik Deutschland, Roman Herzog.

Die Charta der Grundrechte der Europäischen Union wurde am 2. Dezember 2000 anlässlich der Regierungskonferenz über den Vertrag von Nizza vom Europäischen Parlament, dem Rat und der Kommission feierlich proklamiert[21].

Zusätzlich zu Artikel 7 über das Recht auf Achtung des Privat- und Familienlebens garantiert die Charta in Artikel 8 ausdrücklich den Schutz personenbezogener Daten. Die Bestimmung lautet wie folgt:

„(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

21 Veröffentlichung im Amtsblatt 2000/C 364/1.

1.4. Die wichtigsten Entwicklungen in den Mitgliedstaaten zu folgenden Themen:

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

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

C. Wichtige Rechtsprechung

D. Spezifische Themen

E. Website

für die folgenden Länder:

Österreich

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

Im Bereich der Bundesländer, die in Österreich in bestimmten Angelegenheiten Gesetzgebungskompetenz haben, wurden im Berichtszeitraum diverse Gesetze mit besonderer Datenschutzrelevanz vorbereitet bzw. erlassen:

In einigen Bundesländern wurden Novellen zu Landesjugendwohlfahrtsgesetzen erlassen, die insbesondere auch die Erstattung von Meldungen über den Verdacht der Vernachlässigung, Misshandlung oder des sexuellen Missbrauchs von Minderjährigen und die damit verbundene personenbezogene Erfassung dieser Daten näher regeln.

Weiters wurde das Wiener Archivgesetz (LGBl. Nr. 55/2000) erlassen, mit dem gesetzliche Regelungen zur Sicherstellung der Archivierung von Archivgut des Landes Wien und des Zuganges zum Archivgut des Landes und der Stadt Wien für den Bürger und die wissenschaftliche Forschung geschaffen wurden.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Mit BGBl. I Nr. 86/2000 wurde erstmals ein Militärbefugnisgesetz erlassen, das die gesetzliche Verankerung bestimmter im Rahmen der militärischen Landesverteidigung zu erfüllenden Aufgaben enthält und die Befugnisse militärischer Behörden und Organe für bestimmte militärische Aufgaben einschließlich der Verwendung personenbezogener Daten in militärischen Angelegenheiten normiert. In diesem Gesetz werden auch spezielle Rechtsschutzinstrumentarien betreffend den Bereich der militärischen Landesverteidigung, insbesondere ein „Rechtsschutzbeauftragter“, geschaffen.

In einer mit BGBl. I Nr. 85/2000 erlassenen Novelle zum Sicherheitspolizeigesetz wurde der Aufgabenbereich der Sicherheitspolizei auf die so genannte „erweiterte Gefahrenerforschung“ ausgedehnt (wobei dies Aufgabe aber sehr wohl an eine Situation anknüpft, in der es konkrete Anhaltspunkte für das Bestehen einer

sicherheitspolizeilich relevanten Gefahr gibt). Als besonderer Rechtsschutz in diesem sensiblen Bereich wurde ebenfalls die Institution eines die Tätigkeiten der Ermittlungsbehörden begleitend kontrollierenden Rechtsschutzbeauftragten geschaffen.

C. Rechtsprechung

Keine.

D. Spezifische Themen

Die Datenschutzkommission hat im Berichtsjahr ein Kontrollverfahren von grundsätzlicher Bedeutung durchgeführt. Und zwar handelte es sich um die Überprüfung des sogenannten Elektronischen Kriminalpolizeilichen Informationssystems („EKIS"), das vom Bundesministerium für Inneres zur Unterstützung der kriminalpolizeilichen Arbeit der österreichischen Sicherheitsbehörden betrieben wird. Anlass für diese Überprüfung war die Publikation eines Buches durch einen ehemaligen Polizisten, in dem dieser behauptete, dass ungerechtfertigte Abfragen aus dem EKIS, insbesondere über bekannte Politiker und Journalisten, im Polizeibereich häufig vorgenommen würden.

Im Rahmen dieses Systemprüfungsverfahrens wurde insbesondere die Frage aufgeworfen, welche Datenanwendungen aus dem Grund der Verbrechensbekämpfung von der Meldepflicht an die Datenschutzkommission ausgenommen sind. Gemäß § 17 Abs. 3 DSG 2000 sind Datenanwendungen unter anderem für Zwecke des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich bzw. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten nur von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist. Ansonsten besteht eine Meldepflicht. Insbesondere bei Datenanwendungen, deren Inhalt bereits in einem Gesetz determiniert ist, kann wohl keine Ausnahme von der Registrierungspflicht aus dem Grund der notwendigen Geheimhaltung geltend gemacht werden. Dementsprechend wurde dem Bundesministerium für Inneres (als Betreiber des Informationsverbundsystems) empfohlen, die im EKIS enthaltenen Dateien nach der neuen Rechtslage zu überprüfen und die notwendigen Meldungen unverzüglich nachzuholen.

Weiters vertrat die Datenschutzkommission die Ansicht, dass Zugriffsprotokollierungen, deren Auswertungen – rein „technisch" – nur durch sequentielle Suche vorgenommen werden können, sowohl im Sinn der Datensicherheit als auch zur Gewährleistung des Auskunftsrechts des Betroffenen nicht ausreichend seien. Die Protokollierung der Zugriffe auf das EKIS sei derart zu gestalten, dass ohne unverhältnismäßig großen Aufwand feststellbar ist, ob Abfragen über Daten einer bestimmten Person getätigt wurden und wer diese Anfragen aus welchem Anlass vorgenommen hat.

Empfohlen wurde auch, die Überprüfungen des Systems auf mögliche Abfrage-Missbrauchsfälle zu verstärken, wobei insbesondere auch die Entwicklung spezieller Unterstützungs-Software (z.B. Routineauswertungsprogramme) vorangetrieben werden und bald zum Einsatz gelangen sollte.

Das Bundesministerium für Inneres hat seine Bereitschaft bekundet, der Empfehlung Folge zu leisten und schon einige Punkte umgesetzt.

In Österreich laufen seit einiger Zeit Vorbereitungshandlungen für die Einführung einer flächendeckenden Sozialversicherungs-Chipkarte, die jede versicherte Person erhalten soll. Diese Chipkarte soll als Krankenscheinersatz dienen. Ende 2000 beschloss die Bundesregierung, dass diese Chipkarte insbesondere durch die Möglichkeit der Anbringung einer digitalen Signatur auch als „Bürgerkarte" fungieren solle. In weiterer Folge begann auch eine Diskussion darüber, inwieweit weitere personenbezogene Daten auf dieser Karte freiwillig gespeichert werden dürfen.

Weiters wurden im Berichtszeitraum Diskussionen über die Einführung eines Personenkennzeichens, insbesondere für den Bereich der Statistik, geführt. Insbesondere wurde die Frage erörtert, inwieweit bei Verwendung eines Personenkennzeichens technisch Missbrauchmöglichkeiten ausgeschaltet werden und der Datenschutz gewährleistet werden könnten.

E. Website der österreichischen Datenschutzbehörden

http://www.bka.gv.at/datenschutz/

Belgien

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Keine.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Das am 28. November 2000 angenommene Gesetz über die Cyberkriminalität wurde am 3. Februar 2001 im Amtsblatt veröffentlicht.

Zwischen beiden Kammern des belgischen Parlaments fand eine lang anhaltende Auseinandersetzung über die Dauer der Speicherung von Verkehrsdaten durch Betreiber und Diensteanbieter im Telekommunikationssektor statt, bei der es darum ging, ob diese Dauer *mindestens* oder *höchstens* ein Jahr betragen sollte. Schließlich entschied man sich für die Dauer von mindestens einem Jahr – entgegen der offiziellen Stellungnahme der belgischen Datenschutzbehörde (Commission de la Protection de la Vie Privée).

Das Gesetz überlässt es der Exekutive, die exakte Dauer der Aufbewahrung festzusetzen. Ein Erlass in dieser Frage wurde noch nicht verabschiedet.

C. Wichtige Rechtsprechung

Keine.

D. Spezifische Themen

Überwachung am Arbeitsplatz

Aufgrund der wachsenden Zahl von Anfragen an die belgische Datenschutzbehörde in bezug auf die Überwachung der Nutzung von E-Mail und Internet durch die Arbeitnehmer veröffentlichte die Behörde im April 2000 eine Stellungnahme mit Leitlinien und einer Erläuterung der rechtlichen Bestimmungen für eine solche Überwachung. Die Stellungnahme geht auf die wichtigsten anwendbaren Grundsätze ein, d. h. das allgemeine Verbot der Überwachung des Fernmeldeverkehrs, Transparenz und Verhältnismäßigkeit der Kontrollen, Interessenabwägung, begrenzte Speicherung der Daten. Die Datenschutzbehörde vertritt die Auffassung, dass die Überwachung auf begrenzte, objektive Daten gestützt werden müsse und nicht auf eine vorherige und systematische Kenntnisnahme der Inhalte des gesamten Datenverkehrs eines jeden Beschäftigten. Die Behörde schlägt hierfür den Einsatz von Softwarelösungen vor, durch die verdächtige Mitteilungen gezielt aufgespürt werden können.

E-Government

Der Prozess zur elektronischen Weitergabe von Informationen innerhalb der Verwaltung oder zwischen Verwaltung und Allgemeinheit entwickelt sich weiter. Um den Umgang mit Informationen durch natürliche Personen und auch durch Unternehmen zu erleichtern und zu beschleunigen, wurde beschlossen, generell für jede Person eine individuelle Identifikationsnummer zu vergeben. Diese Nummer wird auch in den geplanten elektronischen Personalausweis aufgenommen werden. Die Karte dient dann als Ausweis für alle Kontakte mit der Verwaltung und soll auch zur elektronischen Signatur von Dokumenten im Online-Verkehr eingesetzt werden (z. B. bei der Online-Abgabe der Umsatzsteuervoranmeldung). Die allgemeine Zielsetzung und die Effizienzvorteile des Projekts stehen sicherlich außer Zweifel, doch stellt sich die Frage nach Sicherheitsmaßnahmen, die die Gefahren eines Missbrauchs des Systems begrenzen; dies vor allem mit Blick darauf, dass eine der Hauptzielsetzungen die Erleichterung der Weitergabe von personenbezogenen Informationen zwischen verschiedenen Verwaltungsdienststellen ist.

Elektronischer Geschäftsverkehr

Die Datenschutzbehörde gab eine Stellungnahme ab, in welcher sie an die im elektronischen Geschäftsverkehr geltenden Grundsätze des Schutzes der Privatsphäre erinnerte. In der Stellungnahme wird dargestellt, bei welchen Vorgängen im Internet personenbezogene Daten erhoben werden, und auf die Pflichten des für die Verarbeitung Verantwortlichen zur Unterrichtung der Betroffenen und Wahrung der Verhältnismäßigkeit der Datenerhebung verwiesen. Die Datenschutzbehörde bekräftigt in ihrer Stellungnahme ihre Forderung nach Einholung der Einwilligung („Opt-in“) des Betroffenen vor der Übermittlung von unerbetenen E-Mail-Mitteilungen und erinnert daran, dass der Versand von E-Mails an Adressen, die in öffentlichen Bereichen des Internet erhoben wurden, rechtlich nicht zulässig ist. In der Stellungnahme wird auch auf die wichtigsten Grundsätze für die internationale Übermittlung von Daten hingewiesen.

Schutz von öffentlichen Daten

Bei der Datenschutzbehörde gingen verschiedene Beschwerden bezüglich der Erhebung von Daten über Angehörige bestimmter Berufe (Unternehmen und natürliche Personen), gegen die seitens der belgischen Sozialversicherungsbehörde Ermittlungen laufen und die in Listen für Verfahren vor Arbeitsgerichten geführt werden, durch Kreditauskunfteien ein. In einer Stellungnahme verwies die Datenschutzbehörde darauf, dass öffentlich zugängliche Daten durch die Rechtsvorschriften zum Schutz der Privatsphäre geschützt sind und dass für ihre Verarbeitung mehrere Grundsätze eingehalten werden müssen: Der Zweck der Erhebung (d. h. die Vermarktung der Daten für Kreditauskünfte) darf nicht mit dem ursprünglich vorgesehenen Zweck (in diesem Fall eine Veröffentlichung, mit der Dritten die Möglichkeit zur Teilnahme an dem Verfahren gegeben wird) in Konflikt stehen. Nach Auffassung der Kommission besteht bei dieser Datenerhebung ein Konflikt und zudem ist sie unrechtmäßig, weil die Verarbeitung der Daten, da es sich um gerichtliche Daten handelt, vom Gesetz verboten ist.

Schwarze Listen

Die personenbezogenen Daten derjenigen Kunden von Versicherungsunternehmen, die ein besonderes Risiko darstellen, werden über eine zentrale Datenbank verarbeitet. Ausgehend von den bei ihr eingegangenen Beschwerden hinsichtlich der Kriterien, die zur Übermittlung der Daten einzelner Kunden an die Datenbank führen, stellte die Datenschutzbehörde insbesondere die Angemessenheit der übermittelten Daten, ihre Verhältnismäßigkeit und die Unterrichtung der Betroffenen in Frage. Die Datenschutzbehörde fordert einen Regulierungsrahmen für diese Art von Aktivitäten.

Nationale Datenbank für Verbraucherkredite

Im November 2000 nahm die Datenschutzbehörde eine Stellungnahme zu einem Gesetzentwurf an, mit dem die Qualität der in die nationale Verbraucherkredit-Datenbank aufgenommenen Daten erweitert werden soll, die von der belgischen Zentralbank überwacht wird. Die Datenbank wird nicht nur Kreditinformationen über Zahlungsverzug enthalten, sondern alle Daten eines Verbraucherkreditvertrags. Die Datenschutzbehörde äußerte sich über die Dauer der Speicherung von Zahlungsverzuginformationen und formulierte Bedenken hinsichtlich der Verwendung der nationalen Identifikationsnummer durch die Zentralbank. Darüber hinaus bekundete sie den Wunsch, in die Maßnahmen zur Umsetzung der neuen Rechtsvorschrift einbezogen zu werden.

E. Website

http://www.privacy.fgov.be

Dänemark

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Jahr für Jahr werden verschiedene Gesetze und Verordnungen angenommen, die sich auf den Schutz der Privatsphäre und den Datenschutz auswirken. Herausragend in

diesem Bereich waren 2000 die Änderungen des dänischen Gesetzes über Vermarktungspraktiken.

Die zuständige Aufsichtsbehörde für das Gesetz über Vermarktungspraktiken ist die dänische Verbraucherschutzbehörde. Die wichtigste Änderung des Gesetzes betrifft Abschnitt 6 A.

Abschnitt 6 A Unterabschnitt 1 hat folgenden Inhalt: Wenn ein Lieferant Waren, bewegliches oder unbewegliches Vermögen oder Arbeits- oder Dienstleistungen an Abnehmer verkauft, ist er nicht berechtigt, Personen unter Verwendung von elektronischer Post, automatischen Anrufsystemen oder Telefaxgeräten zum Zweck eines derartigen Verkaufs zu kontaktieren, sofern nicht der betreffende Abnehmer vorher eine derartige Kontaktaufnahme angefordert hat.

Darüber hinaus darf ein Lieferant gemäß Abschnitt 6 A Unterabschnitt 2 eine natürliche Person nicht mit anderen Mitteln der elektronisch vermittelten Kommunikation zum Zweck des Absatzes der in Unterabschnitt 1 genannten Waren oder Dienstleistungen kontaktieren, wenn die betreffende Person den Lieferanten aufgefordert hat, derartige Kontakte zu unterlassen, wenn eine vierteljährlich auf der Grundlage des Meldesystems (CPR) erstellte Liste den Vermerk enthält, dass die betroffene Person die Kontaktaufnahme zu derartigen Marketingzwecken untersagt, oder wenn dem Lieferanten durch Recherche im Meldesystem bekannt ist, dass die betroffene Person eine derartige Kontaktaufnahme untersagt. Darüber hinaus gelten für die telefonische Kontaktaufnahme mit Verbrauchern die Vorschriften für unerbetene Anrufe des Gesetzes über bestimmte Verbraucherverträge.

Unterabschnitt 2 oben gilt nicht in Fällen, in denen der Betroffene zuvor um Kontaktaufnahme durch den Lieferanten ersucht hat.

Und schließlich muss der Lieferant bei einer ersten Kontaktaufnahme gemäß Unterabschnitt 2 oben mit einer bestimmten natürlichen Person, deren Name in der CPR-Liste nicht enthalten ist, diese Person in eindeutiger und verständlicher Form über ihr Recht unterrichten, Kontaktaufnahmen von Lieferanten gemäß Unterabschnitt 2 oben zu untersagen. Gleichzeitig muss der betroffenen Person eine einfache Möglichkeit zur Untersagung derartiger Kontaktaufnahmen geboten werden.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine.

C. Wichtige Rechtsprechung

Alle Rechtsfälle im Zusammenhang mit den beiden Einwohnermeldegesetzen wurden ebenso wie das Gesetz über die Verarbeitung personenbezogener Daten im Jahr 2000 von der dänischen Datenschutzbehörde verwaltungsrechtlich entschieden.

D. Spezifische Themen

1. Eine wichtige Aufgabe der dänischen Datenschutzbehörde war die Erarbeitung von Informationen und Leitlinien über das neue Gesetz über die Verarbeitung

personenbezogener Daten. Darüber hinaus gingen bei der Behörde aufgrund der in dem Gesetz vorgesehenen Übergangslösung zahlreiche Mitteilungen und Anträge ein, die bearbeitet wurden.

2. In einer Stellungnahme wandte sich die dänische Datenschutzbehörde gegen einen Vorschlag, nach dem Polizeikräfte ohne personenbezogene Autorisierung und zugehöriges individuelles und geheimes Kennwort Zugang zum zentralen Straftatenregister erhalten sollen. Bei dieser Lösung wäre es unmöglich gewesen, festzustellen, wer in dem Register eine Recherche durchgeführt hat. Der Empfehlung der Datenschutzbehörde folgend, verlangt die Polizeibehörde für den Zugang zu allen polizeilichen Systemen die Eingabe personenbezogener Autorisierungscodes mit zugehörigem individuellem und geheimem Kennwort.

3. Im Jahr 2000 wurden mehrfach Fragen im Zusammenhang mit genealogischen Forschungen an die Datenschutzbehörde herangetragen. Die Datenschutzbehörde vertritt dabei die Auffassung, dass genealogische Forschungen nicht unter das Gesetz fallen, solange der Genealoge die Herausgabe von Daten auf den engsten Familienkreis beschränkt, da es sich bei der von Genealogen durchgeführten Datenverarbeitung um die Verarbeitung von Daten durch eine natürliche Person handelt, die rein private Aktivitäten betrifft.

Werden die Ergebnisse genealogischer Forschungen z. B. im Internet veröffentlicht, gilt die Verarbeitung nicht mehr als eine rein private Aktivität. In diesem Fall gelten die allgemeinen Vorschriften für die Verarbeitung von Daten. Die Datenschutzbehörde vertritt die Auffassung, dass Daten wie Name, Geburts- und Todesjahr generell ohne Einwilligung der Betroffenen veröffentlicht werden dürfen.

4. Ein weiteres Schwerpunktthema war die elektronische Überwachung von Arbeitnehmern. Die Datenschutzbehörde erkannte, dass der Arbeitgeber ein legitimes Interesse daran hat, die Nutzung von Internet und E-Mail durch die Arbeitnehmer zu kontrollieren. Die Kontrolle muss für die Zwecke des vom Arbeitgeber verfolgten legitimen Interesses notwendig sein und die Interessen der Arbeitnehmer dürfen nicht über dieses Interesse gestellt werden. Die Arbeitnehmer müssen im Voraus in eindeutiger und verständlicher Form über die Kontrolle der Internet- und E-Mail-Nutzung unterrichtet werden.

Private E-Mail-Mitteilungen der Arbeitnehmer dürfen bei der Überprüfung der E-Mail-Mitteilungen vom Arbeitgeber nicht gelesen werden.

5. Im Jahr 2000 befasste sich die Datenschutzbehörde mehrfach mit Fällen, in denen Daten auf Homepages veröffentlicht wurden. Die Datenschutzbehörde vertritt die Auffassung, dass Daten über Arbeitnehmer ohne deren Einwilligung auf einer Homepage veröffentlicht werden dürfen, wenn die Daten mit der Arbeit im Zusammenhang stehen. Die Datenschutzbehörde stimmt generell der Veröffentlichung folgender Daten zu: Name, Tätigkeitsbereich, Beschäftigungsdauer, Telefonnummer und E-Mail-Adresse am Arbeitsplatz.

