# Sechster Jahresbericht

# über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Europäischen Union und in Drittländern

**Berichtsjahr 2001**

**Angenommen am 16. Dezember 2003**

**Inhalt**

# VORWORT VON STEFANO RODOTA, VORSITZENDER DER ARTIKEL 29DATENSCHUTZGRUPPE

Dieser Bericht über die Tätigkeit der Artikel-29-Datenschutzgruppe ist ein umfassender Beleg für die Komplexität der Fragen, die den Schutz personenbezogener Daten betreffen. Nicht allein, dass sich das Ausmaß der akuten Probleme vergrößert hat; auch alte Fragen stellen uns plötzlich vor neue Probleme. Ein flüchtiger Blick auf das Inhaltsverzeichnis zeigt, dass der Datenschutz inzwischen zu einem Spannungsfeld wurde, in dem Grundwerte demokratischer Gesellschaften miteinander im Widerstreit liegen.

Eine erste Folgerung, die sich aus dieser allgemeinen Feststellung ergibt, bezieht sich unmittelbar auf die Rolle und die Zuständigkeiten der Datenschutzgruppe. Artikel 8 der Charta der Grundrechte der Europäischen Union erkennt das Recht des Einzelnen auf Schutz seiner personenbezogenen Daten als eigenständiges Grundrecht an, dessen Wahrung zwingend von unabhängiger Stelle überwacht werden muss. Folglich wuchs der Datenschutzgruppe in noch stärkerem Maße die Aufgabe zu, diesen neuen Aspekt zu beleuchten, der die Freiheitsräume unserer Mitbürger berührt, und seine Beachtung einzufordern.

Das Jahr 2001 war entscheidend geprägt von den terroristischen Gewaltakten gegen die Vereinigten Staaten. Die Ereignisse gaben der alten Diskussion um die Frage eine neue Dimension, wie man der Notwendigkeit einer wirksamen Bekämpfung terroristischer Bedrohungen auf der einen Seite und der Notwendigkeit des Schutzes grundlegender Menschenrechte auf der anderen angemessen Rechnung tragen kann. Nach den Ereignissen des 11. September gab die Datenschutzgruppe eine Stellungnahme ab, in der sie die Notwendigkeit eines ausgewogenen Vorgehens bei der Terrorismusbekämpfung hervorhob. In diesem Zusammenhang unterstrich die Datenschutzgruppe die Selbstverpflichtung der demokratischen Gesellschaften in der EU, die Grundrechte des Einzelnen in erhöhtem Maße zu schützen, auch das Recht des Einzelnen auf Schutz seiner Privatsphäre bei der Erhebung und Verarbeitung personenbezogener Daten, so wie Artikel 8 der Charta der Grundrechte der Europäischen Union dies bestimmt. In ihrer Stellungnahme erinnerte die Datenschutzgruppe daran, dass Maßnahmen zur Terrorismusbekämpfung den Schutz durch die einschlägigen europäischen Vorschriften nicht aushöhlen dürfen und auch nicht aushöhlen müssen; diese Vorschriften umfassen die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und die Richtlinie 97/66/EG über den Schutz der Privatsphäre im Bereich der Telekommunikation. Insbesondere betonte die Datenschutzgruppe: „Maßnahmen gegen den Terrorismus dürfen und müssen das Ausmaß des Schutzes der Grundrechte nicht verringern, der für Demokratien typisch ist. Ein wichtiges Element des Kampfes gegen den Terrorismus ist, dass wir die grundlegenden Werte bewahren, auf denen unsere Demokratien basieren, denn genau diese Werte wollen diejenigen zerstören, die den Einsatz von Gewalt propagieren.“ Man kann ohne Übertreibung feststellen, dass der europäische Ansatz zum Schutz personenbezogener Daten seit Verabschiedung der betreffenden Rechtsvorschriften weltweit zur Bezugsgröße für alle wurde, denen der Schutz der Privatsphäre ein Anliegen ist.

Die Datenschutzgruppe hat aktiv darauf hingearbeitet, dass diese Diskussion geführt wird; dies hat im Übrigen dazu beigetragen, das Bewusstsein der Öffentlichkeit für Datenschutzfragen zu schärfen. Wie bereits in früheren Jahren befasste sich die Datenschutzgruppe mit einer breiten Palette von Fragen, u. a.:

- Bekämpfung der Computerkriminalität;
- Verarbeitung personenbezogener Daten im Zusammenhang mit Beschäftigungsverhältnissen;
- Ermittlung der Mindestanforderungen an die Online-Erhebung personenbezogener Daten;
- Umsetzung der Vereinbarung über den „sicheren Hafen“ (Safe Harbor Agreement);
- grenzüberschreitende Ströme personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden.

Unterstützt von der Kommissionsdienststelle, die die Sekretariatsgeschäfte wahrnimmt, hat die Datenschutzgruppe die Umsetzung der Datenschutzrichtlinie mit überwacht. Drei Jahre nach Ablauf der Frist für die Überführung der Richtlinie in innerstaatliches Recht wurde längst noch nicht alles getan, um die nationalen Rechtsvorschriften in vollem Umfang an die Erfordernisse der Richtlinie anzupassen und eine effizientere und einheitlichere Umsetzung sicherzustellen.

Wir leben in einer Zeit grundlegenden Wandels. Technische Entwicklungen greifen immer stärker in die Tätigkeitsfelder des Menschen ein. In den kommenden Jahren wird der Datenschutz zwangsläufig mit neuen Herausforderungen konfrontiert werden, da unsere zeitgenössische Gesellschaft versuchen wird, Wachstums- und Entwicklungsziele mit der Notwendigkeit in Einklang zu bringen, das Recht des Einzelnen auf Schutz seiner Privatsphäre zu wahren. Vor diesem neuen Hintergrund wird der Datenschutz zunehmend zum herausragenden Symbol für alte und neue Freiheitsrechte - zur unverzichtbaren Voraussetzung für die Weiterentwicklung der Bürgergesellschaft im neuen Jahrtausend.

Der Sechste Jahresbericht spiegelt das Engagement der Datenschutzgruppe für die Einhaltung der Datenschutzgrundsätze in einer Welt des raschen Wandels wider.

# EINFÜHRUNG

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten[1], im Folgenden als die Artikel-29-Datenschutzgruppe bezeichnet, legt ihren sechsten Jahresbericht für das Jahr 2001 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 wurde erstmals in Form einer zweibändigen Broschüre in publikumswirksamer Aufmachung veröffentlicht, wobei ein Teil die üblichen Informationen über die wichtigsten Entwicklungen in der Europäischen Union und in Drittländern enthielt, während in einem völlig neuen Teil die Mitglieder der Artikel-29-Datenschutzgruppe und deren Sekretariat seit ihrer Einsetzung bis zum

---

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 auch den Abschnitt „Aufgaben der Artikel-29-Datenschutzgruppe" in Kapitel 5.

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).

Jahr 2000 vorgestellt wurden. Darüber hinaus erläuterte dieser Teil den Auftrag der Artikel-29-Datenschutzgruppe und ihre Geschäftsordnung und vermittelte einen Überblick über die wichtigsten Themenbereiche ihrer Tätigkeit im Jahr 2000.

Der vorliegende sechste Bericht führt diese Tradition fort. Er wird allerdings nicht mehr in zwei separaten Bänden veröffentlicht, vielmehr wurden beide Teile in einem Band zusammengefasst. Im Jahr 2001 lagen die Tätigkeitsschwerpunkte der Artikel-29-Datenschutzgruppe auf dem Kampf gegen den Terrorismus, der Bekämpfung der Computerkriminalität, der Verarbeitung personenbezogener Daten im Zusammenhang mit Beschäftigungsverhältnissen und den Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union. Mit Bezug auf die Übermittlung personenbezogener Daten in Drittländer verfolgte die Artikel-29-Datenschutzgruppe die weitere Entwicklung auf dem Gebiet der Vereinbarung über den „sicheren Hafen" und prüfte die Angemessenheit der Datenschutzvorschriften Kanadas und Australiens. Daneben gab sie eine positive Stellungnahme zum Entwurf für einen Beschluss der Kommission über Standardvertragsklauseln ab. Auf dem Gebiet der Verhaltensregeln veröffentlichte die Artikel-29-Datenschutzgruppe ein Arbeitsdokument über die empfohlene Praktik 1774 der IATA. Die Zusammenfassung unter der nächsten Überschrift vermittelt einen Überblick über die wichtigsten Aspekte, mit denen sich die Artikel-29-Datenschutzgruppe im Zusammenhang mit den angesprochenen Themen befasste. Eine ausführliche Erläuterung der von der Artikel-29-Datenschutzgruppe vertretenen Standpunkte zu den einzelnen Themen enthält Kapitel 1.3.

Die Artikel-29-Datenschutzgruppe trat 2001 fünfmal zusammen und nahm 14 Dokumente an, die an die Kommission und den Ausschuss nach Artikel 31 und ggf. an den Vorsitzenden des Rates, den Präsidenten des Europäischen Parlaments und andere weitergeleitet wurden[5].

Das Sekretariat der Artikel-29-Datenschutzgruppe stellt die

*Europäische Kommission*
*Generaldirektion Binnenmarkt*
*Referat Datenschutz*[6]

**Die von der Artikel-29-Datenschutzgruppe angenommenen Papiere stehen auf dem Europa-Server der Europäischen Kommission zur Verfügung unter:**

http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_de.htm

**Allgemeine Informationen zum Datenschutz können über folgende Website abgerufen werden:**

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

---

5 Siehe auch den Abschnitt „ Im Jahr 2001 angenommene Dokumente und Verweis auf die Website" in Kapitel 5.

6 Siehe Website http://europa.eu.int/comm/internal_market/privacy/workingroup/secretariat_de.htm

# ÜBERBLICK ÜBER DIE WICHTIGSTEN ANGENOMMENEN STELLUNGNAHMEN UND EMPFEHLUNGEN DES JAHRES 2001

**Kampf gegen den Terrorismus**

Als Reaktion auf bestimmte Initiativen nach dem 11. September nahm die Artikel-29-Datenschutzgruppe im Dezember 2001 ein Stellungnahme zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus an, in der sie an die Verpflichtung unserer Demokratien erinnerte, die Einhaltung der Grundrechte und Freiheiten des Einzelnen sicherzustellen.

**Bekämpfung der Computerkriminalität**

Die Artikel-29-Datenschutzgruppe äußerte sich zum Entwurf einer Konvention des Europarats über Cyberkriminalität und zur Mitteilung der Kommission über die „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität". Sie unterstrich in ihrer Stellungnahme die Wichtigkeit der Achtung der Grundrechte in diesem Zusammenhang und warnte davor, dass die Bekämpfung der Computerkriminalität nicht Anlass dafür sein darf, umfassend Techniken zur Überwachung der Bürger einzuführen.

**Beschäftigung**

In ihrer Stellungnahme und Empfehlung des Jahres 2001 stellte die Datenschutzgruppe erste Leitlinien zu den Besonderheiten der Verarbeitung personenbezogener Daten im Kontext von Beschäftigungsverhältnissen auf und leistete damit einen Beitrag zu einer einheitlicheren Anwendung der Richtlinie auf diesem Gebiet. Die Datenschutzgruppe verweist auf die Wichtigkeit der Einhaltung der elementaren Datenschutzgrundsätze der Zweckbindung, Transparenz, Zulässigkeit, Verhältnismäßigkeit, sachlichen Richtigkeit und Sicherheit und der Sensibilisierung der Beschäftigten. In Bezug auf die Einwilligung der Betroffenen im Beschäftigungsverhältnis vertritt die Datenschutzgruppe die Auffassung, dass die Einwilligung nur in den Fällen in Anspruch genommen werden sollte, in denen der Beschäftigte eine echte Wahl hat.

**Mindestanforderungen für die Online-Erhebung personenbezogener Daten**

Als Reaktion auf die zunehmende Verarbeitung von Daten im Internet nahm die Datenschutzgruppe eine Empfehlung zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union an, in der sie die Auffassung vertritt, dass Mittel bereitgestellt werden sollten, die garantieren, dass die Internet-Nutzer alle Informationen erhalten, die sie benötigen, um in Kenntnis der Sachlage entscheiden zu können, ob die Websites, zu denen sie Verbindung aufnehmen, vertrauenswürdig sind.

## Übermittlungen in Drittländer

Die Datenschutzgruppe verfolgte die Entwicklungen in den Vereinigten Staaten genau und unterhielt regelmäßige Kontakte zu den mit der Umsetzung der Vereinbarung über den „sicheren Hafen“ befassten US-Behörden. Zum Datenschutzniveau des kanadischen Personal Information Protection and Electronic Documents Act gab die Datenschutzgruppe eine positive Stellungnahme ab. Bezüglich der australischen Datenschutzvorschriften für den privaten Sektor gelangte die Datenschutzgruppe zu der Auffassung, dass das Datenschutzniveau nur dann als angemessen betrachtet werden könnte, wenn angemessene Sicherheitsvorkehrungen getroffen würden, die den von ihr dargelegten Bedenken Rechnung tragen. Sie bestärkte die Kommission darin, die Frage weiter zu verfolgen und auf Verbesserungen bei der allgemeinen Anwendung hinzuwirken und die Datenschutzgruppe auf dem Laufenden zu halten. In Weiterführung ihrer Bemühungen um die Schaffung eines vertraglichen Rahmens für Übermittlungen in Drittländer erarbeitete die Datenschutzgruppe für die Kommission zwei Stellungnahmen als Grundlage für deren Entscheidungen über Standardvertragsklauseln[7].

## Verhaltensregeln

Die Datenschutzgruppe veröffentlichte ein Arbeitsdokument über die empfohlene Praktik 1774 der IATA zum Schutz der Privatsphäre und die Übermittlung personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden, in Drittländer.

---

7 2001/497/EG: Entscheidung der Kommission vom 15. Juni 2001 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer und

2002/16/EG: Entscheidung der Kommission vom 27. Dezember 2001 über Standardvertragsklauseln zur Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern nach der Richtlinie 95/46/EG.

# 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

Die Richtlinie wurde mit dem Datenschutzgesetz 2000 umgesetzt. Das „Bundesgesetz über den Schutz personenbezogener Daten“ (Datenschutzgesetz 2000, BGBl. I Nr. 165/1999) vom 17.08.1999 trat am 01.01.2000 in Kraft. Die im Jahr 2001 vorgenommene Gesetzesänderung (BGBl. I Nr. 136/2001) betraf allerdings lediglich den Wechsel der Landeswährung (Euro statt Schilling) in den Sanktionsbestimmungen.
http://www.bka.gv.at/service/publikationen/verfassung.pdf (englische Fassung)
http://www.bka.gv.at/datenschutz/dsg2000d.pdf (deutsche Fassung)

Bedingt durch die föderale Struktur Österreichs und die Aufteilung der Gesetzgebungsbefugnis auf Bund und Länder kann das Datenschutzgesetz 2000 die Richtlinie für den gesamten Bereich der automatisierte Datenverarbeitung und der manuellen Datenverarbeitung umsetzen, soweit diese Verarbeitungen für Zwecke erfolgen, die in die (in Österreich sehr weit reichende) Gesetzgebungskompetenz des Bundes fallen. Bislang sind sieben von neun Bundesländern ihrer Verpflichtung zur Umsetzung der Richtlinie nachgekommen und haben eigene Datenschutzgesetze erlassen.

#### - Belgien

Das Durchführungsgesetz trat am 1. September 2001 in Kraft (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.privacy.fgov.be/textes_normatifs.htm

Der königliche Erlass zur Durchführung des Gesetzes wurde am 13. Februar 2001 angenommen (Amtsblatt von 13. März 2001) und trat sechs Monate nach seiner Veröffentlichung in Kraft, also ebenfalls 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. Die englische Fassung des Gesetzes kann unter folgender Adresse abgerufen werden: http://www.datatilsynet.dk/eng/index.html.

Mit dem Gesetz wird die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umgesetzt.

## - 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 Informationstechnologie (523/1999) umgesetzt, das am 1. Juni 1999 in Kraft trat. 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.
(http://www.tietosuoja.fi/uploads/hopxtvf.HTM)

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

## - Frankreich

Das französische Parlament setzte die Prüfung des Gesetzentwurfs zur Änderung des Gesetzes Nr. 78-17 vom 6. Januar 1978 über Datenverarbeitung, Archive und Grundfreiheiten fort. Der von der Nationalversammlung am 30. Januar 2002 in erster Lesung angenommene Gesetzentwurf enthält keine wesentlichen Änderungen gegenüber den zentralen Vorgaben der Regierung, zu denen die CNIL konsultiert worden war. Mit dem Text werden zwei grundlegende Neuerungen gegenüber dem geltenden Recht eingeführt: Es legt fest, welche Kategorien der Datenverarbeitung im öffentlichen und privaten Sektor spezifische Risiken darstellen und daher einer Vorabkontrolle der CNIL unterliegen (Artikel 20 der Richtlinie), und es überträgt der CNIL die Vollmacht zur Verhängung von Disziplinarmaßnahmen. Die dem Senat 2002 zur Prüfung vorgelegte Textfassung kann eingesehen werden unter ***http://www.assemblee-nat.fr/dossiers/cnil.asp***

## - Deutschland

Bei der Modernisierung des deutschen Datenschutzrechts verfolgt die Bundesregierung einen zweistufigen Ansatz.

In der ersten Stufe ging es im Wesentlichen um die Umsetzung der Richtlinie. Am 14. Juni 2000 verabschiedete das Bundeskabinett einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG). Der Bundesrat gab am 29. September 2000 seine Stellungnahme zu dem Gesetzentwurf ab. Am 13. Oktober 2000 wurde der Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze vom Kabinett dem Bundestag vorgelegt (BT-Drs. 14/4329). Im Jahr 2000 wurden die Erörterungen in den verschiedenen Ausschüssen des Bundestags aufgenommen, an deren Ende das Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze verabschiedet wurde, das am 22. Mai 2001 in Kraft trat (Bundesgesetzblatt Bd. I, S. 904).

An diese Novellierung schließt sich die bereits in Angriff genommene zweite Stufe an, die eine grundlegende Reform des Datenschutzrechts zum Inhalt hat. Einen wichtigen Schritt hierzu bildete die Übergabe des Sachverständigenberichts zur Modernisierung des Datenschutzrechts vom 12. November 2001 an den Bundesinnenminister.
http://www.bfd.bund.de/information/bdsg_hinweis.html
Englische Fassung: http://www.bfd.bund.de/information/bdsg_eng.pdf

### - Griechenland

Das Datenschutzgesetz wurde mit dem Gesetz 2472 über den Schutz von natürlichen Personen bei der Verarbeitung personenbezogener Daten umgesetzt. Am 10. April 1997 wurde das Gesetz 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

Im Laufe des Jahres 2001 fanden mit der Einführung durch den Minister für Justiz, Gleichstellung und Rechtsreform im Dezember 2001 (http://www.dataprivacy.ie/6ai.htm) erste Schritte zu einer Umsetzung der Richtlinie statt. Mit den Verordnungen (die am 1. April 2002 in Kraft traten) werden einige Bestimmungen der Richtlinie umgesetzt – hauptsächlich diejenigen, die die Übermittlung personenbezogener Daten in Drittländer betreffen. Die Artikel 4, 17, 25 und 27 wurden in irisches Recht umgesetzt.

Mit der Veröffentlichung des Gesetzentwurfs zur Änderung des Datenschutzgesetzes im Jahr 2002 wurde ein wichtiger Schritt zur Umsetzung der Richtlinie in Irland getan (http://www.dataprivacy.ie/images/Act2003.pdf). Der Gesetzentwurf, der vom Parlament erörtert wurde, berücksichtigte neben den Anforderungen der Richtlinie eine Reihe zusätzlicher Fragen. Im Mai 2002 wurde die Gesetzesvorlage vom irischen Senat verabschiedet, durch die allgemeinen Wahlen im Mai 2002 und deren Folgewirkungen verzögerte sich ihre Annahme allerdings. Im April 2003 wurde dann das Gesetz beschlossen und trat am 1. Juli 2003 in Kraft.

### - Italien

Die wesentlichen Inhalte der Richtlinie 95/46/EG wurden mit dem Gesetz Nr. 675/1996, dem Datenschutzgesetz in der nachfolgend geänderten und ergänzten Fassung in italienisches Recht umgesetzt.
(http://www.garanteprivacy.it/garante/doc.jsp?ID=228213)

Im Jahr 2001 wurde mit der Gesetzesverordnung Nr. 467 vom 28.12.2001 die Ergänzung dieser Rechtsvorschrift gestattet, um eine noch bessere Übereinstimmung mit bestimmten Grundsätzen der Richtlinie zu erreichen und insbesondere die Anforderungen an und die Voraussetzungen für die Datenverarbeitung zu vereinfachen und zu straffen und zugleich auf der Grundlage der bei der Umsetzung des Datenschutzgesetzes gewonnenen Erfahrungen die Sicherheitsvorkehrungen zugunsten der Betroffenen zu verstärken.

So wurde mit § 12 Absatz 1 Buchstabe h zweiter Spiegelstrich des Datenschutzgesetzes die Anwendung des Grundsatzes der Interessenabwägung bei der Bestimmung von Fällen, in denen keine Einwilligung erforderlich ist (Artikel 7 Buchstabe f der EG-Richtlinie), eine gewisse Flexibilität bei der Beurteilung der Fälle herbeigeführt, in denen die Verarbeitung „gewöhnlicher“ personenbezogener Daten auch ohne die Einwilligung der betroffenen Person erfolgen darf. Es wird Aufgabe der Garante sein, entsprechende Fälle auf der Grundlage der in den maßgeblichen Rechtsvorschriften verankerten Grundsätze zu beurteilen und zu befinden, ob ein berechtigtes Interesse des für die Verarbeitung Verantwortlichen und/oder der Dritten, denen die Daten übermittelt werden, vorliegt und nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Damit wird der Grundsatz der Interessenabwägung zu einem zusätzlichen Kriterium dafür, ob die Verarbeitung von Daten zulässig ist.

In der Frage der Vorabkontrolle (gemäß Artikel 20 der EG-Richtlinie) ist hervorzuheben, dass nach Umsetzung der Mechanismen für die Vorabkontrolle die Verarbeitung von Daten, die möglicherweise spezifische Risiken für die Rechte und Freiheiten der Personen, auf welche sich die verarbeiteten Daten beziehen, beinhalten können, auch im Einklang mit den von der Garante festgelegten Auflagen erfolgen muss.

Mit der vorgenannten Verordnung wurde der Garante die Aufgabe übertragen – auch im Wege allgemein gültiger Bestimmungen – diejenigen Fälle zu ermitteln, in denen das neue Instrumentarium anzuwenden ist, und die Regelungen und Maßnahmen zu bestimmen, die zum Schutz der Betroffenen einzuhalten sind. Diese Vorgehensweise wird die Anwendung der maßgeblichen Bestimmungen vereinfachen.

Weitere mit der vorgenannten Verordnung eingebrachte Gesetzesänderungen betrafen die Meldevorschriften, die ebenfalls vereinfacht wurden. Unter Nutzung des von der Richtlinie gewährten Spielraums werden die derzeit geltenden Mechanismen, die eine generelle, für alle Fälle bis auf diejenigen, in denen Ausnahmen und/oder eine vereinfachte Meldung vorgesehen sind, geltende Meldepflicht vorsehen, durch ein System abgelöst, nach dem eine Meldung nur dann erforderlich ist, wenn die Verarbeitung entweder wegen der jeweiligen Regelungen oder der Art der verarbeiteten Daten negative Folgen für die Grundrechte und –freiheiten der betroffenen Person haben kann.

Eine weitere Vereinfachung betrifft die Angabe der Daten des Verarbeiters in den Informationen an die von der Verarbeitung Betroffenen, insbesondere dann, wenn ein einzelner für die Verarbeitung Verantwortlicher eine größere Zahl von Verarbeitern beauftragt hat.

In weiteren Bestimmungen der vorgenannten Verordnung wurden der Geltungsbereich der maßgeblichen Rechtsvorschriften sowie das geltende Recht genauer spezifiziert. Hierzu wurde vorgeschrieben, dass der Vertreter des für die Verarbeitung Verantwortlichen in Italien anzusprechen ist, wenn der besagte für die Verarbeitung Verantwortliche seinen Sitz außerhalb der EU hat und für die Verarbeitung ständig in Italien stationierte Systeme nutzt.

Besondere Schwerpunkte der Verordnung bilden die Annahme neuer Verhaltensregeln und Leitlinien für die berufliche Praxis, die sich als ein recht wirksames Instrument für die vollständige Umsetzung der Grundsätze des Datenschutzgesetzes (Nr. 675/1996) erwiesen haben, und die Empfehlungen des Europarats für verschiedene Wirtschaftszweige, die alle ausdrücklich angesprochen werden – so z. B. Kommunikationsdienstleistungen, die über elektronische Netze, insbesondere über das Internet, angeboten werden, Direktmarketing, der Umgang mit Arbeitgeber-Arbeitnehmerbeziehungen, kommerzielle Informationen, von privaten Kreditauskunfteien verwaltete Informationssysteme, automatisierte Bilderfassungsgeräte, die Verarbeitung von aus öffentlichen Archiven stammenden Daten. Auf diese Weise erhalten die betroffenen Wirtschaftszweige die Möglichkeit, einen aktiven Beitrag zur Einführung brauchbarer nichttypischer Rechtsquellen zu leisten, die bei der Beurteilung der Zulässigkeit und Billigkeit der Verarbeitung unter Einhaltung des Grundsatzes der angemessenen Darstellung herangezogen werden.

Mit der Verordnung Nr. 467/2001 wurde auch der im Gesetz Nr. 675/1996 vorgesehene Strafansatz durch Änderung der Art einiger weniger Sanktionen – insbesondere im Zusammenhang mit Formverstößen bei Meldeverfahren – geändert und in gewissem Umfang eine Anerkenntnis der „Reue“ eines für die Verarbeitung Verantwortlichen in Bezug auf Verstöße gegen die Bestimmungen über Mindestsicherheitsmaßnahmen ermöglicht.

Zugleich wurde die Strafverfolgungsfähigkeit in Bezug auf die Nichteinhaltung wichtiger Bestimmungen der Garante erweitert – ein Beispiel für die insgesamt größeren Befugnisse, die der Behörde – im Einklang mit der EU-Richtlinie bei der Überwachung von Verarbeitungsvorgängen übertragen wurden. Darüber hinaus stehen schwer wiegende Fälle von Falschaussagen oder falschen Mitteilungen gegenüber der Aufsichtsbehörde jetzt unter Strafandrohung.