Daten wie Bilder, Privatanschrift, private E-Mail-Adresse oder Telefonnummer von Arbeitnehmern dürfen nur mit ausdrücklicher Einwilligung der Betroffenen veröffentlicht werden.

6. Darüber hinaus wurden der Datenschutzbehörde Fälle vorgetragen, in denen entlassene Arbeitnehmer auf eine „schwarze Liste“ gesetzt wurden, oder auch Fälle von Kunden in verschiedenen Wirtschaftszweigen, die Zahlungsverpflichtungen nicht nachgekommen waren oder Betrug begangen hatten. Die Datenschutzbehörde erteilte für einige dieser „schwarzen Listen“ unter bestimmten Auflagen und wenn mit den Listen ein legitimer Zweck verfolgt wird, ihre Zustimmung.

E. Website

Website der Datenschutzbehörde: www.datatilsynet.dk

Die Website ist überwiegend in dänischer Sprache gehalten.

Finnland

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Das Gesetz über personenbezogene Daten schreibt vor, dass der Datenschutzbeauftragte bei der Vorbereitung von legislativen und administrativen Reformen angehört werden muss. Der Datenschutzbeauftragte gab insgesamt 43 Stellungnahmen zu verschiedenen Gesetzentwürfen der Behörden und des Parlaments ab. Gemeinsam mit dem Justizministerium initiierte der Datenschutzbeauftragte eine Umfrage über besondere Rechtsvorschriften mit der das Ziel verfolgt wurde, notwendige Gesetzesänderungen voranzutreiben.

Das wichtigste Gesetz in bezug auf den Schutz der Privatsphäre, das 2000 in Kraft trat, ist das Gesetz über Status und Rechte von Sozialhilfeempfängern (812/2000). Das Gesetz stellt unter anderem das Recht der Sozialhilfeempfänger auf Selbstbestimmung und ihr Recht auf Zugang zu Informationen in den Vordergrund. Am 1. Oktober 2000 trat das Gesetz über die versuchsweise Einführung von nahtlosen Dienstleistungsketten im Sozialbereich und im Gesundheitswesen sowie einer Sozialversicherungskarte in Kraft, mit dem die regionale Zusammenarbeit im Gesundheitsbereich gefördert werden soll. Mit diesem Gesetz soll vor allem festgestellt werden, wie die Informationstechnologie für einen besseren Schutz der Privatsphäre instrumentalisiert werden kann.

Mit der Zunahme der Möglichkeiten, die die Informationstechnologie bietet, wächst auch der Druck zum Austausch von vertraulichen und geheimen personenbezogenen Daten zwischen den Behörden. In diesem Kontext muss der Datenschutzbeauftragte vermehrt nicht nur auf die Abwägung der relativen Bedeutung unterschiedlicher Interessen achten, sondern auch auf die Einhaltung der Voraussetzungen für die technische Übermittlung von Informationen.

Die Regierung legte am 9. Juni 2000 einen Vorschlag für ein Gesetz zum Schutz der Privatsphäre in der Arbeitswelt vor. Das Gesetz wurde vom Parlament am 8. Juni 2001 angenommen und trat am 1. Oktober 2001 in Kraft.

Ebenfalls 2000 wurde mit den Vorarbeiten für ein Gesetz über die Nutzung von elektronischen Diensten begonnen. Die Grundlage hierfür bildet die EU-Richtlinie für elektronische Signaturen.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Die 1999 eingeleitete umfassende Überarbeitung der Rechtsvorschriften für polizeiliche Register mit personenbezogenen Daten wurde 2000 fortgeführt. In Finnland gelten die Grundsätze der Datenschutzrichtlinie auch für die Verarbeitung von Daten im Bereich der zweiten und dritten Säule.

C. Wichtige Rechtsprechung

Keine.

D. Spezifische Themen

Wie vom Gesetz über den Schutz personenbezogener Daten vorgeschrieben, gab der Datenschutzbeauftragte in 20 Fällen Stellungnahmen gegenüber Polizei und Staatsanwaltschaft ab. Neben Fragen der Vertraulichkeit von Kommunikation und Verstößen gegen die Geheimhaltungspflicht betrafen die Fälle zumeist die unrechtmäßige Verwendung von in Verzeichnissen mit personenbezogenen Daten gespeicherten Daten und somit Verstöße gegen die Bestimmung, dass Daten nur für den ursprünglich vorgesehenen Zweck verwendet werden dürfen.

Eine Reihe von Fällen von besonderer Bedeutung im Hinblick auf allgemeine Grundsätze betraf die Verarbeitung personenbezogener Daten in Datennetzen und im Internet. In seiner Stellungnahme zur Verfügbarmachung personenbezogener Daten im Internet verweist der Datenschutzbeauftragte auf geltendes finnisches Recht, wonach personenbezogene Daten, die in Verzeichnissen mit personenbezogenen Daten gespeichert sind, nur mit Einwilligung der Betroffenen oder im Rahmen spezifischer Bestimmungen, die diese Verwendung gestatten, im Internet zugänglich gemacht werden dürfen.

Nach finnischem Recht nimmt der Datenschutzbeauftragte vor allem präventive Aufgaben wahr. Neben der Ausarbeitung von allgemeinen Leitlinien, Informationsmitteilungen, Mustern und Musterformularen für die für die Verarbeitung Verantwortlichen von Verzeichnissen und Daten in Verzeichnissen geführter Personen liegt der Hauptschwerpunkt der Aktivitäten auf der Zusammenarbeit mit verschiedenen Interessengruppen. Der Datenschutzbeauftragte gab offizielle Stellungnahmen zu den 2000 angenommenen Verhaltensregeln der folgenden Organisationen ab:

- Autoalan keskusliitto ry (Zentralverband der Automobilhändler und Reparaturwerkstätten)
- Suomen Suoramarkkinointiliitto (Finnischer Direktmarketingverband)

Außerdem war er an der Ausarbeitung von Verhaltensregeln vor allem im Bereich öffentliche Gesundheitsversorgung und für die finnische Bankenvereinigung beteiligt. Hinzu kommt die Mitwirkung an zahlreichen Aufklärungsaktivitäten (ca. 150 Veranstaltungen) in verschiedenen Bereichen.

Ein besonders heftig umstrittenes Thema im Jahr 2000 war die Durchführung von Drogentests in Schulen und am Arbeitsplatz. In Frage gestellt wurden vor allem die Notwendigkeit der Tests und die Zuverlässigkeit der dabei gewonnenen Informationen. Hierzu vertritt der Datenschutzbeauftragte die Auffassung, dass selbst wenn die Voraussetzungen gegeben sind, Drogentests nur nach vorheriger Aufklärung und Einwilligung der betroffenen Arbeitnehmer durchgeführt und die dabei gewonnenen Daten gesammelt werden dürfen. In seiner Stellungnahme zur Durchführung von Drogentests in Schulen fordert der Datenschutzbeauftragte eine gesetzliche Regelung für die Durchführung derartiger Tests. Solange keine gesetzliche Grundlage geschaffen sei, dürften Tests in Schulen nur nach vorheriger Aufklärung und mit Einwilligung der Betroffenen durchgeführt werden. Eine wichtige Frage, die gesondert geprüft werden müsse, sei das Alter, ab dem diese Einwilligung erteilt werden dürfe. Relevant sei hierbei das Alterslimit von 15 Jahren.

Im Laufe des Jahres verschärfte sich die Diskussion über den Standpunkt zum Gesetz über personenbezogene Daten im Bereich der elektronischen Presse und von Veröffentlichungen in Netzen generell. Die Verarbeitung von personenbezogenen Daten zum Zweck der Veröffentlichung fällt nach wie vor nicht unter den Anwendungsbereich des Gesetzes über personenbezogene Daten. Das geltende finnische Recht unterscheidet an sich nicht zwischen Veröffentlichungen in Netzen und Zeitungen und Zeitschriften, die in herkömmlichen Formaten veröffentlicht werden. Da jedoch durch die Veröffentlichung in Netzen die Gefahren für die Datensicherheit beträchtlich zunehmen, vertritt der Datenschutzbeauftragte den Standpunkt, dass das derzeit in Vorbereitung befindliche Gesetzeswerk über die Freiheit der Meinungsäußerung in Massenmedien der heutigen Situation Rechnung tragen müsse, die sich in bezug auf die Datensicherheit beträchtlich verändert habe. Eine weitere Frage in diesem Zusammenhang betrifft den Sachverhalt, ob sich durch die Veröffentlichung von Nachrichten oder Magazinen und Zeitungen in elektronischen Netzen deren Zweck in Abhängigkeit von verschiedenen Merkmalen im Zusammenhang mit der Veröffentlichung und Informationsrecherche verändert.

Außerdem wurde 2000 die Frage erörtert, ob Telekommunikationsbetreiber das Recht haben, personenbezogene Daten für die Bereitstellung von Lokalisierungsdiensten zu nutzen. Diese Frage wurde im Kontext des Gesetzes über die Datensicherheit im Telekommunikationsbereich und des Gesetzes über personenbezogene Daten diskutiert.

Eine wichtige Herausforderung mit Blick auf den Schutz der Privatsphäre waren die laufenden Aktivitäten zur Neuordnung des kommunalen Dienstleistungsangebots und die vermehrte Fremdvergabe von Dienstleistungen. Eine verstärkte Vernetzung und die sich daraus ergebende vermehrte Fremdvergabe von Datenverarbeitungsdienstleistungen in allen Sektoren sowie die dazugehörigen vertraglichen Regelungen erfordern eine systematischere Planung und eine gezieltere Anwendung der Bestimmungen zum Schutz personenbezogener Daten. Der Datenschutzbeauftragte machte auf die Gefahren derartiger Situationen für die Privatsphäre aufmerksam. Wichtig seien in diesem Zusammenhang auch schriftliche Vereinbarungen und hinreichend detaillierte vertragliche Regelungen für die Verarbeitung personenbezogener Daten. Um die Aktivitäten in diesem Bereich voranzutreiben, erarbeitete der Datenschutzbeauftragte in Zusammenarbeit mit Behörden und Organisationen verschiedene Modelle. Im privaten Sektor konnten bei

Gesetzgebungsvorhaben, bei denen es unter anderem um die Neuregelung der Tätigkeiten von Kreditinstituten und Versicherungen ging, verschiedene wichtige Fragen bezüglich des Schutzes der Privatsphäre angesprochen werden.

Die Einführung elektronischer Ausweiskarten und die entsprechenden Zertifizierungsdienste sind im Prinzip in Finnland seit dem 1. Dezember 1999 möglich. Erst 2000 wurden verschiedene Systeme um Merkmale ergänzt, die die Nutzung von elektronischen Dienstleistungen ermöglichen. Hinsichtlich des Schutzes der Privatsphäre sind bei der Verwendung derartiger Karten bislang keine signifikanten Probleme aufgetreten.

Der Hauptschwerpunkt der Aktivitäten im Jahr 2000 lag auf der Umsetzung der in der Datenschutzrichtlinie vorgesehenen registrierten Rechte auf Zugang zu Informationen. Bei den Aufsichtsmaßnahmen lag der Schwerpunkt auf der Einhaltung der Informationspflicht.

E. Website

http://www.tietosuoja.fi/

Frankreich

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Keine.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine.

C. Wichtige Rechtsprechung

Die französische Datenschutzkommission (Commission Nationale de l'Informatique et des Libertés - CNIL) verwies einen Fall an die Justiz. Es geht dabei um die Speicherung personenbezogener Daten durch die „Spirituelle Vereinigung Ile de France" der „Scientology Church" in ihren Archiven entgegen des Widerspruchs der betroffenen Person.

Die Entscheidung des Gerichts in diesem Fall steht noch aus.

D. Spezifische Themen

Die Anwendung der Datenschutzgrundsätze im Bereich der neuen Technologien (Internet, Biometrie) machte erneut Schlagzeilen. Große Aufmerksamkeit fanden allerdings auch konventionellere und ebenfalls überaus sensible Themen wie z. B. epidemiologische Untersuchungen mit der Einführung einer obligatorischen Erklärung für HIV-positive Personen sowie die Modernisierung des Computersystems der Polizei.

Aufgrund von Beschwerden führte die CNIL darüber hinaus rund 40 Überprüfungen vor Ort durch, hauptsächlich bei Kreditinstituten und Einrichtungen des sozialen Wohnungsbaus.

Generell war das Jahr 2000 wiederum ein sehr arbeitsintensives Jahr, das mit 150 Mitteilungen täglich zu Archiven und der Verarbeitung personenbezogener Daten und 5 900 Beschwerden und Beratungsanfragen im gesamten Jahr das Niveau von 1999 sogar noch übertraf. Insbesondere war bei den Anfragen von Privatpersonen zwecks Überprüfung der über sie gespeicherten polizeilichen Daten ein Anstieg um 21 % zu verzeichnen und es wurden 1 300 Untersuchungen durchgeführt.

Internet: Nachdem ab 1996 eine Aufklärungsaktion für die Zielgruppe der neuen Akteure im Internet durchgeführt worden war, die 1998 und 1999 sowohl im öffentlichen als auch im privaten Sektor nochmals deutlich intensiviert wurde, überprüfte die CNIL im Frühjahr 2000 im Rahmen einer Studie 100 E-Commerce-Websites, um den Erfolg der Kampagne zu bestimmen. Die veröffentlichten Ergebnisse lassen einen recht ermutigenden Grad an Sensibilität auf den überprüften Websites erkennen. So werden die Internet-Nutzer insbesondere über die mögliche Weitergabe von Daten zu Direktmarketingzwecken unterrichtet und sie erhalten bei der Online-Eingabe ihrer Daten die Möglichkeit anzugeben, ob sie der Weitergabe ihrer Daten für diese Zwecke zustimmen. Besonders negativ fiel bei der Studie auf, dass die Nutzer nur unzureichend über Zugangsrechte und über die eigentlichen Zwecke der verwendeten “Cookies” unterrichtet wurden. Um diese Situation zu verbessern, forderte die CNIL Fachorganisationen sowie die Betreiber von Portalen und E-Commerce-Plattformen auf, ihre Stellung als Mittler stärker zu nutzen. Darüber hinaus wandte sich die CNIL an Organisationen, die für die Kennzeichnung von E-Commerce-Websites verantwortlich sind. Ende 2001 entsprachen alle Verweissysteme der in Frankreich tätigen Kennzeichnungsorganisationen den Bestimmungen des Datenschutzgesetzes und den Empfehlungen der CNIL.

Ende 2000 veranlasste die immer stärkere Nutzung des Internet die CNIL, mit Blick auf neue Formen der Internet-Nutzung, die datenschutzrechtliche Fragen aufwarfen, in drei weiteren Bereichen aktiv zu werden. Der erste Bereich betraf die Überwachung der Internet-Aktivitäten von Arbeitnehmern, der zweite Websites zu Gesundheitsfragen und der dritte Websites für Kinder. Mit den dabei durchgeführten Aktivitäten und Studien, die neben Besuchen der Websites und Überprüfungsmaßnahmen auch eine Konzertierung mit den betroffenen Akteuren beinhalteten, wurden die Vorarbeiten für öffentliche Anhörungen geleistet, anhand von deren Ergebnissen 2001 spezifische Empfehlungen aufgestellt werden sollten.

Biometrie: Der vermehrte Einsatz der Biometrie, insbesondere die Verwendung von Fingerabdrücken zur Zugangskontrolle, für die Zeiterfassung und in der Verwaltung von Schulkantinen, wurde einer eingehenden Prüfung unterzogen. Bei Fingerabdrücken handelt es sich um sehr spezifische biometrische Daten, da jeder Mensch im täglichen Leben ständig Fingerabdrücke hinterlässt (auf Tischen, Gläsern, Schultaschen usw.). Somit kann eine Fingerabdruck-Datenbank, unabhängig davon, für welchen Zweck sie eingerichtet wird, als Datenvergleichsinstrument für polizeiliche Zwecke genutzt werden. Angesichts der Gesamtheit der spezifischen

Identifikationsmerkmale von Fingerabdrücken wirft die Einrichtung einer solchen Datenbank Fragen bezüglich der Freiheit des Einzelnen und der Gesellschaft auf.

In Fällen, in denen wichtige Sicherheitsbelange individuelle Authentifizierungsmaßnahmen erforderlich machten, genehmigte die CNIL deren Anwendung (z. B. für den Zugang zu Räumlichkeiten, in denen nationale Untersuchungsunterlagen gelagert sind, für den Zugang zu atomaren Wiederaufbereitungsanlagen und für die Geldtransporter-Sicherheitsschleuse der französischen Zentralbank). Hingegen verweigerte die CNIL ihre Genehmigung für den Einsatz entsprechender Techniken für die Kontrolle des Zugangs zu einer Schulkantine oder für die Überprüfung der Einhaltung von Gleitzeitregelungen in einer Verwaltungsbehörde. Grünes Licht erteilte die CNIL schließlich aufgrund der geringeren Nachteile für die versuchsweise Anwendung von Systemen, die an Stelle von Fingerabdrücken Handkonturen überprüfen, für Zugangskontrollen und für die Überprüfung der Einhaltung von Gleitzeitregelungen (bei Wartungspersonal im Louvre-Museum).

In zwei besonders sensiblen Bereichen fanden intensive Diskussionen zwischen der CNIL, den betroffenen Verwaltungsorganen und Menschenrechtsorganisationen statt. Ein Bereich betraf epidemiologische Seropositivitätsuntersuchungen, der zweite das neue System zur Verwaltung von straftatenbezogenen Datenbeständen der Polizei.

In dem Bemühen um die Bekämpfung der AIDS-Epidemie sieht das Gesetz eine zwar anonyme, jedoch obligatorische Erklärung von HIV-positiven Personen vor. Zum besseren Verständnis der Problematik, bei der es um die Vereinbarkeit von epidemiologischen Forschungen, mit denen genauere Kenntnisse über die Entwicklungstendenzen bei der HIV-Seropositivität gewonnen werden sollen, einerseits und der Rechte und Freiheiten der Betroffenen andererseits geht, legte die CNIL einen umfassenden Bericht zu diesem Thema vor. Als daraufhin die französische Regierung die CNIL um ihre Stellungnahme zu Maßnahmen zur Umsetzung des Rechtstextes bat, sprach sich die CNIL insbesondere für zwei Maßnahmen aus. Die eine ist technischer und organisatorischer Art und ist so konzipiert, dass die im Verlaufe der Zeit erhobenen Daten zu ein und derselben Person bei der Übermittlung an das landesweite Zentralarchiv anonym bleiben. Der wichtigste Aspekt dieser Maßnahme ist die doppelte Verschlüsselung der Identifikationsdaten mit Hilfe eines unumkehrbaren Algorithmus, der an der Datenquelle implementiert wird. Die zweite Maßnahme betrifft die Wahrung der absoluten Anonymität von Personen, die sich an anonyme Früherkennungszentren wenden, die ihre Dienste kostenlos anbieten, um möglichst alle gefährdeten Personen zu erfassen. Hier wurde gefordert, dass solche anonym und kostenlos arbeitenden Früherkennungsstellen keine Seropositivitätserklärungen abgeben dürfen. Die Regierung übernahm die Empfehlungen der CNIL unverändert.

Bei dem System für die Verarbeitung von polizeilich festgestellten Ordnungswidrigkeiten (*Système de Traitement des Infractions Constatées* - STIC), das durch ein 1995 verabschiedetes Gesetz notwendig geworden war, handelt es sich um eine Gesamtdatei, in der landesweit alle Daten zusammengeführt werden, die von den polizeilichen Ermittlungsbehörden erfasst werden und die in den polizeilichen Ermittlungsberichten enthalten sind, die zum Abschluss der polizeilichen Ermittlungen erstellt und den Gerichten vorgelegt werden. Vor ihrer Stellungnahme

führte die CNIL eingehende Gespräche mit den Berufsverbänden von Polizeikräften, Richtern und Rechtsanwälten sowie mit Menschenrechtsorganisationen.

Als Reaktion auf die verschiedenen dabei angesprochenen Fragen wurde eine Reihe von Maßnahmen eingeleitet, die vor allem die Kriterien für die Aufnahme personenbezogener Daten in den Datenbestand betrafen. So dürfen personenbezogene Daten nur dann aufgenommen werden, wenn sie sich auf Personen beziehen, über deren Beteiligung an einem Verbrechen ernst zu nehmende und überzeugende Beweise vorliegen. Keinesfalls dürfen Daten allein aufgrund von Zeugenaussagen gegenüber den Ermittlungsbehörden oder Daten über fälschlich in Verdacht geratene Personen oder Personen, die Gegenstand einer nicht beweisbaren Anzeige geworden sind, in die Datei aufgenommen werden.

Ein technischer „Sperrmechanismus“ macht es darüber hinaus unmöglich, für Verwaltungszwecke Daten von Opfern aus dem STIC abzurufen. Nach einer endgültigen Verurteilung des Täters können zudem die Daten der Opfer aus dem System gelöscht werden. Wenn der Täter nicht identifiziert werden kann, dürfen Opferdaten maximal zehn Jahre gespeichert werden.

Das STIC soll die polizeilichen Ermittlungen erleichtern, indem es unter anderem Gemeinsamkeiten zwischen verschiedenen Fällen aufzeigt oder Zeugen oder Opfern Bilder präsentiert, die zur Täterbeschreibung passen. Die CNIL gestand allerdings zu, dass die Datei in bestimmten Fällen und unter strengen Sicherheitsauflagen, wenn die Sicherheit von Polizeikräften oder anderen Personen gefährdet ist (z. B. Gipfeltreffen von Staats- und Regierungschefs, Sport-Großveranstaltungen u. ä.) auch zur Prävention eingesetzt werden darf.

Da das STIC nicht als Justizdatensystem konzipiert ist, forderte die CNIL ein Verbot der Erstellung einer Zusammenfassung verschiedener STIC-Einträge über eine bestimmte Person zur Aufnahme in die Verfahrensunterlagen in einem Strafverfahren.

Auch die zeitliche Begrenzung der Speicherungsdauer wurde von der CNIL eingehend untersucht. Sie forderte hierbei insbesondere die Begrenzung der Speicherungsdauer für Daten zu bestimmten gewaltlosen und minderschweren Straftaten auf 5 Jahre (statt der ursprünglich vom Innenministerium vorgeschlagenen 10 oder 20 Jahre). Dieser Kategorie sind vor allem die Mehrzahl der Straftaten Minderjähriger sowie Bagatelldiebstähle, Drogenmissbrauch, nicht vorsätzliche Straftaten sowie Zuwiderhandlungen im Straßenverkehr zuzuordnen.

Außerdem wurde die Ergreifung von Maßnahmen zur Aktualisierung der Datei entsprechend dem juristischen Ergebnis der erfassten Fälle gefordert, d. h. Löschung aller entsprechenden Daten aus der STIC-Datei bei Freispruch, Klageabweisung oder Amnestie.

Ergänzend zu verschiedenen Empfehlungen hinsichtlich Sicherheitsmaßnahmen forderte die CNIL abschließend die Vorlage eines jährlichen Tätigkeitsberichts des Leiters der Polizeibehörde, in dem dieser gegenüber der CNIL Rechenschaft über die Verifizierung, Aktualisierung und Löschung der im STIC gespeicherten Daten ablegt.

Dieses Konzept wurde in Form eines Regelwerks niedergelegt, das nach der Stellungnahme der CNIL und unter Berücksichtigung ihrer Empfehlungen in einem Erlass verabschiedet wurde (Erlass Nr. 2001-583 vom 5. Juli 2001, Amtsblatt vom 6. Juli 2001).

E. Website

Frankreich: Die Website der CNIL (www.cnil.fr) wurde 2000 weiter verbessert, so wurde u. a. eine „Kinderecke“ (*Espace Junior*) aufgenommen, um bereits Kinder mit der Wahrnehmung ihrer Rechte vertraut zu machen.

Deutschland

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

1. Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001
(Bundesgesetzblatt I, S. 876)

Das Signaturgesetz wurde angepasst an die Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen – Signaturgesetz auf europäischer Ebene. Es gibt drei verschiedene Signaturen: einfache,fortgeschrittene und qualifizierte Signatur. Je nach Stufe gibt es unterschiedliche technische Rahmenbedingungen entsprechend der Richtlinie. Das Gesetz enthält außerdem Regelungen zur Anerkennung von Signaturen anderer EU-Mitgliedstaaaten.

2. Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (beschlossen am 13. Juli 2001)

Die im Gesetz zur Anpassung von Formvorschriften enthaltene Novellierung des Teledienstedatenschutzgesetzes enthält außer einigen Klarstellungen und Bereinigungen neu das Recht der Diensteanbieter, beim Vorliegen tatsächlicher Anhaltspunkte für mißbräuchliche Nutzung die personenbezogenen Daten der entsprechenden Nutzer zur Aufklärung und Rechtsverfolgung zu verarbeiten.

Außerdem werden Verletzungen wesentlicher datenschutzrechtlicher Pflichten der Anbieter als Ordnungswidrigkeiten klassifiziert und mit Geldbuße bis 100.000 DM bedroht.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 26. Juni 2001 (Bundesgesetzblatt I, S. 1254)

Umsetzung der Entscheidung des Bundesverfassungsgerichts vom 14. Juli 1999 (BVerfGE 100, S. 313 ff.) zur Neuregelung der strategischen Fernmeldeaufklärung des Bundesnachrichtendienstes sowie weitere Änderungen des G 10-Gesetzes

D. Spezifische Themen

Durch das neue Signaturgesetz wurden die Vorgaben der EG-Richtlinie "über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen" in deutsches Recht umgesetzt.

Eine Forschungsgruppe der Universität Bonn konnte zeigen, daß nach dem alten (wohl auch nach dem neuen) Signaturgesetz zugelassenen Verfahren zur digitalen Signatur unter bestimmten Voraussetzungen (Manipulation der Signaturumgebung durch Trojaner) gebrochen werden können (das signierte Dokument entspricht nicht dem Dokument, das dem Benutzer angezeigt wurde).

E. Website

Website des Bundesbeauftragten für den Datenschutz: www.datenschutz.bund.de oder www.bfd.bund.de

Website des Virtuellen Datenschutzbüros: www.datenschutz.de

Die Sites werden ständig aktualisiert. So wurde z.B. das BfD-Angebot bei "Datenschutz und Technik" erweitert um
- Hinweise zum Datenschutz bei der Nutzung von Internet und Intranet und
- Verschlüsselte E-Mail-Kommunikation mit dem BfD.

Auch das Angebot unter "English Texts and Documents wurde beispielsweise erweitert um
- Telecommunications Act,
- Telecommunications Data Protection Ordinance (TDSV) und
- Forthcoming Legislation in Implementation of Directive 95/46/EC.

Griechenland

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Die EU-Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen wurde per Präsidialverordnung in griechisches Recht umgesetzt.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine nennenswerten Änderungen.

C. Wichtige Rechtsprechung

1. Einer Entscheidung der griechischen Datenschutzbehörde folgend werden personenbezogene Daten zur Religionszugehörigkeit sowie die Fingerabdrücke des Inhabers in den griechischen Personalausweisen nicht erfasst. In ihrer Entscheidung bezeichnete die Datenschutzbehörde diese Daten als nicht angemessen, irrelevant und zudem in bezug auf die Zwecke, für welche sie erhoben und weiterverarbeitet werden, überzogen. Diese Entscheidung war sehr umstritten und wurde insbesondere von der griechisch-orthodoxen Kirche angegriffen. Die beim obersten Verwaltungsgericht eingelegte Berufung gegen die Entscheidung wurde vom Gericht abgewiesen.

2. Nach einer weiteren Entscheidung der griechischen Datenschutzbehörde muss die Videoüberwachung öffentlicher Plätze der Datenschutzbehörde angezeigt werden.

3. Die Datenschutzbehörde legte einen Leitfaden für den Datenschutz am Arbeitsplatz vor, in welchem insbesondere die Überwachung der Telefongespräche und E-Mail-Mitteilungen von Arbeitnehmern thematisiert wird.

D. Spezifische Themen

In die Neufassung der griechischen Verfassung wurde ein neues Grundrecht auf den Schutz personenbezogener Daten aufgenommen (Artikel 9A). Gemäß der Verfassung hat jede Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Derartige Daten müssen in angemessener Form und für bestimmte Zwecke erhoben und verarbeitet werden. Darüber hinaus muss die Einhaltung dieser Vorschriften durch eine unabhängige Behörde überwacht werden.

E. Website

http://www.dpa.gr/

Irland

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Im Jahr 2000 trat keine Rechtsvorschrift zur Umsetzung der Richtlinie 95/46 in irisches Recht in Kraft, dies ist jedoch für 2001 vorgesehen.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Im Verlaufe des Jahres veröffentlichte die irische Datenschutzbehörde detaillierte Leitlinien für den Kreditauskunftsektor und den gesamten Bereich des e-Government.

C. Wichtige Rechtsprechung

Generell ist festzuhalten, dass sich die für die Verarbeitung von Daten Verantwortlichen in ihrer Mehrzahl ihrer Verantwortung bewusst sind und entsprechend handeln. Allerdings traten auch 2000 Problemfälle auf, die im Folgenden dargestellt werden. Die Datenschutzbehörde stellte fest, dass das irische Bildungsministerium bei der Heranziehung der Gehaltsdatenbank zur Sperrung der Gehälter von Lehrern, die sich an Streikaktionen beteiligten, nicht bestimmungsgemäß vorging.

Eircom schlug in einem Rundschreiben an ehemalige Dienstteilnehmer vor, personenbezogene Angaben anderen Telekommunikationsfirmen zugänglich zu machen, womit Eircom gegen das Datenschutzgesetz verstieß.

Dem Irish Credit Bureau (ICB) untersagte die Datenschutzbehörde die Praxis der Weitergabe von Kreditauskünften. Im Rahmen dieser Praxis hatte das ICB bei Anfragen einer Bank über die Kreditwürdigkeit bestimmter natürlicher Personen in manchen Fällen auch die Kreditdaten weiterer Personen mit gleichem Namen oder

Anschrift übermittelt. Im Zusammenhang mit der Untersagung dieser Praxis forderte die Datenschutzbehörde die Finanzinstitute auf, sich verstärkt um die genaue Identifizierung ihrer Kunden und die Bestimmung der richtigen Kundenanschriften zu bemühen.

In der Beschwerde einer Einzelperson wurde der irischen Polizei (Gardaí) vorgeworfen, sie hätte nicht ordnungsgemäß auf ein Auskunftersuchen reagiert. Zwar wurden hinsichtlich der über die betreffende Person in der Straftatenregister-Datenbank gespeicherten Daten gewisse Ungenauigkeiten festgestellt (diese Datenbank muss zwingend absolut korrekt geführt werden), doch wurde die Beschwerde, dass die Gardaí nicht umgehend auf das Auskunftersuchen reagiert habe, von der Datenschutzbehörde nicht bestätigt.

Außerdem entschied die Datenschutzbehörde, dass der Ausdruck von Kundenadressen auf Laserkartenquittungen gegen das Datenschutzgesetz verstößt. Das betroffene Finanzinstitut ergriff umgehend Abhilfemaßnahmen, stellte jedoch daraufhin die Sicherheit in Frage.

D. Untersuchungen und Beschwerden

Die Zahl der Anfragen bei der Datenschutzbehörde stieg von 1999 noch 2 200 auf um mehr als 40 % auf über 3 100 im Jahr 2000. Viele dieser Anfragen betrafen Kreditauskünfte, Direktmarketing und Anträge auf Zugang zu Daten. Unternehmen stellten auch Fragen zur neuen Datenschutzgesetzgebung und zum Ablauf der Registrierung gemäß dem Gesetz.

Die Zahl der förmlichen Beschwerden stieg 2000 auf 131 gegenüber 105 im Jahr 1999 – ein Anstieg um 25 %. Die meisten Beschwerden richteten sich gegen Unternehmen im Telekommunikations- und IT-Sektor, Finanzinstitute, Direktmarketingunternehmen und Organisationen des öffentlichen Dienstes.

E. Website

http://www.dataprivacy.ie/

Italien

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Von den im fraglichen Zeitraum eingeleiteten Gesetzgebungsmaßnahmen sind einige in diesem Kontext von Interesse, wenngleich sie sich nicht direkt auf den Schutz personenbezogener Daten beziehen. Im Einzelnen sind hier folgende Maßnahmen zu nennen

- Ein Erlass über die Ausstellung, Ausgabe, Aktualisierung und Verlängerung der Dauerwahlkarte, demzufolge bei allen Verarbeitungsvorgängen, die personenbezogene Daten betreffen, die maßgeblichen Datenschutzbestimmungen einzuhalten sind und die Verarbeitungsvorgänge der Aufsicht des örtlichen Datenverarbeiters unterstellt sind.

- Ein Erlass mit Verordnungen über Verwaltungsdokumente, der vorsieht, dass Dokumente, die an andere öffentliche Verwaltungsstellen übermittelt werden, nur Daten über den Personenstand, Vorkommnisse und Qualifikationen enthalten dürfen, auf die in Gesetzen oder Verordnungen Bezug genommen wird und die für das Erreichen der Zwecke, für die sie erhoben werden, absolut notwendig sind.
- Ein Erlass über das nationale statistische Programm 2001-2003, in dessen Präambel ausdrücklich auf die Verarbeitung personenbezogener Daten Bezug genommen wird, wobei insbesondere auf die Unterrichtung der Betroffenen, deren Recht auf Zugang zu personenbezogenen Daten und die spezifischen Vorsichtsmaßnahmen bei der Verarbeitung sensibler Daten eingegangen wird.

Ein Gesetz vom November 2000 erlaubte Organisationen, die bislang noch nicht in der Lage waren, die so genannten Mindestsicherheitsmaßnahmen einzuführen, unter bestimmten Voraussetzungen die Inanspruchnahme einer neuen, verlängerten Frist bis zum 31. Dezember 2000. Voraussetzung war die Abgabe eines amtlichen Dokuments, in dem die spezifischen technischen und organisatorischen Anforderungen beschrieben werden mussten, die die Inanspruchnahme der Fristverlängerung notwendig machten; die im Plan zur Verbesserung der Sicherheitssysteme vorgesehenen Maßnahmen mit Angabe dazu, ob diese bereits eingeführt wurden oder nicht, und die maßgeblichen Leitlinien waren ebenfalls aufzuführen.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine.

C. Wichtige Rechtsprechung

Besonders hervorzuheben ist die Tatsache, dass im Jahr 2000 erstmals der italienische Kassationshof mit einer Berufung in einer Datenschutzsache angerufen wurde. Die Berufung war gegen das Urteil eines ordentlichen Gerichts in Mailand eingelegt worden, das die Entscheidung der italienischen Datenschutzbehörde Garante vom 19. April 1999 aufgehoben hatte.

In dem Fall ging es um die Beschränkungen der Anwendbarkeit des Datenschutzgesetzes auf Verarbeitungsvorgänge, die für journalistische Zwecke durchgeführt werden. Der Fall bezog sich konkret auf die unrichtige Wiedergabe des Namens einer Person durch Dritte in der Presse.

Das Gericht bestätigte die Entscheidung der Garante und entschied, dass die Betroffene das Recht auf Berichtigung der Daten zur genauen Identifizierung ihrer Person habe. Die Offenlegung der Daten wurde als Verstoß gegen eines der Betroffenen in Abschnitt 1 des Gesetzes Nr. 675/1996 (Datenschutzgesetz) zuerkannten Rechte erkannt.

In der bedeutendsten Kategorie von Verfahren, die bei der Garante eingeleitet wurden, d. h. die von Betroffenen nach Abschnitt 29 des Datenschutzgesetzes eingelegten Beschwerden wegen fehlender Möglichkeiten zur Wahrnehmung der Rechte auf Zugang, Berichtigung usw., stieg die Zahl der diesbezüglichen Entscheidungen im Jahr 2000 auf insgesamt 187 an.

Aus der Art der bei der Garante eingereichten Beschwerden, die sich vorrangig auf den Zugang zu personenbezogenen Daten von Arbeitnehmern und/oder personenbezogene Daten in gerichtsmedizinischen Berichten, Daten in übertragbaren Darlehensscheinen, Verarbeitungsvorgänge bei Banken und Finanzinstituten und die Verarbeitung für journalistische Zwecke beziehen, lassen sich interessante Schlüsse ziehen.

In acht Fällen wurden gemäß Abschnitt 29 Absatz 6 des Gesetzes Nr. 675/1996 Entscheidungen der Datenschutzbehörde vor dem zuständigen ordentlichen Gericht angefochten. In drei Fällen, in denen die Entscheidungen der Behörde von den Gerichten aufgehoben wurden, legten die Parteien beim Kassationshof Berufung ein.

Dabei ging es unter anderem um die Möglichkeit der Klage gegen die Garante in Verfahren vor einem ordentlichen Gericht oder vor dem Kassationshof gegen Entscheidungen der Behörde und um die Möglichkeit der Garante, sich vor Gericht rechtmäßig durch die Generalstaatsanwaltschaft vertreten zu lassen. Letzere gab zu dieser Frage eine positive Stellungnahme ab. Darin betonte sie, dass das Auftreten der Garante vor Gericht eigentlich auf solche Fälle beschränkt werden sollte, in denen es spezifisch um die Wahrung des Interesses der Allgemeinheit geht, und auf Fälle im Zusammenhang mit Fragen von allgemeinem Interesse, die die ordnungsgemäße Umsetzung von Datenschutzgesetzen betreffen.

D. Spezifische Themen

Nachstehend eine kurze Zusammenfassung wichtiger Fragen, in denen die Garante im Rahmen ihrer Aktivitäten in ihrer Aufsichtsfunktion tätig wurde:

a) Beurteilung der Einhaltung von Datenschutzgrundsätzen in bezug auf Verarbeitungsvorgänge für Zwecke des Gesetzesvollzugs. Aus den von der Garante nach Berichten über einzelne Verarbeitungsvorgänge bei den Carabinieri eingeleiteten Untersuchungen ergab sich, dass in diesem Bereich die Vorgehensweisen nicht ausreichend vereinheitlicht sind; dies läßt sich durch spezifische Rechtsvorschriften ändern, während die übrigen Probleme durch organisatorische Maßnahmen behoben werden können. In diesem Zusammenhang wird auf seit langem geübte Praktiken verwiesen, zu denen die Garante eine Reihe von Änderungen vorschlug, wie beispielsweise angemessenere Kriterien für die Aufbewahrung von Daten, diversifizierte Konsultationspolitiken, regelmäßige Überprüfung der Relevanz der erhobenen Informationen.

In diesem Zusammenhang führte die Garante eine eingehendere Analyse durch, bei der speziell die Anwendung von Datenschutzgrundsätzen auf entsprechende Aktivitäten in den Mitgliedstaaten der Europäischen Union untersucht wurde – unter anderem in Workshops im Rahmen des Projekts Falcone zum Schutz personenbezogener Daten und zu polizeilichen und justiziellen Aktivitäten, auf das nachfolgend noch näher eingegangen wird.

b) Kontrollen spezifischer, von den zuständigen Ermittlungs- und Sicherheitsstellen durchgeführter Verarbeitungsvorgänge bezüglich personenbezogener Daten. Die Garante lenkte die Aufmerksamkeit der Regierung auf diesen Themenbereich. Sie forderte die stärkere Beachtung des Grundsatzes der Datenrelevanz, der Auswahl von

verfügbaren Informationen und der Regelungen für den Zugang zu und die Speicherung von Daten in bezug auf dezentrale Vorgänge, wobei allerdings zu keinem Zeitpunkt die Rechtmäßigkeit und die Angemessenheit der betreffenden Verarbeitungsvorgänge in Zweifel stand.

c) Aufbau von umfangreichen Datenbanken. Im Zusammenhang mit der Stellungnahme der Garante gegenüber dem Innenministerium zum Entwurf für einen Erlass zur Einrichtung einer nationalen Liste der Zensusregister, forderte die Datenschutzbehörde mit Nachdruck, dass in bezug auf die Einrichtung und Regulierung – insbesondere des Zugangs externer Nutzer – die maßgeblichen Gesetze und Verordnungen eingehalten werden müssen. Dies ist eine Grundvoraussetzung für die Gewährleistung der Transparenz von Datenströmen auf der Grundlage einheitlicher Kriterien, die den Datenschutz entsprechend der geltenden Grundsätze bezüglich Relevanz, Vollständigkeit und Angemessenheit der Daten erlaubt.

d) Überprüfung der Rechtmäßigkeit einer von RAI-TV (staatlicher italienischer Rundfunk- und Fernsehsender) geübten Praxis beim Versand von Zahlungserinnerungen über die jährlichen Gebühren an mögliche Rundfunk- und Fernsehteilnehmer. Aufgrund der zahlreichen eingegangenen Meldungen und Beschwerden untersuchte die Garante, nach welchen Kriterien Zahlungserinnerungen an Personen verschickt wurden, deren Namen nicht in den Teilnehmerverzeichnissen enthalten waren, wobei insbesondere die Vorgehensweise bei der Datenerhebung geprüft wurde.

e) Beurteilung und Regelung von Videoüberwachungsmaßnahmen. Wegen des zunehmenden Einsatzes dieser Technologie und der besonderen Sensibilität der Bürger diesbezüglich bildete dieser Themenkomplex einen Schwerpunkt der Aktivitäten der Behörde. Nachdem noch keine entsprechenden Rechtsvorschriften vorliegen, gelten die Vorschriften des allgemeinen Datenschutzgesetzes. Eingehend auf zahlreiche Anfragen von kommunalen Stellen, die die Behörde um ihre Stellungnahme zu Initiativen zur Einführung elektronischer Überwachungsanlagen ersucht hatten, bekräftigte die Garante, dass für die Verarbeitung von Bildern mittels Videoüberwachungssystemen das Datenschutzgesetz maßgeblich ist – unabhängig davon, ob die Daten gespeichert oder Dritten zugänglich gemacht werden.