## - Luxemburg

Der Gesetzentwurf 4735 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zur Umsetzung der Richtlinie 95/46/EG in luxemburgisches Recht wurde dem Parlament am 7. Dezember 2000 vorgelegt.

Im Verlauf des Jahres 2001 gingen vier Stellungnahmen zum Gesetzentwurf 4735 ein:

1) Stellungnahme des Verbands der Beamten und Angehörigen des öffentlichen Dienstes (*Chambre des Fonctionnaires et Employés Publics*)
(Eingang: 22.5.2001, Parlamentsakte 4735-1)

2) Stellungnahme des Verbands der Beschäftigten in der Privatwirtschaft (*Chambre des Employés Privés*)
(Eingang: 30.10.2001, Parlamentsakte 4735-4)

3) Stellungnahme der Arbeitskammer (*Chambre de Travail*)
(Eingang: 14.11.2001, Parlamentsakte 4735-3)

4) Stellungnahme der Handwerkskammer *(Chambre des Métiers)*
(Eingang: 22.11.2001, Parlamentsakte 4735-5)

## - Niederlande

Die Richtlinie 95/46/EG wurde mit dem Gesetz vom 6. Juli 2000 (http://www.cbpweb.nl/structuur/pag_wetten.htm)[8] in niederländisches Recht umgesetzt. Das Gesetz (*Wet bescherming persoonsgegevens; WBP)*, das das alte Datenschutzgesetz (*Wet persoonsregistraties; WPR*) vom 28. Dezember 1988 ablöst, trat am 1. September 2001 in Kraft. Gleichzeitig wurde eine Namensänderung der Datenschutzbehörde wirksam, die jetzt nicht mehr *Registratiekamer*, sondern *College bescherming persoonsgegevens* (*CBP*) heißt. Beim Übergang vom alten zu dem neuen Gesetz besteht ein hohes Maß an Kontinuität.

Seit dem 1. September 2001 gelten für sämtliche neuen Verarbeitungen die neuen Bestimmungen. Die einjährige Übergangsfrist für bereits bestehende Verarbeitungen endete am 1. September 2002.

## - Portugal

Die Richtlinie 95/46/EG wurde 1998 mit dem Datenschutzgesetz (Gesetz 67/98 vom 26. Oktober 1998) in nationales Recht umgesetzt.
http://www.cnpd.pt/Leis/lei_6798en.htm

## - Spanien

Im Jahr 2001 bestand keine Notwendigkeit für die Annahme neuer Vorschriften zur Umsetzung der Richtlinie, da – wie aus dem Vorjahresbericht ersichtlich – die Richtlinie 95/46/EG mit dem Inkrafttreten des Organgesetzes Nr. 15/1999 über den Schutz personenbezogener Daten in spanisches Recht umgesetzt wurde.
http://europa.eu.int/comm/internal_market/privacy/docs/organic-law-99.pdf

## - Schweden

Die EG-Richtlinie 95/46 wurde am 24. Oktober 1998 mit dem Inkrafttreten des Gesetzes über personenbezogene Daten (1998:204) am 24. Oktober 1998 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.

---

8 Wet van 6 juli 2000, Stb. 302, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). Eine nicht-amtliche englische Übersetzung des Gesetzes kann auf der Website der niederländischen Datenschutzbehörde, www.cbpweb.nl, abgerufen werden.

Für die gesamte manuelle Verarbeitung, die vor dem 24. Oktober 1998 aufgenommen wurde, gelten ab dem 1. Oktober 2007 die neuen Rechtsvorschriften.

#### - Vereinigtes Königreich

Das Vereinigte Königreich hat die Richtlinie 95/46/EG mit dem Datenschutzgesetz (Data Protection Act) 1998 umgesetzt.
(http://www.hmso.gov.uk/acts/acts1998/19980029.htm).
Der Information Commissioner ist als die unabhängige Datenschutzbehörde des Vereinigten Königreichs für die Durchsetzung beider Rechtsvorschriften verantwortlich. Darüber hinaus fungiert er als die vom Vereinigten Königreich bestellte Kontrollstelle für Europol, das Zollinformationssystem, das Schengener Informationssystem, Eurodac und Eurojust.

### 1.1.2. Vertragsverletzungsverfahren

Deutschland und Frankreich führten die Notifizierung 2001 durch, daher entschied die Kommission, die Klageanträge gegen diese beiden Mitgliedstaaten vor dem Europäischen Gerichtshof (C-2000/443 und C-2000/449) einzustellen. Im Fall Irlands wurde am 29.11.2001 beim Europäischen Gerichtshof Klage eingereicht (C-2001/459). Gegen Luxemburg erging am 4.10.2001 ein Urteil (C-450/00) wegen nicht erfolgter Mitteilung.

## 1.2. Richtlinie 97/66/EG

### 1.2.1. Umsetzung in nationales Recht

#### - Österreich

Die Richtlinie wurde mit dem Telekommunikationsgesetz (TKG), Bundesgesetzblatt I Nr. 100/1997, umgesetzt.

#### - Belgien

Die Richtlinie wurde – wie im 4. Jahresbericht dargestellt – in belgisches Recht umgesetzt.

#### - 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. 786 vom 19. September 2002) 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.

## - Frankreich

Die Verordnungen vom 25. Juli und 23. August 2002 haben die Umsetzung der Richtlinie 97/66/EG und der Richtlinie über den Fernabsatz in französisches Recht zum Inhalt. Diese Rechtstexte vervollständigen die geltenden rechtlichen Bestimmungen, welche die Mehrzahl der Forderungen der Richtlinien bereits erfüllten, durch die Verankerung der Forderung nach Einholung der vorherigen Einwilligung der von Direktvermarktung durch automatische Anrufsysteme oder Fax betroffenen Personen.

## - Deutschland

Telekommunikationsdatenschutzverordnung (TDSV) vom 18. Dezember 2000, in Kraft getreten am 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

Die Richtlinie wurde vom Minister für Unternehmungen der öffentlichen Hand im Wege der Telekommunikationsverordnungen (Datenschutz und Schutz der Privatsphäre) 2002 mit Wirkung vom 8. Mai 2002 in irisches Recht umgesetzt.

## - Italien

Die *EG-Richtlinie 97/66* wurde mit der Gesetzesverordnung Nr. 171/1998 über den Schutz der Privatsphäre im Bereich der Telekommunikation in nationales Recht umgesetzt.

Allerdings befand die Europäische Kommission den Umfang der Umsetzung nicht für ausreichend, insbesondere mit Blick auf Artikel 9 der Richtlinie, der die Ergreifung geeigneter Maßnahmen zur Aufhebung der Unterdrückung der Rufnummernanzeige des Anrufers bei Notrufen vorsieht, sowie im Hinblick auf alternative Zahlungsmodalitäten, weshalb sie gegen Italien ein Vertragsverletzungsverfahren einleitete. Das italienische Parlament sah sich daher zu einer Ergänzung der Verordnung Nr. 171/1998 durch spezifische Bestimmungen veranlasst, die auch Gegenstand der Verordnung Nr. 467/2001 sind.

Die Bestimmungen betreffen im Einzelnen Regelungen für die konkrete Bereitstellung alternativer Zahlungsmodalitäten, die die Anonymität der Nutzer sicherstellen, sowie die Pflicht für Betreiber von Telekommunikationsdiensten, die Öffentlichkeit angemessen über Rufnummernanzeigedienste zu unterrichten und zu gewährleisten, dass bei Notrufen die Unterdrückung der Rufnummernanzeige aufgehoben wird.

Allerdings ist darauf hinzuweisen, dass nach der Überarbeitung der Richtlinie 97/66/EG zum Zwecke der Anpassung ihrer Grundsätze an die technische Entwicklung im (Tele-)Kommunikationsbereich der neue Richtlinientext den bisherigen Text in vollem Umfang ersetzen wird.

## - Luxemburg

Zum Ende des Jahres 2001, auf das sich der vorliegende Bericht bezieht, hatte das Großherzogtum noch keine Gesetzesinitiative zur Umsetzung der Richtlinie 97/66 des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ergriffen.

Nachdem die Richtlinie 97/66/EG durch die Richtlinie 2002/58/EG abgelöst wird, hielt es die luxemburgische Regierung nicht für sinnvoll, eine Richtlinie umzusetzen, die ohnehin abgelöst wird.

Der dem Parlament am 11. Juli 2003 vorgelegte Gesetzentwurf 5181 sieht die Umsetzung der neuen Richtlinie 2002/58/EG vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vor, die die wichtigsten Grundsätze der Vorläuferrichtlinie 97/66/EG aufgreift, modifiziert und vervollständigt und zugleich an die Entwicklung der Märkte und Technologien der elektronischen Kommunikation anpasst.

## - Niederlande

Die maßgebliche Rechtsvorschrift mit sektorspezifischen Vorschriften zu diesem Bereich ist das Telekommunikationsgesetz *(Telecommunicatiewet; Tw)*[9] vom 19. Oktober 1998. Mit diesem Gesetz werden Teile der Richtlinie 97/66/EG in niederländisches Recht umgesetzt, die verbleibenden Aspekte werden im Zusammenhang mit der Umsetzung der Richtlinie 2002/58/EG zu berücksichtigen sein. Die CBP beriet die Regierung im Dezember 2002 zum Entwurf für eine Novelle des Telekommunikationsgesetzes.

## - 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.

---

[9] Wet van 19 oktober 1998, Stb. 610, houdende regels inzake de telecommunicatie (Telecommunicatiewet).

### - Spanien

Die Richtlinie 97/66/EG wurde mit dem Allgemeinen Telekommunikationsgesetz, 11/1998, und dem königlichen Erlass 1736/1998 vom 31. Juli 1998 zur Annahme von Titel III dieses Gesetzes umgesetzt.

### - 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, das am 24. Oktober 1998 in Kraft trat. Die Vertraulichkeit von Kommunikationen (Artikel 5 der Richtlinie) wird zusätzlich zu den Bestimmungen des Telekommunikationsgesetzes auch in Abschnitt 8 Kapitel 4 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 Richtlinie 97/66/EG wurde vom Vereinigten Königreich mit den Telekommunikationsverordnungen (Datenschutz und Schutz der Privatsphäre) von 1999 umgesetzt. Der Information Commissioner ist als die unabhängige Datenschutzbehörde des Vereinigten Königreichs für die Durchsetzung beider Rechtsvorschriften verantwortlich. Darüber hinaus fungiert er als die vom Vereinigten Königreich bestellte Kontrollstelle für Europol, das Zollinformationssystem, das Schengener Informationssystem, Eurodac und Eurojust.

## 1.2.2. Vertragsverletzungsverfahren

Im Januar 2001 erging ein Urteil gegen Frankreich wegen Nichteinhaltung der Notifizierungspflicht mit Ausnahme von Artikel 5. Die laufenden Verfahren (gegen Frankreich, Irland und das Vereinigte Königreich) wegen Nichtumsetzung der Richtlinie wurden auf der Grundlage der Bestimmungen von Artikel 5 der Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation abgeschlossen.

# 1.3. Von der Artikel-29-Datenschutzgruppe behandelte Themen

## 1.3.1. Übermittlung von Daten in Drittländer

### *1.3.1.1. USA: Die Grundsätze des „sicheren Hafens“*

Die Vereinbarung über die Grundsätze des sicheren Hafens trat am 1. November 2000 mit der Eröffnung des Online-Selbstzertifizierungsprozesses für US-Unternehmen, die bereit sind, sich der Vereinbarung über den sicheren Hafen anzuschließen, in Kraft.

Im Jahr 2001 nahm die Datenschutzgruppe keine Papiere zu diesem Thema an, verfolgte jedoch die Entwicklungen in den Vereinigten Staaten sehr genau und unterhielt regelmäßige Kontakte zu den mit der Umsetzung der Vereinbarung befassten US-Behörden.

### *1.3.1.2. Kanada*

Der kanadische Personal Information and Electronic Documents Act wurde am 13. April 2000 durch Royal Assent ausgefertigt. Das Gesetz gilt für privatwirtschaftliche Organisationen, die im Rahmen kommerzieller Tätigkeiten personenbezogene Daten erheben, verarbeiten oder weitergeben. Die Vorschriften zum Schutz der Privatsphäre in Anhang 1 des Gesetzes entsprechen dem Musterkodex für den Schutz personenbezogener Daten (Model Code for the Protection of Personal Information) der Canadian Standards Association (CSA), der 1996 als nationale Norm in Kanada anerkannt wurde.

In ihrer am 26. Januar 2001 angenommenen Stellungnahme 2/2001 zum Datenschutzniveau des kanadischen Personal Information and Electronic Documents Act (PIPEDA) verglich die Datenschutzgruppe die Bestimmungen des PIPEDA unter Berücksichtigung ihrer Stellungnahme zur Übermittlung personenbezogener Daten in Drittländer nach Artikel 25 und 26 der EU-Datenschutzrichtlinie mit den wichtigsten Bestimmungen der Richtlinie.

Im Lichte der von ihr angesprochenen Punkte wies die Datenschutzgruppe die Kommission und den Ausschuss nach Artikel 31 darauf hin, dass das Gesetz nur für privatwirtschaftliche Organisationen gilt, die personenbezogene Daten im Rahmen kommerzieller Tätigkeiten erheben. Zudem wird das Gesetz in drei Stufen in Kraft treten, so dass es erst 2004 vollständig umgesetzt sein wird.

Sie empfahl deshalb, bei einer Entscheidung darüber, ob der Personal Information and Electronic Documents Act einen angemessenen Schutz bietet, den begrenzten Anwendungsbereich und den Umsetzungszeitplan zu berücksichtigen.

Darüber hinaus forderte die Datenschutzgruppe die Kommission und den Ausschuss nach Artikel 31 auf zu ermitteln, wie der Begriff „weitgehend ähnlich“ definiert wird, und festzustellen, ob es sinnvoll ist, die Rechtsvorschriften der Provinzen einzeln dahingehend zu prüfen, ob sie ein angemessenes Schutzniveau gewährleisten, oder ob dasselbe Ziel über einen „Order in Council“ auf Bundesebene erreicht werden kann.

Die Datenschutzgruppe forderte die Kommission außerdem auf, die Entwicklungen bei den Gesundheitsdaten zu beobachten, und sie begrüßte sämtliche Initiativen, die auf schlüssige, in ganz Kanada geltende Vorschriften abzielen.

Schließlich begrüßte die Datenschutzgruppe auch sämtliche Bemühungen der kanadischen Behörden, die darauf ausgerichtet sind, für sensible Daten das höchstmögliche Datenschutzniveau zu gewährleisten und dafür zu sorgen, dass ein vergleichbares Schutzniveau besteht, wenn Daten von Kanada in ein anderes Land übermittelt werden.

#### *1.3.1.3. Australien*

Die Privacy Amendment (Private Sector) Bill 2000 wurde im Dezember 2000 vom australischen Parlament verabschiedet und durch Royal Assent ausgefertigt. Die neue Rechtsvorschrift enthält Ergänzungen gegenüber dem Commonwealth Privacy Act, der die Handhabung personenbezogener Daten durch privatwirtschaftliche Organisationen regelt. Sie trat im Dezember 2001 in Kraft.

In ihrer Stellungnahme 3/2001 zum Datenschutzniveau des australischen Privacy Amendment (Private Sector) Act 2000 verglich die Datenschutzgruppe dessen Bestimmungen unter Berücksichtigung ihrer Stellungnahme zur Übermittlung personenbezogener Daten in Drittländer nach Artikel 25 und 26 der EU-Datenschutzrichtlinie mit den wichtigsten Bestimmungen der Richtlinie.

Die Datenschutzgruppe begrüßte die Verabschiedung des Gesetzes und erkannte den innovativen Wert dieses Koregulierungssystems an, das die Kluft zwischen Gesetzgebung und Selbstregulierung dadurch zu überbrücken sucht, dass der Selbstregulierung Gesetzeskraft verliehen wird.

Die Datenschutzgruppe stellte allerdings mit Besorgnis fest, dass das Gesetz einige Sektoren und Tätigkeiten ausnimmt. Dies gilt besonders für Kleinunternehmen, Arbeitnehmerdaten, öffentlich zugängliche Daten sowie bestimmte Ausnahmen von materiellrechtlichen Datenschutzgrundsätzen aufgrund gesetzlicher Zulässigkeit. Darüber hinaus diskriminiert das Gesetz EU-Bürger insofern als es dem Datenschutzbeauftragten nur dann das Recht einräumt, eine Handlung oder Praktik zu untersuchen, wenn diese die Datenschutzbelange australischer Bürger oder von Personen, die dort ihren ständigen Wohnsitz haben, beeinträchtigt. Weitere Bedenken der Datenschutzgruppe betreffen die Regelung im Hinblick auf Direktmarketing, besonders schützenswerte Daten, Transparenz für die betroffenen Personen und die Übermittlung von Daten aus Australien in Drittländer.

Die Datenschutzgruppe gelangte zu dem Fazit, dass Datenübermittlungen nach Australien nur dann als zulässig betrachtet werden können, wenn angemessene Schutzvorkehrungen getroffen würden, die den dargelegten Anliegen Rechnung tragen. Sie bestärkte die Kommission darin, die Frage weiter zu verfolgen und auf Verbesserungen bei der allgemeinen Anwendung hinzuwirken.

## 1.3.2. Standardvertragsklauseln

***STELLUNGNAHMEN 1/2001 UND 7/2001 ZUM ENTWURF EINER ENTSCHEIDUNG DER KOMMISSION ÜBER STANDARDVERTRAGSKLAUSELN***

Im Jahr 2001 nahm die Europäische Kommission zwei Entscheidungen über Standardvertragsklauseln an: zum einen eine Entscheidung betreffend die Übermittlung personenbezogener Daten in Drittländer und zum anderen eine Entscheidung über die Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern. Die Artikel-29-Datenschutzgruppe leistete zu diesem Prozess – wie bereits im Jahr 2000 – einen beachtenswerten Beitrag.

So gaben mit der ersten Stellungnahme der Datenschutzgruppe im Jahr 2001[10] die nationalen Datenschutzbehörden grünes Licht für weitere Gespräche mit dem Ausschuss nach Artikel 31 mit Blick auf eine Annahme. Inhalt und Intention der Stellungnahme 1/2001 gehen insofern über die zu dem betreffenden Zeitpunkt zur Diskussion stehenden Möglichkeiten bzw. Fragen hinaus, als sich die Datenschutzgruppe in diesem wichtigen Papier mit Themen befasst, die für die weitere Entwicklung von Interesse sein könnten. Insbesondere geht es dabei um die Frage, ob die Kommission und die Mitgliedstaaten einen von Vertretern der Wirtschaft vorgelegten Mustervertrag berücksichtigen sollten.

Nachdem die Artikel-29-Datenschutzgruppe eine positive Stellungnahme abgegeben hatte, gelangte der Ausschuss nach Artikel 31 sehr rasch zu einer Einigung mit der Kommission, die daraufhin im Juni die erste Entscheidung hinsichtlich Standardvertragsklauseln (Auftragsverarbeiter)[11] annahm.

Noch vor Veröffentlichung der Entscheidung im Amtsblatt hatte die Kommission bereits einen ersten Entwurf für eine zweite Entscheidung der Kommission vorgelegt, in der es um die Übermittlung personenbezogener Daten an Datenverarbeiter ging. Die Arbeitsgruppe „Standardvertragsklauseln“ nahm daraufhin sofort wieder die Arbeit auf, so dass die Artikel-29-Datenschutzgruppe bereits im September 2001 eine zweite positive Stellungnahme[12] abgeben konnte. An diese rasche Reaktion der Datenschutzgruppe schloss sich vor Jahresende eine ebenfalls befürwortende Stellungnahme des Ausschusses nach Artikel 31 an. Als abschließendes Ergebnis dieser Bemühungen konnte die Kommission am 27. Dezember 2001 die zweite

---

10 Stellungnahme 1/2001 zum Entwurf der Kommission betreffend Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach Artikel 26 Absatz 4 der Richtlinie 95/46 (WP 38)

11 Entscheidung der Kommission 2001/497 vom 15. Juni 2001 nach der Richtlinie 95/46/EG – ABl. L 181/19 vom 4.7.2001

12 Stellungnahme 7/2001 zum Entwurf der Entscheidung der Kommission in der Fassung vom 31. August 2001 über die Standardvertragsklauseln zur Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern nach Artikel 26 Absatz 4 der Richtlinie 95/46 (WP 47)

Entscheidung über Standardvertragsklauseln[13] verabschieden, die den vertraglichen Rahmen vervollständigt.

Im September 2001 legte eine Gruppe von Wirtschaftsverbänden unter Federführung der Internationalen Handelskammer einen alternativen Mustervertrag vor, der alternative Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer enthielt. Erklärtes Ziel dieses Vorschlags war es, mit wirtschaftsfreundlicheren Mitteln ein gleichrangiges Datenschutzniveau zu erreichen. Die Kommissionsdienststellen äußerten sich informell zu diesem ersten Entwurf, was die Verfasser dazu veranlasste, eine überarbeitete Fassung vorzulegen, die von der Arbeitsgruppe Standardvertragsklauseln im Jahr 2002 eingehend erörtert werden sollte.

## 1.3.3. Internet und Telekommunikation

***EMPFEHLUNG 2/2001 ZU EINIGEN MINDESTANFORDERUNGEN FÜR DIE ONLINE-ERHEBUNG PERSONENBEZOGENER DATEN IN DER EUROPÄISCHEN UNION***

Im Mai 2001 nahm die Datenschutzgruppe eine Empfehlung zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union an. Die Empfehlung soll praktische Orientierungshilfen dafür geben, wie die in den Datenschutzrichtlinien festgeschriebenen Regeln auf die gängigsten Verarbeitungen im Internet anzuwenden sind. Die Datenschutzgruppe vertritt die Auffassung, dass Mittel bereitgestellt werden sollten, die garantieren, dass die Internet-Nutzer alle Informationen erhalten, die sie benötigen, um in Kenntnis der Sachlage entscheiden zu können, ob die Websites, zu denen sie Verbindung aufnehmen, vertrauenswürdig sind.

## 1.3.4. Verhaltensregeln

***ARBEITSDOKUMENT ÜBER DIE EMPFOHLENE PRAKTIK 1774 DER IATA***

1997 legte die IATA der Datenschutzgruppe das Dokument über die 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) – zur Genehmigung als Verhaltenskodex der Gemeinschaft gemäß Artikel 27 Absatz 3 der Richtlinie vor.

Auf ihrer 11. Sitzung am 10. September 1998 beschloss die Datenschutzgruppe, diesen Entwurf zu prüfen und setzte eine Arbeitsgruppe mit dem Mandat ein, die Stellungnahme der Datenschutzgruppe zur RP 1774 vorzubereiten.

Die Arbeitsgruppe prüfte diesen Entwurf, erörterte ihn mit der IATA und berichtete der Datenschutzgruppe. In der Folge legte die IATA überarbeitete Fassungen vor, die ebenfalls geprüft und erörtert wurden. Nachdem die IATA entschieden hatte, dass sie den Entwurf nicht weiter ändern konnte, weil er sonst von ihren Mitgliedern nicht

13 2002/16/EG: Entscheidung der Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG.

angenommen würde, wurde RP 1774 im Oktober 2000 auf der Passenger Services Conference der IATA angenommen.

In ihrem am 14. September 2001 angenommenen Arbeitsdokument über die Empfohlene Praktik 1774 – *Schutz der Privatsphäre und grenzüberschreitende Flüsse personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden* – gelangt die Datenschutzgruppe zu dem Schluss, dass das von der IATA vorgelegte Papier nicht die in Artikel 27 der Richtlinie geforderten Voraussetzungen erfüllt, aber dennoch als eine nützliche Grundlage dienen könne.

Kennzeichen einer Empfohlenen Praktik ist, dass sie nicht verbindlich ist und kein Mechanismus besteht, um ihre Einhaltung zu prüfen. Es muss klar sein, dass die Entschließungen und Empfohlenen Praktiken der IATA nicht vom IATA-Sekretariat auferlegt werden, sondern dass sie von den IATA-Mitgliedern auf dem demokratischen Forum der Konferenzen freiwillig angenommen werden. Eine Empfohlene Praktik ist in vielen Fällen nur ein Vorschlag für einen Rahmen, den die einzelnen Mitglieder ihren nationalen Bestimmungen und ihren eigenen Geschäftspraktiken anpassen können. RP 1774 ist nicht als endgültiger Verhaltenskodex anzusehen, der als solcher von den der IATA angeschlossenen Fluggesellschaften benutzt werden soll. Er soll vielmehr auf einige Hauptpunkte der Datenschutzrichtlinie eingehen und den einzelnen Mitgliedern (oder einer Gruppe von Mitgliedern) als Vorlage für die Erstellung eines Verhaltenskodex dienen, der den zuständigen Datenschutzbehörden unterbreitet werden soll.

Die Datenschutzgruppe begrüßte die Initiative der IATA und ihre Verpflichtung, gemeinsame Grundsätze für ihre Mitglieder festzulegen, um den Schutz des Grundrechts auf Privatsphäre der Fluggäste zu gewährleisten und zugleich weltweite Flüsse personenbezogener Daten zu ermöglichen. Die Empfohlene Praktik 1774 könnte als Grundlage für weitere Entwicklungen dienen und sollte – insbesondere im Hinblick auf Übermittlungen in Drittländer – dazu benutzt werden, IATA-Mitglieder in Drittländern aufzufordern, auf einen angemessenen Schutz hinzuarbeiten.

## 1.3.5. Beschäftigung

***STELLUNGNAHME 8/2001 ZUR VERARBEITUNG PERSONENBEZOGENER DATEN VON BESCHÄFTIGTEN***

Die Datenschutzgruppe nahm 2001 zwei Papiere zum Thema Datenschutz in Beschäftigungsverhältnissen an – zum einen eine Empfehlung hinsichtlich Beurteilungsdaten von Beschäftigten und zum anderen eine umfangreiche Stellungnahme zur Verarbeitung personenbezogener Daten von Beschäftigten.

Mit der Empfehlung leistete die Datenschutzgruppe gemäß ihrem Auftrag einen Beitrag zu einer einheitlicheren Anwendung der Maßnahmen, mit denen die Mitgliedstaaten die Richtlinie umgesetzt haben. Die Datenschutzgruppe verweist darin auf die Definition personenbezogener Daten in der Richtlinie, derzufolge der Begriff nicht nur aus objektiven Faktoren abgeleitete Informationen umfasst, sondern dass personenbezogene Daten unter bestimmten Umständen auch in subjektiven Wertungen und Beurteilungen zu finden sind.