Ausgehend von diesen Tatsachen entschloss sich die Garante zur Durchführung einer Erhebung, für die signifikante Örtlichkeiten – z. B. die Innenstädte verschiedener Großstädte, darunter Rom - ausgewählt und die Zahl der installierten (Video-)Kameras ermittelt wurde. Diese Erhebung ergab ein detaillierteres Bild des Stands der Videoüberwachung. Die Ergebnisse der Erhebung wurden Vertretern maßgeblicher Stellen und der Presse mitgeteilt. Die Garante erstellt anschließend auf der Grundlage dieser Erhebung einen Katalog mit Leitlinien für die Installation fester Videoüberwachungsanlagen, der auf der Website der Garante (www.garanteprivacy.it) eingesehen werden kann. Ergänzend wurden im Parlament verschiedene Gesetzentwürfe eingebracht, mit denen die Anwendung dieser Technologie entsprechend den Empfehlungen des Leitlinienkatalogs geregelt werden soll.

f) Datenschutz am Arbeitsplatz. Der Bedeutung dieses Themas trug die Garante mit einigen Entscheidungen Rechnung, die vor allem die Fernüberwachung von

Arbeitnehmern – ein eng mit dem Einsatz von Videoüberwachungstechniken im Zusammenhang stehendes Thema -, den Zugang von Arbeitnehmern zu den sie betreffenden Daten – einschließlich Beurteilungen, Aufzeichnungen über Fehlzeiten, Lohn- und Gehaltsdaten, Aufgaben usw. – betrafen. Zu dem letztgenannten Aspekt machte die Garante deutlich, dass Arbeitgeber in ihrer Eigenschaft als für die Verarbeitung von Daten Verantwortliche verpflichtet sind, Arbeitnehmer auf Antrag alle sie betreffenden Daten zur Verfügung zu stellen. Weitere wichtige Entscheidungen betrafen die Pflicht von Arbeitnehmern zum Tragen von Mitarbeiterausweisen und mögliche Gefahren für die Privatsphäre der Arbeitnehmer.

g) Verarbeitung von genetischen Daten. Für die Verarbeitung von genetischen Daten ist – unabhängig davon, wer als Verarbeiter auftritt – gemäß Abschnitt 17 Absatz 5 der Gesetzesverordnung Nr. 135 vom 11.05.1999 und der Änderungen und Ergänzungen von Abschnitt 16 der Gesetzesverordnung Nr. 281 vom 30.07.1999 eine spezielle Genehmigung der Garante erforderlich.

Mit der allgemeinen Genehmigung Nr. 2/2000 legte die Datenschutzbehörde fest, dass gemäß der Abschnitte 22 und 23 des Datenschutzgesetzes die Verarbeitung genetischer Daten mit schriftlicher Einwilligung des Betroffenen gestattet ist, und zwar *„in bezug auf die Informationen und Operationen, die notwendig sind, um die körperliche Unversehrtheit und Gesundheit entweder des Betroffenen, eines Dritten oder der Gemeinschaft als Ganzes zu wahren.“*

Die vorstehende allgemeine Genehmigung ist nicht anwendbar, wenn die Verarbeitung genetischer Daten notwendig ist, um die Gesundheit von Dritten oder der Gemeinschaft als Ganzes zu schützen und der Betroffene keine Einwilligung erteilt hat. In diesem Fall ist eine Ad-hoc-Genehmigung der Garante einzuholen.

Weitere Initiativen der Garante

Im September 2000 war die Garante Gastgeber der 22. Internationalen Konferenz der Datenschutzbeauftragten, die vom 28.-30. September erstmals in Italien stattfand, Veranstaltungsort war Venedig. Auf der Konferenz unter dem Titel *„One World, One Privacy – Towards Electronic Citizenship“* wurden zahlreiche Themen im Zusammenhang mit dem Schutz der Privatsphäre und dem Datenschutz angesprochen.

Erwähnenswert war insbesondere die Teilnahme der Aufsichtsbehörden von „neuen“ Ländern, die ein Beleg dafür ist, dass Regelungen zum Schutz der Privatsphäre weltweit auf dem Vormarsch sind und die deutlich macht, wie wichtig es vielen Ländern ist, einheitliche und aufeinander abgestimmte Grundsätze für diesen Bereich zu entwickeln.
Hierzu sei auch auf die einstimmig angenommene Abschlusserklärung verwiesen, die als „Charta von Venedig“ bekannt wurde und von den Vertretern aller 27 Teilnehmerländer unterzeichnet wurde. Mit der Erklärung treten die Unterzeichner für das Ziel ein, angesichts der sozialen Entwicklung und des Fortschritts sowie der Entwicklungen in Wissenschaft und Technik den Schutz der Grundrechte zu verbessern. Mit der Bekräftigung der Feststellung, dass der Schutz der Privatsphäre ein menschliches Grundrecht und ein wichtiger Bestandteil der bürgerlichen Freiheiten ist, unterstreicht die Erklärung den allgemeinen Konsens über gemeinsame Grundsätze und Kriterien für den Datenschutz, wie er bereits in den OECD-Leitlinien,

der Europarats-Konvention Nr. 108/1981 und den Richtlinien der Europäischen Union zum Ausdruck kommt. Die genannten Instrumente bilden nicht das Ende, sondern vielmehr einen Ausgangspunkt und können dazu beitragen, dass die Bemühungen um ihre Verbreitung auf der ganzen Welt neue Motivation erhalten.

Im Rahmen des von der Europäischen Union unterstützten *„Falcone-Programms“*, mit dem die Zusammenarbeit zwischen Justiz und Zollbehörden bei der Bekämpfung des organisierten Verbrechens verbessert werden soll, erhielt die Garante Mittel für ein zwischenzeitlich abgeschlossenes Projekt zur Analyse der Aktivitäten von Polizei und Justiz bei der Erhebung, Verarbeitung und Auswertung von Daten unter dem Aspekt des vermehrten Zusammenarbeit bei polizeilichen und – in jüngster Zeit – auch justiziellen Aktivitäten.

Im Rahmen dieses Projekts wurden zwei Workshops veranstaltet; die Schlusskonferenz, die im Dezember 2000 in Rom stattfand, bot die Gelegenheit zur öffentlichen Vorstellung der durchgeführten Aktivitäten.

Die Diskussionen während der Workshops und die Antworten auf die vorab verteilten Fragebogen erbrachten recht interessante und aussagefähige Beiträge, so ergaben sie, dass – je nach geltenden nationalen Rechtsvorschriften – die Bürger Europas in einigen wenigen, jedoch wichtigen Punkte unterschiedlich behandelt werden. Dies betrifft unter anderem den Einsatz von Videoüberwachungstechniken, die Dauer der Aufbewahrung von und die Regelungen für Telefonverkehrsdaten, den Zugang von Polizei und Justiz zu Telefonverzeichnissen, Regelungen für die Erhebung und Verarbeitung genetischer Daten sowie deren Verwendung und Aufbewahrung.

Beiträge und Schlussbericht des Falcone-Projekts wurden von der Garante in einem in englischer und italienischer Sprache vorliegenden Band veröffentlicht.

Eine weitere wichtige Tätigkeit der Garante – in ihrer Eigenschaft als Aufsichtsbehörde für das nationale Schengener Informationssystem (N.SIS) – im zurückliegenden Jahr betraf die Beantwortung der zahlreichen Anträge auf Verifizierung der in dem System gespeicherten personenbezogenen Daten und die Rechtmäßigkeit von Verarbeitungsvorgängen nach dem Schengener Durchführungsübereinkommen und dem Gesetz Nr. 675/1996.

Bei der Zahl der Anträge war ein deutlicher Anstieg zu verzeichnen. Die meisten Anträge wurden von Betroffenen direkt übermittelt, in einigen wenigen Fällen stellten die zuständigen Aufsichtsbehörden anderer Schengen-Länder ein diesbezügliches Amtshilfeersuchen.

Um die Verfahren zu beschleunigen und die zahlreichen von Betroffenen eingegangenen Anträge rasch zu beantworten, vereinbarte die Garante eine Reihe von Zusammenkünften mit den zuständigen Abteilungen des Innenministeriums zur Festlegung wirksamerer und schnellerer Verifizierungsmechanismen und –verfahren.

E. Website

www.garanteprivacy.it

Luxemburg

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Keine.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Am 14. August 2000 wurde ein Gesetz über den elektronischen Geschäftsverkehr verabschiedet, am 1. Juni 2001 wurde eine Großherzogliche Verordnung über elektronische Signaturen, elektronische Zahlungssysteme und die Einsetzung des Ausschusses für den elektronischen Handel angenommen.
Die entsprechenden Dokumente können über die Website www.chd.lu unter *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche simplifiée, Mémorial A, Commerce Electronique,* abgerufen werden.

Am 4. Mai 2001 wurde dem Parlament ein Gesetzentwurf für die Annahme des Zollübereinkommens vorgelegt.
Das Dokument kann über die Website www.chd.lu unter *PORTAIL DOCUMENTAIRE, Recherche d'archives, Recherche Avancée. Dossier parlementaire N° 4794*, abgerufen werden.

C. Wichtige Rechtsprechung

Keine.

D. Spezifische Themen

Keine.

Niederlande

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Keine.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine.

C. Wichtige Rechtsprechung

Erwähnenswert erscheint ein Urteil des Regionalgerichts Haarlem vom 16. Juni 2000, das die Überwachung von Arbeitnehmern am Arbeitsplatz betrifft. Darin verwies der Richter auf die so bezeichnete Privatisierung des Arbeitsplatzes in der heutigen Gesellschaft, die zur Folge hat, dass der Arbeitgeber in gewissen Grenzen akzeptieren muss, dass während der Arbeitszeit private Kontakte gepflegt werden. Der Arbeitgeber muss die Privatheit dieser Kontakte gewährleisten.

D. Spezifische Themen

Videoüberwachung
Die Überwachung öffentlicher Räume durch Videokameras nahm 2000 deutlich zu. Nach Auffassung der niederländischen Datenschutzbehörde kann der gezielte Einsatz von Überwachungskameras ein wichtiger Bestandteil eines umfangreicheren Pakets von Sicherheitsmaßnahmen sein. Damit ist allerdings der Nachteil verbunden, dass technisch immer weiter entwickelte Erkennungssysteme eine weit reichende Überwachung der Verhaltensweisen der Bürger ermöglichen. Die Datenschutzbehörde fordert daher eine bewusste Einschränkung des Einsatzes von Videoüberwachungsanlagen. Wichtig erscheint ihr auch, dass die Regierung die Kontrolle über den öffentlichen Bereich behält. Der Bürger muss wahrgenommen werden, darf jedoch nicht ständig überwacht werden.

Gesundheitswesen
Mit Blick auf die qualitative Verbesserung des Gesundheitswesens (u. a. Zugänglichkeit und Effizienz) werden hohe Erwartungen in die Möglichkeiten der Informations- und Kommunikationstechnologie gesetzt. Im Gesundheitswesen fallen immense Datenmengen an, von der direkten Betreuung von Patienten und deren Finanzierung bis hin zu Forschung und Gesundheitspolitik. Die Datenschutzbehörde weist darauf hin, dass in diesem Kontext bislang zu wenig auf den Schutz personenbezogener Daten und die Geheimhaltungspflicht im medizinischen Bereich geachtet wird. Dies betrifft insbesondere die Gegebenheiten, die mit der wachsenden Bedeutung der Krankenversicherungen zusammenhängen. Weiter verweist die Datenschutzbehörde darauf, dass dies Konsequenzen für die Neuordnung des Gesundheitssystems haben müsse.

Die jüngsten Pläne für den Sektor im Bereich Pflegezuweisung und Wartelisten im Rahmen des Gesetzes für medizinische Sonderausgaben sehen die Erhebung umfangreicher Daten über den einzelnen Patienten vor. Das Ministerium für Gesundheit, Soziales und Sport, die niederländischen Krankenversicherer und der Krankenkassenbeirat wollen auf der Grundlage dieses Gesetzes ein nationales Registrierungssystem entwickeln, das die Rückverfolgung der Daten bis hin zur Individualebene ermöglicht. Die Datenschutzbehörde setzte die Beteiligten über ihre erheblichen Zweifel hinsichtlich der rechtlichen Zulässigkeit dieses Konzepts in Kenntnis.

Schutz der Privatsphäre und Internet
Aufgrund der Besorgnis der Öffentlichkeit und diverser Anfragen untersuchte die Datenschutzbehörde verschiedene Aspekte der privaten Nutzung von Internet und E-Mail. Viele Internet-Diensteanbieter erfassen Daten und Verhaltensweisen ihrer Klienten im Internet für kommerzielle Zwecke. Die Datenschutzbehörde gelangte zu dem Schluss, dass der Schutz personenbezogener Daten bei den Internet-Diensteanbietern sehr im argen liegt. Außerdem wurde ein Bericht vorgelegt, der auf die Untersuchung der von Arbeitgebern angewendeten Kontrollmaßnahmen für die Nutzung von Internet und E-Mail am Arbeitsplatz zurückgeht. Es wurden Leitlinien für eine realistische Anwendung entsprechender Kontrollen auf der Grundlage einer sorgfältigen Abwägung der Interessen von Arbeitgebern und Arbeitnehmern aufgestellt. Zur Bekämpfung der Cyberkriminalität fordern die

Strafverfolgungsbehörden umfangreiche Ermittlungsbefugnisse. Die Datenschutzbehörde hat die Zweite Kammer des Parlaments nachdrücklich dazu aufgefordert, bei der Beratung des geplanten Übereinkommens über die Cyberkriminalität (Europarat) die von der Verfassung vorgegebenen Grenzen staatlicher Vollmacht zu respektieren.

E. Website

www.cbpweb.nl

Die wichtigsten Veröffentlichungen 2000:

Klant in het web (Der Kunde im Internet), Juni 2000. Eine Darstellung des Schutzes der Privatsphäre im Internet.
Herkomst van de klant (Herkunft der Kunden), Oktober 2000. Eine Untersuchung über Spannungen im Zusammenhang mit der Eingliederung oder Ausgrenzung von Menschen aufgrund ihrer Rasse oder ethnischen Zugehörigkeit beim Produktmarketing.
De gewaardeerde klant (Der bewertete Kunde), Oktober 2000. Eine Untersuchung über die Bewertung der Kreditwürdigkeit unter Beteiligung Dritter wie z. B. Kreditauskunfteien.

Politiegegevens beschermd (Der Schutz von polizeilichen Daten), Juni 2000. Eine Darstellung des geschlossenen Datenbereitstellungssystems im Gesetz über polizeiliche Daten.

Goed werken in netwerken (Arbeit en in Netzen), Dezember 2000. Ein Bericht über die Kontrolle der Nutzung von E-Mail und Internet am Arbeitsplatz.

Zorg voor gegevens bij indicatiestelling – aanbevelingen voor de praktijk van indicatiestelling (Schutz von Daten über medizinische Diagnosen – Praktische Empfehlungen für den Umgang mit Diagnosedaten), August 2000. Ein Bericht über Grenzen und Möglichkeiten bei der Erhebung, Verwendung, Übermittlung und Speicherung von Patientendaten zur Diagnose im Gesundheitswesen im Rahmen des Gesetzes für medizinische Sonderausgaben.

Bankverzekeraars en privacy (Bankenversicherer und der Schutz der Privatsphäre), November 2000. Ein Bericht über den Stand der Verarbeitung personenbezogener Daten in Mischkonzernen des Finanzwesens.

Techniken zum besseren Schutz der Privatsphäre: Der Weg zur Anonymität – Nachdruck aufgrund der großen Nachfrage.

Portugal

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Keine.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Keine.

D. Spezifische Themen

Die portugiesische Datenschutzbehörde erteilte Genehmigungen für rund 500 Datenbanken, von denen 80 dem Telekommunikationssektor zuzurechnen sind. Bei der Behörde gingen 150 Beschwerden ein (davon 30 im Telekommunikationsbereich). Die Datenschutzbehörde führte 135 Überprüfungen vor Ort durch, zumeist aufgrund von Beschwerden von Bürgern, aber auch im Rahmen von auf eigene Initiative eingeleiteten Verifizierungsverfahren, darunter auch die Prüfung eines GSM-Telekommunikationsbetreibers.

Die Datenschutzbehörde verhängte in drei Fällen Strafgebühren (wegen nicht erfolgter Unterrichtung, Nichteinhaltung des Informationsrechts und unzulässiger Videoüberwachung) und sperrte eine Website des Justizministeriums, auf der online der vollständige Text von Entscheidungen des Obersten Gerichtshofs in Strafsachen mit personenbezogenen Angaben zu Minderjährigen, Opfern von Straftaten wie Vergewaltigung usw., einzusehen waren. Sämtliche Entscheidungen wurden daraufhin binnen 30 Tagen anonymisiert.

Verhaltensregeln für die Pharmaindustrie befinden sich in Vorbereitung.

Daten über „säumige Zahler“: Die Datenschutzbehörde bearbeitete eine Anfrage eines Verbraucherkreditunternehmens, das beabsichtigte, personenbezogene Daten über Klienten mit Zahlungsrückständen bei Mobilfunkbetreibern zu verarbeiten. Auf diese „schwarze Liste“ sollten alle Betreiber Zugriff haben. Die Datenschutzbehörde erteilte für diese Art der Verarbeitung keine Genehmigung, da diese nach den geltenden rechtlichen Bestimmungen und Vertragsregelungen nicht zulässig sei.

Stellungnahme zum Übereinkommen über die Cyberkriminalität: Die portugiesische Datenschutzbehörde gelangt in ihrer Stellungnahme zu den gleichen Schlussfolgerungen wie die Artikel 29-Datenschutzgruppe.

Geheimhaltungspflicht: Die Datenschutzbehörde nahm eine Bewertung des Niveaus der Datengeheimhaltung unter dem Aspekt vor, dass Kommunikationsinhalte und Verkehrsdaten durch das Telekommunikationsgeheimnis geschützt sind und Rechnungs- und Forderungsdaten unter das Berufsgeheimnis fallen. Die Diensteanbieter können selbst vor Gericht die Herausgabe dieser Daten verweigern; dies gilt auch für Strafverfahren. Wenn das Gericht die angeforderten Informationen für zwingend erforderlich erachtet, muss es den Fall an ein höheres Gericht verweisen, das dann entscheidet, ob der Diensteanbieter die Daten offenlegen muss. Telefonnummer und Anschrift eines Teilnehmers sind im Bereich der Telekommunikation – außer in Fällen, in denen der Teilnehmer die Geheimhaltung ausdrücklich beantragt hat – nicht geschützt.