Die Stellungnahme ist als Leitlinie zu den Besonderheiten der Verarbeitung personenbezogener Daten im Kontext von Beschäftigungsverhältnissen gedacht und soll zu einer einheitlicheren Anwendung der Richtlinie beitragen. In ihrem Papier verweist die Datenschutzgruppe auf die Wichtigkeit der Einhaltung der elementaren Datenschutzgrundsätze, deren sich Arbeitgeber bei der Verarbeitung personenbezogener Daten von Beschäftigten stets bewusst sein sollten.
Hierzu zählen die Grundsätze der Zweckbindung, Transparenz, Zulässigkeit, Verhältnismäßigkeit, sachlichen Richtigkeit und Sicherheit und der Sensibilisierung der Beschäftigten. In Bezug auf die Einwilligung der Betroffenen im Beschäftigungsverhältnis vertritt die Datenschutzgruppe die Auffassung, dass die Einwilligung nur in den Fällen in Anspruch genommen werden sollte, in denen der Beschäftigte eine echte Wahl hat.

## 1.3.6. Justiz und Inneres

***STELLUNGNAHME 10/2001 ZUR NOTWENDIGKEIT EINES AUSGEWOGENEN VORGEHENS IM KAMPF GEGEN DEN TERRORISMUS***

Als Reaktion auf bestimmte Initiativen nach dem 11. September nahm die Artikel-29-Datenschutzgruppe im Dezember 2001 eine Stellungnahme zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus an. Die Datenschutzgruppe erkennt darin an, dass der Kampf gegen den Terrorismus wirksam geführt werden muss, verweist in ihrer Stellungnahme allerdings auf bestimmte Bedingungen, die zu beachten sind. Sie erinnert an die Verpflichtung unserer Demokratien, die Einhaltung der Grundrechte und Freiheiten des Einzelnen (auch des Rechtes auf Schutz personenbezogener Daten) sicherzustellen, und hebt hervor, dass Maßnahmen gegen den Terrorismus das Ausmaß des Schutzes der Grundrechte nicht verringern dürfen und müssen. Ein wichtiges Element des Kampfes gegen den Terrorismus muss die Bewahrung der grundlegenden Werte sein, auf denen unsere Demokratien basieren, denn genau diese Werte wollen diejenigen zerstören, die den Einsatz von Gewalt propagieren.

***STELLUNGNAHME 9/2001 ZUR MITTEILUNG DER KOMMISSION ÜBER DIE „SCHAFFUNG EINER SICHEREREN INFORMATIONSGESELLSCHAFT DURCH VERBESSERUNG DER SICHERHEIT VON INFORMATIONSINFRASTRUKTUREN UND BEKÄMPFUNG DER COMPUTERKRIMINALITÄT“***

Im November 2001 nahm die Artikel-29-Datenschutzgruppe eine Stellungnahme zur Mitteilung der Kommission über die „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“ an. Die Datenschutzgruppe begrüßt darin grundsätzlich die Vorlage dieses Textes, hebt jedoch hervor, dass die Bekämpfung der Computerkriminalität nicht Anlass dafür sein darf, umfassend Techniken zur Überwachung der Bürger einzuführen, ohne zuvor die Alternativen zur Bekämpfung der Computerkriminalität eingehend zu prüfen. Sie vertritt die Auffassung, die Bedeutung einer wirksamen Prävention hätte stärker hervorgehoben werden können, anstatt repressiven Maßnahmen Vorrang einzuräumen und erinnert in diesem Zusammenhang an die Verpflichtungen, die sich aus den Datenschutzrichtlinien ergeben. Die Datenschutzgruppe verweist auch auf die

Wichtigkeit einer sachgerechten Definition des Begriffs der Computerkriminalität als Grundlage für verfahrensrechtliche Maßnahmen und hebt diesbezüglich hervor, dass bei Handlungen, die, wenn sie offline begangen würden, keine Eingriffsmaßnahmen rechtfertigen würden, solche Maßnahmen nicht allein deshalb ergriffen werden dürfen, weil Informations- und Kommunikationstechnologien benutzt wurden. Darüber hinaus fordert die Datenschutzgruppe eine Abgrenzung von Straftaten, die der Computerkriminalität zuzuordnen sind, gegenüber solchen Straftaten, die sich auf den Schutz der Privatsphäre und den Schutz personenbezogener Daten beziehen. Die Datenschutzgruppe betont, dass verfahrensrechtliche Maßnahmen so definiert werden müssen, dass die Achtung der Grundrechte und Grundfreiheiten der betroffenen Personen garantiert und insbesondere die Vereinbarkeit mit dem Rechtsrahmen für den Datenschutz gegeben ist. Abschließend macht die Datenschutzgruppe darauf aufmerksam, dass Verhaltenskodizes als Instrumente zur Verbrechensbekämpfung nur begrenzt geeignet sind.

***STELLUNGNAHME 4/2001 ZUM ENTWURF EINER KONVENTION DES EUROPARATS ÜBER CYBERKRIMINALITÄT***

Im März 2001 nahm die Datenschutzgruppe eine kritische Stellungnahme zum Entwurf für ein Übereinkommen des Europarats über Cyberkriminalität an, in der sie insbesondere hervorhob, dass mit der in dem Entwurf vorgesehenen Harmonisierung der Bestimmungen des materiellen Rechts und des Verfahrensrechts nicht zugleich eine Harmonisierung der Schutzbestimmungen verbunden ist. Zugleich kritisierte die Datenschutzgruppe die vage Formulierung bestimmter Artikel in dem Entwurf, die keine ausreichende Grundlage für Gesetze und zwingende Maßnahmen bietet, mit denen Grundrechte und –freiheiten ggf. rechtmäßig eingeschränkt werden sollen. Weiter betonte die Datenschutzgruppe, dass die meisten Bestimmungen des Übereinkommensentwurfs weit reichende Auswirkungen auf die Grundrechte haben und dass eine der Kernfragen in diesem Zusammenhang lautet, ob eine Maßnahme in einem bestimmten Fall notwendig ist, und wenn ja, ob sie angemessen und verhältnismäßig ist und nicht über das Notwendige hinausgeht. Einige der Elemente im Übereinkommensentwurf sind vollkommen neu, und die Datenschutzgruppe stellte in Frage, ob deren Wirkung auf die Grundrechte hinreichend geprüft wurde.

## 1.3.7. Verschiedenes

***STELLUNGNAHME 5/2001 ZUM SONDERBERICHT DES EUROPÄISCHEN BÜRGERBEAUFTRAGTEN AN DAS EUROPÄISCHE PARLAMENT***

Die Datenschutzgruppe wurde darauf hingewiesen, dass das Europäische Parlament die Frage des Zugangs der Öffentlichkeit zu Unterlagen und die Datenschutzfragen erörtern werde, die der Sonderbericht aufwirft, den der Europäische Bürgerbeauftragte dem Europäischen Parlament im Anschluss an den Empfehlungsentwurf an die Europäische Kommission in der Beschwerde 713/98/IJH vorgelegt hatte, und dass das Europäische Parlament aufgefordert worden war, diese Empfehlung als Entschließung zu verabschieden. Die Datenschutzgruppe vertrat die Auffassung, dass eine solche Entschließung beträchtliche Auswirkungen auf den Datenschutz bei der Verarbeitung personenbezogener Daten auf Gemeinschaftsebene haben könnte und hielt es daher für ihre Pflicht, eine Stellungnahme zu den wichtigsten rechtlichen Aspekten dieser datenschutzrechtlichen Frage abzugeben.

Die Datenschutzgruppe analysierte die für den Schutz der Privatsphäre relevanten Aspekte der Weitergabe der einer Verwaltungsbehörde oder anderen öffentlichen Stelle vorliegenden personenbezogener Daten. Dabei gelangte die Datenschutzgruppe unter anderem zu der Auffassung, dass das Recht der Öffentlichkeit auf Datenzugang und das Recht auf den Schutz personenbezogener Daten ihrer Art, ihrer Bedeutung und ihrem Stellenwert nach gleich sind und gemeinsam angewandt werden sollten, daher wird bei jedem Antrag eine Abwägung der Interessen vorgenommen werden müssen. Dies setzt eine Analyse der im jeweiligen Einzelfall bestehenden Rechte und Interessen unter Berücksichtigung aller Begleitumstände voraus, bei der bestimmt wird, ob die Weitergabe als eine Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise zu betrachten ist. Weiter darf sie nicht mit dem ursprünglichen Zweck ihrer Erhebung und Verarbeitung, für den die personenbezogenen Daten von der Verwaltungsbehörde oder anderen öffentlichen Stelle erhoben und weiterverarbeitet wurden, unvereinbar sein. Außerdem muss bei einer solchen Beurteilung festgestellt werden, ob die Verarbeitung als für die Erfüllung einer rechtlichen Verpflichtung, für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder den Dritten wahrgenommen wird, denen die Daten übermittelt werden, – sofern diese Interessen das Recht der betroffenen Person auf Datenschutz überwiegen – notwendig erachtet wird. Wenn das Recht der Öffentlichkeit auf Zugang zu Informationen als vorrangig eingestuft wird, sind personenbezogene Daten der Öffentlichkeit zugänglich zu machen. Wird der Datenschutz für wichtiger befunden, ist eine Freigabe der Daten abzulehnen.

### *BESCHLUSS 1/2001 ÜBER DIE TEILNAHME VON VERTRETERN DER KONTROLLSTELLEN IN DEN BEITRITTSLÄNDERN AN SITZUNGEN DER ARTIKEL-29-DATENSCHUTZGRUPPE*

Im Vorfeld der Erweiterung der Europäischen Union sieht die Strategie der Gemeinschaft unter anderem vor, die Beitrittsländer mit den Politiken und Verfahren der Union vertraut zu machen. Wie die Kommission betont hatte, liegt es im Interesse der Europäischen Union, die Beitrittsländer an den Verfahren zu beteiligen, in denen der Besitzstand entwickelt wird, um sicherzustellen, dass die Rechtsvorschriften in diesen Ländern wirksamer angewandt werden und um diese Länder mit den Gemeinschaftsverfahren vertraut zu machen.

Die Datenschutzgruppe schloss sich dem Standpunkt der Kommission an und traf daher Vorkehrungen, damit der Vorsitzende die Vertreter der Kontrollstellen der Beitrittsländer zur Teilnahme als Beobachter an den Sitzungen der Datenschutzgruppe einladen konnte.

# 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

## - Österreich

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Das österreichische E-Commerce-Gesetz auf der Grundlage der Richtlinie 2000/31/EG wurde 2001 verabschiedet (Bundesgesetzblatt I Nr. 152/2001).

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Im Jahr 2001 fand eine neuerliche Diskussion über die Notwendigkeit und die Vertretbarkeit von Gesetzen statt, die die Überwachung und Verknüpfung von Datenbanken zur Verbrechensprävention gestatten („Rasterfahndung“ und „Automationsunterstützter Datenabgleich“, § 149 Buchstabe i ff. Strafprozessordnung). Entsprechende Maßnahmen waren 1997 befristet erlaubt worden (Bundesgesetzblatt I Nr. 105/1997).

### *C. Wichtige Rechtsprechung*

1. Der Österreichische Verfassungsgerichtshof entschied am 16. März 2001 in der Sache G 94/00, dass sich das Recht auf Löschung personenbezogener Daten aus einer polizeilichen Datenbank, in der die Daten aller polizeilich bekannten verdächtigen Personen gespeichert werden, auf solche Fälle bezieht, in denen die verdächtige Person freigesprochen oder das Verfahren eingestellt wurde. Nur in besonderen Fällen kann die weitere Speicherung derartiger Daten mit der Notwendigkeit begründet werden, diese Informationen im Interesse der Verbrechensvorbeugung verfügbar zu halten.

2. Die wichtigsten Entscheidungen der Datenschutzkommission können online abgerufen werden unter http://www.ris.bka.gv.at/dsk/.

   Eine der Entscheidungen des Jahres 2001 der Datenschutzkommission stieß in der Öffentlichkeit auf breites Interesse: Nach längerer Diskussion über die Rechtmäßigkeit eines von den österreichischen Banken eingeführten Systems zur

Meldung säumiger Schuldner („Warnliste“) formulierte die Datenschutzbehörde in einer Empfehlung die Rahmenbedingungen für Führung der Warnliste. In der Folge ist die Erstattung der Meldung an das Datenverarbeitungsregister an die Einhaltung einer Reihe von Auflagen an die involvierten Kreditinstitute gebunden. Die Einhaltung der Auflagen ist durch Sanktionen abgesichert. (Bescheid K095.014/021-DSK/2001 vom 23. November 2001).

Die wichtigsten Auflagen:

- Gemäß dem Grundsatz der Datenverwendung nach Treu und Glauben besteht die Pflicht zur Information des Betroffenen anlässlich der Eintragung in die Warnliste.
- Die Eintragung von Daten in die Liste erfolgt ausschließlich aus den im Bescheid genau bezeichneten Anlässen.
- Vor Eintragung in die Warnliste hat der Auftraggeber den betroffenen Kunden ordnungsgemäß zu mahnen; falls innerhalb der gesetzten Zahlungsfrist eine vollständige Zahlung erfolgt oder eine andere Vereinbarung getroffen wird, ist die Eintragung in die Liste untersagt. Die vollständige Bezahlung der Forderung muss in der bestehenden Eintragung in der Warnliste unverzüglich ersichtlich gemacht werden.
- Der Auftraggeber hat zu veranlassen, dass eine begründete Bestreitung der Forderung in der Warnliste durch einen Bestreitungsvermerk unverzüglich ersichtlich gemacht wird.
- Eintragungen dürfen nur vorgenommen werden, wenn die Forderungen die Höhe von 1 000 EUR überschreiten.
- In folgenden Fällen müssen die Daten gelöscht werden:
    1. unverzüglich, wenn das Nichtbestehen der Forderung rechtskräftig festgestellt wurde;
    2. drei Jahre nach vollständiger Bezahlung der Schuld bzw. in allen anderen Fällen sieben Jahre nach Tilgung der Schuld.
- Es ist eine gemeinsame Schlichtungsstelle aller teilnehmenden Kreditinstitute einzusetzen.

3. Das neue Datenschutzgesetz 2000 enthält besondere Bestimmungen für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung und Statistik (§§ 46 und 47 DSG 2000). Insbesondere kann die Datenschutzkommission in Fällen, in denen die Einwilligung der betroffenen Personen nicht ohne unvertretbar hohe Kosten eingeholt werden kann, die Verwendung personenbezogener Daten für bestimmte wissenschaftliche Projekte genehmigen (§ 46 Absatz 3 DSG 2000). Diese Möglichkeit wurde verschiedentlich in Anspruch genommen, wobei es hauptsächlich um den Zugang zu Informationen für historische Nachforschungen ging, die für die Entschädigung von verschleppten Zwangsarbeitern des Zweiten Weltkriegs notwendig waren.

4. Nach dem neuen Datenschutzgesetz 2000 ist die Datenschutzkommission befugt, förmlich über Beschwerden bezüglich des Zugangsrechts gegen für die Verarbeitung Verantwortliche aus dem öffentlichen und dem privaten Sektor zu entscheiden. Der Datenschutzkommission wurden 2001 zahlreiche derartige Beschwerden vorgetragen, die sich meist gegen Direktmarketingunternehmen, Kreditauskunfteien und Banken richteten. In einer Reihe von Fällen waren auch

Telekom-Unternehmen betroffen, die vor Vertragsabschlüssen Kreditauskünfte einholen.

Die Datenschutzkommission kann auch bei gegen privatwirtschaftliche für die Verarbeitung Verantwortliche gerichteten Anträgen auf Berichtigung oder Löschung von Daten angerufen werden. Für eine amtliche und durchsetzbare Entscheidung in derartigen Fällen muss der für die Verarbeitung Verantwortliche allerdings gerichtlich verklagt werden.

### *D. Spezifische Themen*

Wie in vielen anderen Ländern, so bemüht man sich auch in Österreich darum, Behördendienste durch den Einsatz moderner Technologien für die Bürger leichter zugänglich zu machen. Da bei den meisten der so genannten E-Government-Anwendungen personenbezogene Daten involviert sind, stellen solche elektronischen Behördendienste immer auch ein Datenschutzproblem dar.

2001 wurde besonders die Problematik der Identifizierung von Bürgern, die elektronische Behördendienste in Anspruch nehmen, beleuchtet. An diesem Projekt beteiligte sich auch die Datenschutzkommission. Die nunmehr gefundene Lösung sieht vor, dass anstelle einer einzigen PIN mehrere Kennnummern für die Bürger generiert werden. Die Generierung erfolgt mit Hilfe von Verschlüsselungsverfahren automatisch durch eine Zentralstelle, dadurch wird ein Eindringen in die Privatsphäre durch die Verknüpfung von Daten erschwert.

In Kombination mit Chipkarten mit elektronischer Signaturfunktion, die von den Behörden bald landesweit an die Bürger ausgegeben werden sollen, wird dieses Identifizierungsverfahren bei allen künftigen E-Government-Anwendungen eine wichtige Rolle spielen.

### *E. Website*

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

Die Website steht in deutscher und englischer Sprache zur Verfügung.

## - 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 Cyberkriminalität** wurde am 3. Februar 2001 im belgischen Amtsblatt veröffentlicht. Das Gesetz sieht vor, dass Verkehrsdaten von Betreibern und Diensteanbietern im Telekommunikationsbereich grundsätzlich mindestens ein Jahr gespeichert werden sollen. Diese Bestimmung wurde entgegen der offiziellen Stellungnahme der belgischen Datenschutzbehörde aufgenommen.

Allerdings ist die Bestimmung noch nicht in Kraft getreten, da noch keine abgeleitete Rechtsvorschrift angenommen wurde, in der die Dauer der Speicherung genau festgelegt ist.

Der Datenschutzbehörde wurde ein Gesetzentwurf zur **Überwachung von Telekommunikationsdaten** vorgelegt. Dieser Text sieht die Einrichtung einer zentralen Überwachungsstelle und eine Vereinfachung der Voraussetzungen für den Zugang zu Verkehrsdaten im Zuge kriminalpolizeilicher Ermittlungen vor. Die Datenschutzbehörde forderte gegenüber dem Gesetzentwurf verstärkte Sicherheiten in Bezug auf die Voraussetzungen für den Zugang zu Verkehrsdaten ein und bestand zudem auf der Einhaltung der Grundsätze der Verhältnismäßigkeit und der Angemessenheit im Hinblick auf die Voraussetzungen für die Anforderung und den Charakter der angeforderten Daten (Stellungnahme 01/2001).

## *C. Wichtige Rechtsprechung*

Keine.

## *D. Spezifische Themen*

**E-Government**
Der im 5. Jahresbericht beschriebene Prozess zur elektronischen Weitergabe von Informationen innerhalb der Verwaltung oder zwischen Verwaltung und Allgemeinheit befindet sich weiterhin in der Entwicklung.

Die Datenschutzbehörde befasste sich insbesondere mit den Fragen, die die geplante Einführung eines elektronischen Personalausweises aufwirft. Im Jahr 2002 gab sie hierzu eine offizielle Stellungnahme ab (Nr. 19/2002), in welcher sie an erster Stelle auf die Notwendigkeit des Schutzes der elektronisch auf der neuen Ausweiskarte gespeicherten Daten, auf restriktive Voraussetzungen für den Zugang zu personenbezogenen Daten im landesweiten Melderegister und für die Verwendung der individuellen Kennnummer verwies.

**Medizinische Daten**
Die Datenschutzbehörde nahm eine offizielle Stellungnahme (Nr. 30/2001) zu einem Gesetzentwurf über Patientenrechte an. Mit Blick auf den Schutz der Privatsphäre sieht der Gesetzentwurf insbesondere ein Recht des Patienten auf Unterrichtung über seinen Gesundheitszustand, Voraussetzungen für den Zugang zu den medizinischen Unterlagen sowie Voraussetzungen für den Zugang der Eltern zu den medizinischen Unterlagen von Verstorbenen vor. Die Datenschutzbehörde sprach sich in erster Linie für ein ausgewogeneres Verhältnis zwischen der Ermessensfreiheit des Arztes und dem Rechtsanspruch des Patienten (oder seiner Eltern) in Bezug auf das Recht auf Informationen über den Inhalt von medizinischen Unterlagen aus.

Daneben setzt sich der Gesetzentwurf mit der Frage auseinander, welche medizinischen Daten im Rahmen des Abschlusses eines Versicherungsvertrags an Versicherungen weitergegeben werden dürfen. Die Datenschutzbehörde befürwortete die Vorlage, die Beschränkungen hinsichtlich der Anzahl der medizinischen Daten, die an Versicherungen weitergegeben werden dürfen, vorsieht.

**Urheberrecht und Schutz der Privatsphäre**
Die Datenschutzbehörde gab eine offizielle Stellungnahme (Nr. 44/2001) zu einem Fall ab, in dem es um die Verarbeitung von Telekommunikationsdaten durch die International Federation of the Phonographic Industry (IFPI) ging.

Die Datenschutzbehörde stand seit Februar 2001 in Kontakt mit Vertretern der IFPI in Belgien und der belgischen Schutzvereinigung für die Rechte von Schriftstellern und Komponisten (SABAM). Die Auseinandersetzung begann damit, dass die Musikindustrie in den Medien über die Methoden Auskunft gab, mit denen sie Personen ermittelt, die Musikdateien in Websites im Internet abspeichern.

Hierzu ließen sich IFPI-Mitarbeiter bei MP3-Musiksites registrieren und luden dann Musikdateien von belgischen Urhebern herunter. Während des Download-Vorgangs konnten sie die IP-Adresse der Person identifizieren, die die Musikdatei zum Download ins Netz gestellt hatte.

Anhand dieser Verbindungsdaten verschickte die IFPI im Wege einer Zusammenarbeit mit den Internet-Diensteanbietern, bei denen die Identifikationsdaten gespeichert waren, Warnungen an die so ermittelten Personen.

Die Datenschutzbehörde wies darauf hin, dass es sich bei IP-Adressen um personenbezogene Daten handelt und dass deren Erhebung und Verarbeitung gegen die Rechtsvorschriften zum Schutz der Privatsphäre und für den Telekommunikationsbereich verstößt. In ihrer Stellungnahme sprach sie auch die Rolle der Internet-Dienstleistungsanbieter in diesem Fall an. Eine systematische Zusammenarbeit und die Rolle als Versender von Warnungen könnten als Anmaßung der Funktion eines Erfüllungsgehilfen der Justiz gesehen werden, die ihre Befugnisse überschreite.

Die Datenschutzbehörde übermittelte ihren Standpunkt auch dem Justizministerium, das der Behörde Recht gab.

**Ahnenforschung im Internet**
Die Datenschutzbehörde erhält eine wachsende Zahl von Anfragen von Ahnenforschern, in denen es darum geht, welche Grundsätze bei der Veröffentlichung von oder der Suche nach genealogischen Datenbanken im Internet zu beachten sind.
Die Datenschutzbehörde stellte daher eine Broschüre mit Informationen über die Grundsätze des Rechts auf Schutz der Privatsphäre zusammen.
In der Broschüre wird auf die Anwendbarkeit des Rechts auf die Daten lebender Personen hingewiesen und mit Blick auf einen angemessenen Qualitätsstandard der gesamten Datenbank empfohlen, die (Mehrzahl der) Datenschutzgrundsätze auch auf die Daten Verstorbener anzuwenden.
Weiter enthält die Broschüre Angaben über im belgischen Datenschutzrecht vorgesehene besondere Pflichten in Bezug auf die Verarbeitung von Daten zu Zwecken der Geschichtsforschung. Unter anderem werden die Grundsätze der Information und der Genauigkeit erläutert und Maßnahmen zur Kontrolle und/oder Beschränkung des Zugangs zu den auf einer Website eingestellten genealogischen Informationen empfohlen.

**Allgemeine Wirtschafts- und Sozialerhebung**
Im Jahr 2001 wurde in Belgien eine allgemeine und verbindliche Volksbefragung durchgeführt, aufgrund derer bei der Datenschutzbehörde innerhalb einer Woche über 300 Beschwerden eingingen, die überwiegend den stark in die Privatsphäre eindringenden Charakter verschiedener Fragen des Fragebogens betrafen.

Die Datenschutzbehörde gab daraufhin auf eigene Initiative eine Stellungnahme ab, in der sie offiziell auf die für eine derartige Erhebung geltenden Datenschutzgrundsätze hinwies. Insbesondere verwies sie auf die Tatsache, dass die Erhebung den Datenschutzvorschriften unterliege, und betonte, dass es sich bei den erhobenen Daten um namentlich gekennzeichnete Daten handle. Die Datenschutzbehörde verwies auf die Pflicht zur Einhaltung strikter Voraussetzungen in Bezug auf sensible Daten (u. a. über Gesundheit und Sexualleben) und hob hervor, dass die betroffenen Personen verständliche und ausführliche Informationen erhalten müssten, dass die Erhebung auf angemessene Daten beschränkt werden müsse und dass für die Erhebung besondere Sicherheitsmaßnahmen ergriffen werden müssten.

In der Folge fanden weitere Gespräche zwischen der Datenschutzbehörde, dem nationalen statistischen Institut und dem Wirtschaftsministerium statt, die dazu führten, dass einzelne Bedingungen der Erhebung und Verarbeitung der Daten verbessert wurden. Die Datenschutzbehörden verfolgt die weitere Entwicklung in dieser Angelegenheit.

**Nationale Verbraucherkredit-Datenbank**
Im November 2000 hatte die Datenschutzbehörde eine Stellungnahme zu einem Gesetzentwurf angenommen, mit dem die Qualität der in die nationale Verbraucherkredit-Datenbank aufgenommenen Daten verbessert werden sollte. Als für die Verarbeitung verantwortliche Stelle für diese Datenbank fungiert die belgische Zentralbank. Das Gesetz wurde am 10. August 2001 angenommen und trat am 1. Juni 2003 in Kraft. Ab diesem Zeitpunkt wird die Datenbank nicht nur Kreditinformationen über Zahlungsverzug enthalten, sondern sämtliche Daten eines Verbraucherkreditvertrags.
Ende 2001 wurde ein Ad-hoc-Ausschuss eingesetzt, in dem die Datenschutzbehörde mit zwei Mitgliedern vertreten ist.

### *E. Website*

http://www.privacy.fgov.be

Die Website steht in französischer und niederländischer Sprache zur Verfügung.

## - Dänemark

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Nach Maßgabe von § 57 des Gesetzes über die Verarbeitung personenbezogener Daten muss bei der Ausarbeitung von Verordnungen, Runderlassen und ähnlichen allgemeinen Rechtsvorschriften, die für den Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung von Daten von Bedeutung sind, eine Stellungnahme der Datenschutzbehörde eingeholt werden. Diese Bestimmung gilt

auch für Gesetzentwürfe. Die Datenschutzbehörde gab Stellungnahmen zu verschiedenen Gesetzen und Verordnungen mit Auswirkungen auf die Privatsphäre und den Datenschutz ab.

Einer der interessantesten Fälle des Jahres 2001 betraf eine Gesetzesvorlage zum Grundbuchgesetz, mit der die Möglichkeiten für den Zugang zu elektronischen Grundbuch-Datensätzen über externe Datenstationen ausgeweitet werden sollten.

Die Datenschutzbehörde gelangte zu der Auffassung, dass die Gesetzesänderung datenschutzrechtlich unbedenklich sei, da die Grundbuchinformationen schon seit jeher öffentlich zugänglich sind und seit 1992 in elektronischer Form vorliegen. Bezüglich des Schutzes von Familiennamen vertrat die Datenschutzbehörde die Auffassung, dass diese Information generell nicht weitergegeben werden sollte.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Nach den Ereignissen vom 11. September wurden im Zuge des weltweiten Kampfes gegen den Terrorismus gewisse Änderungen der dänischen Rechtsvorschriften vorgenommen. Das Justizministerium brachte eine Gesetzesvorlage ein, die u. a. Änderungen des Strafrechts, des Justizverwaltungsgesetzes und des Ausweisungsgesetzes vorsah. Eine der wichtigsten Änderungen betraf Protokolldateien über Internet- und Telekommunikationsverkehrsdaten.

Die Datenschutzbehörde legte die datenschutzrechtlichen Bedenken im Hinblick auf den Gesetzentwurf dar und schlug die Aufnahme einer Revisionsklausel vor.

### *C. Wichtige Rechtsprechung*

Alle Fälle mit Bezug zum Gesetz über die Verarbeitung personenbezogener Daten wurden im Jahr 2001 von der Datenschutzbehörde verwaltungsrechtlich entschieden. In einem Fall, der einen schwer wiegenden Verstoß gegen die gesetzlich verankerten Vorschriften für Marketingpraktiken betraf, erstattete die Behörde Anzeige gegen den für die Verarbeitung Verantwortlichen. Dieser (ein Zeitungsverlag) akzeptierte ein Bußgeld in Höhe von 25 000 DKK (ca. 3 300 EUR).

### *D Spezifische Themen*

1. Im Jahr 2001 setzte sich die Datenschutzbehörde mit der **Problematik von Due-Diligence-Prüfungen** auseinander. Im Zusammenhang mit Verhandlungen über den Verkauf von Unternehmen oder Unternehmensteilen wird in der Regel eine so genannte „Due-Diligence-Prüfung“ vorgenommen. Im Kern geht es bei dieser Prüfung darum, dass der Berater des Kaufinteressenten, z. B. eine Anwaltskanzlei, Gelegenheit erhält, verschiedene Unterlagen über das Unternehmen zu prüfen, damit sich der Käufer ein – sowohl rechtlich als auch finanziell und betriebswirtschaftlich – möglichst umfassendes Bild des Unternehmens verschaffen kann.

Nach Auffassung der Datenschutzbehörde ist die Weitergabe von Daten des Verkäufers an die Berater des potenziellen Käufers als eine Verarbeitung personenbezogener Daten zu betrachten. Für die Weitergabe derartiger Daten sind

daher die Bestimmungen des Gesetzes über die Verarbeitung personenbezogener Daten maßgeblich.

Nach Ansicht der Datenschutzbehörde dürfen gewöhnliche, nicht sensible Daten, auch Daten, die im Rahmen einer Due-Diligence-Prüfung entsprechend dem Grundsatz der Interessenabwägung (Artikel 7 Buchstabe f) weitergegeben werden, in der Regel verarbeitet werden. Dies betrifft allgemeine Daten zur Identität, Gehaltsdaten, Daten über Ausbildung und Arbeitsbereich usw.
Im Hinblick auf diese Prüfung ist es nach Meinung der Datenschutzbehörde von Bedeutung, dass der Verkäufer und der potenzielle Käufer beide ein berechtigtes Interesse an der Verarbeitung haben und dass dieses den Interessen der betroffenen Person, insbesondere in Bezug auf den Charakter dieser Daten, nicht entgegensteht. In diesem Zusammenhang geht die Datenschutzbehörde auch davon aus, dass für die Weitergabe von Daten die Geheimhaltungspflicht gilt.

Aus Formgründen wies die Datenschutzbehörde gleichzeitig darauf hin, dass die Einwilligung der betroffenen Person die Grundlage für die Weitergabe bilden kann, vgl. Artikel 7 Buchstabe a der Richtlinie.

Die Datenschutzbehörde vertritt generell die Auffassung, dass die Weitergabe sensibler Daten nur mit Einwilligung der betroffenen Person erfolgen darf, vgl. Artikel 8 Absatz 2 Buchstabe a der Richtlinie.

In gleicher Weise muss für die Weitergabe von Strafregisterdaten, Daten über gravierende soziale Probleme und sonstige Daten rein privater Natur in der Regel die ausdrückliche Einwilligung der betroffenen Person eingeholt werden. Es sind allerdings Situationen denkbar, in denen die Weitergabe derartiger Daten ohne die Einwilligung der betroffenen Person erfolgen kann. Eine solche Entscheidung setzt eine konkrete Bewertung des Einzelfalls voraus.

Die Datenschutzbehörde empfiehlt auch, dass sensible Daten vor der Weitergabe soweit als möglich anonymisiert werden sollen und dass in Bezug auf die Weitergabe besondere Vorsichtsmaßnahmen angewandt werden sollen. In diesem Zusammenhang verweist die Datenschutzbehörde auf die Vorschrift nach Artikel 6 Absatz 1 Buchstabe c, der zufolge die verarbeiteten Daten den Zwecken entsprechen müssen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sein müssen und nicht darüber hinausgehen dürfen.
Naturgemäß spricht nichts gegen die Weitergabe anonymer Daten jedweder Art gegenüber einem potenziellen Käufer im Rahmen einer Due-Diligence-Prüfung.

Mit Blick auf Due-Diligence-Berichte äußerte sich die Datenschutzbehörde wie folgt: Nach Auffassung der Datenschutzbehörde gilt der übergeordnete Grundsatz, dass jede nachfolgende Verwendung des Berichts für andere Zwecke oder z. B. im Rahmen einer Weiterübertragung des Unternehmens an Dritte gegen die Bestimmungen von Artikel 6 Absatz 1 Buchstabe b verstoßen würde und auch als Verstoß gegen die Verarbeitungsvorschriften der Artikel 7 und 8 zu werten wäre.

2. Die Datenschutzbehörde gab im Jahr 2001 eine Stellungnahme zu einem Fall ab, in dem es um die **Weitergabe von Informationen über Gemeinderatsmitglieder durch eine Organisation** ging. Ein Gemeinderat hatte Beschwerde dagegen

eingelegt, dass auf einer Homepage ohne Einwilligung der Betroffenen Informationen über Gemeinderatsmitglieder veröffentlicht worden waren.

Die Homepage enthielt mit Bildern der Betroffenen versehene Angaben über Aufwandsentschädigungen und Reisekosten einiger Gemeinderatsmitglieder. An die Informationen war die Organisation gelangt, indem sie beim Gemeinderat Zugang zu Unterlagen beantragt hatte.

In ihrer Stellungnahme verwies die Datenschutzbehörde zunächst auf die Bedeutung von Abschnitt 2 Absatz 2 des dänischen Datenschutzgesetzes. Diesem Abschnitt zufolge ist das Gesetz dann nicht anzuwenden, wenn dadurch gegen das Recht auf Informations- und Meinungsfreiheit verstoßen wird, vgl. Artikel 10 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten.

Weiter vertrat die Datenschutzbehörde die Auffassung, dass es sich bei den auf der Homepage veröffentlichten Informationen nicht um sensible Daten handle. Ein Teil der Informationen war von den Gemeinderatsmitgliedern selbst veröffentlicht worden. Zudem hatte die Organisation nach Meinung der Datenschutzbehörde ein berechtigtes Interesse daran, die Informationen auf ihrer Homepage zu veröffentlichen, gegenüber welchem das Interesse der Gemeinderatsmitglieder nicht überwogen.

3. In einem weiteren Fall, mit dem sich die Datenschutzbehörde befasste, ging es um den **Zugang zum Schengener Informationssystem** (SIS). Ein Beschwerdeführer hatte sich an die Datenschutzbehörde gewandt, weil sich die nationale Polizeibehörde geweigert hatte, ihm darüber Auskunft zu geben, ob das SIS eine ihn betreffende Ausschreibung gemäß Artikel 95 und 98-100 des Schengener Durchführungsübereinkommens enthielt.

Die Datenschutzbehörde stellte fest, dass für den dargestellten Fall nach Maßgabe von Artikel 109 Absatz 1 des Schengener Durchführungsübereinkommens die Bestimmungen des dänischen Gesetzes über die Verarbeitung personenbezogener Daten anzuwenden seien.

Weiter gelangte die Datenschutzbehörde zu der Auffassung, dass auf diesen Fall, wenn in das SIS eine Ausschreibung für die betroffene Person aufgenommen worden war, § 30 Absatz 2 Ziffer 4 des dänischen Gesetzes über die Verarbeitung personenbezogener Daten anzuwenden sei. Gemäß diesem Paragraphen können Ausnahmen von § 28 Absatz 1 und § 29 Absatz 1 sowie § 30 siehe § 32 Absatz 1 auch dann geltend gemacht werden, wenn wichtige öffentliche Interessen gegenüber dem Interesse der betroffenen Personen an dieser Auskunft überwiegen, wozu insbesondere folgende Interessen zählen:
Vorbeugung, Untersuchung, Aufdeckung und Verfolgung von Straftaten oder von Verstößen gegen die ethischen Bestimmungen für reglementierte Berufe.

Die Datenschutzbehörde führte an, dass eine Auskunft gegenüber der betroffenen Person negative Folgen für den Zweck der Ausschreibung gemäß Artikel 109 Absatz 2 des Übereinkommens haben könnte.

Weiter vertrat sie die Auffassung, dass die betroffene Person, wenn das Schengener Informationssystem keine sie betreffende Ausschreibung enthielt, keinen Anspruch

auf diesbezügliche Informationen habe. Dies wurde damit begründet, dass bei einer entsprechenden Auskunft gegenüber der betroffenen Person Personen, die keine solche Auskunft erhielten, hieraus folgern könnten, dass das SIS eine sie betreffende Ausschreibung enthalte.

Daher bestätigte die Datenschutzbehörde die Rechtmäßigkeit der Ablehnung des Antrags auf Zugang zu SIS-Daten durch die Polizeibehörde.

4. Die Datenschutzbehörde befasste sich von sich aus mit einem Fall, in dem es um **Festplatten dänischer Firmen und Organisationen** ging**, die außerhalb Dänemarks entdeckt worden waren**, wobei die auf den Festplatten gespeicherten Daten nicht wirksam gelöscht worden waren.

Die Firmen hatten einem Unternehmen (Datenverarbeiter) die Löschung der ihm übergebenen Festplatten überlassen, und der Datenverarbeiter hatte sich vertraglich verpflichtet, die Festplatten vor dem Weiterverkauf wirksam zu löschen.

Die Datenschutzbehörde stellte hierzu fest, dass dieser Fall insofern einen Verstoß gegen das dänische Gesetz über die Verarbeitung personenbezogener Daten darstellte, als unbefugte Personen Zugang zu Daten erhalten hatten, da die Festplatten, auf denen die betreffenden Daten gespeichert waren, vor dem Weiterverkauf nicht wirksam gelöscht worden waren.

Hauptverantwortlicher für die unwirksame Löschung war der Datenverarbeiter. Die Datenschutzbehörde gelangte zu dem Schluss, dass der Verarbeiter sich nicht an die Vorgaben der Auftraggeber gehalten und damit gegen § 41 Absatz 1 des dänischen Datenschutzgesetzes verstoßen hatte. Außerdem hatte er durch das Außerachtlassen der notwendigen Sicherheitsmaßnahmen auch gegen § 41 Absatz 3 verstoßen. Die Datenschutzbehörde kritisierte dies als schweren Verstoß gegen das dänische Datenschutzgesetz.

Mit Blick auf die Pflichten der für die Verarbeitung Verantwortlichen stellte die Datenschutzbehörde fest, dass die Verantwortlichen in irgendeiner Weise die Löschung der Festplatten hätten kontrollieren müssen. Hierzu hätten beispielsweise Stichproben vorgenommen werden können – vgl. § 41 Absatz 1 des dänischen Datenschutzgesetzes.

## *E. Website*

Website der dänischen Datenschutzbehörde:

www.datatilsynet.dk

Die Website steht in dänischer und englischer Sprache zur Verfügung.

## - Finnland

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Neben dem Gesetz über personenbezogene Daten als *lex generalis* existieren in Finnland rund 650 Bestimmungen, die die Verarbeitung personenbezogener Daten regeln. Bei der Inkraftsetzung oder Änderung derartiger Bestimmungen muss der Datenschutzbeauftragte gehört werden. Im Jahr 2001 wurde der Datenschutzbeauftragte zu etwa 30 Gesetzesvorlagen der Regierung konsultiert. Außerdem wirkte ein Vertreter der Datenschutzbehörde entweder als Mitglied des zuständigen Ausschusses oder als Sonderberater an der Ausarbeitung einiger der wichtigsten Gesetzentwürfe mit.

Das wichtigste Gesetz des Jahres 2001 war unter Datenschutzaspekten vermutlich das **Gesetz über den Schutz der Privatsphäre bei der Arbeit** (477/2001), das am 1. Oktober 2001 in Kraft trat. Es handelt sich hierbei gegenüber dem zum Gesetz über personenbezogene Daten um ein *lex specialis*, das Bestimmungen über die Anforderungen hinsichtlich der Notwendigkeit personenbezogener Daten, die Erhebung personenbezogener Daten über Arbeitnehmer und Stellenbewerber und die Informationspflicht des Arbeitgebers, Persönlichkeits- und Eignungsbeurteilungen, genetische Tests, die Verarbeitung von Informationen über die Gesundheit von Arbeitnehmern, die zur technischen Überwachung und zur Kontrolle der Nutzung von Datennetzen verwendeten Methoden und die Verfügbarkeit des Datenschutzgesetzes am Arbeitsplatz enthält. Über die Einhaltung des Gesetzes wachen neben dem Datenschutzbeauftragten die für Sicherheit und Gesundheitsschutz bei der Arbeit zuständigen Behörden.

Als ein weiteres für den Schutz der Privatsphäre der Bürger wichtiges Gesetz ist das Gesetz (409/2001) über die **statistische Tätigkeit des finnischen Forschungs- und Entwicklungszentrums für Wohlfahrt und Gesundheit** (STAKES) zu nennen. Das Gesetz enthält spezifische Bestimmungen für die Erstellung von Verzeichnissen sowie über die Rechte von STAKES von rechts wegen bei für die Verarbeitung Verantwortlichen bzw. öffentlichen und privaten im sozialen Bereich tätigen Organisationen Daten über Sozialhilfeempfänger, in Betreuungseinrichtungen untergebrachte Personen und in Heimen und bei Pflegefamilien lebende Kinder zu erheben und in nationale Sozialregister zu integrieren. Voraussetzung für die Erhebung von Identifikationsnummern zur Identifizierung von Personen ist deren Notwendigkeit für die Erstellung der betreffenden Statistiken. Darüber hinaus enthält das Gesetz Bestimmungen über die Grundsätze für die Speicherung von Daten. Daten aus derartigen Verzeichnissen dürfen gegenüber Dritten nicht weitergegeben werden.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Ein vom Innenministerium eingesetzter Ausschuss legte einen Vorschlag für eine Änderung der Rechtsvorschriften für die polizeilichen Personendatenregister vor. Zur Vorbereitung eines Gesetzentwurfs wurden daraufhin Stellungnahmen verschiedener Fachgruppen und Interessengruppen eingeholt. In Finnland gelten die in der Datenschutzrichtlinie verankerten Grundsätze auch für die Verarbeitung von Daten zu Angelegenheiten im Bereich der zweiten und dritten Säule.

## *C. Wichtige Rechtsprechung*

Der terroristische Angriff vom 11. September in New York hatte auch in Finnland Konsequenzen: die Finanzaufsichtsbehörde veröffentlichte eine ihr vorliegende Liste von Terrorismusverdächtigen. Dieser Vorgang fand internationale Beachtung. Die Situation war auch mit Blick auf die Öffentlichkeitswirkung kritisch: Dient der Datenschutz auch dem Schutz von Terroristen? Die Datenschutzbehörde reagierte rasch und begründete ihre Auffassung, weshalb sie das Internet nicht für das geeignete Medium für die Veröffentlichung derartiger Daten hielt.

Zum Thema Videoüberwachung in Taxis entschied die Datenschutzbehörde aufgrund eines Antrags des finnischen Taxiverbands, dass für die Installation von Kameras in Taxis keine Sondererlaubnis erforderlich sei, da aus den Erklärungen des nationalen Beirats zur Verbrechensvorbeugung und sonstiger Sachverständiger hervorging, dass Kameras wesentlich zur Verbesserung der Sicherheit von Taxifahrern beitragen können. Diese Entscheidung unterstützt auch die Auslegung, der zufolge das Gesetz über personenbezogene Daten auch für Videokamerasysteme maßgeblich ist, bei denen die erfassten Bilder aufgezeichnet werden. Die Entscheidung bedeutete in diesem Fall also, dass personenbezogene Daten auf der Grundlage des besonderen Verhältnisses zwischen Fahrgast und Taxiunternehmer/-fahrer erhoben werden können und dass die bei der Kameraüberwachung aufgezeichneten Daten als bei diesem zugrunde liegenden Verhältnis notwendig erachtet werden. Der finnische Taxiverband gab später diesbezügliche Leitlinien für die Anwendung heraus, mit denen unter anderem sichergestellt werden soll, dass die Privatsphäre des Fahrgastes nicht unnötig beeinträchtigt wird.

## *D. Spezifische Themen*

In Finnland wurde für den öffentlichen Sektor ein vom Zentralen Einwohnerregister angebotener Zertifizierungsdienst für elektronische Ausweiskarten eingeführt. Allerdings sind die elektronischen Ausweiskarten bislang noch nicht sehr verbreitet, was unter anderem damit zusammenhängt, dass die Bereitschaft zur Online-Nutzung noch relativ gering ist. Dem finnischen Parlament liegt ein Vorschlag für ein Gesetz über elektronische Signaturen vor, mit dem die diesbezügliche EU-Richtlinie umgesetzt werden soll. Zu gegebener Zeit wird sich mit einem solchen Gesetz auf allgemeinerer Ebene feststellen lassen, für wie vertrauenswürdig die verschiedenen Parteien die elektronische Signatur befinden.

Mit dem Fortschreiten der Informationsgesellschaft ist die Gesellschaft in immer höherem Maße auf Datenverbindungen und –systeme angewiesen. Im öffentlichen Sektor ist man sich der Anfälligkeit der Informationstechnologie durchaus bewusst. Der vom Finanzministerium eingesetzte Lenkungsausschuss für Datensicherheit in der staatlichen Verwaltung, dem auch der Datenschutzbeauftragte angehört, legte Entwürfe für eine Reihe von Leitlinien und Berichten für verschiedene Akteure im Bereich des Risikomanagements vor. Daneben wurden weitere Projekte und Koordinierungsgruppen für die Überwachung und Förderung der Datensicherheit gebildet, die zum Teil die gleichen Zwecke verfolgen.

Die Weiterentwicklung der Informationstechnologie hat zudem verschiedene Bereiche und Behörden zur Intensivierung ihrer Zusammenarbeit veranlasst.

Kommunen suchen aus der Kommunikation auf regionaler Ebene Nutzen zu ziehen. Ein Thema ist auch die Zusammenarbeit zwischen verwandten Sektoren wie z. B. Sozial- und Gesundheitssektor. Im Zusammenhang mit derartigen Vorhaben treten nicht selten komplexe Fragen zum Datenschutz auf: Inwieweit ist die Weitergabe operativ wichtiger Daten an andere Organisationen zulässig? Da die Systeme der Kooperationspartner oder der Betreiber, die diese Systeme entwickeln, operativ oder technisch nicht für die unterschiedlichen Erfordernisse im Datentransfer angelegt sind, entstehen bei der Umsetzung von Entwicklungsvorhaben beträchtliche Risiken in Bezug auf den Datenschutz. Ein weiteres Problem besteht darin, dass diese Entwicklungsvorhaben nicht immer mit den Rechtsvorschriften im Einklang stehen. Es zählt zu den vordringlichen Aufgaben derjenigen, die Vorlagen für Rechtsvorschriften ausarbeiten, den Finger am Puls der Zeit zu behalten und den Gang der technologischen Entwicklung möglichst vorwegzunehmen. Aus Sicht des Datenschutzes besteht das Problem bei den verschiedenen Vorhaben nicht selten darin, dass sie aus der Perspektive der Betreiber und nicht der Betroffenen gesehen werden, wenngleich etwa in Bereichen wie dem Gesundheitswesen die Förderung des Schutzes der Privatsphäre durch den Einsatz von Technologie Ausgangspunkt der wichtigsten Pilotprojekte ist.

Generell werden die Instrumente, die das Gesetz über personenbezogene Daten bietet, um eine möglichst reibungslose Verwaltung und Verarbeitung von Daten zu erreichen, nicht voll genutzt. Hier sowohl auf nationaler als auch auf europäischer Ebene eine Besserung herbeizuführen, ist in der Tat eine Herausforderung an die Datenschutzbehörden.

Im Verlaufe des Jahres 2001 wurden für verschiedene Wirtschaftszweige sektorspezifische Verhaltensregeln erstellt, so unter anderem die überarbeiteten Leitlinien für den Datenschutz des finnischen Psychologenverbands, der vom Kirchenrat vorgelegte Entwurf für einen Verhaltenskodex für die gesamte kirchliche Verwaltung und der vom Verband der medizinischen Zentren ausgearbeitete Verhaltenskodex für private medizinische Zentren.

Bei den Projekten im Rahmen des Programms „Lernende Regionen“ sollen regionale Informationsnetze dazu genutzt werden, den Gemeinsinn unter den Bewohnern einer Region zu stärken, sie besser auf informationsintensive Tätigkeiten vorzubereiten und sie zu einer vermehrten Beteiligung zu bewegen; Untersuchungen zufolge ist dies gelungen. Für die Nutzung regionaler Informationsnetze wurde eine eigene innovative Anwendung entwickelt. Computerterminals wurden an Standorten aufgestellt, wo sie besonders gut zugänglich sind. Unter Datenschutzgesichtspunkten treten hierbei gewisse Probleme auf, etwa ob die Projektmitarbeiter den Schutz der Privatsphäre hinreichend berücksichtigen und die Nutzer angemessen aufklären, und ob die Nutzer sich ihrer Verantwortung bei der Nutzung der Informationssysteme bewusst sind.

### *E. Website*

http://www.tietosuoja.fi/
Die Website steht in finnischer und in englischer Sprache zur Verfügung.

## - Frankreich

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

**Gesundheit – Zugang von Patienten zu ihren Krankenakten**
Das Gesetz über Patientenrechte, zu dem die CNIL 2001 angehört wurde, wurde am 4. März 2002 angenommen. Es gewährt Patienten das Recht auf Zugang zu ihren Krankenakten, was Patienten bislang nur unter Einschaltung eines Arztes ihrer Wahl möglich war. Dieses Recht ist – etwa im Hinblick auf psychiatrische Erkrankungen – an bestimmte Voraussetzungen geknüpft ist, doch räumt es nun Minderjährigen das Recht ein zu bestimmen, dass ihre Eltern nicht über Notfallbehandlungen (z. B. Abtreibungen) unterrichtet werden; außerdem verankert es den in der Rechtsprechung immer wieder erklärten Rechtsanspruch berechtigter Personen auf Zugang zu den Krankenakten von Verstorbenen unter bestimmten Umständen. Und nicht zuletzt wird mit dem Gesetz die Genehmigungspflicht für Betreiber von Internetseiten zu Gesundheitsthemen eingeführt.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

**Elektronische Kommunikationen - Verbindungsdaten**
Nach Maßgabe des Gesetzes über die innere Sicherheit vom 15. November 2001 wurden für einen auf drei Jahre befristeten Zeitraum Regelungen für die zulässige Dauer der Speicherung von Internet-Verbindungsdaten für justizielle Zwecke verabschiedet. Zwar war das Gesetz erst nach den Ereignissen vom 11. September 2001 zur Abstimmung gelangt, doch hatte es über die fraglichen Regelungen – ebenso wie in den anderen Mitgliedstaaten– bereits zuvor weitreichende Diskussionen gegeben. Die Regelungen sehen vor, dass Daten über Internet-Verbindungen nicht länger als ein Jahr aufbewahrt werden dürfen und verweisen bezüglich der genauen Vorschriften über die Zeiträume, über die verschiedenen Arten von Daten (Internet-Verbindungsdaten, Daten über Aufenthaltsorte im Mobilfunkverkehr usw.), die aufbewahrt werden dürfen, auf eine nach Anhörung der CNIL zu erlassende Verordnung des Staatsrates. Der Entwurf für die Verordnung liegt der CNIL bislang nicht vor. In dem Gesetz ist ausdrücklich festgelegt, dass die aufbewahrten Daten keinesfalls dafür genutzt werden dürfen, Verbindungen eines bestimmten Internet-Nutzers zu ermitteln; allerdings kann die Polizei bei Vorliegen eines Straftatbestands Zugang zu den betreffenden Daten beantragen. In ihrer offiziellen Stellungnahme zu dem Entwurf hatte die CNIL befürwortet, die Aufbewahrungsfrist für Verbindungsdaten gesetzlich festzulegen, und hatte sich – entsprechend der Vorgaben der Artikel-29-Datenschutzgruppe – für einen Zeitraum von drei Monaten statt einem Jahr ausgesprochen.