E. Website

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

Spanien

A und B – Änderungen im Bereich der ersten, zweiten und dritten Säule

- Entsprechend dem **königlichen Erlass Nr. 994/1999 vom 11. Juni 1999**, mit dem die Verordnung über die Sicherheitsmaßnahmen für automatische Archivierungssysteme, die personenbezogene Daten enthalten, genehmigt wurde, wurden die Sicherheitsmaßnahmen der Grundstufe für alle automatisierten Archive sowie die Sicherheitsmaßnahmen der mittleren Stufe für bestimmte Arten von Archiven rechtskräftig.

- **Anweisung der Datenschutzbehörde Nr. 1/2000 vom 1. Dezember bezüglich der Vorschriften für internationale Datenbewegungen**, veröffentlicht im *Boletín Oficial del Estado* vom 16. Dezember 2000. Die Anweisung enthält die Leitlinien der Datenschutzbehörde für die Verarbeitung von Daten bei der Übermittlung im internationalen Bereich. Darin wird die Verfahrensweise der Datenschutzbehörde bei der Durchsetzung der Vorschriften für internationale Datenbewegungen erklärt. Die Anweisung ist auch insofern sehr nützlich, als sie die verschiedenen Bestimmungen zu diesem Thema in einem Text zusammenführt. Die Anweisung besteht aus zwei Teilen, im ersten geht es um die Kriterien für die internationale Übermittlung von Daten, im zweiten um spezifische Sachverhalte.

- **Entscheidung der Datenschutzbehörde vom 30. Mai 2000 über die Zulassung von Standardmitteilungen auf Papier, magnetischen und telematischen Datenträgern für Anträge auf Eintragung öffentlicher und privater Archive im Allgemeinen Datenschutzregister**, veröffentlicht im *Boletín Oficial del Estado* am 27. Juni 2000. Mit dem Inkrafttreten des neuen Gesetzes Nr. 15/1999 über den Schutz personenbezogener Daten wurde es notwendig, neue Anweisungen zu erlassen und neue Formen der Registrierung bekanntzugeben, u. a. Genehmigung der Mitteilung über die Verarbeitung über das Internet.

C. Wichtige Rechtsprechung

3.1 Rechtsprechung des Verfassungsgerichts

Das Verfassungsgericht erließ im Jahr 2000 **drei** Urteile, die die Tätigkeit der Datenschutzbehörde berühren.

Zu diesen Urteilen gehören die Entscheidungen Nr. 290/2000 und Nr. 292/2000 vom 30. November 2000, die auf die Anfechtung der verfassungsrechtlichen Gültigkeit des Gesetzes Nr. 15/1999 über den Schutz personenbezogener Daten und das durch dieses Gesetz außer Kraft gesetzte Vorläufergesetz, das Organgesetz Nr. 5/1992 über den Datenschutz zurückgehen.

1.- Entscheidung Nr. 290/2000 betraf die verschiedenen Anfechtungen der verfassungsrechtlichen Gültigkeit des Organgesetzes Nr. 5/1992 durch den

Exekutivrat der Generalitat de Catalunya, das katalonische Regionalparlament, den Datenschutzbeauftragten und 56 Parlamentsabgeordnete.

Im wesentlichen ging es in der Entscheidung darum, ob bestimmte Artikel des vorhergehenden Datenschutzgesetzes in bezug auf die der Datenschutzbehörde im Datenschutzgesetz übertragenen Pflichten und Befugnisse gegen den in der spanischen Verfassung festgelegten Grundsatz der Gewaltenteilung zwischen dem Staat und den autonomen Regionen verstießen. Das Gericht entschied, dass die Bestimmungen voll mit dem in der Verfassung verankerten Grundsatz der Gewaltenteilung im Einklang stehen.

2.- Entscheidung Nr. 292/2000 bestätigte die vom Datenschutzbeauftragten eingereichte Anfechtung der verfassungsrechtlichen Gültigkeit der Artikel 21 Absatz 1 und 24 Absatz 1 und 2 des Organgesetzes Nr. 15/1999 über den Schutz personenbezogener Daten. Dieses Urteil ist für den Datenschutz insofern von entscheidender Bedeutung, als es das Grundrecht auf den Schutz personenbezogener Daten ausdrücklich als ein eigenständiges Recht bestätigt und feststellt, dass „der von dem Grundrecht auf Datenschutz geschützte Gegenstand nicht allein auf die privaten und personenbezogenen Daten von natürlichen Personen beschränkt ist, sondern alle Arten von personenbezogenen Daten, seien diese privat oder auch nicht, einschließt, deren Kenntnis oder Verwendung durch Dritte geeignet ist, die Grundrechte natürlicher Personen grundlegend oder in anderer Weise zu beeinträchtigen, da dieses Recht nicht nur die durch Artikel 18 Absatz 1 der spanischen Verfassung geschützte Privatsphäre natürlicher Personen betrifft, sondern auch personenbezogene Daten."

In seiner Entscheidung erkennt das Gericht, dass der Text einzelner Gedankenstriche der Artikel 21 und 24 des Organgesetzes Nr. 15/1999 über den Datenschutz, die sich auf verschiedene Fälle beziehen, in denen Daten rechtmäßig zwischen öffentlichen Verwaltungen übermittelt oder übertragen werden dürfen, gegen die Verfassung verstößt und somit ungültig ist, und schränkt die Ausnahmen von den Rechten auf Unterrichtung und Zugang in bezug auf die Verarbeitung im öffentlichen Sektor ein.

3.- Die dritte wichtige Entscheidung, **Nr. 202/1999**, betrifft die Verarbeitung von Daten über die Gesundheit der Arbeitnehmer durch den Arbeitgeber. Das Verfassungsgericht bekräftigte das Recht des Klägers auf Schutz der Privatsphäre gemäß Artikel 18 Absatz 1 und 4 der spanischen Verfassung. Das Gericht erkannte eine Verletzung des Rechts auf Schutz der Privatsphäre des Klägers, wenn der Arbeitgeber ohne ausdrückliche Einwilligung und ohne diesbezügliche vertragliche Vereinbarung einen Arbeitnehmer betreffende medizinische Diagnosedaten in eine Datenbank über Krankmeldungen aufnimmt, die nicht für den Zweck der Gesunderhaltung der Arbeitnehmer, sondern zur Überwachung des Krankenstands geführt wird. Darüber hinaus erkannte das Gericht auch mit der Anerkennung seines Rechts auf Löschung derartiger Daten zugunsten des Klägers.

Das Gericht vertrat die Auffassung, dass die von dem Unternehmen durchgeführte Verarbeitung unverhältnismäßig in bezug auf die dafür angegebenen Gründe sei.

3.2 Entscheidungen der Verwaltungsgerichte

In 45 Fällen wurde gegen Entscheidungen der Datenschutzbehörde Berufung eingelegt, wobei die Gerichte in der Mehrzahl der Fälle zugunsten der Behörde entschieden. Dies bedeutet gegenüber der Zahl der Entscheidungen des Vorjahres einen Anstieg um 86 %.

Bei den Entscheidungen ging es zumeist um folgende Themen: Kredit- und Bonitätsauskünfte, Banken und Versicherungen, gewerbliche Akquisitions- und Werbemaßnahmen, Übermittlung von Daten aus dem Melderegister oder Übermittlung von Daten zwischen Konzernunternehmen.

Nachstehend eine Reihe besonders wichtiger Entscheidungen:

- In verschiedenen Entscheidungen des zurückliegenden Jahres wurden Urteile aus dem Jahr 1999 dahingehend aufgegriffen, dass die Daten des Wählerverzeichnisses in keine öffentlich zugängliche Datenquelle aufgenommen dürfen und dass daher die Erhebung entsprechender Daten für Akquisitions- und Werbezwecke unrechtmäßig ist.

- In einer Entscheidung über die Übermittlung von Daten aus dem Melderegister wurde die von der Datenschutzbehörde gegen eine Gemeindeverwaltung verhängte Geldstrafe wegen der Übermittlung von Daten aus dem Melderegister der Gemeinde an eine privatwirtschaftliche Organisation bestätigt. Daraufhin kam der Fall vor das Gericht der ersten Instanz.

- Die Gerichte bestätigten auch die Auffassung der Datenschutzbehörde, dass die Übertragung von Daten zwischen Konzernunternehmen eine Datenübermittlung darstellt und daher der Zustimmung der Betroffenen oder entsprechender rechtlicher Vollmachten bedarf.

- In einer weiteren wichtigen Entscheidung wurde die Berufung gegen eine von der Datenschutzbehörde verhängte Geldstrafe abgewiesen. In diesem Fall hatte eine natürliche Person Beschwerde dahingehend eingelegt, dass sie einen Werbekatalog von einer Firma erhalten hatte, der diese Daten von einer anderen Firma übermittelt worden waren, die als zugelassener Verarbeiter für einen Dritten tätig war, welchem der Betroffene seine Daten beim Kauf eines bestimmten Produkts angegeben hatte. Das Gericht erkannte in seiner Entscheidung, dass es sich hierbei um eine Übermittlung von Daten handle, die in der vertraglichen Beziehung für die Dienstleistungserbringung nicht geregelt sei, da ein Verarbeiter nicht zur Überlassung von Daten an Dritte – auch nicht zum Zweck der Aufbewahrung - und auch nicht zur Verwendung der Daten für andere als die im Dienstleistungsvertrag festgelegten Zwecke berechtigt ist.

D. Spezifische Themen

Im zurückliegenden Jahr war ein bemerkenswerter Anstieg des Interesses der Bürger an genaueren Informationen über das Recht auf Datenschutz zu verzeichnen. Dies geht auch aus den 19 262 Anfragen an die Datenschutzbehörde gemäß ihrer **Informationspflicht gegenüber dem Bürger** hervor. Die Mehrzahl der Anfragen – 14 420 (25 % mehr gegenüber dem Vorjahr) - wurde telefonisch beantwortet; 2 964

(70 % mehr als im Vorjahr) schriftlich und 1 878 (63 % mehr als im Vorjahr) in persönlichen Gesprächen. Die 1 173 056 registrierten Zugriffe auf die Website der Datenschutzbehörde bedeuten einen Anstieg um 132 % gegenüber dem Vorjahr. Die Website enthält auch einen „Fragen und Antworten"-Bereich mit Informationen zu den häufigsten Anfragen: Werbezusendungen, Telefonrechnung, Telefonverzeichnisse, Geltungsbereich des Datenschutzgesetzes, Zugang zu einem bekannten Verarbeiter, Zugang zur Datenschutzbehörde bei Fragen zu personenbezogenen Daten, Kredit- und Bonitätsdateien – Bonitätsaufzeichnungen einschließlich Daten aus öffentlich zugänglichen Quellen, Adressen von Bonitätsauskunftsarchiven, Registrierung von Archiven, Vorschriften für die Deklaration von Datenbeständen, Sicherheitsdokumente und Sicherheitsmaßnahmen allgemein. Darüber hinaus gingen Anfragen zu Arbeitgeber-Arbeitnehmer-Beziehungen, Gesundheitsdaten, Versicherung, Telekommunikation, Internet und Websites, Wahrnehmung der Rechte auf Zugang zu, Berichtigung und Löschung von Daten, Datenübermittlung und Einspruchsrechten ein.

Die Zahl der von der **Rechtsabteilung** bearbeiteten **Anfragen von für die Verarbeitung von Daten Verantwortlichen** stieg im um 63,78 % gegenüber dem Vorjahr. Insgesamt gingen 235 Anfragen von öffentlichen Verwaltungen – als für die Verarbeitung Verantwortliche in öffentlichem Eigentum – und 371 Anfragen von für die Verarbeitung Verantwortlichen aus der Privatwirtschaft ein.

Im Laufe des Jahres wurde die Datenschutzbehörde um Genehmigung von insgesamt 21 Bestimmungen ersucht, von denen die Folgenden besonders erwähnenswert erscheinen:

- Der Entwurf für einen königlichen Erlass zur Einsetzung der und zur Festsetzung der Tätigkeit der Interministeriellen Kommission zur Bekämpfung von Aktivitäten, die gegen geistiges und gewerbliches Urheberrecht verstoßen;
- der zweite Entwurf der Ministerialverordnung zur Einsetzung des Ausschusses im Ministerium für Gesundheit und Verbraucherschutz für die Durchführung eines Zensus von an Haemophilie und anderen kongenitalen Koagulopathien leidenden Menschen, die infolge einer Behandlung im Rahmen des staatlichen Gesundheitssystems mit dem Hepatitis-C-Virus infiziert wurden, und die Verordnung zur Einrichtung von diesbezüglichen Archiven;
- der Entwurf für einen königlichen Erlass über die Eintragung spanischer Staatsbürger in die Verzeichnisse der konsularischen Vertretungen im Ausland;
- der Entwurf für einen königlichen Erlass zur Umsetzung des vom Prüfungsamt der Sozialversicherung verwalteten internen Kontrollsystems;
- der Vorschlag für eine Verordnung mit Gesetzesstatus zur Aktualisierung der Verordnung zur Regelung der Aktivitäten des Risikobewertungszentrums der Banco de España (*Central de Riesgos del Banco de España*, CIRBE);
- der Entwurf für eine Ministerialverordnung zur Regelung der automatisierten Archive mit personenbezogenen DNS-Daten des Innenministeriums;
- der Vorentwurf für ein Datenschutzgesetz der Stadt Madrid;
- der Vorschlag der sozialistischen Fraktion für ein Gesetz betreffend die Maßnahmen, die notwendig sind, um die massenhafte Verarbeitung personenbezogener Daten durch Telefondienstbetreiber zu verhindern;
- der Entwurf für einen königlichen Erlass zur Genehmigung der Verordnung über den Schutz der Gesundheit vor ionisierender Strahlung.

Auch die Zahl der Anträge auf Eintragung von Archiven in das **Allgemeine Datenschutzregister** stieg deutlich an. Insgesamt 10 512 Anträge auf die Registrierung von Archiven machten 25 760 Registrierungsvorgänge erforderlich, da jeder Antrag mehrere Mitteilungen zu Registrierungszwecken bedingt. Der Anstieg gegenüber dem Vorjahr betrug damit 400 %. Seit Juli 2000 kann die Registrierung auch per Internet beantragt werden; bis Dezember wurden aufgrund von Anträgen 2 445 Vorgänge zur Registrierung, Änderung oder Löschung von privaten Dateien und 21 Vorgänge für öffentliche Archive durchgeführt, hinzu kommen insgesamt 1 995 Vorgänge, die im Fall von privaten Archiven durch Zusendung von Magnetdatenträgern abgeschlossen wurden.

Bis zum 31. Dezember 2000 wurden insgesamt 249 209 Archive in das Allgemeine Datenschutzregister aufgenommen, darunter 31 155 in öffentlichem Eigentum und 218 054 in privatem Eigentum. Von den im Jahr 2000 registrierten öffentlichen Archiven, die sich auf Aktivitäten im Bereich der dritten Säule bezogen, betrafen sechs Vorgänge der Strafverfolgungsbehörden für polizeiliche Zwecke – von insgesamt 2 063 bis zum 31. Dezember registrierten Operationen – und 13 betrafen Justizverfahren – von insgesamt 880 bis zum 31. Dezember 2000 registrierten Verfahren.

Erwähnenswert ist auch, dass der Datenschutzbehörde 1 352 internationale Übermittlungen von Daten gemeldet wurden, wobei 51 Vorgänge Daten in öffentlichem Eigentum betrafen und 1 301 Daten in privatem Eigentum.

Von den im Jahr 2000 gemeldeten Archiven betrafen 272 internationale Datenübermittlungen.

Weiter ist zu vermerken, dass es einen Anstieg bei der Zahl der von Bürgern eingereichten Beschwerden und somit bei den von der Behörde durchgeführten **Datenkontroll**maßnahmen gab. Hier war ein deutlicher Anstieg gegenüber dem Vorjahr zu verzeichnen, der für die Verarbeitung von Daten Verantwortliche sowohl in öffentlichem als auch in privatem Eigentum betraf. 2000 fällte der Direktor der Datenschutzbehörde 622 endgültige Entscheidungen in administrativen Fällen aufgrund von Beschwerden, Verfahren und Revisionen.

Die Kontrollmaßnahmen lassen sich in **zwei große Kategorien** einteilen: Maßnahmen, die auf **Beschwerden** zurückgehen, die von natürlichen Personen aufgrund von Verstößen gegen geltendes Recht eingereicht wurden, und Aktivitäten im Rahmen von **sektorbezogenen Kontrollplänen**, bei denen überprüft wird, inwieweit die Vorschriften zum Schutz personenbezogener Daten im öffentlichen und im privaten Sektor eingehalten werden.

Die auf **Beschwerden** bezüglich **Archiven in privatem Eigentum** zurückgehenden Aktivitäten betrafen insbesondere die Verarbeitung personenbezogener Daten durch **Telekommunikationsdienste**: Datenverarbeitung ohne Einwilligung der Betroffenen, der Grundsatz der Datenqualität und die daraus hervorgehende Pflicht, dass die Daten zutreffend und auf dem aktuellen Stand sein müssen, um ein wahrheitsgemäßes Bild der Betroffenen wiederzugeben; Einhaltung der für den Bereich der Telekommunikation geltenden Datenschutzverordnungen, von Gesetz Nr. 11/1998,

dem allgemeinen Gesetz für den Bereich der Telekommunikation, und des königlichen Erlasses Nr. 1736/1998, mit dem die Verordnung zur Umsetzung von Titel III des allgemeinen Gesetzes für den Bereich der Telekommunikation bezüglich des Universaldienstes im Bereich der Telekommunikation angenommen wird (beide Rechtsvorschriften setzen die Richtlinie 97/66 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation in spanisches Recht um); die Verarbeitung personenbezogener Daten im **Internet**: unzulässige Offenlegung personenbezogener Daten, Versand von E-Mail-Mitteilungen oder Verwendung von im Internet erhobenen Daten für andere Zwecke als diejenigen, für die sie ursprünglich erhoben wurden; der Fall der Vereinigung gegen Folter, der nach einer Beschwerde eingeleitet wurde und in dem der Direktor der Datenschutzbehörde Geldstrafen verhängte, weil keine Einwilligung der Betroffenen vorlag, weil Daten unrechtmäßig übermittelt worden waren und weil dieses Archiv strafbare Handlungen außerhalb des geltenden Rechts ermöglichte. Besonders viele Beschwerden betrafen auch den Bereich **Direktmarketing und Direktwerbung**: Direktmailing, Datenübermittlungen, Verarbeitung von Daten ohne Einwilligung und nichterfolgte Löschungen. Zahlreiche Beschwerden und damit auch viel Arbeit für die Behörde gab es auch aufgrund von **Dienstleistungen im Bereich Kredit- und Bonitätsauskunft**. Ebenfalls betroffen war das **Gesundheitswesen**, wobei die schwerwiegendsten Beschwerden die unrechtmäßige Übermittlung personenbezogener Gesundheitsdaten betrafen. Weitere Beschwerden, wenngleich in geringerer Zahl als in den vorgenannten Sektoren, betrafen **Berufsverbände, politische Parteien** und **Gewerkschaften**.

In bezug auf Archive in privatem Eigentum in diesem Bereich wurden infolge einer auf **Initiative des Direktors der Datenschutzbehörde** durchgeführten Kontrolle der Fernsehsendung „Big Brother“ Strafgebühren wegen Verstoßes gegen gesetzliche Bestimmungen verhängt, die für die Verarbeitung besonders geschützter Daten die Einholung einer Einwilligung, die Wahrung der Informationsrechte der Betroffenen, die Ergreifung geeigneter Sicherheitsmaßnahmen sowie die Einhaltung der gesetzlich vorgeschriebenen Garantien in bezug auf die Übermittlung von Daten vorschreiben.

Ein bedeutender Fall wurde durch Berichte in den Medien ausgelöst, dass personenbezogene Daten der Telefonteilnehmer eines großen Telefondienstbetreibers über das Internet zugänglich seien. Die einleitenden Untersuchungen ergaben eine Reihe von Fakten, die zur Verhängung von Sanktionen wegen Nichteinhaltung der Pflicht des für die Verarbeitung Verantwortlichen zur Wahrung der Sicherheit und wegen Verstoßes gegen die Sicherheitsverordnung, mit der diese Forderung umgesetzt wird, führten.

Ein weiterer bemerkenswerter Fall hat seinen Ursprung im Sommer 2000 als die Datenschutzbehörde Datenträger erhielt, auf denen angeblich über zwölftausend Benutzercodes und Passwörter von Internet-Benutzern gespeichert waren, die einen Dienstleistungsvertrag mit dem Eigentümer des betreffenden Portals geschlossen hatten. Daraufhin wurden Untersuchungen eingeleitet, um zu ermitteln, ob in bezug auf die nicht erfolgte Geheimhaltung der Daten ein Gesetzesverstoß vorlag. Am Ende des Verfahrens wurden Sanktionen wegen der Nichteinhaltung der Pflicht zur Ergreifung der notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit und wegen der nicht erfolgten Löschung der Daten nach Erreichen des Zwecks, für den sie erhoben worden waren, verhängt.

Es sei darauf hingewiesen, dass mit **proaktiven Sektorplänen** bestimmt werden soll, wie in den kontrollierten Sektoren personenbezogene Daten verarbeitet werden, um gegebenenfalls entsprechend dem Datenschutzgesetz Disziplinarmaßnahmen zu ergreifen. Zum Abschluss derartiger Prüfungen spricht der Direktor der Datenschutzbehörde üblicherweise gemäß den ihm von der Geschäftsordnung der Behörde übertragenen Befugnissen Empfehlungen aus, die für die kontrollierten Organisationen und von allen in dem Sektor tätigen Organisationen beachtet werden sollten, um durch Anpassung ihrer Prozesse die Grundsätze und Vorschriften des Datenschutzgesetzes einzuhalten.

Im Jahr 2000 wurde – zurückgehend auf die proaktiven Sektorpläne des Jahres 1999, die die staatliche Steuerverwaltung, die Generaldirektion Verkehr, den **Gesundheitssektor** (das Gómez-Ulla-Militärkrankenhaus, das psychiatrische Vollzugskrankenhaus Alicante und das nationale AIDS-Register des nationalen Epidemiologiezentrums) sowie den **privaten Forschungssektor** betrafen – eine Reihe von **Empfehlungen** ausgesprochen.

Im Jahr 2000 maß die Datenschutzbehörde den proaktiven Sektorplänen besondere Bedeutung bei, es wurden **proaktive Prüfungen** in den Bereichen **E-Commerce, Internet-Diensteanbieter, Kartenmanagement in Supermärkten**, im **Telekommunikationssektor** und beim ***Consorcio de Compensación de Seguros*** (Clearingkonsortium für das Versicherungswesen) durchgeführt.

Besonders erwähnenswert sind in diesem Zusammenhang Kontrollen der Datenschutzmaßnahmen im **E-Commerce**-Sektor, bei denen private Initiativen zur Selbstregulierung geprüft wurden: die Ethikgrundregeln für den Schutz personenbezogener Daten im Internet des spanischen E-Commerce- und Direktmarketingverbandes, die 1998 in das Allgemeine Datenschutzregister eingetragen worden waren, und die Regeln für berufliche Standards von Internet-Diensteanbietern des sektorübergreifenden Verbands der spanischen Elektronikunternehmen.

Aus dem Fazit dieses proaktiven Sektorplans geht hervor, dass Internet-Nutzern nicht in allen Fällen (27 %) der Name der für die Verarbeitung von Archiven, in denen erhobene personenbezogene Daten gespeichert sind, verantwortlichen Person mitgeteilt wird. Auch haben nicht alle für die Verarbeitung Verantwortlichen (36 %) für die untersuchten Websites ihre Archive beim Allgemeinen Datenschutzregister angemeldet, wobei in praktisch allen untersuchten Fällen offensichtlich ist, dass von den betroffenen Websites Daten erhoben werden. Ein weiterer wichtiger Punkt betrifft die Tatsache, dass die Nutzer sich zumeist registrieren lassen müssen, bevor sie Bestellungen aufgeben können, wobei sie Daten zu ihrer Identifikation angeben müssen. Was die Datensicherheit anbelangt, so wurde festgestellt, dass lediglich 54 % der untersuchten Websites HTTPS-Protokolle für den Aufbau einer sicheren Verbindung zwischen Servern und Nutzern für die Übertragung personenbezogener Daten verwendeten.

Die wichtigsten Datenkontrollmaßnahmen der Datenschutzbehörde in bezug auf **Archive in öffentlichem Eigentum** konzentrierten sich auf die folgenden staatlichen Organe: die staatliche Steuerverwaltung, gegen die auch Beschwerden von Steuerzahlern eingingen, die Finanzverwaltung der Sozialbehörde, die

Sozialversicherung (wobei der Direktor in seinen Empfehlungen das Amt verpflichtete, bei der Erhebung von Daten das Informationsrecht einzuhalten und zu gewährleisten, dass bei der Verarbeitung von Daten wie z. B. Daten über Behinderungen und andere besonders geschützte Daten wie Unterhaltszahlungen für Kinder und Ehegatten die schnellstmögliche Einholung der Einwilligung der Betroffenen gewährleistet ist), das staatliche Arbeitsamt, gegen das verschiedene Beschwerden vorlagen, die Generaldirektion Verkehr, die Provinzregierung von Castilla y León, das Verteidigungsministerium, das Ministerium für Bildung und Kultur und das Außenministerium.

Kontrollen infolge von **Beschwerden von natürlichen Personen** wurden bei den Dienststellen der autonomen Regionen Baleares, La Rioja, Asturias, Andalucía und Valencia durchgeführt. Außerdem fanden proaktive Kontrollen bei den Dienststellen der autonomen Regionen Murcia und Catalonia sowie bei lokalen Gebietskörperschaften statt.

Sechs Kontrollen wurden bei den staatlichen Strafverfolgungsbehörden durchgeführt.

Die Datenschutzbehörde traf zudem sieben Entscheidungen in Beantwortung verschiedener Kooperationsanträge nach Artikel 114 Absatz 2 des Schengener Übereinkommens, die vom Präsidenten der französischen Datenschutzbehörde ***Commission Nationale de L'Informatique et des Libertés*** **(CNIL)** an sie gerichtet worden waren. Die Anträge betrafen den Zugang zu und die Löschung von Dateien im **Schengener Informationssystem (SIS)** über Personen, denen die Einreise in den Schengenraum zu verwehren ist und deren Daten von den spanischen Behörden eingegeben worden waren. Es wurde daher geprüft, ob die Daten dieser Personen nach geltendem Recht richtigerweise erfasst worden waren. In jedem Einzelfall wurden Archive und Aufzeichnungen der Ausländerbehörde und die Akten der Polizeibehörde geprüft; dabei wurde festgestellt, dass die betroffenen Personen aufgrund gerichtlicher oder administrativer Entscheidungen aus dem Staatsgebiet ausgewiesen und ihnen die Wiedereinreise verweigert worden war. In jedem untersuchten Einzelfall wurde die CNIL über die Maßnahmen und die Gründe für die Erfassung der betroffenen Personen im SIS unterrichtet.

Ein einzelner Fall der Zusammenarbeit zwischen der CNIL und der spanischen Datenschutzbehörde verdient besondere Erwähnung: Im November 2000 ging bei der Behörde eine Erklärung der CNIL ein, dass eine spanische Organisation, die einen europaweiten Dienstleistungsführer erstellte und veröffentlichte, in Frankreich ansässigen Bürgern – von welchen einer die Beschwerde eingereicht hatte - Rechnungen für Anträge auf Aufnahme ihrer Daten in eines der Jahrbücher der Organisation gestellt hatte, obwohl diese nie einen solchen Antrag ausgefüllt hatten. Der Direktor erteilte der Datenkontrollstelle den Auftrag, alle notwendigen Schritte zu unternehmen, um den Sachverhalt zu klären. Nach Abschluss der Kontrolle wurde entschieden, die Sache zu den Akten zu legen, weil festgestellt wurde, dass die für den Versand verwendeten Daten aus öffentlich zugänglichen Quellen stammten – insbesondere Telefonverzeichnissen verschiedener europäischer Länder, darunter Frankreich – und dass die nachfolgende Datenverarbeitung mit ausdrücklicher schriftlicher Einwilligung der Betroffenen erfolgt war.

Bei zwei Gelegenheiten im Jahr 2000 trat der Direktor der Datenschutzbehörde vor dem Verfassungsausschuss der Abgeordnetenkammer auf, um im Rahmen der Aufsichtsfunktion des Parlaments für die Aktivitäten der Datenschutzbehörde den Jahresbericht der Datenschutzbehörde zu erörtern und die von den Fraktionen im Parlament angesprochenen Fragen in bezug auf die Tätigkeit der Datenschutzbehörde darzulegen. Hierbei ging es unter anderem um den Datenschutz bei Übermittlungen in Drittländer, den Datenschutz in öffentlichen Verwaltungen und Fragen bezüglich der Verordnung über Sicherheitsmaßnahmen.

Am 12. Juni 2000 unterzeichnete der Direktor der Datenschutzbehörde für die Behörde ein **Protokoll über die informationelle Zusammenarbeit zwischen der Datenschutzbehörde und dem Rat der offiziellen Industrie-, Handels- und Navigationskammern** zwecks Entwurf, Koordination und Aufstellung von gemeinsamen Kriterien für alle Kammern mit Blick auf die Bestimmung und Abgrenzung der Bewertung ihrer Dateien und die Zusammenarbeit der Parteien bei der Auslegung interpretationsbedürftiger Fragen bezüglich der Anwendung des Organgesetzes Nr. 15/1999 sowie zur Bildung von Arbeitsgruppen für die Festlegung geeigneter Koordinationsverfahren.

Am 13. April 2000 unterzeichnete der Direktor für die Datenschutzbehörde ein **Protokoll über die Zusammenarbeit mit dem Notariatsrat**, das die Einsetzung von Arbeitsgruppen für die gemeinsame Klärung, Information und Zusammenarbeit bezüglich der bestmöglichen Anwendung des Gesetzes im Einzelfall ermöglichen soll.

Weiter ist das **Protokoll über die Zusammenarbeit mit dem Verband der freien Berufe**, in dem Kammern und Generalräte der verschiedenen freien Berufe zusammengeschlossen sind, zu nennen, das am 15. Juni 2000 unterzeichnet wurde.

Ziel aller genannten Initiativen ist es, die vorrangigen Probleme verschiedener Gruppen von für die Verarbeitung von Daten Verantwortlichen zur ermitteln und zu bestimmen und einheitliche Antworten bezüglich der Anwendung des Datenschutzgesetzes für die Vertretungsorganisationen zu erarbeiten, die diese an ihre Mitglieder weitergeben können.

E. Website

https://www.agenciaprotecciondatos.org/

Schweden

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

Spezielle Registergesetze, zum Beispiel:

Grundbuchgesetz (2000:224) (Lagen om fastighetsregister)

Das Grundbuchgesetz (2000:224) regelt die Verarbeitung personenbezogener Daten im Grundbuch und legt fest, dass im Rahmen der nationalen Grundstückserhebung eine Grundbuch mit genauen Angaben über den Grundbesitz geführt werden soll.

Gesetz (2000:832) über qualifizierte elektronische Signaturen
Mit dem Gesetz (2000:832) über qualifizierte elektronischen Signaturen soll die Verwendung von elektronischen Signaturen erleichtert werden. Mit diesem Gesetz wird die EG-Richtlinie 99/93 über elektronische Signaturen umgesetzt. Abschnitt 16 regelt die Erhebung personenbezogener Daten; darin heißt es u. a., dass eine Organisation, die Zertifikate ausstellt, personenbezogene Daten nur von derjenigen Person erheben darf, auf welche sich die Daten beziehen oder von Personen, die hierzu ihre ausdrückliche Einwilligung erteilt haben.

Gesetz (2000:344) über das Schengener Informationssystem
Das Gesetz (2000:344) über das Schengener Informationssystem legt fest, dass die nationale Polizeibehörde für die Zwecke ihrer Aufgabe als schwedische Sektion des Schengener Informationssystems (SIS) ein Register führt. Das Gesetz regelt die Verarbeitung personenbezogener Daten in der schwedischen Sektion des SIS durch die nationale Polizeibehörde.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Spezielle Registergesetze, zum Beispiel:

Gesetz (2000:344) über das Schengener Informationssystem

C. Wichtige Rechtsprechung

Das Stadtgericht Göteborg verhängte gegen eine Pflegekraft eine Geldstrafe wegen unerlaubtem Zugriff auf Daten. Ein Minister der schwedischen Regierung war erkrankt und in ein Krankenhaus eingeliefert worden, wo er verstarb. Später wurde festgestellt, dass zahlreiche Krankenhausmitarbeiter die Krankenakte des Verstorbenen eingesehen hatten. Eine Untersuchung ergab, dass mehrere dieser Personen nicht mit der eigentlichen Behandlung des Ministers befasst gewesen waren und daher kein Recht auf Zugang zu den Daten gehabt hatten. Gegen die Entscheidung wurde Berufung eingelegt.

Eine Mitarbeiterin einer Kirchengemeinde hatte ohne deren Einwilligung Informationen über ihre Kollegen auf einer Website veröffentlicht. Einige der Kollegen waren über die Darstellung verärgert, daraufhin erstattete die Gemeindemitarbeiterin Selbstanzeige bei der Polizei, um untersuchen zu lassen, ob sie gegen das Datenschutzgesetz verstoßen hatte. Die Datenschutzkommission wurde um Stellungnahme zu dem daraufhin eingeleiteten Rechtsverfahren gebeten. Die Datenschutzkommission stellte fest, dass die veröffentlichten personenbezogenen Daten nicht ohne Einwilligung der Betroffenen veröffentlicht werden durften und dass es sich zum Teil um sensible Daten (Gesundheitsdaten) handelte. Die Kommission stellte darüber hinaus fest, dass personenbezogene Daten in Zuwiderhandlung gegen das Datenschutzgesetz in Drittländer übermittelt und dass die Betroffenen nicht gemäß dem Gesetz über die Verarbeitung unterrichtet worden waren. Allerdings kam die Kommission auch zu dem Schluss, dass gemäß einer jüngsten Änderung des

Gesetzes bei Bagatelldelikten auf eine Bestrafung verzichtet werden kann. Das Bezirksgericht war allerdings nicht der Auffassung, dass es sich hier um ein Bagatelldelikt handelte und verurteilte die Frau zu einer Geldstrafe wegen Verstoßes gegen das Datenschutzgesetz. Gegen die Entscheidung des Gerichts wurde Berufung eingelegt, das Berufungsgericht forderte eine Stellungnahme des Europäischen Gerichtshofs an.

D. Spezifische Themen

Die Datenschutzkommission veröffentlichte eine Informationsbroschüre über personenbezogene Daten und das Internet. Zudem befasste sich die Kommission mit Fällen, in denen es um die Veröffentlichung personenbezogener Daten im Internet ging sowie um Ausnahmeregelungen für Verarbeitungsvorgänge, die für journalistische Zwecke durchgeführt werden.

Nach einer Diskussion in den Medien über die Handhabung von Kreditauskünften und insbesondere von unzutreffenden Daten in diesem Zusammenhang führte die Datenschutzkommission in einer Gemeinschaftsaktion mit der schwedischen Finanzaufsichtsbehörde eine Untersuchung der Tätigkeit der Kreditauskunfteien durch. Das Ergebnis dieser Aufsichtsmaßnahme war der Bericht „Missvisande kreditupplysningar – åtgärder och förslag“, der auch auf der Website der Datenschutzkommission veröffentlicht wurde.

Die schwedische Regierung setzte einen Untersuchungsausschuss zur Frage des Schutzes der Privatsphäre am Arbeitsplatz ein. Ein Mitarbeiter der Datenschutzkommission wurde als Sachverständiger in den Untersuchungsausschuss berufen.

E. Website

www.datainspektionen.se

Vereinigtes Königreich

A. Angenommene legislative Maßnahmen im Bereich der ersten Säule

Im Vereinigten Königreich wurden Rechtsvorschriften eingeführt, die dem Einzelnen besseren Zugang zu den bei öffentlichen Organen gespeicherten Informationen geben.

Das Gesetz über die Informationsfreiheit (Freedom of Information Act) 2000 gestattet natürlichen Personen den Zugang zu personenbezogenen ebenso wie nicht-personenbezogenen Informationen aller Art. Darüber hinaus schreibt das Gesetz vor, dass die Behörden Veröffentlichungssysteme einführen und unterhalten müssen, in denen sie ihre Regelungen für die Veröffentlichung von Informationen bekanntgeben. Die Rechtsvorschrift tritt am 30. November 2005 in vollem Umfang in Kraft, für die Durchsetzung zeichnet die Datenschutzbeauftragte (Information Commissioner) verantwortlich.

Eine weitere Rechtsvorschrift mit Auswirkungen auf das Datenschutzgesetz und darüber hinaus ist das Menschenrechtsgesetz (Human Rights Act) 1998. Das Gesetz, mit dem erstmals die Europäische Menschenrechtskonvention in britisches Recht umgesetzt wird, trat im Oktober 2000 in Kraft. Das Gesetz stellt einen wichtigen Beitrag zu dem Rechtsrahmen dar, innerhalb dessen die Datenschutzbeauftragte das Datenschutzgesetz auslegt und anwendet. Es hat auch Auswirkungen darauf, wie sie als öffentliches Organ mit denjenigen umgeht, die sich an sie wenden, und mit denjenigen, für die sie Regeln festsetzt.

Das Gesetz über die Regelung von Ermittlungsvollmachten (Regulation of Investigatory Powers Act) 2000 führte Bestimmungen ein, die die Überwachung von Telekommunikationssystemen regeln und bezieht dabei erstmals auch private Systeme ein, wie sie an den meisten Arbeitsplätzen zum Einsatz kommen. Mit dem Gesetz wurde Artikel 5 der Richtlinie 97/66/EG umgesetzt. Das Gesetz enthält auch umstrittene Bestimmungen, die den Strafverfolgungsbehörden Befugnisse zur Untersuchung von verschlüsselten elektronischen Daten geben. Mit dem Gesetz wäre die Überwachung der elektronischen Kommunikation am Arbeitsplatz durch den Arbeitgeber unrechtmäßig geworden, daher wurden die Verordnungen über rechtmäßige Geschäftspraktiken (Lawful Business Practice Regulations) 2000 eingeführt, welche die Überwachung der Kommunikation durch den Arbeitgeber unter bestimmten Voraussetzungen erlauben. Durch die Verordnungen wird die Pflicht des Arbeitgebers zur Einhaltung des Datenschutzgesetzes nicht aufgehoben, doch führten die Umstände ihrer Einführung zu erheblichen Missverständnissen. Die Datenschutzbeauftragte sah sich veranlasst klarzustellen, dass die Verordnungen – unabhängig von Datenschutzanforderungen - Arbeitgebern nicht das Recht geben, die Kommunikationen ihrer Arbeitnehmer routinemäßig zu überwachen.

B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule

Infolge der Umsetzung des Europol-Übereinkommens wurde ein gemeinsames Datenschutz-Kontrollorgan eingesetzt, das eine systematische Prüfung von Europol einführte. An diesen Aktivitäten wirkte die Datenschutzbeauftragte aktiv mit. Im Bereich des Übereinkommens von Schengen erklärte sich das Vereinigte Königreich zwischenzeitlich bereit, sich den Regelungen für die gemeinsame Nutzung polizeilicher Daten anzuschließen, an der gemeinsamen Schengener Kontrollstelle für den Datenschutz wird sich das Vereinigte Königreich mit Beobachterstatus beteiligen.

C. Wichtige Rechtsprechung

Im Jahr 2000 wurden gegen zwei Unternehmen förmliche Zwangsmaßnahmen wegen Zuwiderhandlung gegen die Telekommunikationsverordnungen (Datenschutz und Schutz der Privatsphäre) 1999 in bezug auf den Versand von unerbetenen Direktmarketing-Faxmitteilungen verhängt. Die Zwangsmaßnahmen stützten sich auf zahlreiche bei der Datenschutzbeauftragten eingegangene Beschwerden. Die betroffenen Unternehmen legten Berufung ein.

Vor der Anhörung und nach umfangreichen Regelungen erklärten sich die Unternehmen mit den Zwangsmaßnahmen einverstanden. Die Datenschutzbeauftragte wird die Einhaltung der Bestimmungen durch diese und andere Firmen weiterhin überwachen, um die Einhaltung der Telekommunikationsverordnungen zu

gewährleisten. Im Rahmen ihres Auftrags stellte die Datenschutzbeauftragte im Verlaufe des Jahres drei weiteren Organisationen Androhungen über Zwangsmaßnahmen zu.