### *C. Wichtige Rechtsprechung*

**Überwachung des Internetverkehrs von Mitarbeitern**
In einer Entscheidung vom 2. Oktober 2001 hatte die Sozialkammer des Kassationsgerichts ein Unternehmen schuldig gesprochen, das persönliche E-Mail-Mitteilungen eines Mitarbeiters überwacht hatte, die dieser an einem dem Unternehmen gehörenden Rechner gesendet oder empfangen hatte, obwohl die Beschäftigten des Unternehmens darüber unterrichtet worden waren, dass die Rechner nicht für persönliche Mitteilungen genutzt werden durften.

**Nicht erfolgte Löschung eines ehemaligen Mitglieds der Scientology Church Ile de France aus deren Datenbank**
Aufgrund der von der CNIL vorgelegten zwingenden Fakten (siehe 5. Jahresbericht der Datenschutzgruppe für das Jahr 2000) und der von der Pariser Staatsanwaltschaft im Jahr 2000 zusammengestellten justiziellen Unterlagen verhängte die Pariser Strafkammer in ihrem Urteil vom 17. Mai 2002 in dieser Sache eine Geldstrafe.

## *D. Spezifische Themen*

Generell erwies sich das Thema „Datenverarbeitung und Grundfreiheiten" auch in diesem Jahr in Frankreich als sehr aktuell. Das Volumen der von der CNIL behandelten Fälle und die Zahl der von ihr durchgeführten Diskussionen belegen das Interesse an diesem Thema und auch den erreichten „Reifegrad" im Hinblick auf die Berücksichtigung neuer Technologien.

Anhand einiger Zahlen lässt sich der aktuelle Stand zusammenfassen: pro Tag gingen durchschnittlich 160 Verarbeitungsmeldungen bezüglich personenbezogener Daten ein, die Zahl der Meldungen von durchgeführten Verarbeitungen bei Internet-Sites stieg um 20 % (7 400 im Jahr 2001 gegenüber 6 000 im Jahr davor). Die Zahl der Beschwerden und Beratungsanträge blieb 2002 nahezu unverändert (+2 %). Die Aufgliederung ergibt einen deutlichen Rückgang der Anträge auf Löschung aus Direktmarketingverzeichnissen (-34 %), während die Zahl der Anträge von natürlichen Personen auf Zugang zu und Prüfung der Archive, die bei der Polizei über sie geführt werden, zunahm und 1 400 Untersuchungen zur Folge hatte (+22 % im Jahr 2000, + 2% im Jahr 2002). Bei 25 % der überprüften Polizeiarchive konnten die Daten den Betroffenen übermittelt werden, und auf Antrag der CNIL wurden zahlreiche Berichtigungen vorgenommen. Was die Datei der im SIS ausgeschriebenen Personen betrifft, so ergab die 2001 durchgeführte Fünfjahresüberprüfung, dass von den 571 Ausschreibungen, zu denen Beschwerden vorlagen, auf Intervention der CNIL bei 25 % der Fälle unrichtige oder irreführende Personenbeschreibungen gelöscht wurden. Zu einem geringen Prozentsatz hiervon lagen Meldungen der französischen Behörden vor, die übrigen, zu denen Meldungen in anderen europäischen Ländern eingegangen waren, konnten durch die Zusammenarbeit mit CNIL-Partnerorganisationen in den betreffenden Mitgliedstaaten gelöscht werden.

**Was geschieht bei Unternehmenszusammenschlüssen mit den Kundendateien?**
Angesichts der zahlreichen Neuordnungen und Zusammenschlüsse von Unternehmen stellt sich die Frage, was hierbei mit den Kundendateien geschieht. In einer grundsätzlichen Stellungnahme stellte die CNIL fest, dass – ausgehend vom Grundsatz der Zweckbindung – eine aus rechtlich verschiedenen Körperschaften, von denen einige unter Umständen völlig unterschiedliche Tätigkeiten ausüben, bestehende Kapitalgruppe nicht allein aufgrund von Kapitalverflechtungen die Datenbanken verschiedener Kundenkreise unterschiedslos untereinander verbinden darf, ohne hierbei auf die Rechte der betroffenen Personen Rücksicht zu nehmen. Die Betroffenen sollten über derartige Vorhaben unterrichtet werden und die Möglichkeit haben, die Weitergabe ihrer Daten für andere Zwecke als die, für welche sie sie ursprünglich mitgeteilt hatten, und insbesondere für kommerzielle Zwecke, zu unterbinden.

**Internet**

Zwecks Beurteilung der Frage, welche Fortschritte bei Internet-Nutzern und –Hosts in Frankreich im Hinblick auf Datenschutzbelange seit 1996 zu verzeichnen sind, verweist die CNIL auf die beiden vorangegangenen Berichte der Datenschutzgruppe. Im Jahr 2001 konzentrierten sich die Aktivitäten der CNIL vorrangig auf die folgenden Gebiete:

*Internet und Minderjährige*. Die CNIL initiierte eine Reihe von Aktionen, mit denen Jugendliche und deren Kontaktpersonen sensibilisiert werden sollen. Außerdem wurden Informationen und Empfehlungen für Jugendbetreuer (über das Verbot, von Jugendlichen Daten über deren Familie und Bekannte zu erheben, und das Verbot, von Jugendlichen ohne Nachweis der Einwilligung ihrer Eltern sensible Daten zu erheben und diese an Dritte weiterzugeben) verbreitet, die „Junior"-Website der CNIL wurde aktualisiert und Informationen über diese Website an Schulen verteilt. Außerdem wurden Konferenzen für Lehrer, Jugendliche und Eltern veranstaltet, auf denen das Thema Datenschutz im Rahmen einer vom Ministerium für Jugend, Bildung und Forschung geförderten Initiative mit dem Titel „Internet, Jugendliche und personenbezogene Daten" als Beitrag zum Internet-Festival (*La fête de l'internet*) behandelt wurde.

*Gesundheits-Websites*. Auf der Grundlage der 2000 durchgeführten Studie und nach Absprache mit den Beteiligten gab die CNIL eine an die betreffenden Websites und Behörden gerichtete Empfehlung ab, die im Wesentlichen folgende Punkte enthielt: Einführung der Pflicht zur Einholung der Einwilligung der Betroffenen für die Speicherung ihrer Verbindungsdaten auf einer Website, mit der die Bewegungen von Surfern im Internet verfolgt werden, und Verbot der Weitergabe und Vermarktung von personenbezogenen Daten, die über eine Website erfasst wurden, an Dritte.

*Überwachung des Internet-Verkehrs von Mitarbeitern*. Nach einer 2000 durchgeführten umfassenden öffentlichen Anhörung zum Thema der Überwachung der Internet-Nutzung von Mitarbeitern stießen die Schlussfolgerungen und Empfehlungen der CNIL auf breites Interesse. Die CNIL gelangte zu dem Schluss, dass ein Verbot der Nutzung des Internet für private Zwecke nicht realisierbar ist. Ihrer Auffassung nach ist es gesellschaftlich akzeptiert, das Internet in vertretbarem Umfang für private Zwecke zu nutzen. Eine nachträgliche statistische und somit nicht individuelle Überwachung nach Absprache mit Arbeitnehmervertretern und angemessener Unterrichtung der Mitarbeiter müsste in aller Regel ausreichen. Mitteilungen offenkundig privater Natur dürfen vom Arbeitgeber nicht abgefangen werden. Systemadministratoren, deren Hauptaufgabe darin besteht, die Sicherheit des Netzes zu gewährleisten, sind an das Berufsgeheimnis gebunden und können nicht dazu verpflichtet werden, personenbezogene Daten weiterzugeben. Es sollte ein auf der Verfolgung (Tracing) der Aktivitäten der Mitarbeiter basierender Jahresbericht über Sicherheitsmaßnahmen erstellt und den Mitarbeitern zugänglich gemacht werden. Es sollte ein Datenschutzbeauftragter benannt werden, der in Verhandlungen zwischen Arbeitgeber und Arbeitnehmern die Interessen der Arbeitnehmer vertritt.

*Einstellen von gerichtlichen Entscheidungen in das Internet*. Gerichtliche Entscheidungen werden veröffentlicht, um die Unparteilichkeit der Justiz zu

gewährleisten. Die Verbreitung über das Internet veranschaulicht jedoch besonders gut, welche Vorsichtsmaßnahmen notwendig sind, wenn die moderne Technik das Maß an Transparenz möglich macht, das sich Demokratien als Schutz gegen mögliche Ungerechtigkeiten der Bürokratie so sehr wünschen. Der Stellungnahme der Datenschutzgruppe zu öffentlich zugänglichen Daten folgend rät die CNIL in ihrer in Frankreich zu diesem Thema vorgelegten Empfehlung dazu, alle Entscheidungen, die über eine Website öffentlich zugänglich gemacht werden, zu anonymisieren, damit die Beteiligten nicht über die rechtlich vorgeschriebenen Verfahren hinaus unter dem Vorwand, dass juristische Lehrmeinungen verbreitet werden müssten, ihr Leben lang auf Schritt und Tritt durch ihre Vergangenheit belastet werden. Diese Empfehlung wird von den Betroffenen nach und nach umgesetzt.

*Verbreitung von Mitgliederverzeichnissen französischer Freimaurerlogen*. Die Speicherung personenbezogener Daten, die direkt oder indirekt Aufschluss über die Überzeugungen – in diesem Fall die philosophischen Überzeugungen – von natürlichen Personen geben (Artikel 8 der Richtlinie, Artikel 31 des französischen Datenschutzgesetzes), ohne Einwilligung der Betroffenen in Computerspeichern ist verboten. Die CNIL wandte sich daher nachdem bei ihr eine diesbezügliche Beschwerde eingegangen war, an den Host-Betreiber der betreffenden Website, um die Rechte der betroffenen Personen zu schützen. Die Website wurde daraufhin sofort geschlossen, und die CNIL erhielt Auskunft zur Identität der für diesen Rechtsverstoß verantwortlichen Person. Die Pariser Staatsanwaltschaft leitete aufgrund der von der CNIL vorgelegten Angaben ein Verfahren ein. Nachdem der Fall in den Medien große Beachtung fand, wurden ähnliche Websites in Belgien und dem Vereinigten Königreich ebenfalls geschlossen.

**Biometrie**

In Anbetracht des gegenwärtigen Trends zu einem verstärkten Einsatz der Biometrie als Ersatz für computergestützte Geräte, die vergessen oder verlegt werden können, zu Identifizierungszwecken oder zur Kontrolle des Zugangs zu Software-Anwendungen entschloss sich die CNIL, als Grundlage für spätere Empfehlungen eine eingehende Untersuchung dieser Technologien durchzuführen. Aufgrund verschiedener Einzelfälle hatte sich die CNIL bereits in den Jahren zuvor veranlasst gesehen, Grundzüge für einen eigenen Standpunkt zu diesem Thema zu erarbeiten (siehe CNIL-Beitrag zum 5. Jahresbericht für das Jahr 2000). Aus Sicht der Praxis besteht der zentrale Aspekt darin, nach Kräften dafür zu sorgen, dass biometrische Identifikationssysteme nicht auf der Erstellung von Datenbanken basieren, die für andere, insbesondere polizeiliche Zwecke genutzt werden könnten. Systemen mit Abtastung der Iris oder der Handkontur ist daher gegenüber Systemen, die den Aufbau von Fingerabdruck-Datenbanken beinhalten, der Vorzug zu geben. Zur Authentifizierung der Nutzung einer Zugangskarte können Fingerabdrücke allerdings verwendet werden, wenn die Fingerabdrücke ausschließlich auf der Karte gespeichert sind. Fragen hinsichtlich der bürgerlichen und individuellen Grundfreiheiten wirft allein die Kombination der beiden Faktoren Fingerabdrücke und Erstellung einer Datenbank auf. Die CNIL vertritt daher den Standpunkt, dass Fingerabdrücke nur für justizielle Zwecke oder zur Kontrolle von Aktivitäten, die mit einem sehr hohen Risiko für die Gesellschaft verbunden sind, in Datenbanken gespeichert werden sollten.

**Aussagefähigere Daten über Gesundheitsaufwendungen (soziale Sicherheit)**

Durch die Umsetzung eines Gesetzes aus dem Jahr 1999 über die Finanzierung der sozialen Sicherheit ist ein landesweites System entstanden, das aussagefähigere Daten über Gesundheitsanwendungen liefern soll und in dem alle Daten zu ärztlichen Behandlungen, bezogenen Leistungen und nicht zuletzt Diagnosen aller für die soziale Sicherheit zuständigen Organe erfasst werden sollen. Die CNIL wirkte an der Aufstellung einer Reihe von Maßnahmen mit, die die Anonymität der Daten gewährleisten sollen. Name und Anschrift der Leistungsbezieher werden von den verschiedenen Organen nicht an die Datenbank übermittelt, außerdem veranlassen diese die unumkehrbare Verschlüsselung der Sozialversicherungsnummer der Versicherten. Beim Einlesen in die Datenbank werden die Daten nochmals mittels eines unumkehrbaren Algorithmus verschlüsselt, so dass Informationen zu Einzelpersonen immer wieder ergänzt werden können, ohne dass eine Rückverfolgung zur ursprünglichen Versicherungsnummer möglich ist. Nicht zuletzt besteht ein Verbot für bestimmte Querverweise auf der Grundlage von Variablen, die eine Identifizierung von Einzelpersonen ermöglichen könnten (insbesondere das Geburtsdatum in Verbindung mit dem Wohnbezirksschlüssel, dem detaillierten Leistungsschlüssel, Behandlungsterminen, Krankheitsschlüssel).

**Elektronische Behördendienste**
Im Kontext der in Frankreich stattfindenden Aktivitäten zur verstärkten Einführung elektronischer Behördendienste galt das besondere Augenmerk dem Datenschutz. Speziell zu diesem Thema enthält der Jahresbericht der CNIL eine Zusammenfassung der diesbezüglichen Stellungnahmen und Beiträge der CNIL (siehe Website der CNIL).

### *E. Website*

Die Website der CNIL (www.cnil.fr) wurde 2001 weiter verbessert, so wurde u. a. eine „Kinderecke“ (*Espace Junior*) aufgenommen, um bereits Kinder mit der Wahrnehmung ihrer Rechte vertraut zu machen. Die Website steht in französischer, spanischer und englischer Sprache zur Verfügung.

## - Deutschland

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Mit dem Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18. Mai 2001 (BGBl. I S. 904), geändert durch Artikel 3 des Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254), zuletzt geändert durch Artikel 21 des Gesetzes vom 3. Dezember 2001 (BGBl. I S. 3306) wurde das Bundesdatenschutzgesetz den Vorgaben der EU-Richtlinie 95/46/EG vom 24. Oktober 1995 angepasst. Die wichtigsten der darüber hinaus vorgenommenen Änderungen sind:

- Datenvermeidung und Datensparsamkeit (§ 3 a BDSG); damit werden Hersteller und verantwortliche Stellen verpflichtet, die Gestaltung und Auswahl von datenverarbeitenden Systemen an dem Ziel auszurichten, keine oder so wenig wie möglich personenbezogene Daten zu verarbeiten.

- Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung, § 6 b BDSG); sie ist nur begrenzt und für genau zu bestimmende Zwecke zulässig und muss transparent gemacht werden.

- Mobile personenbezogene Speicher- und Verarbeitungsmedien/Chipkarten (§ 6 c BDSG); bei mobilen Medien müssen die Verantwortlichkeiten in Bezug auf die einzelnen technisch verbundenen Verarbeitungen offen gelegt werden; der Betroffene wird vor verdeckter Verarbeitung geschützt und vor besonderen Risiken gewarnt.

- Datenschutzaudit (§ 9 a BDSG); es soll die Voraussetzungen dafür schaffen, dass der Datenschutz durch Marktprozesse dynamisiert wird.

### *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)

Mit diesem Gesetz wird der Entscheidung des Bundesverfassungsgerichts vom 14. Juli 1999 über die Zulässigkeit der strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes (BND) Rechnung getragen. Das Gericht hat diese Überwachung zum Teil für unzulässig erklärt; dabei hat es den Schutz des Fernmeldegeheimnisses bekräftigt und entschieden, dieser Schutz erstrecke sich auch auf den anschließenden Informations- und Kommunikationsprozess einschließlich der Weitergabe der Daten.

### *C. Wichtige Rechtsprechung*

Keine.

### *D. Spezifische Themen*

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-Mitgliedsstaaten.

Eine Forschungsgruppe der Universität Bonn konnte zeigen, dass nach dem alten (wohl auch nach dem neuen) Signaturgesetz zugelassene 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).

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.

### *E. Website*

Website des Bundesbeauftragten für den Datenschutz: www.datenschutz.bund.de oder www.bfd.bund.de
Die Website steht in deutscher, englischer und französischer Sprache zur Verfügung.

## - Griechenland

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Keine.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Im Jahr 2001 trat ein neues Gesetz (2928/2001) über die Änderung des Strafrechts zum Schutz der Bürger vor kriminellen Vereinigungen in Kraft. Im Vorfeld hatte das Justizministerium die griechische Datenschutzbehörde um Stellungnahme, insbesondere zur Frage der Erhebung und Verwendung von DNA-Proben der Beteiligung an strafbaren Handlungen verdächtiger Personen durch die Strafverfolgungsbehörden, gebeten. Die Datenschutzbehörde gab hierzu eine Stellungnahme (15/2001) ab. Die wichtigsten Ausführungen der Behörde wurden vom Gesetzgeber aufgegriffen und in das Gesetz aufgenommen.

Nach dem Gesetz

- dürfen DNA-Proben nur für in dem Gesetz konkret benannte strafbare Handlungen erhoben und verarbeitet werden;
- ist die Verwendung von DNA-Proben nur in solchen Fällen zulässig, in denen schwer wiegende Verdachtsmomente für eine Beteiligung an kriminellen Handlungen vorliegen, und nur unter Einhaltung der vom Gesetz vorgesehenen juristischen Sicherheiten;
- dürfen DNA-Proben nur für den für die Zweckerfüllung notwendigen Zeitraum aufbewahrt werden.

### *C. Wichtige Rechtsprechung*

Keine.

### *D. Spezifische Themen*

**Datenschutz am Arbeitsplatz**
Die Datenschutzbehörde gab eine Stellungnahme zum gesamten Themenkomplex des Datenschutzes am Arbeitsplatz und insbesondere zur Überwachung von Telefongesprächen und E-Mails der Beschäftigten ab.

**Einsatz der Biometrie**
Die Datenschutzbehörde nahm zwei Entscheidungen zum Einsatz der Biometrie an, in welchen sie auf die Grundsätze der Zweckbindung und der Angemessenheit Bezug nahm. Beide Fälle betrafen den Einsatz der Biometrie zur Kontrolle des Zugangs von Mitarbeitern zum Arbeitsplatz.

**Videoüberwachung**
Die Datenschutzbehörde gab eine Stellungnahme zur Videoüberwachung öffentlicher Plätze ab, in der sie zwischen Videoüberwachung mit Speicherung personenbezogener Daten und Videoüberwachung ohne Speicherung personenbezogener Daten unterschied. Im ersteren Fall ist der für die Verarbeitung Verantwortliche verpflichtet, das System bei der Datenschutzbehörde zu melden.

**Zuständigkeit der Datenschutzbehörde**
Aufgrund der wachsenden Zahl an sie gerichteter Anfragen bezüglich der Verwendung personenbezogener Daten vor Gericht sah sich die Datenschutzbehörde veranlasst, eine Stellungnahme abzugeben. In dieser Stellungnahme machte die Datenschutzbehörde deutlich, dass sie in schwebende Verfahren nicht eingreifen darf.

**Wahl des Vorsitzenden und der Mitglieder der Datenschutzbehörde**
Nach dem neuen Gesetz (3051/2002) zur Umsetzung der Änderungen der griechischen Verfassung müssen der Vorsitzende und die künftigen Mitglieder der Datenschutzbehörde vom Parlament gewählt werden.

### *E. Website*

www.dpa.gr
Die Website steht in griechischer und englischer Sprache zur Verfügung.

## - Irland

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Keine.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Die irische Datenschutzbehörde veröffentlichte allgemeine Leitlinien bezüglich der Notwendigkeit von Verfahrensregeln im Allgemeinen, insbesondere jedoch für den Gesundheitssektor.

## *C. Wichtige Rechtsprechung*

Die Datenschutzbehörde traf in allen anhängigen Fällen eine Entscheidung; gegen die Entscheidungen wurden keine Berufungsverfahren vor Gericht angestrengt, wie sie per Gesetz möglich sind. Außerdem wurden per amtlicher Mitteilung Informationen eingeholt, die die Datenschutzbehörde für ihre Untersuchungen zu bestimmten Fällen benötigte. Der Jahresbericht der Datenschutzbehörde wurde dem Parlament am 10. Juni 2002 vorgelegt.

## *D. Spezifische Themen*

**Beschwerden**
Generell ist festzustellen, dass sich die Mehrzahl der für die Verarbeitung Verantwortlichen ihrer Verantwortung durchaus bewusst sind. Nachstehend dennoch die herausragendsten Beschwerdefälle des Jahres 2001.

*Kreditkartenunternehmen*
Verschiedene Personen fühlten sich durch unerwünschte Telefonanrufe eines großen Kreditkartenunternehmens belästigt. Andere Personen erhielten weiterhin Postsendungen, obwohl sie wiederholt um Einstellung der Zusendung gebeten hatten. Die Datenschutzbehörde erörterte die Sachverhalte mit dem Unternehmen, das seine Praktiken seither gebessert hat.

*Fernhinzufügung („Teleappending")*
Im Rahmen der Untersuchung im Fall des Kreditkartenunternehmens stellte die Datenschutzbehörde fest, dass Direktmarketingfirmen Zugang zu einer „Superdatenbank" hatten, die aus dem Wählerverzeichnis bestand, das von der nationalen Telekommunikationsgesellschaft automatisch durch Fernhinzufügung („Teleappending") um Telefonnummern ergänzt worden war. Die Datenschutzbehörde untersagte diese Praxis, weil hierfür keine willentliche Einwilligung der betroffenen Telefonteilnehmer vorlag.

*Fluggesellschaft*
Die Datenschutzbehörde befasste sich mit einer Beschwerde über die missbräuchliche Verwendung von Kreditkartendaten durch eine Fluggesellschaft. Der Beschwerde wurde nicht stattgegeben. Außerdem untersuchte die Datenschutzbehörde einen Fall, in dem die staatliche Fluggesellschaft personenbezogene Daten namentlich genannter Passagiere öffentlich gemacht hatte. Die Datenschutzbehörde wies darauf hin, dass Unternehmen der Pflicht zur Geheimhaltung von Kundendaten unterliegen.

*Bank und Versicherung*
Die Datenschutzbehörde kritisierte die mangelnde Transparenz und Offenheit eines Cross-Marketingkonzepts, bei dem eine Bankkreditkarte unter der Marke einer Versicherung beworben wurde. Die Datenschutzbehörde forderte, dass bei derartigen Cross-Marketingangeboten die tatsächliche Identität der beteiligten Unternehmen klar ersichtlich sein müsse.

*Anwaltskanzlei*
Nur unter Anwendung ihrer rechtlichen Befugnisse konnte die Datenschutzbehörde eine Anwaltskanzlei dazu bewegen, die für die Untersuchung einer Beschwerde

benötigten Informationen herauszugeben. Die Datenschutzbehörde äußerte ihre Besorgnis darüber, dass sie sich aufgrund mangelnder Kooperationsbereitschaft eines Angehörigen eines juristischen Berufs zu diesem Schritt gezwungen sah.

*Anwaltskanzlei*

Auf der Suche nach Daten über einen weiteren Beschwerdeführer inspizierte die Datenschutzbehörde vor Ort die EDV-Anlage einer Anwaltskanzlei. In diesem Fall zeigte sich die Kanzlei allerdings kooperationsbereit, der Beschwerde wurde nicht stattgegeben.

*Kreditkartendaten*

Es wurde festgestellt, dass eine Firma durch Speicherung der Kreditkartendaten eines Betroffenen gegen das Datenschutzgesetz verstoßen hatte. Die Firma hatte die Daten für die Berechnung einer zu einem späteren Zeitpunkt erbrachten Leistung – dem Streitgegenstand – verwendet. Die Datenschutzbehörde erkannte dass Kreditkartendaten, die für eine bestimmte Transaktion erhoben werden, ohne Einwilligung der betroffenen Person nicht für weitere Transaktionen verwendet werden dürfen.

*Gemeinnützige Organisation*

Eine gemeinnützige Organisation verstieß – allerdings unbeabsichtigt – gegen das Datenschutzgesetz, als sie ihre Datenbank einem Finanzinstitut für Direktmarketingzwecke zur Verfügung stellte.

*Hilfe für Verbrechensopfer*

Die Datenschutzbehörde stellte klar, dass Daten über Verbrechensopfer von der Polizeibehörde (An Garda Síochána) ohne vorherige Einwilligung der Betroffenen nicht routinemäßig der Hilfsorganisation Victim Support zur Verfügung gestellt werden dürfen. Eine formelle schriftliche Einwilligung wird hierfür allerdings nicht für notwendig erachtet.

**Verhaltensregeln**

Die Datenschutzbehörde forderte Branchenorganisationen, unter anderem des medizinischen Sektors und des Direktmarketingbereichs, auf, Verhaltensregeln aufzustellen, die in den betreffenden Branchen den Schutz der Privatsphäre gewährleisten sollen.

Für den Gesundheitssektor legte die Datenschutzbehörde Empfehlungen für Verhaltensregeln vor. Verhaltensregeln stellen kein Hindernis für die wirksame Gesundheitsfürsorge dar, sondern unterstützen diese vielmehr entsprechend dem Grundsatz, wonach Patientendaten parallel zur Behandlung der Patienten weitergegeben werden sollen. Die Datenschutzbehörde hob hervor, dass Geheimhaltung und Sicherheit der Patientendaten mit Aufklärungsaktivitäten und der Pflicht zur Einholung der Einwilligung der Patienten gekoppelt werden sollten, damit die Patienten die Verwendung ihrer personenbezogenen Daten angemessen kontrollieren können.