D. Spezifische Themen

Das Datenschutzgesetz 1998 sieht vor, dass die Datenschutzbeauftragte die Übernahme bewährter Verfahren und die Einhaltung der Anforderungen des Gesetzes durch die für die Verarbeitung von Daten Verantwortlichen fördert. Zu diesem Zweck kann sie Verhaltensregeln für die für die Verarbeitung Verantwortlichen erstellen und verbreiten. Die ersten derartigen Verhaltensregeln für den Einsatz von Videoüberwachungsanlagen wurden im Juli 2000 herausgegeben. Die Verhaltensregeln wurden von den Verantwortlichen ebenso wie von den Betroffenen positiv aufgenommen. Sie sollen verständliche und eindeutige Ratschläge für die Einhaltung des Gesetzes und für die Anwendung bewährter Verfahren beim Einsatz von Videoüberwachungsanlagen auf öffentlichen Plätzen vermitteln.

Die Datenschutzbeauftragte erteilte ihrer Dienststelle den Auftrag, entsprechende Verhaltensregeln für die Verwendung personenbezogener Daten im Arbeitgeber-Arbeitnehmer-Verhältnis zu erarbeiten. Ein im Oktober 2000 vorgelegter Entwurf fand großes Interesse, insbesondere, was die Überwachung von E-Mail- und Internet-Zugang am Arbeitsplatz betrifft. Das Projekt ist noch nicht abgeschlossen. In ihrer Endfassung werden die Verhaltensregeln nicht nur für das herkömmliche Arbeitgeber-Arbeitnehmer-Verhältnis, sondern auch für weitere Gruppen wie z. B. ehrenamtlich Tätige, Mitarbeiter von Zeitarbeitsfirmen und Zeitarbeitskräfte gelten.

Seit August 2000 beteiligt sich die Dienststelle der Datenschutzbeauftragten auch an einer Gemeinschaftsinitiative zusammen mit dem Ministerium für soziale Sicherheit und der Finanzverwaltung. Mit dieser als Baird-Projekt bekannt gewordenen Initiative sollen natürliche Personen und Organisationen dingfest gemacht werden, die sich unrechtmäßig und systematisch personenbezogene Daten für Dritte zu verschaffen versuchen. Die Initiative zeigt Erfolg und hat bereits zu einer Reihe von Anklagen geführt.

Im Vereinigten Königreich wird das Wählerverzeichnis, das Name und Anschrift aller Wahlberechtigten enthält, seit jeher öffentlich zum Verkauf angeboten. Es wird für Marketingzwecke, zum Auffinden von Schuldnern und für eine Reihe weiterer Zwecke verwendet. Auf Druck der Datenschutzbeauftragten und anderer Stellen sieht nunmehr das Volksvertretungsgesetz (Representation of the People Act) 2000 die Erstellung von zwei Wählerverzeichnissen vor. Das erste Verzeichnis, das für Wahlzwecke erstellt wird, ist das vollständige Verzeichnis, in das alle wahlberechtigten Personen ihre Angaben eintragen lassen müssen. Bei dem zweiten Verzeichnis handelt es sich um eine bearbeitete Fassung. Wählern steht offen, ob sie ihre Daten in das Verzeichnis eintragen lassen wollen oder nicht. Verkauft wird nur das bearbeitete Verzeichnis. Verordnungen, mit denen die Neuregelungen in Kraft gesetzt werden, stehen noch aus. Noch zu klären ist unter anderem die entscheidende Frage, für wen und zu welchen Zwecken das vollständige Verzeichnis zugänglich sein wird.

Im Jahr 2000 führte die Datenschutzbeauftragte in den Medien eine umfangreiche Kampagne durch, um die Einwohner über ihre Rechte nach dem Datenschutzgesetz aufzuklären und die Öffentlichkeit vermehrt für den Datenschutz zu sensibilisieren. Im Rahmen der Kampagne wurden unter anderem Werbespots in einem der großen britischen Fernsehsender ausgestrahlt. Über Telefonnummern zum Ortstarif konnte bei einer beauftragten Versandfirma Informationsmaterial über die Datenschutzrechte natürlicher Personen angefordert werden. Eine Umfrage ergab, dass 19 % der Befragten die Werbekampagne bekannt war.

Durch die Einführung des Datenschutzgesetzes 1998 und die Medienkampagne hat die Arbeit der Datenschutzbeauftragten zugenommen. Trotz der mit dem neuen Gesetz eingeführten umfangreichen Ausnahmeregelungen in bezug auf die Mitteilungspflicht umfasst das Verzeichnis der für die Verarbeitung von Daten Verantwortlichen mittlerweile über 220 000 Einträge. Die telefonische Auskunftsstelle bearbeitet jährlich rund 55 000 Anfragen. Im Jahr 2000 gingen 8 000 Beschwerden von Betroffenen ein, die zu Beurteilungsanträgen nach dem neuen Gesetz führten.

Auch im Jahr 2000 trat die Datenschutzbeauftragte aktiv für die Abordnung von Bediensteten an ihr Amt und aus ihrem Amt ein, so wurde unter anderem ein Assistent der Datenschutzbeauftragten für die Ausarbeitung eines noch nicht veröffentlichten Berichts über den Schutz der Privatsphäre bei der gemeinsamen Nutzung von Daten zur Dienststelle Leistung und Innovation der Kanzlei des Premierministers abgestellt.

E. Website

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

1.5. Aktivitäten der Europäischen Union und der Gemeinschaft

1.5.1. Datenschutz in Einrichtungen und Organen der Gemeinschaft

Mit dem Vertrag von Amsterdam wurde der neue Artikel 286 in den Vertrag über die Gründung der Europäischen Gemeinschaft aufgenommen. Die Bestimmungen dieses Artikels schreiben vor, dass die Einrichtungen und Organe der Gemeinschaft ab dem 1. Januar 1999 die Gemeinschaftsvorschriften für den Schutz personenbezogener Daten, wie sie im wesentlichen in den Richtlinien 95/46/EG und 97/66/EG festgelegt sind, anwenden müssen. Darüber hinaus legt der Artikel fest, dass die Anwendung dieser Vorschriften von einer unabhängigen Kontrollinstanz überwacht werden muss. Dieser Gedanke stand auch hinter der Aufnahme des Rechts auf Schutz personenbezogener Daten in Artikel 8 der Grundrechtecharta der Europäischen Union.

Diesem Mandat entsprechend hatte die Kommission am 14. Juli 1999 ihren Vorschlag für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft vorgelegt. Die Kommission, der Rat und das Parlament kündigten daraufhin ihr gemeinsames Ziel an, die Verordnung bereits in der ersten Lesung des

Mitentscheidungsverfahrens anzunehmen. Demzufolge stimmte das Parlament nach einem politischen Kompromiss in Form eines konsolidierten Texts am 14. November 2000 über eine Reihe von Änderungsanträgen ab, die Kommission nahm die Änderungsanträge an und legte ihren geänderten Vorschlag vor, den der Rat am 30. November 2000 einstimmig genehmigte. Damit war die Verordnung am 18. Dezember 2000 angenommen.

Die Verordnung enthält eine Reihe von Grundsätzen für die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft. Parallel hierzu sieht die Verordnung die Einsetzung einer unabhängigen Kontrollinstanz, des *Europäischen Datenschutzbeauftragten*, vor, der den Auftrag hat, die Anwendung der Bestimmungen der Verordnung zu gewährleisten.

1.5.2. Entwurf einer Richtlinie über den Schutz der Privatsphäre und personenbezogener Daten in der elektronischen Kommunikation

Im Rahmen des Überprüfungspakets für den Telekommunikationsbereich legte die Kommission den Entwurf für eine Richtlinie zum Schutz der Privatsphäre[22] vor, in dem verschiedene Vorschläge für die Aktualisierung des Regelungsrahmens für ein zusammenwachsendes technologisches Umfeld enthalten sind. Der Richtlinienentwurf soll die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ablösen, die vom Europäischen Parlament und dem Rat am 15. Dezember 1997 angenommen worden war und bis 24. Oktober 1998 umgesetzt werden musste.

Inhaltlich soll die bestehende Richtlinie nicht wesentlich geändert werden, vielmehr sieht der Vorschlag eine Anpassung und Aktualisierung der derzeitigen Bestimmungen an neue und vorhersehbare Entwicklungen bei Diensten und Technologien im Bereich der elektronischen Kommunikation vor.

Die meisten Bestimmungen der geltenden Richtlinie werden daher in den neuen Vorschlag übernommen und lediglich geringfügig überarbeitet.

Im Zusammenhang mit der 1999 erfolgten Überprüfung des Regulierungsrahmens für Dienste im Bereich der elektronischen Kommunikation wurde als Regulierungsgrundsatz unter anderem das Ziel formuliert technologieneutrale Vorschriften aufzustellen, die keine Technologie einseitig bevorzugen oder benachteiligen, die jedoch gewährleisten, dass gleiche Dienste in gleicher Weise reguliert werden, unabhängig von der Technologie, mit der sie erbracht werden.

Die vorgeschlagenen Änderungen betreffen Definitionen und Terminologie (z. B. als Bestätigung, dass die Richtlinie auch auf die Erbringung von E-Mail-Diensten anwendbar ist), Verkehrsdaten (Klarstellung, dass auch Internet-Verkehrsdaten miteingeschlossen sind), Standortdaten (Erlaubnis der Nutzung von Standortdaten für

---

22 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM(2000)385, 12. Juli 2000, ABl. C 365 E/223 vom 19.12.2000.

die Erbringung von Mehrwertdiensten mit Einwilligung der Nutzer), Verzeichnisse (freie Entscheidungsmöglichkeit der Nutzer über ihre Aufnahme in Telefon-, Mobilfunk- und E-Mail-Verzeichnisse), unerbetene Kommunikationen (Harmonisierung der nationalen Vorschriften durch vorgeschriebene vorherige Einwilligung der Adressaten von Marketingmitteilungen, die per E-Mail versendet werden) und die Wahrung der Privatsphäre durch die für elektronische Kommunikationsdienste eingesetzte Soft- und Hardware.

Die von der Artikel 29-Datenschutzgruppe abgegebenen Stellungnahmen[23] zu dem Richtlinienentwurf wurden berücksichtigt.

1.5.3 Technologien für einen besseren Schutz der Privatsphäre

Neben den im Rahmen des Programms IST eingeleiteten technischen Projekten im Bereich der Technologien für einen besseren Schutz der Privatsphäre (Privacy Enhancing Technologies – PET) beteiligte sich die Artikel 29-Datenschutzgruppe an der *e*Europe-Aktion zur Förderung von PET und von deren Anwendung, einschließlich geeigneter Verhaltensregeln und einer Angleichung der Praktiken. Mit dieser Aktion werden die bereits von der Gemeinsamen Forschungsstelle als Teil ihrer institutionellen Aufgaben durchgeführten Arbeiten weitergeführt. Im Rahmen der Aktion sind vor allem zwei Maßnahmen geplant.

Im Mittelpunkt der ersten Maßnahme steht die Veranstaltung von Themenworkshops unter Beteiligung aller Akteure:

- Ein Workshop unter dem Thema „The role of technology in facilitating on-line privacy“ (Die Rolle der Technologie beim besseren Schutz der Privatsphäre in Online-Diensten) (12. Mai 2000)
- Ein Workshop zum Thema „PET and privacy practice“ (PET und der Schutz der Privatsphäre in der Praxis) am 5. Juni 2001 (Veranstalter: EICTA)
- Ein Themenworkshop „Privacy and Identity in Information Society“ (Privatsphäre und Identität in der Informationsgesellschaft) (4./5. Oktober 2001)

Bei der zweiten Maßnahme geht es um den Aufbau und die Belebung des **e-Forum on Privacy in Information Society** (E-Forum für den Schutz der Privatsphäre in der Informationsgesellschaft) (eprivacy.jrc.it) als Portal für Aktivitäten zur Sensibilisierung für technische Belange, das zugleich den Erfahrungsaustausch und die Anwendung vorbildlicher Verfahren beim Einsatz von PET fördern soll.

- Eine Sitzung der ISTC-Arbeitsgruppe „T&C“ unter dem Motto „Biometry and PET“ (Biometrie und PET) (5. Juli 2001).

---

23 WP 29 5009/00) Stellungnahme 2/2000 zur allgemeinen Neugestaltung des Rechtsrahmens für den Telekommunikationssektor, angenommen am 3.2.2000.
WP 36 (5042/00) Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000 – KOM(2000)385 (siehe auch Teil I.3 – Überblick über die wichtigsten angenommenen Stellungnahmen und Empfehlungen).

1.5.4. Standardisierung

Die Initiative for Privacy Standardization in Europe (Initiative für die Standardisierung im Bereich des Schutzes der Privatsphäre) (IPSE) von CEN (Europäisches Komitee für Normung) / ISSS (Informationsgesellschafts-Standardisierungssystem) arbeitet an einem Bericht über die mögliche Rolle der Standardisierung bei der Unterstützung der Umsetzung der Richtlinie 95/46/EG. Hierfür erhielt die Initiative ein Mandat der Europäischen Kommission, die diese Arbeit aktiv unterstützt.

Für die Durchführung dieser Arbeit setzte das CEN eine Lenkungsgruppe ein, der Vertreter aller Beteiligten – Industrie (als Anbieter und als Endbenutzer von Lösungen), Verbraucher, Datenschutzbehörden, Normungsorganisationen usw. – angehören. Die Lenkungsgruppe wird von einem kleinen Sachverständigengremium unterstützt, das Berichtsentwürfe als Diskussionsgrundlage zur Annahme durch die Lenkungsgruppe erarbeitet.

Entsprechend dem von der Europäischen Kommission erteilten Mandat zur Untersuchung der Möglichkeiten und der Notwendigkeit der Standardisierung zur Unterstützung der Umsetzung der EU-Datenschutzrichtlinie veranstaltete das CEN am 23./24. März 2000 ein offenes Seminar unter dem Titel „Standardization - A business tool for Data Privacy“ (Standardisierung – Ein Business-Instrument für den Schutz der Privatsphäre im Datenbereich), bei dem neben Vertretern von Datenschutzbehörden auch Generaldirektor John F. Mogg von der Generaldirektion Binnenmarkt der Europäischen Kommission seine Ansicht über den Standardisierungsbedarf, insbesondere auf internationaler Ebene und auf dem Gebiet der PET erläuterte.

Zwecks Bestimmung konkreter Themenbereiche, die für Maßnahmen geeignet wären, setzte die „Initiative on Privacy in Standardisation in Europe“ (IPSE) eine Lenkungsgruppe ein, die 2000 dreimal zusammentrat. Weiter wurde die Einsetzung des CEN/ISSS-Projektteams beschlossen, das die Aufgabe hat, den Entwurf für den IPSE-Bericht zu erarbeiten. Daraufhin wurde eine offene Ausschreibung für Sachverständige auf dem Gebiet des Schutzes der Privatsphäre und des Datenschutzes durchgeführt (Frist war der 26. Mai 2000) und ein Projektteam gebildet. In der ersten Sitzung des Projektteams am 10./11. Oktober 2000 wurden Umfang, Gliederung und Inhalt des Berichts besprochen und ein erster Zeitplan vorgeschlagen.

Im Anschluss an die Sitzung legte die IPSE-Lenkungsgruppe den Erfassungsbereich des Berichts fest und benannte das Sachverständigenteam. Der erste Bericht des Sachverständigenteams wurde 2001 zur öffentlichen Anhörung vorgelegt[24].

[24] Draft IPSE Report from CEN/ISSS on Privacy Standardisation. http://www.cenorm.be/isss/Projects/DataProtection/IPSE/IPSE-ET%20DraftFinalReportv05.pdf.

1.5.5. Dritte Säule

Gemeinsame Geschäftsstelle

Am 17. Oktober 2000 nahm der Rat einen Beschluss zur Einrichtung einer Geschäftsstelle für die Gemeinsamen Kontrollinstanzen für Datenschutz, die mit dem Übereinkommen über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen), dem Übereinkommen über den Einsatz der Informationstechnologie im Zollbereich und dem Übereinkommen zur Durchführung des Übereinkommens von Schengen betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen (Schengener Durchführungsübereinkommen) geschaffen wurden, an[25] .

Mit diesem Beschluss wird eine gemeinsame unabhängige Geschäftsstelle für den Datenschutz eingesetzt, die bei der Wahrnehmung ihrer Aufgaben den vorgenannten Übereinkommen verpflichtet ist.

Eurodac

Am 11. Dezember 2000 nahm der Rat die Verordnung (EG) Nr. 2725/2000 über die Einrichtung von „Eurodac“ für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens[26] an.

Das Eurodac-System ermöglicht Mitgliedstaaten die Identifizierung von Asylbewerbern und Personen, die in Verbindung mit dem illegalen Überschreiten einer Außengrenze der Gemeinschaft aufgegriffen werden. Durch Vergleich der Fingerabdrücke können die Mitgliedstaaten feststellen, ob ein Asylbewerber oder Ausländer, der sich illegal in einem Mitgliedstaat aufhält, in einem anderen Mitgliedstaat Asyl beantragt hat.

Eurodac besteht aus einer bei der Kommission angesiedelten Zentraleinheit, die eine computergestützte zentrale Datenbank für Fingerabdruckdaten betreibt, und elektronischen Einrichtungen für die Datenübertragung zwischen den Mitgliedstaaten und der zentralen Datenbank. Neben den Fingerabdrücken enthalten die von den Mitgliedstaaten übermittelten Daten insbesondere Angaben zum Herkunftsmitgliedstaat, Ort und Datum des Asylantrags (soweit zutreffend), Geschlecht und Kennnummer. Daten werden von allen Personen über vierzehn Jahre erhoben, die Daten werden direkt in die Datenbank der Zentraleinheit oder des Herkunftsmitgliedstaats eingegeben. Im Fall von Asylbewerbern werden die Daten für zehn Jahre aufbewahrt, es sei denn, die betreffende Person hat die Staatsangehörigkeit eines Mitgliedstaats erworben. Daten von Ausländern, die in Verbindung mit dem illegalen Überschreiten einer Außengrenze eines Mitgliedstaats aufgegriffen werden, werden für zwei Jahre ab dem Zeitpunkt der Abnahme der Fingerabdrücke aufbewahrt, es sei denn dem Ausländer wird eine Aufenthaltsgenehmigung erteilt oder er hat das Hoheitsgebiet der Mitgliedstaaten verlassen.

---

25 ABl. L 271, 24.10.2000, S. 1 – 3.

26 ABl. L 316 , 15.12.2000, S. 1 – 10.

Fingerabdrücke von Ausländern, die sich illegal in einem Mitgliedstaat aufhalten, können mit Hilfe von Eurodac mit den Fingerabdrücken in der zentralen Datenbank verglichen werden, um festzustellen, ob die betreffende Person in einem anderen Mitgliedstaat einen Asylantrag gestellt hat. Fingerabdrücke, die zu Vergleichszwecken übermittelt wurden, werden nicht in Eurodac gespeichert.

Der Herkunftsmitgliedstaat ist verantwortlich für die Rechtmäßigkeit der Abnahme der Fingerabdrücke und für die Rechtmäßigkeit aller Verarbeitungsvorgänge im Zusammenhang mit der Verwendung, Übermittlung, Speicherung, Aufbewahrung und Löschung der Daten.

Ergänzend zu den nationalen Datenschutzbehörden wird eine unabhängige gemeinsame Kontrollstelle eingesetzt, die sich aus höchstens zwei Vertretern der nationalen Kontrollstellen der einzelnen Mitgliedstaaten zusammensetzt. Die gemeinsame Kontrollstelle hat die Aufgabe, die Tätigkeit der Zentraleinheit daraufhin zu kontrollieren, ob durch die Verarbeitung oder Nutzung der bei der Zentraleinheit vorhandenen Daten die Rechte der betroffenen Personen verletzt werden; darüber hinaus ist die gemeinsame Kontrollstelle zuständig für die Prüfung von Anwendungsfragen im Zusammenhang mit dem Betrieb von Eurodac. Die gemeinsame Kontrollstelle wird mit der Errichtung der unabhängigen Kontrollinstanz nach Artikel 286 Absatz 2 des Vertrags und der Verordnung Nr. 45/2001/EG[27] aufgelöst.

Europol

Am 27. März 2000 verabschiedete der Rat der Europäischen Union einen Beschluss zur Ermächtigung des Direktors von Europol, Verhandlungen über den Abschluss von Vereinbarungen mit Drittstaaten und Nicht-EU-Stellen aufzunehmen[28].

Diesem Beschluss zufolge darf der Direktor von Europol erst dann Verhandlungen über die Übermittlung personenbezogener Daten aufnehmen, wenn der Rat sich unter Berücksichtigung der Rechtsvorschriften und der Verwaltungspraxis des betreffenden Drittstaates oder der betreffenden Nicht-EU-Stelle im Bereich des Datenschutzes davon überzeugt hat, dass es für die Aufnahme solcher Verhandlungen keine Hindernisse gibt. Mit dem Beschluss wird der Direktor von Europol ermächtigt, Verhandlungen mit einer ersten Gruppe von Drittstaaten und Nicht-EU-Stellen aufzunehmen, der Bulgarien, Estland, Island, Kanada, Kolumbien, Lettland, Litauen, Malta, Marokko, Norwegen, Peru, Polen, Rumänien, die Russische Föderation, die Schweiz, die Slowakei, Slowenien, die Tschechische Republik, die Türkei, Ungarn, die Vereinigten Staaten von Amerika und Zypern sowie IKPO-Interpol, UNDCP (Drogenkontrollprogramm der Vereinten Nationen) und die Weltzollorganisation angehören.

Zusammen mit dem Beschluss wurden auch zwei Erklärungen des Rates im Amtsblatt veröffentlicht. Die erste Erklärung betrifft die Beziehungen zwischen Europol und

27 Siehe Kapitel 1.5.1 Datenschutz in Einrichtungen und Organen der Gemeinschaft.
28 ABl. C 106, 13.04.2000.

Drittstaaten und Nicht-EU-Stellen. Der Rat erklärt, dass er die Rechtsvorschriften und die Verwaltungspraxis der betreffenden Drittstaaten und Nicht-EU-Stellen im Bereich des Datenschutzes bei seiner Beschlussfassung über die Ermächtigung des Direktors von Europol, förmliche Verhandlungen über den Abschluss von Vereinbarungen betreffend die Übermittlung personenbezogener Daten durch Europol aufzunehmen, berücksichtigen wird. Damit er ordnungsgemäß prüfen kann, ob es für die Aufnahme solcher Verhandlungen Hindernisse gibt, ersucht der Rat Europol, Berichte über die Rechtsvorschriften und die Verwaltungspraxis dieser Drittstaaten und Nicht-EU-Stellen im Bereich des Datenschutzes auszuarbeiten und ihm vorzulegen. Der Rat ersucht die Kommission, die Erstellung dieser Berichte dadurch zu unterstützen, dass sie alle ihr vorliegenden relevanten Informationen zur Verfügung stellt.

Die zweite Erklärung betrifft die Drittstaaten und Nicht-EU-Stellen, denen Priorität einzuräumen ist, wobei der Rat festlegt, dass den Beitrittsländern, den Schengen-Kooperationspartnern (Island und Norwegen), der Schweiz und Interpol Priorität einzuräumen ist.

Eurojust

Der Europäische Gipfel von Nizza einigte sich am 9. Dezember 2000 über weitere Schritte in bezug auf Eurojust zur Verbesserung der justiziellen Zusammenarbeit in Strafsachen (siehe Artikel 31 des Vertrags von Nizza). Die Stelle soll mit Staatsanwälten, Richtern oder Polizeibeamten mit gleichwertigen Befugnissen besetzt werden, die von den Mitgliedstaaten entsprechend ihrem jeweiligen Rechtssystem entsandt werden.

2. EUROPARAT[29]

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

Der Beratende Ausschuss (T-PD) für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) nahm den Entwurf des Zusatzprotokolls zum Übereinkommen SEV Nr. 108 über die Tätigkeit von Kontrollorganen und internationale Datenströme am 8. Juni 2000 an. Der Text wurde daraufhin dem Ministerkomitee zur Annahme und zur Freigabe zur Unterzeichnung durch die Parteien des Übereinkommens vorgelegt.

Die Projektgruppe Datenschutz (CJ-PD) nahm am 13. Oktober 2000 den Entwurf für eine Empfehlung zum Schutz personenbezogener Daten, die für Versicherungszwecke erfasst und verarbeitet werden, sowie die entsprechende Begründung an. Beide Texte wurden dem Europäischen Ausschuss zur Zusammenarbeit in Rechtsfragen (CD-CJ) zur Genehmigung vorgelegt. Die Artikel 29-Datenschutzgruppe nahm eine Stellungnahme für den CD-CJ und den Sachverständigenausschuss für Fragen der Cyberkriminalität (PC-CY) zum Entwurf eines Übereinkommens über die

[29] http://stars.coe.fr/index_e.htm

Cyberkriminalität an. Der Bericht von Giovanni BUTTARELLI über Videoüberwachung wurde erörtert und über Folgemaßnahmen beraten.

Die Gemeinschaft, vertreten durch die Kommission, interveniert sowohl bei der CJ-PD als auch beim Beratenden Ausschuss (T-PD), 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 oben genannten Texten der Fall. Diese Zusammenarbeit mit dem Europarat soll die vollständige Übereinstimmung mit den Richtlinien der Gemeinschaft gewährleisten.

3. WICHTIGE ENTWICKLUNGEN IN DRITTLÄNDERN

3.1. Europäischer Wirtschaftsraum

3.1.1. Island

Die Richtlinie 95/46/EG wurde in Island im Jahr 2000 mit dem Gesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Nr. 77/2000 umgesetzt. Das Gesetz wurde am 23. Mai 2000 angenommen und trat am 1. Januar 2001 in Kraft. Mit diesem Gesetz, das ältere Rechtsvorschriften zu diesem Bereich ablöst, ist die Richtlinie in vollem Umfang umgesetzt. Das erste isländische Gesetz für die Verarbeitung personenbezogener Daten wurde 1981 verabschiedet. Das Gesetz Nr. 77/2000 sieht die Einsetzung einer neuen, unabhängigen staatlichen Datenschutzbehörde (Personuvernd) mit einem fünfköpfigen Vorstand vor, der derzeit von Prof. Pall Hreinsson geleitet wird. Entsprechend dem Gesetz übernahm Personuvernd die Aufgaben der vormaligen Datenschutzkommission, deren Mitglieder vom Justizministerium ernannt worden waren. Die Geschäfte der Personuvernd werden von einem Kommissar wahrgenommen, dessen Amtszeit auf vier Jahre festgesetzt ist. Zur ersten Kommissarin wurde am 18. Juli 2000 Sigrun Johannesdottir ernannt, deren Amtszeit am 1. August 2000 begann.

Verschiedene der im Laufe des Jahres 2000 in Island verabschiedeten Legislativmaßnahmen hatten auch Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz. Die wichtigsten diesbezüglichen Rechtsakte:

- Gesetz über die Teilnahme Islands an der Schengen-Zusammenarbeit Nr.15/2000 und Gesetz über das Schengener Informationssystem Nr. 16/2000. Entsprechend den geltenden Rechtsvorschriften überwacht Personuvernd die Anwendung des Informationssystems in Island, um zu gewährleisten, dass die Rechte der erfassten Personen geschützt werden.
- Gesetz über Haustürgeschäfte und Vertragsabschlüsse im Fernabsatz Nr. 46/2000. In Artikel 14 des Gesetzes sind die Rechte der Empfänger von Direktmarketingkommunikationen festgelegt, darunter das „Opt-out“-Recht durch Eintrag in ein öffentliches Verzeichnis.
- Gesetz über biologische Datenbanken (Biobanken) Nr. 110/2000. Mit dem Gesetz wird ein Rechtsrahmen für den Aufbau und den Betrieb von biologischen Datenbanken geschaffen, der u. a. Firmen und Einrichtungen betrifft, die vom Menschen gewonnene biologische Muster speichern. Gemäß dem Gesetz legt Personuvernd die Kriterien für den Schutz personenbezogener Daten und deren Verarbeitung fest, die von den Biobanken eingehalten werden müssen.

3.1.2. Norwegen

Die norwegische Datenschutzbehörde wurde 1980 eingesetzt und war bis zum 1. Januar 2001 beauftragt, die Anwendung des Gesetzes über personenbezogene Datenverzeichnisse von 1978 zu überwachen.

Mit dem 1. Januar 2001 trat das neue Gesetz über personenbezogene Daten (Gesetz vom 14. April 2000 Nr. 13 über die Verarbeitung personenbezogener Daten) in Kraft. Das Gesetz hat den Schutz natürlicher Personen vor der Verletzung ihres Rechtes auf Schutz der Privatsphäre durch die Verarbeitung personenbezogener Daten zum Inhalt. Das Gesetz soll gewährleisten, dass bei der Verarbeitung personenbezogener Daten das Grundrecht auf Achtung der Privatsphäre eingehalten wird.

Die norwegische Datenschutzbehörde, ein unabhängiges Verwaltungsorgan, ist seit dem 1. Januar 2001 dem Ministerium für Arbeit und staatliche Verwaltung unterstellt. Davor war die Behörde dem Justizministerium zugeordnet.

Mit dem Gesetz über personenbezogene Daten erhielt die Datenschutzbehörde neue Aufgaben.
Die Behörde ist nun nicht mehr mit Genehmigungsanträgen befasst, sondern sie überwacht die Einhaltung von Gesetzen und Verordnungen und stellt Informationen über den Schutz der Privatsphäre und die Datensicherheit bereit.

Das norwegische Datenschutzgesetz betont das Recht natürlicher Personen auf die Kontrolle der Verarbeitung der ihn betreffenden personenbezogenen Daten, indem es die weit reichende Anwendung der förmlichen Einwilligung des Betroffenen vorsieht. Aus diesem Grundsatz heraus ergeben sich auch Grundrechte für die Betroffenen, wie z. B. das Recht auf Zugang zu den sie betreffenden Informationen sowie Unterrichtung über die Datenverarbeitung und das Recht auf Berichtigung und Löschung unrichtiger Daten und unnötiger Informationen.

Die norwegische Datenschutzbehörde führte insgesamt 19 Kontrollen durch. Mit dem Gesetz wird vor allem auch die Absicht verfolgt, mehr Kontrollen durchzuführen. Dies erfordert allerdings auch größere Ressourcen und eine auf schnellere Ergebnisse ausgerichtete Organisation der Behörde.

Das Gesetz über personenbezogene Daten gibt der Berufungsstelle für den Schutz der Privatsphäre das Recht, über Berufungen gegen Entscheidungen der Datenschutzbehörde zu befinden. Die Berufungsstelle ist als unabhängiges Verwaltungsorgan dem König und dem Ministerium unterstellt und besteht aus sieben Mitgliedern. Bislang war die Stelle erst mit einer Berufung befasst.

Die Datenschutzbehörde legt größten Wert darauf sicherzustellen, dass sowohl der für die Verarbeitung der Daten Verantwortliche als auch der Verarbeiter durch eine planmäßige und systematische Vorgehensweise eine zufriedenstellende Sicherheit der Daten in bezug auf Geheimhaltung, Integrität und Zugänglichkeit bei der Verarbeitung personenbezogener Daten gewährleisten.

Der Faktor Öffentlichkeitsarbeit spielt bei der Aufklärung der Bevölkerung über ihre Rechte und Pflichten eine wichtige Rolle. Die Datenschutzbehörde setzt hierbei unter anderem auf Konferenzen, Pressemitteilungen und Informationen im Internet wie „FAQ“-Bereiche und Newsletters.

3.2. Beitrittsländer

Die intensivierte Heranführungsstrategie zielt bei allen Beitrittsländern darauf ab, diesen Ländern die Integration des gemeinschaftlichen Besitzstandes zu ermöglichen. In diesem Sinne liegt der Schwerpunkt zum einen auf der Annahme von Rechtsvorschriften, in diesem Fall der Richtlinie 95/46/EG, und zum anderen auf der Schaffung der für die wirksame Umsetzung des gemeinschaftlichen Besitzstandes erforderlichen Verwaltungsstrukturen, beispielsweise unabhängiger Datenschutzbehörden.

In einer Reihe von Beitrittsländern sind entsprechende Entwicklungen auf diesen Gebieten zu verzeichnen. In Lettland wurden im März, in der Tschechischen Republik im Juni und in Litauen im Juli neue allgemeine Rechtsvorschriften zur Übernahme des gemeinschaftlichen Besitzstands und insbesondere zur Umsetzung der Richtlinie 95/46/EG angenommen. Slowenien nahm eine spezifische Rechtsvorschrift für den Bereich der Gesundheitsdaten an. Die Konvention SEV Nr. 108 des Europarates wurde von Estland, Litauen, der Slowakei, der Tschechischen Republik und Lettland unterzeichnet und von der Slowakei ratifiziert.

3.3. Vereinigte Staaten von Amerika

Die Artikel 29-Datenschutzgruppe setzte sich mit den aus den Gesprächen zwischen der Europäischen Kommission und dem US-Handelsministerium im Februar, März, Mai, Juni und Juli hervorgegangenen Papieren auseinander.

Im Februar äußerte die Artikel 29-Datenschutzgruppe in einer Stellungnahme, dass bei einer begrenzten Zahl grundlegender Fragen noch einige letzte Schritte gesetzt werden könnten, bevor über die Angemessenheit befunden werden könne. Die noch offenen Fragen betrafen im Einzelnen die Wirksamkeit der vorgeschlagenen Durchsetzungsmechanismen und die Rolle der FTC auf diesem Gebiet sowie eine Aussprache über den Text der FAQ. Unabhängig hiervon sicherte die Artikel 29-Datenschutzgruppe ihre weitere Unterstützung für die Gespräche zu und begrüßte die in den von der US-Regierung vorgelegten Texten erreichten Verbesserungen.

In ihrer Sitzung im März nahm die Artikel 29-Datenschutzgruppe die Stellungnahme 3/2000 an; sie setzte ihre Erörterung über die Inhalte der Vereinbarung fort und sicherte der Europäischen Kommission ihre Unterstützung bei den Gesprächen mit den USA zu. In der Sitzung im Mai wurde eine weitere Stellungnahme diskutiert und angenommen (Stellungnahme 4/2000). Die Mitglieder der Artikel 29-Datenschutzgruppe gelangten zu dem Konsens, dass die Gruppe ungeachtet der weiterhin bestehenden Bedenken bezüglich des von der Vereinbarung gewährten Schutzniveaus der Tatsache Rechnung trägt, dass gewisse Kompromisse eingegangen werden mussten, um zu einer funktionierenden Vereinbarung zu gelangen. Darüber hinaus bestehe nach dessen Einführung immer die Möglichkeit zu prüfen, wie das System in der Praxis funktioniert.

In ihrer Sitzung im Juli prüfte die Artikel 29-Datenschutzgruppe die genaue Rechtsgrundlage für die Annahme der Vereinbarung zum „sicheren Hafen“ und

erörterte die in der Entschließung des Europäischen Parlaments zu dieser Frage geäußerten Vorbehalte. Im Oktober setzte sich die Artikel 29-Datenschutzgruppe mit den internen Arbeitsverfahren des Beirats der Datenschutzbehörden (Data Protection Authority Panel) auseinander, das als Durchsetzungsmechanismus für Organisationen im Bereich des „sicheren Hafens“ fungiert. Das Schlussdokument wurde in der Novembersitzung angenommen. Die Artikel 29-Datenschutzgruppe behielt sich allerdings ausdrücklich das Recht vor, zu einem späteren Zeitpunkt aufgrund der weiteren Erfahrungen auf die in ihren Stellungnahmen angesprochenen Themenbereiche zurückzukommen.

3.4. Andere Drittländer

3.4.1. Australien

Im Juni 2000 legte die Kommission der Artikel 29-Datenschutzgruppe eine Einreichung gegenüber der australischen Regierung bezüglich des Gesetzentwurfs über eine Änderung des Schutzes der Privatsphäre für den privaten Sektor (Privacy Amendment Private Sector Bill) 2000 vor, in der sie feststellte, dass das Gesetz in seiner derzeitigen Fassung als nicht angemessen gemäß der Richtlinie 95/46/EG bewertet werde. Als Reaktion hierauf ließ die australische Regierung einen Bericht erarbeiten, in dem 23 Empfehlungen zur Verbesserung des mit dem Gesetz gewährten Schutzes formuliert wurden.

Die Artikel 29 -Datenschutzgruppe diskutierte diesen Vorgang in ihrer Sitzung am 13. Juli 2000 und äußerte ihre Übereinstimmung mit der Kommission dahingehend, dass der Gesetzentwurf hinsichtlich des Schutzes des Rechts auf Achtung der Privatsphäre nicht weit genug gehe. Die Artikel 29-Datenschutzgruppe äußerte die Hoffnung, dass sie einen konstruktiven Beitrag zu den Gesprächen zwischen der Europäischen Kommission und der australischen Regierung über den Gesetzentwurf leisten könne. In ihrer Sitzung im Oktober 2000 beschloss die Gruppe, in naher Zukunft eine Stellungnahme zu dem Thema abzugeben.

3.4.2. Kanada

In der Sitzung im Mai 2000 wurde an die Mitglieder der Artikel 29-Datenschutzgruppe eine Kopie des kanadischen Gesetzes über den Schutz personenbezogener Daten und elektronischer Dokumente (Personal Information Protection and Electronic Documents Act), das in Kanada im Vormonat angenommen worden war, verteilt, damit die Mitglieder den Inhalt mit Blick auf die Annahme einer Stellungnahme zu dessen Angemessenheit prüfen konnten.

In ihrer Sitzung im Oktober 2000 diskutierten die Mitglieder nach erfolgter Prüfung der Rechtsvorschrift die Sachlage und gelangten zu der Auffassung, dass sensible Daten und öffentlich zugängliche Daten kritische Punkte darstellten. Die Artikel 29-Datenschutzgruppe einigte sich grundsätzlich darauf, in den darauffolgenden Monaten eine entsprechende Stellungnahme zu erarbeiten.

3.4.3. Jersey, Guernsey und Isle of Man

Nach Vorlage einer vorläufigen Analyse zu den genannten Gebieten im Februar und einem Schreiben der britischen Datenschutzbeauftragten übermittelte der Vorsitzende der Artikel 29-Datenschutzgruppe im November jeder der Datenschutzbehörden der als „Crown Dependencies“ bezeichneten Außengebiete ein Schreiben, in dem er um Klärung verschiedener problematischer Punkte ersuchte.

4. SONSTIGE ENTWICKLUNGEN AUF INTERNATIONALER EBENE

4.1 Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD)[30]

Die Arbeitsgruppe für Informationssicherheit und Privatsphäre (WPISP) der OECD setzt sich für eine international abgestimmte Vorgehensweise bei politischen Entscheidungen in den Bereichen Sicherheit und Schutz der Privatsphäre bzw. Schutz personenbezogener Daten ein, um zur Schaffung von Vertrauen in die globale Informationsgesellschaft und zur Erleichterung des elektronischen Geschäftsverkehrs beizutragen. Eine wichtige Voraussetzung für die Vertrauenswürdigkeit globaler Netze ist der wirksame Schutz personenbezogener Daten.

Der Aufforderung dieser Gruppe folgend wurde ein Bericht über vertragliche Vereinbarungen für die internationale Übermittlung personenbezogener Daten im weiteren Rahmen der Mechanismen zum Schutz der Privatsphäre in globalen Netzen für die Öffentlichkeit freigegeben. Auch der „Online Privacy Policy Statement Generator“ wurde freigegeben und auf der OECD-Website zugänglich gemacht. Hierbei handelt es sich um ein Online-Tool, das Webmaster und Administratoren bei der Generierung von Datenschutzhinweisen, die die Besucher einer Website über die Datenschutzmaßnahmen der betreffenden Organisation informieren, auf ihrer Website unterstützt. Gemeinsam mit der Haager Konferenz über internationales Privatrecht und der Internationalen Handelskammer veranstaltete die OECD eine Konferenz über alternative Möglichkeiten der Beilegung von Streitfällen im Online-Umfeld als ein erster Schritt zur Etablierung wirksamer Durchsetzungsmechanismen sowohl in bezug auf die Nichteinhaltung von Grundsätzen zum Schutz der Privatsphäre als auch zur Gewährleistung des Zugangs zu Rechtsmitteln.

[30] http://www.oecd.org/EN/home/0,,EN-home-0-nodirectorate-no-no-no-0,FF.html