**Besorgnis hinsichtlich Registrierungen von Angehörigen der Rechtsberufe**

Die Datenschutzbehörde brachte ihre Besorgnis darüber zum Ausdruck, dass sich nur eine relativ geringe Zahl von Angehörigen der Rechtsberufe bei der Behörde

registrieren lässt. Dieser Sachverhalt war zwar bereits der Law Society und dem Bar Council als Standesvertretungen der Rechtsberufe vorgetragen worden, doch kündigte die Datenschutzbehörde für das kommende Jahr weitere proaktive Schritte an, um die Angehörigen der Rechtsberufe zu veranlassen, ihrer gesetzlichen Pflicht nachzukommen.

Die Zahl sonstiger Organisationen, die sich bei der Datenschutzbehörde registrieren ließen, stieg von 2880 im Jahr 2000 auf 3099 im Jahr 2001.

**Beschwerden und Anfragen**
Die Datenschutzbehörde meldete einen leichten Rückgang der Zahl der Anfragen von 3100 im Jahr 2000 auf etwas über 2900 im Jahr 2001. Dieser leichte Rückgang ist auf den wachsenden Bekanntheitsgrad der offiziellen Datenschutz-Website zurückzuführen, die im Dezember 2000 ins Internet gestellt wurde, und die während des Jahres 17 000 Besucher verzeichnen konnte. Viele der Anfragen betrafen Kreditauskünfte, Direktmarketing und Zugangsanträge. Unternehmen, die sich an die Datenschutzbehörde wandten, stellten unter anderem Fragen zum neuen Datenschutzrecht und zur Registrierung gemäß dem Datenschutzgesetz. Zugenommen hat auch die Komplexität der Anfragen, da sich Einzelpersonen vermehrt um ihr Recht auf Respektierung ihrer Privatsphäre sorgen und verantwortungsbewusst handelnde Organisationen verstärkt auf ihre Pflichten zum Datenschutz achten.

Die Zahl der formellen Beschwerden stieg 2001 auf 233 gegenüber 131 im Vorjahr, dies entspricht einem Anstieg um 78 %. Die meisten Beschwerden betrafen Unternehmen im Telekommunikations- und IT-Bereich, Finanzinstitute, Direktmarketingunternehmen und Behörden. 35 % der Beschwerden wurde stattgegeben, 33 % wurde nicht stattgegeben, die übrigen 32 % wurden auf informellem Wege beigelegt.

### *E. Website*

http://www.dataprivacy.ie

## - Italien

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Von den im fraglichen Zeitraum angenommenen Rechtsvorschriften sind die Folgenden von besonderem Belang:

- ein Gesetz, das die Stimmrechte italienischer Bürger im Ausland regelt und das Bestimmungen für die Führung von Konsulatsarchivsystemen enthält;
- ein Gesetz über die Einführung des Euro, das unter anderem Bestimmungen über die „Rückführung“ von Kapital aus dem Ausland enthält und hierzu vorsieht, dass bei der Meldung an die zuständigen Behörden die Geheimhaltungspflicht gewahrt bleiben muss.

## *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Die Garante nahm unter anderem zu folgenden Rechtsvorschriften Stellung:

- zu einem Gesetz zur Novellierung des Fremdenverkehrsrechts, das besondere Regelungen für die so genannten „Meldekarten“ vorsieht. Die bisherigen Bestimmungen wurden dahingehend geändert, dass Hotelmanager nunmehr verpflichtet sind, den zuständigen Behörden Daten ihrer Hotelgäste durch Übermittlung einer Kopie der jeweiligen Meldekarten weiterzugeben. Alternativ können die Daten auch entsprechend den Bestimmungen einer Verordnung des Innenministeriums über elektronische und/oder computergestützte Netze übermittelt werden. Hingegen enthält das Gesetz keine Angaben über Regelungen bzw. Beschränkungen für die Verarbeitung der von den Strafverfolgungsbehörden erhobenen personenbezogenen Daten;

- zu einer Verordnung, in welcher die Anbringung und Nutzung von elektronischen Geräten und technischen Einrichtungen zur *Überwachung von Personen, die unter Hausarrest stehen oder sich im Strafvollzug befinden* – den so genannten „elektronischen Fesseln“ – geregelt wird. Gemäß § 4 dieser Verordnung, die die Verarbeitung personenbezogener Daten betrifft, muss beim Einsatz dieser Geräte und Einrichtungen die Würde der betroffenen Personen gewahrt werden, die Daten dürfen nur über einen bestimmten Zeitraum gespeichert werden und es muss im Einklang mit den Sicherheitsmaßnahmen gemäß § 15 des Gesetzes Nr. 675/1996 festgelegt werden, wer zur Verarbeitung derartiger Daten berechtigt ist.

## *C. Wichtige Rechtsprechung*

Zunehmend machen betroffene Personen – entweder direkt oder über Rechtsvertreter – von der Möglichkeit einer Beschwerde bei der Garante als Rechtsmittel Gebrauch.

Während anfangs nahezu sämtliche Beschwerden den Zugang zu personenbezogenen Daten betrafen, hat in jüngster Zeit die Zahl der Anträge auf Ergänzung, Berichtigung und Löschung von Daten und/oder Widersprüche gegen die Verarbeitung personenbezogener Daten zugenommen.

**Revision von Entscheidungen der Garante**
Einige wenige Beschwerdeführer forderten die Revision und/oder Änderung von Entscheidungen der Behörde, wobei es insbesondere um die Zuweisung von Kosten und sonstigen Aufwendungen ging. Die Garante vertritt den Standpunkt, dass für die Revision einer Entscheidung der Datenschutzbehörde ausschließlich das ordentliche Gericht zuständig ist, vor dem die Entscheidung gemäß § 29 Absatz 6 des Datenschutzgesetzes angefochten wird.

Bislang wurde lediglich eine geringe Zahl von Entscheidungen der Garante angefochten, wobei es insbesondere um Entscheidungen zu Beschwerden ging, die gemäß § 29 des Datenschutzgesetzes geltend gemacht wurden.

Ein weiterer Punkt, der in diesem Zusammenhang angesprochen wurde, betrifft die passive Rechtsfähigkeit der Garante, d. h. die der Behörde gegebene Möglichkeit, vor einem ordentlichen Gericht und/oder dem Revisionsgericht aufzutreten, um die

rechtliche Begründung der angefochtenen Entscheidungen zu verteidigen. Diesbezüglich vertritt die Garante den Standpunkt, dass eine Entscheidung über die ihr gegebene Möglichkeit, vor Gericht aufzutreten, lediglich bei Vorliegen von Rechtsfragen relevant ist, die mit der bestimmungsgemäßen Anwendung des Datenschutzgesetzes (Nr. 675/1996) insgesamt und der maßgeblichen Sicherheiten zu tun haben, während dies bei rein faktischen Fragen oder Fragen, die ausschließlich das Verhältnis zwischen den Parteien betreffen, in der Regel nicht der Fall ist.

## *D. Spezifische Themen*

Am 28. Februar 2001 wurden die vier Mitglieder des Vorstands der italienischen Datenschutzbehörde vom Abgeordnetenhaus und dem Senat gewählt. Der neue Vorstand bestätigte Prof. Stefano Rodotà als Vorsitzenden und Prof. Giuseppe Santaniello als Stellvertretenden Vorsitzenden der Garante.

Der Schwerpunkt der Tätigkeit der Garante lag auf den folgenden Themenbereichen, zu denen die Mehrzahl der Entscheidungen zu konkreten Beschwerden und/oder Berichte sowie die meisten allgemeineren Maßnahmen verabschiedet wurden.

**Schutz der personenbezogenen Daten und Beurteilungsdaten von Arbeitnehmern und Zugang von betroffenen Arbeitnehmern zu personenbezogenen Daten**

Dieser Themenkomplex nahm in der Tätigkeit der Garante einen beträchtlichen Stellenwert ein. Die Datenschutzbehörde befasste sich in ihren Entscheidungen insbesondere mit der Fernüberwachung von Arbeitnehmern, wobei es im Einzelfall um die Vorkehrungen von Arbeitgebern für die Überwachung des Zugangs von Mitarbeitern zu elektronischen Netzen und E-Mail-Diensten ging.

Im Hinblick auf Beschwerden war festzustellen, dass Arbeitnehmer zunehmend bei ihren Arbeitgebern den Zugang zu sämtlichen personenbezogenen Daten beantragen, die der Arbeitgeber über sie speichert; hiervon betroffen sind auch – vor allem im Falle von Angestellten und Führungskräften – Daten und Informationen in Beurteilungsunterlagen, Leistungsbewertungen und/oder Jahresberichten. Nach unvermeidlichen Anlaufschwierigkeiten ist festzuhalten, dass die für die Verarbeitung Verantwortlichen inzwischen schneller und vollständiger Auskunft auf entsprechende Anträge geben. Den Betroffenen stehen somit weitreichende Möglichkeiten offen, sich die fraglichen Auskünfte auf Papier oder anderen Datenträgern zu beschaffen.

**Gesundheitsdaten und Daten in gerichtsmedizinischen Unterlagen**

Die Garante befasste sich mit mehreren Fällen, in denen der volle Zugang zu entsprechenden Daten bei Krankenhäusern und/oder Gesundheits- und Pflegediensten beantragt wurde. In einigen Fällen betrafen die Anträge recht umfangreiche Datenbanken mit Daten zu verschiedenen Aktivitäten von Gesundheitsdiensten sowie zu besonders komplexen Krankheiten.

Wiederholt behandelte die Garante auch Fälle, in denen es um die Verarbeitung von medizinischen Daten aus gerichtsmedizinischen Unterlagen im Zusammenhang mit Versicherungspolicen ging. Über dieses Thema wird derzeit auch auf der Grundlage der bestehenden Rechtsprechung heftig diskutiert.

**Daten über Kinder**
Mehrere Beschwerden gingen zu Anträgen auf Zugang zu personenbezogenen Daten ein, die entweder von Psychologen oder von Sozialhilfe- und Gesundheitsorganen im Rahmen komplexer Rechtsstreitigkeiten verarbeitet wurden, in denen es um Scheidungs- und Sorgerechtsfragen ging. In den betreffenden Fällen hatte ein Elternteil Antrag auf Zugang zu personenbezogenen Daten seines Kindes bzw. seiner Kinder und zugleich zu sensiblen personenbezogenen Daten zu dem anderen Elternteil gestellt.
In diesem Zusammenhang galt das besondere Augenmerk der Garante auch den Fachleuten, die die betreffenden Unterlagen erstellen.

**Von Privatdetekteien verarbeitete Daten**
Die bestimmungsgemäße Verwendung von Informationen durch Privatdetekteien, deren Tätigkeit durch besondere Bestimmungen im Datenschutzgesetz (Nr. 675/1996) sowie durch eine allgemeine Ad-hoc-Genehmigung zur Verarbeitung sensibler Daten geregelt ist, stand im Mittelpunkt wichtiger Entscheidungen der Garante. Hierbei ging es um Umfang und Einschränkungen von Ermittlungstätigkeiten, und es wurde der Versuch unternommen, zwischen der Ausübung von Tätigkeiten, die für die volle Wahrung des Rechts auf Verteidigung von grundlegender Bedeutung sind, und den Auflagen in Bezug auf den Schutz der Privatsphäre einen Ausgleich zu schaffen.

**Von privaten Kreditauskunfteien verarbeitete Daten**
Die meisten der von Betroffenen eingereichten Beschwerden betrafen auch 2001 wieder die Tätigkeit von Kreditauskunfteien. Gegenstand der Beschwerden waren der Zugang zu, die Berichtigung und – recht häufig – die Löschung von personenbezogenen Daten. Im Einzelnen befasste sich die Garante mit der sensiblen Frage der Dauer der Speicherung personenbezogener Daten, was wiederum Anlass zu einer generellen Neubetrachtung der geltenden Regelungen für die Erhebung, Verarbeitung und Speicherung der Daten gab, welche beträchtliche Auswirkung auf die ungehinderte Ausübung von Wirtschaftstätigkeiten durch die Betroffenen haben können.
In einer allgemeinen Empfehlung, die die zahlreichen, von Einzelpersonen und von Verbraucherverbänden vorgetragenen Fälle berücksichtigt, stellte die Garante eine erste Anzahl von Mindestvoraussetzungen für die Verarbeitung, Aufbewahrung und Verwendung der in den Datenbanken von Kreditauskunfteien gespeicherten und von Banken und Finanzinstituten genutzten Daten auf.

**Daten über den Fernmeldeverkehr**
Auch zu diesem Themenbereich gingen zahlreiche Anträge auf Zugang zu und Berichtigung von Daten über Inhaber von Telefonkarten ein. Außerdem wurden Anträge auf Zugang zu Informationen zu ankommenden und abgehenden Telefongesprächen von bestimmten Telekommunikations-Endgeräten gestellt. In ihren Entscheidungen bekräftigte die Garante, dass die betroffenen Personen Anspruch auf vollständigen Zugang zu den personenbezogenen Daten haben, die in Telefonrechnungen mit Einzelaufstellung über abgehende Telefongespräche aufgeführt sind – ohne Löschung der letzten drei Ziffern der angewählten Telefonnummern.
Was den Charakter der Daten zum ankommenden Fernmeldeverkehr anbelangt, wird die Auffassung der Garante durch § 6 der Rechtsverordnung Nr. 467/2001 gestützt, mit der § 14 Absatz 1 des Datenschutzgesetzes (Nr. 675/1996) um den Buchstaben e

zweiter Spiegelstrich ergänzt wird. Diesem Paragraphen zufolge gilt das Recht auf Zugang nicht für Daten, die von „Anbietern öffentlich zugänglicher Telekommunikationsdienste in Bezug auf die personenbezogenen Daten [erhoben werden], die eine Identifizierung der rufenden Leitung ermöglichen, sofern dieser Zugang nicht Grundvoraussetzung für die Ausübung von Ermittlungen eines Verteidigers in einem Strafprozess ist“.

**Errichtung umfangreicher Datenbanken und Volkszählung**
Dieses Thema wird von der Garante bereits seit langem mit Interesse verfolgt, um die Auswirkungen neuer Technologien auf die Grundrechte natürlicher Personen beurteilen zu können. Auf Ersuchen des Ministeriums für Innovation und Technologie beteiligte sich die Garante an der Erarbeitung der Ausschreibung für E-Government-Projekte für das Jahr 2002 und erklärte sich auch bereit, eine Bewertung dieser Projekte mit Blick auf den Schutz personenbezogener Daten vorzunehmen.
Gleichermaßen befasste sich die Garante auch im Zusammenhang mit der Volkszählung mit verschiedenen Abwicklungsphasen von der Beratung bis hin zur Überwachung. Hier stand die Garante den Behörden wiederholt beratend zur Seite und zeigte Lösungswege auf, so z. B. für die Erhebung von Informationen über die Sprachzugehörigkeit, die in einigen Regionen Italiens erfragt werden. Die kritischen Fragen, die dieser Teil der Erhebung aufwirft, wurden auch den zuständigen Organen der EU zur Kenntnis gebracht.

**Videoüberwachung**
Diesem Thema widmet sich die Garante mit besonderem Interesse, weil zum einen diese Technik zunehmend weitere Verbreitung findet und weil sich zum anderen die Bürger in dieser Hinsicht hochgradig sensibel zeigen. Nachdem spezifische Rechtsvorschriften noch nicht vorliegen, gelten die Bestimmungen des Datenschutzgesetzes. Nach einer eingehenden Untersuchung zu dem Thema, in deren Verlauf die Garante umfassende Informationen sammelte, entschloss sich die Behörde zur Veröffentlichung eines zehn Punkte umfassenden Katalogs mit Leitlinien für die diesbezügliche Datenverarbeitung. Die Datenschutzbehörde bekundete ihre Bereitschaft zur Zusammenarbeit mit den zuständigen örtlichen und nationalen Behörden bei einer vorherigen Prüfung von Vorhaben zur Überwachung der Aktivitäten in bestimmten Bereichen mittels elektronischer Einrichtungen.

Zusätzlich wurde beschlossen, ausgehend von Meldungen von Bürgern, aber auch von Amts wegen Audits durchzuführen. Im Rahmen dieser Audits sollten die Praktiken von Unternehmen, Organisationen und Verbänden beleuchtet werden, die Kameras an öffentlichen oder öffentlich zugänglichen Orten installiert hatten, ohne die hierfür vorgeschriebenen Informationen vorgelegt zu haben. Die Prüfungen ergaben diverse Verstöße, unter anderem von zwei Unternehmen und einer Behörde im Verkehrssektor sowie von zwei Supermärkten einer in ganz Italien vertretenen großen Handelskette, zwei Banken und einer Organisation, die im Besitz der öffentlichen Hand befindliche Sportanlagen verwaltet.

**Verarbeitung von biometrischen Daten**
Nach eingehenden Ermittlungen ordnete die Garante die Deaktivierung von Systemen zur Erfassung biometrischer Daten (Fingerabdruckdaten) an, die von verschiedenen Banken installiert worden waren. In ihrer diesbezüglichen Entscheidung wies die Garante darauf hin, dass der pauschale Einsatz solcher Systeme nicht generell erlaubt

ist, vielmehr dürfen diese nur in Fällen eingesetzt werden, in welchen objektiv und unabhängig von der Einschätzung des betreffenden Finanzinstituts spezifische und konkrete Risiken bestehen.

Der Einsatz derartiger Techniken ist insbesondere bei Banken ein sehr sensibles Thema, da die Erbringung bzw. die Verweigerung der Erbringung von Dienstleistungen einer Bank, zu welcher der Zugang nur in Verbindung mit der Erhebung biometrischer Daten möglich ist, entscheidend davon abhängig gemacht werden kann, ob die Betroffenen die Einwilligung zur Abtastung ihrer Fingerabdrücke geben.

In einer Entscheidung vom September 2001 befasste sich die Garante auf Antrag verschiedener Banken mit spezifischen Sicherheitsanforderungen im Zusammenhang mit der bevorstehenden Einführung der Einheitswährung sowie mit den bei den Bankniederlassungen vorrätig gehaltenen größeren Bargeldbeständen. Die Garante legte schließlich verschiedene Voraussetzungen fest, unter denen befristet Systeme für die automatische Erfassung biometrischer Daten installiert werden durften.

**Verhaltensregeln und Leitlinien für die berufliche Praxis**

Die Aktivitäten zur Aufstellung von Verfahrensregeln und Leitlinien für die berufliche Praxis wurden 2001 fortgeführt. Die Verhaltensregeln für die Verarbeitung personenbezogener Daten für historische Zwecke konnten fertig gestellt werden. Diese Verhaltensregeln sollen dafür sorgen, dass bei der Verwendung von personenbezogenen Daten, die im Zuge historischer Recherchen sowie im Zusammenhang mit der Wahrnehmung des Rechts auf Forschung und Information und mit der Tätigkeit von Archiven erhoben werden, die Rechte und Grundfreiheiten sowie die Würde der betroffenen Personen und insbesondere deren Anspruch auf Schutz der Privatsphäre und ihrer Identität ohne eine Beeinträchtigung dieser Aktivitäten, sondern vielmehr im Sinne einer Förderung der Forschungsarbeiten gewahrt werden.

Das unabhängig vom nationalen statistischen System durchgeführte Verfahren zur Annahme der Verhaltensregeln für Aktivitäten im Bereich der Statistik und der wissenschaftlichen Forschung stand 2001 ebenfalls kurz vor dem Abschluss. Bei der Aufstellung von Verhaltensregeln für die Verarbeitung personenbezogener Daten durch Strafverteidiger und Privatdetektive kam die Garante 2001 ebenfalls deutlich voran.

**Weitere Initiativen der Garante**

Die *Audit-Aktivitäten* der Garante wurden in den verschiedenen Formen, in denen diese von der Behörde ausgeübt werden können, tatkräftig weiter betrieben, so unter anderem

- Kontrollen (mit und ohne Vorankündigung)
- Zugang zu Datenbanken
- Kooperationsmaßnahmen
- Untersuchungen
- Befragungen

So wurden bei verschiedenen Kommunen stichprobenweise Kontrollen durchgeführt, um zu prüfen, welche Erhebungsmethoden die Zensusbeauftragten bei der

Volkszählung 2001 tatsächlich anwandten, um Daten über Familien und Unternehmen zu erheben. Außerdem wurden die Angemessenheit der vom nationalen statistischen Institut an die Zensusbüros herausgegebenen Leitlinien und die von den einzelnen Kommunen angewandten Sicherheitsmaßnahmen geprüft.

Einen besonderen Schwerpunkt bildeten auch die *Kommunikationsaktivitäten* der Garante. Neben herkömmlichen Methoden wie Pressemitteilungen, Newsletters und Pressekonferenzen setzte die Behörde hier auf Multimedia- und interaktive Initiativen, mit denen Dokumente und Veröffentlichungen über die Website der Datenschutzbehörde verbreitet und zugänglich gemacht wurden. Dabei zeigte sich, dass der Newsletter nicht nur als Mitteilungsinstrument sondern auch als eine Art „Archiv" genutzt werden kann, das Recherchen zu den verschiedenen Bereichen ermöglicht, in denen das Datenschutzgesetz angewandt wird und in denen die Garante operiert.

Das digitale Archiv mit der Bezeichnung *„Bürger und Informationsgesellschaft"* erlebte 2001 seine fünfte Auflage. Es umfasst sämtliche Unterlagen und Aufzeichnungen zur Tätigkeit der Garante, vom nationalen und internationalen Verweisrecht bis hin zu den verschiedenen Veröffentlichungen. Die CD-ROM wird auf Anfrage kostenlos verschickt. 2001 wurden über 9 000 Exemplare an Behörden, private Körperschaften, Fachleute und interessierte Bürger verteilt.

Nicht zuletzt sei in diesem Zusammenhang auf das Magazin *„Bürger und Informationsgesellschaft"* hinweisen, in dem die Garante ihre Entscheidungen sowie relevante Rechtsvorschriften, Pressemitteilungen und sonstige Dokumente von Interesse veröffentlicht.

### *E. Website*

www.garanteprivacy.it
Die Website steht in italienischer und englischer Sprache zur Verfügung.

## - Luxemburg

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Im Jahr 2001 wurden drei Verordnungen mit Bezug zum Gesetz vom 31. März 1979 über die Verarbeitung personenbezogener Daten im Bereich der Informationstechnologie angenommen:

1) Großherzogliche Verordnung vom 11. August 2001 über die Errichtung und Nutzung einer Datenbank mit den personenbezogenen Daten der Endbegünstigten von finanziellen Beihilfen im Rahmen von Projekten des Europäischen Sozialfonds
(Amtsblatt A Nr. 115 vom 14. September 2001, S. 2400)

2) Großherzogliche Verordnung vom 20. Juni 2001 zur Genehmigung der Errichtung und Nutzung einer Datenbank mit personenbezogenen Daten über Schüler
(Amtsblatt A Nr. 74 vom 3. Juli 2001, S. 1506)

3) Großherzogliche Verordnung vom 18. Januar 2001

1. über die allgemeine Erhebung der Bevölkerung, der Wohnungen und der Gebäude im Großherzogtums Luxemburg am 15. Februar 2001
2. zur Genehmigung der Errichtung und Nutzung einer Datenbank mit diesbezüglichen personenbezogenen Daten
(Amtsblatt A Nr. 11 vom 30. Januar 2001, S.613)

Darüber hinaus enthält das Gesetz vom 18. April 2001 über Urheberrechte, Nachbarschaftsrecht und Datenbanken (Amtsblatt A Nr. 50 vom 30. April 2001, S.1041) die maßgeblichen Bestimmungen für Datenbanken im Bereich des geistigen Urheberrechts.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

**Einbringung des Gesetzentwurfs 4794 am 4. Mai 2001**
zur Annahme

- des Übereinkommens aufgrund von Artikel K.3 über den Einsatz der Informationstechnologie im Zollbereich, unterzeichnet in Brüssel am 26. Juli 1995;
- der Übereinkunft über die vorläufige Anwendung des Übereinkommens zwischen einigen Mitgliedstaaten der Europäischen Union aufgrund von Artikel K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, unterzeichnet in Brüssel am 26. Juli 1995.

**Großherzogliche Verordnung vom 1. Juni 2001 über elektronische Signaturen, elektronische Zahlungssysteme und die Einsetzung des Ausschusses für den elektronischen Geschäftsverkehr**
(Amtsblatt A Nr. 71 vom 22. Juni 2001, S. 1413)

Diese Verordnung wurde angenommen in Anwendung des Gesetzes vom 14. August 2000 über den elektronischen Geschäftsverkehr zur Umsetzung der Richtlinie 1999/93 über einen gemeinschaftlichen Rahmen für elektronische Signaturen, der Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft und bestimmter Vorschriften der Richtlinie 97/7/EWG über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz.

### *C. Wichtige Rechtsprechung*

Arbeitsgericht Esch-sur-Alzette, 16. Mai 2002

In dem betreffenden Fall erkannte das Gericht, dass der Berufungskläger die Bestimmungen der Richtlinie 95/46/EG nicht geltend machen konnte, da die Richtlinie noch nicht in nationales Recht umgesetzt worden war. Zwar ist die Möglichkeit einer direkten Wirkung von Gemeinschaftsrichtlinien nicht zwangsläufig ausgeschlossen, doch ist auch klar, dass ihnen im Prinzip nur eine vertikale Wirkung zuerkannt wird. Hieraus folgt, dass die Bestimmungen der Richtlinie 95/46/EG in einem horizontalen Verfahren, in dem es um die Überwachung am Arbeitsplatz geht und in welchem sich zwei Privatpersonen bzw. privatrechtliche Körperschaften gegenüberstehen, keine Anwendung finden können.

Die Entscheidung vom 16. Mai 2002 ist dazu angetan, die Erwartungen an die verspätete Umsetzung der Richtlinie 95/46/EG in nationales Recht weiter zu verstärken. Hierzu ist anzumerken, dass das Gesetz vom 2. August 2002 zum Schutz personenbezogener Daten, mit dem die Richtlinie95/46/EG in nationales Recht umgesetzt werden soll, ausdrücklich den Sachverhalt der Überwachung am Arbeitsplatz in den Gesetzeskorpus einbezieht.

### *D. Spezifische Themen*

Keine.

## - Niederlande

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Im April 2001 wurde ein Gesetz zur Anpassung aller bereits existierenden Rechtsvorschriften an die Bestimmungen der Richtlinie 95/46/EG *(Aanpassingswet WBP)*[14] verabschiedet. Die weitreichendsten Änderungen betrafen hierbei das Gesetz über kommunale Datenbanken (personenbezogene Daten) *(Wet gemeentelijke basisadministratie persoonsgegevens)*[15] und das Gesetz über die Informationsfreiheit *(Wet openbaarheid van bestuur, WOB)*[16]. Das Gesetz über kommunale Datenbanken (personenbezogene Daten), das vom WBP ausgenommen ist, jedoch mit der Richtlinie voll im Einklang steht, untersagt jetzt Dritten mit kommerziellen Zielen die Nutzung von Melderegistern. Das Gesetz über die Informationsfreiheit enthält nach der Änderung eine Bestimmung dahingehend, dass im Falle sensibler Daten keine Informationen weitergegeben werden dürfen, sofern nicht eindeutig feststeht, dass die Privatsphäre natürlicher Personen dadurch nicht beeinträchtigt wird.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Im November 2001 lag dem Parlament ein Gesetzentwurf zur Änderung der Verordnung über DNA-Untersuchungen in Strafsachen vor, mit dem der Geltungsbereich der Verordnung dahingehend ausgeweitet werden sollte, dass die Möglichkeit aufgenommen werden sollte, äußerlich erkennbare Merkmale von Personen anhand von Zellmaterial zu bestimmen. In ihrer Stellungnahme zu der Vorlage sprach sich die Datenschutzbehörde für eine genauere Abgrenzung der Definition von äußerlich erkennbaren Merkmalen von Personen aus. In der gegenwärtigen Fassung der Vorlage werden entsprechend dieser Empfehlung die äußerlich erkennbaren Merkmale von Personen, die nach dem Stand der Technik mit hinreichender Genauigkeit bestimmt werden können, im Gesetz bezeichnet. Damit wird eine schleichende Ausweitung der Anwendbarkeit auf andere Merkmale von Personen verhindert, die anhand der DNA weniger sicher bestimmt werden können.

---

14 Wet van 5 april 2001, Stb. 180, tot wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens.

15 Stb. 1994, 494.

16 Stb. 1991, 703.

2001 wurde die Verordnung über die besondere Erhebung numerischer Daten von Telekommunikationen *(Besluit bijzondere vergaring nummergegevens telecommunicatie)*[17] angenommen, die Betreiber öffentlicher Telekommunikationsnetze dazu verpflichtet, eine begrenzte Zahl von Daten über Prepaid-Telefonkarten über einen Zeitraum von drei Monaten aufzubewahren. Diese Pflicht gilt nicht für Anwendungen, bei denen dem Betreiber die Teilnehmerdaten der Nutzer bekannt sind.

## *C. Wichtige Rechtsprechung*

**Der eBay-Fall**
Die Datenschutzbehörde prüfte die geplante Weitergabe von Verbraucherdaten durch das Unternehmen iBazar, das in verschiedenen EU-Ländern Auktions-Websites betreibt, an das US-Unternehmen eBay, nachdem iBazar von eBay übernommen worden war. Es wurde vorgeschlagen, die Weitergabe von Verbraucherdaten zu gestatten, sofern die Kunden sich nicht gegen die Weitergabe entschieden („Opt-out"-Verfahren), dass die Daten in den USA allerdings nur nach Einwilligung der Kunden verwendet werden dürften („Opt-in"-Verfahren). Die Datenschutzbehörde stellte fest, dass die Richtlinie 95/46/EG ein angemessenes Schutzniveau für die Weitergabe personenbezogener Daten in Drittländer vorschreibt und eBay nicht angeboten hatte, sich der Vereinbarung über den „sicheren Hafen" anzuschließen. Da keine weiteren Ausnahmeregelungen der Richtlinie für die Weitergabe geltend gemacht werden könnten, sei die unzweifelhafte Einwilligung der betroffenen Person erforderlich. In diesem Fall reiche somit ein „Opt-out"-Verfahren nicht aus, da die Einwilligung eine freiwillige Willensbekundung voraussetze. Nach dieser Entscheidung sagte eBay zu, in diesem Fall nach dem gleichen Verfahren vorzugehen wie bei der Weitergabe von Kundendaten von iBazar France (20. Juli 2001, Nr. 2001-0784, siehe vollständiger Text im englischsprachigen Bereich von www.cbpweb.nl).

**Weitere Fälle**
Außerdem befasste sich die Datenschutzbehörde mit dem Verkauf personenbezogener Daten nach einem Konkurs. Sie entschied, dass ein solcher Verkauf nur zulässig ist, wenn die nachfolgende Weitergabe personenbezogener Daten mit dem Zweck vereinbar ist, für den die Daten erhoben wurden und wenn die Interessen der betroffenen Personen berücksichtigt wurden. In diesem Zusammenhang sei insbesondere auf den Charakter der Daten und die Folgen der Weitergabe für die betroffenen Personen zu achten. Die Datenschutzbehörde verlangte als weitere Voraussetzung eine ordnungsgemäße Information der betroffenen Personen über die beabsichtigte Weitergabe, wobei diese der Weitergabe nicht widersprochen haben dürfen (13. November 2001, Nr. 2001-1242).

Um die Definition von „personenbezogenen Daten" ging es in zwei Fällen. Die Datenschutzbehörde entschied, dass digitale Aufnahmen von öffentlichen Bereichen, einschließlich detaillierter Aufnahmen einzelner Gebäude, als „personenbezogene Daten" zu betrachten sind, sofern diese Daten für Zwecke verwendet werden, die die

[17] Besluit van 18 december 2001 (Stb. 2002, 31), houdende regels voor de vergaring van nummergegevens door middel van afwijkend frequentiegebruik en bestandsanalyse met het oog op het onderzoek van telecommunicatie (Besluit bijzondere vergaring nummergegevens telecommunicatie).

Interessen der jeweiligen Eigentümer betreffen (z. B. Besteuerung von Grundbesitz), und wenn es sich bei diesen Eigentümern um identifizierbare natürliche Personen handelt (16. Februar 2001, Nr. 2000-0075). Außerdem stellte die Datenschutzbehörde fest, dass IP-Adressen in vielen, wenngleich nicht in allen Fällen als „personenbezogene Daten" betrachtet werden könnten und dass die Umstände des jeweiligen Einzelfalls zu berücksichtigen seien (19. März 2001, Nr. 2000-0340).

## *D. Spezifische Themen*

**Schutz der Privatsphäre und IKT**

Die Datenschutzbehörde untersuchte 2001 die Gefahren für den und die Möglichkeiten zum Schutz der Privatsphäre im Zusammenhang mit der Informations- und Kommunikationstechnologie (IKT). Sie veröffentlichte einen Bericht über den Schutz personenbezogener Daten *(Beveiliging van persoonsgegevens)*, in dem sie anhand von Rahmenvorgaben aufzeigt, wie Informationssysteme so gestaltet werden können, dass sie dem niederländischen Datenschutzgesetz entsprechen. Im Verlauf des Jahres wurden auch die in Zusammenarbeit mit dem öffentlichen und dem privaten Sektor entwickelten Instrumente für ein „Privacy Audit" öffentlich herausgestellt, die für Bewertungen und Audits von Informationssystemen eingesetzt werden sollen.

Mit großem Einsatz engagierte sich die Datenschutzbehörde dafür, die Vorteile von PET – Technologien zum besseren Schutz der Privatsphäre – einer breiteren Öffentlichkeit bekannt zu machen. PET verhindern die nicht zwingend notwendige Verarbeitung personenbezogener Daten in Informationssystemen und tragen damit dazu bei, bei Neuentwicklungen den entwurfsimmanenten Schutz der Privatsphäre („Privacy by Design") zu fördern. Als eine besonders zukunftsorientierte Initiative auf diesem Gebiet ist das europäische Projekt PISA zu nennen, an dem die Datenschutzbehörde mitwirkte. Das Projekt PISA (Privacy Incorporated Software Agents) verfolgt das Ziel, Entwurfsspezifikationen für autonome Software-„Agenten" zu entwickeln, die ihrem „Eigentümer" die Möglichkeit bieten, verschiedenartige elektronische Transaktionen durchzuführen oder zu autorisieren, ohne dabei die Kontrolle über seine personenbezogenen Daten aus der Hand zu geben.

In naher Zukunft dürfte es in den Niederlanden zahlreiche öffentliche und private „Trusted Third Parties" (TTP) geben, denen als Aussteller digitaler Identitätszertifikate eine wichtige Funktion zukommen wird. Die Datenschutzbehörde sah sich daher 2001 zur Veröffentlichung eines Berichts unter dem Titel *„Sleutels van vertrouwen"* (Der Schlüssel zum Vertrauen) veranlasst, in dem sie eine erste Untersuchung der Implikationen der europäischen Datenschutzrichtlinie und des niederländischen Datenschutzgesetzes für den TTP-Sektor vornimmt.

**Elektronische Behördendienste**

Die (mangelnde) Sorgfalt staatlicher Organe und sonstiger Einrichtungen beim Austausch personenbezogener Daten bot der Datenschutzbehörde verschiedentlich Anlass zu beträchtlicher Sorge. Insbesondere dann, wenn mehrere Institutionen im Wege einer Zusammenarbeit personenbezogene Daten austauschen, ist nicht immer klar ersichtlich, wer jeweils der für die Verarbeitung Verantwortliche für die betreffenden Verarbeitungsvorgänge ist. Unter entsprechenden Umständen kann die effiziente Datenverarbeitung im Konflikt zu den Interessen der Betroffenen stehen

oder gar gegen geltendes Recht verstoßen. Schon in absehbarer Zeit werden die Zusammenarbeit und der Datenaustausch zwischen Behörden einen Stand erreicht haben, an dem eine formelle Informationsstruktur besteht. Die Datenschutzbehörde veranlasste daher 2001 eine Untersuchung zur Frage des Schutzes der Privatsphäre im Zusammenhang mit elektronischen Behördendiensten, zu der sie 2002 in einem von ihr veröffentlichten Papier Stellung nehmen wird.

**Ermittlungsbefugnisse**
In der Vergangenheit wurden Unternehmen und sonstige Organisationen nicht selten von Polizei und Justiz dazu aufgefordert oder per Anordnung veranlasst, digitalisierte personenbezogene Daten (z. B. über Kunden) weiterzugeben oder den Zugang zu solchen Daten zu ermöglichen. Entsprechende Anordnungen waren allerdings in vielen Fällen rechtswidrig. Die fraglichen Unternehmen sahen sich somit in eine schwierige Position gebracht. Nach Eingang zahlreicher Beschwerden wandte sich die Datenschutzbehörde mit der Forderung nach Leitlinien für diesen Themenkomplex an das Justizministerium, worauf sich der Justizminister gegen diese Form der Informationserhebung aussprach.

Mit der Frage der polizeilichen Befugnisse befasste sich 2001 auch der Ausschuss für die Informationserhebung im Zuge strafrechtlicher Ermittlungen („Mevis-Ausschuss“). Der Ausschuss schlug vor, Polizei und Staatsanwaltschaft umfangreiche Befugnisse zu übertragen, um ihnen die Möglichkeit zu geben, Unternehmen und staatliche Stellen zur Hilfestellung bei ihren Untersuchungen durch Bereitstellung von Informationen zu verpflichten. Die Datenschutzbehörde wandte sich gegen diese Bestrebungen; ihrer Auffassung nach sind gesetzliche Regelungen notwendig, um eine eindeutigere Festlegung der Rechte aller Beteiligten zu gewährleisten. Sie argumentiert, dass weder kommerzielle noch staatliche Organisationen in Ermittlungen einfach als „verlängerter Arm“ von Polizei oder Staatsanwaltschaft zu betrachten sind.

Ermittlungsorgane müssten größere Sensibilität im Umgang mit Informationen beweisen. Die Vorschläge, die derzeit geprüft werden, hätten zur Folge, dass Informationen über viele Menschen zugänglich gemacht würden, die keines Vergehens verdächtig sind. Damit würden die Befugnisse von Polizei und Staatsanwaltschaft beträchtlich ausgeweitet, obwohl es den betreffenden Organen bislang nicht gelungen sei, die bestehenden Vorschriften einzuhalten.

**Wiedereingliederung nach Erwerbsunfähigkeit**
Die Datenschutzbehörde befasste sich 2001 eingehend mit Fragen der sozialen Sicherheit, und hier insbesondere mit der Wiedereingliederung von Arbeitnehmern nach zeitweiliger Erwerbsunfähigkeit. Die ersten Strukturänderungen wurden am 1. Januar 2002 mit dem Inkrafttreten des Arbeits- und Einkommensimplementierungsstrukturgesetzes (SUWI-Gesetz) wirksam. Die Datenschutzbehörde forderte die Regierung auf, für völlige Transparenz der Datenströme im Zusammenhang mit dem Gesetz zu sorgen. Es müsse für alle Beteiligten – natürliche Personen, Institutionen und Unternehmen – eindeutig ersichtlich sein, welche Informationen rechtmäßig zwischen welchen Stellen und zu welchen Zwecken ausgetauscht werden dürfen. Eindeutigkeit in diesen Fragen lasse sich durch die sorgfältige Formulierung der Regelungen erreichen, mit denen die zulässigen Ziele der Informationsbereitstellung festgelegt werden.

Mit der beruflichen Wiedereingliederung von Arbeitnehmern, die über einen längeren Zeitraum arbeitsunfähig waren, werden zunehmend private Unternehmen beauftragt. Im Rahmen ihrer Beratung der Regierung zu verschiedenen Fragen der Rechtsetzung verwies die Datenschutzbehörde immer wieder auf die Notwendigkeit spezifischer Regelungen – vorzugsweise in Form von Rechtsvorschriften – für den Austausch von Informationen im Zusammenhang mit Wiedereingliederungsmaßnahmen. Personen, die vor der Wiedereingliederung in den Beruf stehen, befinden sich in einer schwierigen Situation, und bei den Daten, die in diesem Zusammenhang ausgetauscht werden, handelt es sich im Wesentlichen um medizinische Daten. Hier wird ein Konflikt zwischen der Pflicht zum Schutz der Privatsphäre und der Pflicht, den Menschen zur Wiedereingliederung in die Arbeitswelt zu verhelfen, deutlich aufgrund dessen die Anbieter von Wiedereingliederungsmaßnahmen sicherlich von Leitlinien profitieren würden. Derartige Leitlinien fehlen bislang.

**Überwachung von Arbeitnehmern**
IKT finden an modernen Arbeitsplätzen zunehmen Anwendung. Dies hat zur Folge, dass Arbeitnehmer heute nahezu täglich mit Geräten und Ausrüstung – digitale Zugangskarten, Sicherheitskameras, GSM-Telefone, RSI-Programme und sonstige Software – zu tun haben, die auch zu ihrer Überwachung genutzt werden können. Die Überwachung des E-Mail-Verkehrs und der Internet-Nutzung von Arbeitnehmern war 2001 ein wichtiges Thema. In ihren Beiträgen zur öffentlichen Diskussion hob die Datenschutzbehörde hervor, dass jede Organisation entsprechend ihrem Arbeitsumfeld ihre eigenen Regelungen für die Überwachungen entwickeln sollte. Die Behörde stellte hierfür eine Reihe von Hilfsmitteln zur Verfügung, die den Organisationen 2002 erneut angeboten werden sollen, wirkt jedoch selbst nicht direkt an der Überwachung von Arbeitnehmern mit.

### *E. Website*

www.cbpweb.nl
Die Website steht in niederländischer und englischer Sprache zur Verfügung.

## - Portugal

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

- Entschließung des Parlaments 47/2001: Genehmigung von Maßnahmen zum Schutz der Würde des Einzelnen und der genetischen Identität des Menschen
- Entschließung des Ministerrats 77/2001: Einführung einer einheitlichen Ausweiskarte für portugiesische Staatsbürger
- Gesetzesverordnung 143/2001: Umsetzung der Richtlinie 97/7/EG in nationales Recht
- Gesetzesverordnung 13/2001: Festlegung besonderer Verfahren für die Registrierung von Neugeborenen in Gesundheitseinrichtungen
- Ratifizierung der europäischen Sozialcharta
- Ratifizierung des Übereinkommens von Oviedo

## *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

- Verordnung 9/2001: Regelungen für Einreise, Aufenthalt und Ausreise von ausländischen Staatsbürgern
- Verordnung 39/2001: Genehmigung der Verfahrensrichtlinien für die Speicherung von Daten im Justizvollzug
- Entschließung des Ministerrats 1/2001: Regelungen für das Fernüberwachungssystem für Personen in Sicherungsverwahrung, die unter Hausarrest stehen.

## *C. Wichtige Rechtsprechung*

Die Datenschutzbehörde erteilte Genehmigungen für rund 500 Datenbanken. Es gingen 190 Beschwerden und 250 Anträge auf Zugang zu personenbezogenen Daten ein. Die Datenschutzbehörde führte 221 Vor-Ort-Überprüfungen durch, die in der Mehrzahl auf Beschwerden von Bürgern zurückgingen, es wurden allerdings auch Überprüfungsverfahren auf eigene Initiative durchgeführt.

Die Datenschutzbehörde verhängte 23 Geldstrafen (wegen Nichteinhaltung der Datenschutzgrundsätze, nicht erfolgter Meldung, Nichteinhaltung des Rechts auf Information, Nichteinhaltung des vorgeschriebenen Maximalzeitraums für Datenspeicherungen) und sperrte eine Datenbank eines Unternehmens, das unberechtigterweise Daten von Supermarktkunden verarbeitete (mit Auflistung aller gekauften Waren und Erstellung von Verbraucherprofilen).

Gegen ein Unternehmen, das Daten eines Bürgers in eine Warnliste für ungedeckte Schecks aufgenommen hatte, ohne den Betroffenen hiervon in Kenntnis zu setzen, wurde eine Geldstrafe verhängt. Das Unternehmen legte gegen die Entscheidung der Datenschutzbehörde Berufung ein. Das Gericht entschied zugunsten der Datenschutzbehörde und erhielt die Geldstrafe mit der Begründung aufrecht, dass der für die Verarbeitung Verantwortliche zur Information des Betroffenen verpflichtet ist und widrigenfalls – der Kläger hatte angeführt, dass die betroffene Person nicht unterrichtet werden konnte, weil die Adresse nicht erhoben worden sei – die Daten nicht verarbeitet werden dürfen.

Noch bevor dieses Urteil erging, hatte der für die Verarbeitung Verantwortliche eine weitere Berufung eingelegt, über die noch nicht entschieden wurde.

## *D. Spezifische Themen*

<u>Die wichtigsten Stellungnahmen</u>

- Stellungnahme zu einer Gesetzesvorlage über den Zugang der GD Verkehr zum Schengener Informationssystem
- Stellungnahme zur Anwendung der Übereinkunft über das ZIS-Übereinkommen
- Stellungnahme zum Entwurf für einen Beschluss des Rates über Eurojust
- Stellungnahme zu einem Gesetzentwurf, der die Tätigkeit des nationalen Statistischen Amtes und die Weitergabe von Daten regelt
- Stellungnahme zum Gesetzentwurf über personenbezogene genetische Informationen

- Stellungnahme zu einem Gesetzentwurf zum System für die Erhebung von Gewerkschaftsbeiträgen
- Stellungnahme zur Vereinbarkeit des Arbeitsrechts in Bezug auf die Weitergabe von Personalakten mit dem Datenschutzgesetz
- Stellungnahme zu einem Gesetzentwurf über gerichtliche Mahnverfahren
- Stellungnahme zur Verarbeitung personenbezogener Daten durch das Handelsregister

Entscheidungen von allgemeiner Bedeutung

Im Laufe des Jahres 2001 traf die portugiesische Datenschutzbehörde zwei wichtige Entscheidungen über den Zugang Dritter zu personenbezogenen Daten:
- Zugang zu Gesundheitsdaten (für Gerichte, Strafverfolgungsbehörden, Einrichtungen des Gesundheitssystems, Sozialversicherungsorgane, Versicherungsunternehmen, Verwandte im Falle des Todes der betroffenen Person)
- Zugang zu den Daten in der Wählerverzeichnis-Datenbank

### *E. Website*

Die beiden genannten Entscheidungen können in portugiesischer Sprache eingesehen werden unter http://www.cnpd.pt

## - Spanien

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

**Nationale Rechtsvorschriften**
*1) Maßgebliche Bestimmungen für automatisierte Archivsysteme*, die personenbezogene Daten enthalten und die von verschiedenen Organen geführt werden:

Mit Inkrafttreten des Datenschutzgesetzes im Jahr 2000 mussten die Vorschriften, die regeln, wie die einzelnen Ministerien die von ihnen verwalteten Archivsysteme organisieren, an die Bestimmungen des neuen Gesetzes angepasst werden. Das Innenministerium gab hierzu 2001 diesbezügliche Ministerialerlasse mit Datum vom 5. Februar, 30. Juli und 30. Oktober (für die Drogenarchive und die Archive der *Guardia Civil*) heraus, das Wirtschaftsministerium erließ am 22. Januar einen Beschluss und am 11. Dezember einen Erlass für verschiedene Archivierungssysteme in der Energiewirtschaft und beim nationalen Münzamt (*Fábrica de Moneda y Timbre)*, das Gesundheitsministerium erließ ebenfalls Vorschriften für seine Archive über Neuinfektionen (Erlass vom 18. Dezember) und über Forschungsaktivitäten (Erlass vom 10. September) sowie für Archive mit eigenen Datenbeständen des Ministeriums und die Daten des Gesundheitsinstituts Carlos III. Das Ministerium für innere Entwicklung, Arbeit und Soziales sowie das Verteidigungsministerium und das Büro des Ministerpräsidenten ergriffen ebenfalls entsprechende Maßnahmen.

Die Datenschutzbehörde genehmigte die entsprechenden Bestimmungen zur Anpassung der Archivsysteme an das neue Gesetz mit der **Entschließung vom**

**27. Juli 2001**, aus der unter anderem das Schutzniveau der Sicherheitsmaßnahmen (einfach, mittel, hoch) für die einzelnen Systeme hervorgeht.

*2) Gesetzentwurf (Proposición de Ley) über das Recht auf Information in Bezug auf die Gesundheit und Unabhängigkeit von Patienten und medizinische Unterlagen*

Die Initiative für diese Rechtsvorschrift mit direktem Bezug zum Schutz von Daten im Gesundheitsbereich ging vom Senat aus. Sie wurde von allen Fraktionen im Senat mitgetragen und am 21. März 2001 im Plenum erörtert. Die Gesetzesvorlage durchläuft nun als *Proyecto de ley* das Parlament (Lesung im Kongress, Erörterung von Änderungsanträgen, Annahme durch den Senat etc.).

**Regionale Rechtsvorschriften**
*3) Datenschutzgesetz 8/2001 vom 13. Juli, Comunidad de Madrid* (APDCM), veröffentlicht im Juli 2001

In Artikel 41 Absatz 1 des Datenschutzgesetzes, der die Zuständigkeit der Autonomen Behörden regelt, heißt es, dass die in deren Zuständigkeitsbereich fallenden Funktionen „soweit sie Archivierungssysteme mit personenbezogenen Daten betreffen, die von den Autonomen Regionen und von der örtlichen Verwaltung in deren Gebiet erstellt oder verwaltet werden, von den entsprechenden Organen der jeweiligen Autonomen Region wahrgenommen werden, die als Aufsichtsbehörden gelten und denen bei der Wahrnehmung ihrer Pflichten völlige Unabhängigkeit und Objektivität zugesichert wird“. Die *Comunidad de Madrid* nahm ein neues Datenschutzgesetz an, mit dem der Behörde der *Comunidad de Madrid* die Zuständigkeit für lokale amtliche Archivsysteme und die Systeme der Körperschaften öffentlichen Rechts, die die wirtschaftlichen und berufsständischen Interessen innerhalb des Gebiets der *Comunidad de Madrid* vertreten, übertragen wird.

*4) Bestimmungen für automatisierte Archivsysteme,* die personenbezogene Daten enthalten und die von verschiedenen Organen innerhalb der einzelnen Autonomen Regionen verwaltet werden.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Im Laufe des Jahres 2001 wurde mit der Gesetzesvorlage zur **Vorbeugung und Sperre der Finanzierung des Terrorismus** ein weiteres Verfahren zur Einführung von Rechtsvorschriften für den Datenschutz eingeleitet, dieses Mal allerdings im Bereich der dritten Säule.
Im vergangenen Mai gingen Änderungsanträge der verschiedenen beteiligten Gruppierungen zu der Gesetzesvorlage ein. Als nächstes steht die Aussprache im zuständigen Kongressausschuss an.

### *C. Wichtige Rechtsprechung*

**1) Rechtsprechung des Verfassungsgerichts**
Die wichtigsten Urteile des spanischen Verfassungsgerichts zu den Datenschutzrechten ergingen bereits 2000, im Jahr 2001 gab es lediglich eine diesbezügliche Entscheidung vom 15. Oktober, über **die Vertraulichkeit personenbezogener Daten in einer Steuerprüfungsakte (STC 203/2001).**

Ein Kongressabgeordneter forderte von der Regierung einen Bericht über verschiedene Verfahren wegen Verstoßes gegen die Steuergesetzgebung an. Das Präsidium des Kongresses *(Mesa del Congreso)*, als Führungsgremium dieser Parlamentskammer für die Weiterleitung von Anträgen der Abgeordneten zuständig, lehnte den Antrag mit der Begründung ab, dass die betreffenden Daten unter die Geheimhaltungspflicht nach Artikel 113 Absatz 1 des allgemeinen Steuergesetzes *(Ley General Tributaria)* fielen. Seine Entscheidung begründete das Präsidium damit, dass es hierbei um die Wahrung des „vertraulichen Charakters der Daten, Berichte und Aufzeichnungen gehe, die die Steuerbehörden in Ausübung ihrer Aufgaben erhalten"; diese dürften nur unter den unter Buchstabe a bis e von Artikel 113 Absatz 1 des vorgenannten Steuergesetzes genannten Voraussetzungen an Dritte weitergegeben werden, somit beziehe sich der – zweifellos generische – Verweis auf die in dieser Vorschrift definierte „Sphäre der Geheimhaltung" auf ein Verfassungsrecht.

Der Abgeordnete legte gegen diese Entscheidung Berufung ein, worauf das Verfassungsgericht in seiner Entscheidung ausführte, dass der negative Bescheid des Präsidiums an den Kläger mit der generischen Begründung durch eine Gefährdung nicht gerechtfertigt gewesen sei, vielmehr hätte das Präsidium die Steuerbehörden entsprechend bescheiden müssen, nachdem es zuvor unter Berücksichtigung der besonderen Umstände des Falles geprüft hatte, ob eine derartige Gefährdung tatsächlich bestand. Aus den genannten Gründen erkannte das Gericht, dass die in der Berufungsklage angefochtenen Vereinbarungen in der Tat die Rechte des Klägers gemäß Artikel 23 Absatz 2 der spanischen Verfassung – in diesem Fall das Recht auf Ausübung eines öffentlichen Amtes – verletzten, indem sie ihn davon abhielten, die ihm mit Artikel 7 der Verordnung über die Abgeordneten des Kongresses übertragene Befugnis wahrzunehmen, von der Regierung Auskunft zu verlangen.

**2) Entscheidungen des Obersten Gerichts**

Am 26. November 2001 verkündete die Sozialkammer des Obersten Gerichts eine wichtige Entscheidung über die Nutzung der Telekommunikationsmedien eines Unternehmens durch die Gewerkschaften zum Versand von Informationen an Gewerkschaftsmitglieder.

Das Oberste Gericht gab damit der Berufung einer renommierten spanischen Bank, die es der Gewerkschaft untersagt hatte, das interne E-Mail-Netz für Mitteilungen an ihre Mitglieder und die Mitarbeiter der Bank zu nutzen, mit der Begründung statt, dass durch die massive und unkontrollierte Nutzung dieses Mediums die für die Geschäftstätigkeit der Bank notwendige reguläre Kommunikation blockiert wurde.

In dieser ersten Entscheidung des Obersten Gerichts wird die Nutzung von elektronischer Post im Rahmen von Arbeitsbeziehungen untersucht. Aus der Entscheidung lässt sich ableiten, dass nach Auffassung des Obersten Gerichts die in einem Unternehmen vorhandenen Waren und Dienstleistungen dazu dienen, gewisse wirtschaftliche Ergebnisse zu erzielen und die Arbeitnehmer in die Lage zu versetzen, die in ihren Zuständigkeitsbereich fallenden Tätigkeiten auszuführen.

Daneben kann nur durch entsprechende Rechtsvorschriften oder tarifvertragliche Regelungen vereinbart werden, dass diese zu einem anderen als dem angegebenen Zweck genutzt werden, so wie z. B. in den im Organgesetz über die Freiheit der Zugehörigkeit zu einer Gewerkschaft festgelegten Fällen. Jede darüber

hinausreichende Nutzung bedeutet eine einseitige Überinterpretation der spanischen Rechtsvorschriften.

**3) Entscheidungen der Verwaltungsgerichte**

Die Organe der Verwaltungsgerichte sprachen 2001 insgesamt 110 Urteile über Berufungsklagen gegen Entscheidungen des Direktors der Datenschutzbehörde. Dies bedeutet einen Anstieg von 49 % gegenüber dem Vorjahr (mit 54 Entscheidungen). Dennoch wird deutlich, dass die Zunahme der Zahl der Berufungen im Zeitraum 2000-2001 geringer ausfiel als im Zeitraum 1999-2000 (fast 86 %), dem ersten Jahr nach Inkrafttreten des Datenschutzgesetzes.

Bei den Entscheidungen ging es zumeist um folgende Themen: Kredit- und Bonitätsauskünfte, Banken und Versicherungen, Werbe- und Marktforschungsaktivitäten, Berufsverbände, Telekommunikation, elektronischer Geschäftsverkehr und allgemeine Verwaltungsfragen.

Nachstehend eine Reihe besonders wichtiger Entscheidungen:

- *Insolvenz- und Kreditdateien*: Die Entscheidung der Datenschutzbehörde bezüglich der Speicherung unrichtiger Daten in den fraglichen Dateien wurde vom Gericht bestätigt. Die Bank ist verpflichtet, Daten, die an die allgemeine Datei gemeldet werden, zu löschen bzw. zu aktualisieren.

- *Aufnahme von bekannten, jedoch nicht öffentlich zugänglichen Informationen in eine Datenbank ohne Einwilligung der betroffenen Person:* Hierzu wird die Auffassung vertreten, dass die Tatsache, dass personenbezogene Daten bekannt sind, nicht zur Folge hat, dass das Datenschutzgesetz für diese Daten nicht anwendbar ist; daher dürfen die betreffenden Daten (in diesem Fall die Mitgliedschaft einer Person in oder deren Sympathie für eine bestimmte politische Partei) nicht ohne Einwilligung der betroffenen Person per Computer verarbeitet werden. Würden Daten, die allgemein bekannt sind, vom Rechtsschutz ausgenommen, so würden hierdurch gefährliche und weder verfassungsrechtlich noch juristisch haltbare Ausnahmen vom Schutz der Grundrechte geschaffen.

- *Öffentlicher Charakter von Gerichtsverfahren*: In Gerichtsakten und -archiven enthaltene Daten sind in der Definition von „für die Öffentlichkeit zugänglichen Daten“ des spanischen Rechts nicht eingeschlossen. In diesem Fall besteht keine Ausnahme von der in Artikel 6 Absatz 2 des Organgesetzes 5/1992 festgelegten Pflicht zur Einholung der Einwilligung, daher begeht der für die Verarbeitung der Daten Verantwortliche einen schweren Verstoß gegen die Rechtsvorschriften gemäß Artikel 43 Absatz 3 Buchstabe d des Organgesetzes 5/1992, wenn er Daten ohne Einwilligung der Betroffenen gemäß Artikel 6 Absatz 1 des Gesetzes öffentlich zugänglich macht.

- *Versand von Informationen durch Berufsverbände an ihre Mitglieder:* Die Pflichten von Berufsverbänden in Bezug auf den Schutz personenbezogener Daten, wenn die betroffene Person ausdrücklich und wiederholt den Wunsch geäußert hat, kein Werbematerial zu erhalten, müssen strikt ausgelegt werden.

## *D. Spezifische Themen*

### 1) Debatten im Parlament

Die Datenschutzbehörde befasste sich unter anderem mit Beziehungen zwischen den Institutionen. In diesem Zusammenhang trat der Direktor der Datenschutzbehörde 2001 vor Ausschüssen des Parlaments *(Cortes Generales)* auf, um Auskunft zu verschiedenen Fragen zu geben – zweimal vor dem Senatsausschuss zur informations- und wissensbasierten Gesellschaft und ein drittes Mal vor dem Verfassungsausschuss des Kongresses.

Bei seinem ersten Auftreten stand die Analyse von vier Schwerpunktthemen im Mittelpunkt der Ausführungen des Direktors, nämlich die Aktivitäten, mit denen die Behörde darauf hinarbeitet, selbst Teil der Informationsgesellschaft zu werden, eine Untersuchung des Datenschutzrechts im Hinblick auf dessen Anwendbarkeit auf den elektronischen Geschäftsverkehr, die Aktivitäten der Behörde in Bezug auf den elektronischen Geschäftsverkehr und zuletzt die von der Behörde durchgeführte amtliche Überprüfung von „Internet-Shops".

Der zweite Anlass war das Auftreten des Direktors vor der Berichterstattungsgruppe des Senatsausschusses zur informations- und wissensbasierten Gesellschaft zur Untersuchung der Rechte von Teilnehmern und Publikum im Zusammenhang mit Wettbewerben, Spiel- und Wettveranstaltungen. Bei dieser Gelegenheit informierte der Direktor die Gruppe über Strafverfahren im Zusammenhang mit der Verarbeitung von Daten bei Wettbewerben. Auf Zweifel der Senatsmitglieder eingehend sprach sich der Direktor dafür aus, eine amtliche Überprüfung vorzunehmen, um die Einhaltung des Gesetzes in Bezug auf die Verarbeitung der Daten von Teilnehmern und Publikum von Wettbewerbsveranstaltungen zu verifizieren. Die Mitglieder der Gruppe nahmen diesen Vorschlag an, daraufhin führte die Datenschutzbehörde im Jahr 2002 die Überprüfung durch.

Vor dem Verfassungsausschuss des Kongresses erläuterte der Direktor den Bericht der Datenschutzbehörde für das Jahr 2000. Außerdem befragten die Fraktionen des Parlaments den Direktor zu zwei wichtigen Tagesordnungspunkten: zu den Maßnahmen der Datenschutzbehörde in Bezug auf die Pflicht zur Geheimhaltung im Besitz des Staats befindlicher personenbezogener Daten von Angehörigen der Öffentlichkeit und insbesondere von bei der staatlichen Steuerverwaltung *(Agencia Estatal de Administración Tributaria)* gespeicherten Daten und zum Plan der Generaldirektion der spanischen Polizei, im Zusammenhang mit der Bekämpfung der illegalen Einwanderung ein neues Archiv einzurichten.

### 2) Amtliche Kontrollen

Zu den wichtigsten Tätigkeiten der Datenschutzbehörde zählt die Durchführung der Jahrespläne für die Kontrolle bestimmter Wirtschaftszweige. Hierbei werden verschiedene öffentliche und private Sektoren einer Prüfung unterzogen, die mit verbindlichen Auflagen einhergeht, und mit der gewährleistet werden soll, dass die betreffenden Wirtschaftszweige bei der Verarbeitung von Daten die Datenschutzvorschriften einhalten.

Im Jahr 2001 nahm die Datenschutzbehörde Überprüfungen des Clearingkonsortiums für das Versicherungswesen *(Consorcio de Compensación de Seguros)* sowie der

Supermarktbranche und des E-Commerce-Sektors vor und gab entsprechende Empfehlungen ab. Außerdem legte die Behörde einen Bericht mit den Schlussfolgerungen der durchgeführten Überprüfungen im Mobilfunksektor vor.

Weitere Pläne sahen neben der Überprüfung des lokalen Zensus und der Durchführung der Erhebung über Bevölkerung und Wohnungen die Kontrolle der für die Verwaltung des Kfz-Versicherungsarchivs Verantwortlichen, der nationalen Europol-Stelle, des Telebankingsektors sowie der Verantwortlichen für die bedeutendsten Bonitäts- und Kreditarchive vor. Die Schlussfolgerungen und Empfehlungen aus allen genannten Kontrollen sind dem Jahresbericht der Datenschutzbehörde *(Memoria Anual de la Agencia de Protección de Datos)* zu entnehmen.

**3) Verhaltensregeln**
Im Jahr 2001 wurden folgende Verhaltensregeln registriert:

*3.1 Ethikregeln für den Schutz von digital erfassten personenbezogenen Daten in Unternehmen und Berufsverbänden*

Mit der Aufstellung dieses Regelwerks vereinbaren die Beteiligten, in Bezug auf personenbezogene Daten, zu deren Speicherung sie verpflichtet sind, bestimmte proaktive Maßnahmen zu ergreifen, um das Vertrauen der Kunden zu stärken, die ihre Daten übermitteln, die es ihnen ermöglichen sollen, das „TID-Datenschutzsiegel“ zu führen (TID ist das spanische Akronym für computergestützte bzw. digitale Datenverarbeitung). Die Unterzeichner des Regelwerks verpflichten sich unter anderem, personenbezogene Daten über telematische Verbindungen nur mittels sicherer Verbindungssysteme zu erfassen, auf ihren Websites keine Technologien einzusetzen, die dazu genutzt werden könnten, maschinell Informationen über die Besucher der Websites zu extrahieren, ihre Archive nicht für kommerzielle Zwecke zu nutzen und keine Suchmaschinen einzusetzen, die näherungsweise Ergebnisse liefern und dabei dynamisch Aufstellungen personenbezogener Daten generieren.
Daneben wird ein kostenloser Beratungsdienst zu Datenschutzfragen angeboten und ein Datenschutzausschuss eingesetzt, der die Einhaltung der in den Ethikregeln festgesetzten Vereinbarungen entsprechend den Selbstregulierungsbestimmungen überwacht. Der Ausschuss setzt gegebenenfalls die Datenschutzbehörde von Verstößen gegen die im Datenschutzgesetz verankerten Grundsätze in Kenntnis.

*3.2. ACES-Standardkodex*

Bei dem zweiten im Jahr 2001 registrierten Verhaltenskodex handelt es sich um den ACES-Standardkodex des Verbands der katalanischen Gesundheitseinrichtungen *(Agrupació Catalana d’Establiments Sanitaris,* ACES).
Die ACES ist eine privatwirtschaftliche Non-Profit-Organisation mit eigener Rechtspersönlichkeit, in der private Gesundheitszentren und –einrichtungen der Autonomen Region Katalonien zusammengeschlossen sind. Zweck von ACES ist die Beratung und Vertretung ihrer Mitglieder, die Optimierung von Arbeitsmethoden und die Verfolgung allgemeiner Zielsetzungen unter besonderer Berücksichtigung der Förderung der sozialen, tätigkeitsbezogenen, berufsständischen und kulturellen Interessen der Mitglieder.

Hervorzuheben ist, dass mit den nunmehr angenommenen Verhaltensregeln eine einvernehmliche Lösung für alle Fragen und Zweifel gefunden wurde, die von den Mitgliedern im Zuge der Anpassung an die Bestimmungen des Datenschutzgesetzes und der zugehörigen Durchführungsverordnungen in einem – wegen des besonderen Schutzes, den Gesundheitsdaten genießen – sehr sensiblen Sektor aufgeworfen wurden. Die Verhaltensregeln sehen vor, dass die Kosten für die Einhaltung der Rechtsvorschriften von den Mitgliedern gemeinsam getragen werden, sie ermöglichten die Einrichtung eines ACES-einheitlichen Systems für den Schutz personenbezogener Daten und sie sorgen dafür, dass die für den Zugang zu personenbezogenen Daten autorisierten Mitarbeiter über ihre Pflichten, die Bestimmungen des Standardkodex und die Rechtsansprüche und Pflichten im Rahmen des Datenschutzgesetzes unterwiesen werden.

### *E. Website*

www.agpd.es

Die Website steht in spanischer und englischer Sprache zur Verfügung.

## - Schweden

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Zwar ist das Datenschutzgesetz grundsätzlich auf sämtliche Verarbeitungen personenbezogener Daten in allen Bereichen der Gesellschaft anwendbar, doch existieren für einige Bereiche besondere Regelungen. Nachstehend sind einige Beispiele für derartige spezifische Vorschriften dargestellt, die 2001 angenommen wurden. Soweit die spezifischen Vorschriften die unter den Geltungsbereich der Richtlinie 95/46/EG fallende Verarbeitung personenbezogener Daten betreffen, müssen diese den Bestimmungen der Richtlinie entsprechen.

Es wurde ein Paket mit Rechtsvorschriften zu Steuer- und Zollverwaltung, nationaler Registrierung usw. angenommen, das folgende Gesetze umfasst: Gesetz (2001:181) über die Verarbeitung personenbezogener Daten in der Steuerverwaltung der Steuerbehörden, Gesetz (2001:182) über die Verarbeitung personenbezogener Daten im Rahmen der nationalen Registrierungstätigkeit der Steuerbehörden, Gesetz (2001:183) über die Verarbeitung personenbezogener Daten im Rahmen von Wahlen und Volksabstimmungen, Gesetz (2001:184) über die Verarbeitung personenbezogener Daten im Strafverfolgungsdienst und Gesetz (2001:185) über die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeit der Zollbehörden. Diese Gesetze gelten anstelle des Gesetzes über personenbezogene Daten, allerdings beinhalten die genannten Gesetze einen Großteil der Bestimmungen des Gesetzes über personenbezogene Daten. Darüber hinaus enthalten die Gesetze genauere Regelungen z. B. zu Zweck, Inhalt und Weitergabe personenbezogener Daten gegenüber privatrechtlichen Körperschaften oder natürlichen Personen durch automatisierte Medien, zu direktem Zugang, Recherchemöglichkeiten und der Rechte natürlicher Personen usw. In jedem Gesetz ist festgelegt, welche Behörden direkten Zugang zu personenbezogenen Daten in verschiedenen Datenbanken haben. Darüber hinaus bieten die Gesetze der Regierung eine Möglichkeit, natürlichen Personen den direkten Zugang zu bestimmten, sie betreffenden Informationen zu gestatten.

Außerdem haben Betroffene Anspruch auf Berichtigung oder Löschung unzutreffender Daten und auf Schadenersatz.

Ein weiteres 2001 angenommenes Gesetz (2001:454) regelt die Verarbeitung personenbezogener Daten im Bereich der sozialen Dienstleistungen. Das Gesetz, welches das Gesetz über personenbezogene Daten ergänzt, enthält genauere Bestimmungen darüber, in welchen Fällen die Verarbeitung personenbezogener Daten zulässig ist. Es gewährt natürlichen Personen das Recht auf Berichtigung und auf Schadenersatz und überträgt dem Staat bzw. einer vom Staat beauftragten Stellen die Aufgabe, detaillierte Leitlinien für Recherchemöglichkeiten, direkten Zugang und Datenabgleich aufzustellen.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Das Schwedische Parlament nahm 2001 eine neue Rechtsvorschrift zur Verarbeitung personenbezogener Daten bei strafrechtlichen Ermittlungen der Zollbehörden an. Die neue Rechtsvorschrift, welche das Gesetz über personenbezogene Daten ergänzt, enthält genauere Bestimmungen hinsichtlich Zweckbindung, Inhalt und Verarbeitung sensibler Daten sowie zur Weitergabe von Daten. Nachdem die Zollbehörden nunmehr über erweiterte Möglichkeiten zur Verarbeitung personenbezogener Daten verfügen, setzte die Regierung eine Kommission ein, die die Umsetzung der neuen Rechtsvorschrift untersuchen und prüfen soll, ob Änderungen notwendig sind. Die Kommission wird ihren Bericht Ende 2002 vorlegen.

Im Herbst 2001 waren Rechtsvorschriften in Vorbereitung, die das Einfrieren von Geldvermögen ermöglichen sollen. Diese Vorbereitungen wurden allerdings nicht abgeschlossen, da zwischenzeitlich die Verordnung des Rates über spezifische, gegen bestimmte Personen und Organisationen gerichtete restriktive Maßnahmen (angenommen am 27. Dezember 2001) angenommen worden war. Die im Anhang zu der Verordnung enthaltene Liste der Personen, gegen die restriktive Maßnahmen angewandt werden sollten, enthielt die Namen von drei schwedischen Staatsbürgern.

### *C. Wichtige Rechtsprechung*

In Juni 2001 sprach das Oberste Gericht sein erstes Urteil zum Gesetz über personenbezogene Daten. Ein Geschäftsmann hatte auf seiner Website beleidigende Äußerungen über eine große Zahl von Personen aus dem Banken- und Finanzsektor veröffentlicht und nahm für sich in Anspruch, dass das in der Verfassung garantierte Recht auf freie Meinungsäußerung ihm das Recht gebe, diese Informationen im Internet zu veröffentlichen. Vom Stadtgericht Stockholm und dem Berufungsgericht war er deshalb wegen Verstoßes gegen das schwedische Datenschutzrecht verurteilt worden. Das Oberste Gericht gelangte allerdings zu der Auffassung, dass der Zweck der Website, der nach Angaben des Geschäftsmanns darin bestand, auf die von Banken, Finanzinstituten und einzelnen Investoren verursachten Schäden hinzuweisen, durchaus dem journalistischen Zweck der Information, Kritik und Anregung von Diskussionen über gesellschaftliche Fragen von allgemeinem Interesse zuzurechnen sei. Weiter erkannte das Oberste Gericht, dass die Veröffentlichung ausschließlich für den genannten journalistischen Zweck erfolgt sei. Das Oberste Gericht befand daher den Geschäftsmann für eine Verletzung des Gesetzes über

personenbezogene Daten im Sinne von § 7 Absatz 2 und der Ausnahmeregelung für journalistische Zwecke nicht schuldig.

Im November 2001 entschied das Verwaltungsberufungsgericht in einem Fall, in dem es um Kreditinformationen im Internet ging. Eine Kreditauskunftei hatte eine Website in das Internet gestellt, auf der sie Informationen über alle erfassten Fälle nicht bezahlter Forderungen an natürliche und juristische Personen innerhalb der letzten drei Jahre aufführte. Diese Website war den Klienten der Agentur zugänglich, denen Suchmöglichkeiten nach Name und Kennnummer zur Verfügung standen. Die Kreditauskunftei beanspruchte für ihre Darstellung das Grundrecht auf freie Meinungsäußerung und damit eine Ausnahme von den Vorschriften des Kreditinformationsgesetzes, wonach Informationen nur an Personen weitergegeben werden dürfen, die einen berechtigten Bedarf an diesen Informationen nachweisen können. Die Datenschutzkommission befand allerdings, dass es sich bei der Kreditauskunftei nicht um ein Massenmedienunternehmen handelte und daher das Grundrecht auf freie Meinungsäußerung nicht anwendbar sei. Die Datenschutzkommission forderte die Auskunftei daher auf, Abhilfemaßnahmen zu ergreifen. Das Verwaltungsgericht Stockholm war jedoch anderer Auffassung und entschied, dass das Grundrecht auf freie Meinungsäußerung sehr wohl anwendbar sei. In seinem Urteil vom November 2001 bestätigte das Verwaltungsberufungsgericht die Entscheidung des Verwaltungsgerichts. Das Oberste Verwaltungsgericht entschied jetzt, die Berufung zuzulassen, doch stand im November 2002 noch kein Verhandlungstermin fest.

## *D. Spezifische Themen*

Am 1. Oktober 2001 trat das Gesetz über personenbezogene Daten in Schweden in vollem Umfang in Kraft, und das Datengesetz, das während der drei Jahre zuvor provisorisch für Verarbeitungen gegolten hatte, die vor dem 24. Oktober 1998 eingeleitet worden waren, verlor seine Gültigkeit für die automatisierte Verarbeitung personenbezogener Daten. Im Zusammenhang mit dem vollen Inkrafttreten des Gesetzes über personenbezogene Daten verstärkte die Datenschutzkommission ihre Informationstätigkeit nochmals und führte unter anderem zahlreiche Seminare für Datenschutzbeauftragte durch.

Zahlreiche von der Regierung eingesetzte Untersuchungsausschüsse, die im Jahr 2001 ihre Ergebnisse vorlegten, befassten sich mit Datenschutzfragen. Ein Ausschuss hatte den Auftrag, Aufgaben und Tätigkeit der Datenschutzkommission im Hinblick auf das Inkrafttreten des Gesetzes über personenbezogene Daten und das rasche Fortschreiten der Entwicklung in der Informationstechnologie zu überprüfen. Zudem beinhaltete der Auftrag des Ausschusses die Erarbeitung von Vorschlägen für Zielsetzung und Zielrichtung, Umfang und Finanzierung der zukünftigen Tätigkeit der Datenschutzkommission. In seinen im Dezember 2001 vorgetragenen Ergebnissen hob der Ausschuss unter anderem hervor, dass es wichtig sei, dass die Datenschutzkommission ihre Ressourcen auch weiterhin konzentriert für Information und Überwachung einsetze. Weiter vertrat der Ausschuss die Auffassung, dass die Datenschutzkommission künftig Ansätze zur Selbstregulierung verstärkt fördern solle.

Ein weiterer Untersuchungsausschuss befasste sich mit der Verarbeitung personenbezogener Daten im polizeilichen Bereich. Der Ausschuss hatte den Auftrag,

Vorschläge zu erarbeiten, die einen angemessenen Ausgleich zwischen dem Recht der Polizei zum Einsatz moderner Technologien und dem Recht natürlicher Personen auf Schutz ihrer Privatsphäre schaffen sollten. So schlug der Ausschuss unter anderem vor, dass das im Gesetz über personenbezogene Daten enthaltene Verbot der Weitergabe personenbezogener Daten an Drittländer für die polizeiliche Tätigkeit keine Gültigkeit haben solle, was zur Folge hätte, dass nicht geheimhaltungspflichtige personenbezogene Daten im Internet offen gelegt werden könnten. Um die Privatsphäre zu schützen schlug der Ausschuss allerdings vor, Mitteilungen über polizeilich gesuchte Personen nur dann über das Internet zu verschicken, wenn das begangene oder mutmaßlich begangene Verbrechen mit einer Haftstrafe von mindestens zwei Jahren geahndet wird oder die gesuchte Person nach Auffassung der Polizei die öffentliche Sicherheit gefährdet. Darüber hinaus enthält der Bericht des Ausschusses auch Vorschläge für spezifische Vorschriften für die Verarbeitung von Daten über Personen, die keines Verbrechens verdächtig sind, sowie für die Verarbeitung von Daten über DNA-Analysen, Fingerabdrücke usw. im Rahmen von strafrechtlichen Ermittlungen.

Der Untersuchungsausschuss zum Thema „Schutz der Privatsphäre am Arbeitsplatz“ setze seine Tätigkeit 2001 fort.

### *E. Website*

www.datainspektionen.se
Die Website steht in schwedischer und englischer Sprache zur Verfügung.

## - Vereinigtes Königreich

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

Eine Reihe von Initiativen der Regierung im Berichtszeitraum warf schwierige Fragen in Bezug auf den Datenschutz auf. So wurden Vorschläge für eine vermehrte gemeinsame Nutzung von und den ministerienübergreifenden Zugang zu Datenbeständen der Ministerien veröffentlicht (Performance and Innovation Unit Report). Die Datenschutzbehörde war an der Gestaltung dieser Vorschläge maßgeblich beteiligt, was sich in dem Bericht in der Feststellung niederschlug, dass entsprechende Entwicklungen immer mit den notwendigen Maßnahmen zur Wahrung des Datenschutzes einhergehen müssen. Die Regierung überprüfte und änderte die gesetzlichen Bestimmungen für den Verkauf von Wählerverzeichnissen, was eine Einschränkung der Fälle zur Folge hatte, in denen diese Daten für kommerzielle Zwecke genutzt werden dürfen. Diese Änderung der Rechtsvorschriften wurde dadurch beschleunigt, dass eine natürliche Person ein Gerichtsverfahren nach dem Datenschutzgesetz 1998 angestrengt hatte. Während sich die rechtliche Situation durch die Änderungen der Rechtsvorschriften gebessert hat, geben die derzeitige Formulierung und der Stellenwert der Mitteilung an natürliche Personen, mit denen diese Gelegenheit erhalten, sich gegen eine weiter gehende Nutzung auszusprechen („Opt-out“-Verfahren) weiterhin Anlass zur Sorge. Auch die breite Verfügbarkeit weiterer öffentlicher Verzeichnisse wie des Aktionärsverzeichnisses und das Fehlen von Beschränkungen hinsichtlich der möglichen Nutzung dieser Informationen stoßen bei der Datenschutzbehörde auf schwer wiegende Bedenken.

## *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

Die Regierung erarbeitete eine Reihe von Gesetzesvorlagen zum Thema Verbrechen und Kriminalität, die vielfach ernste datenschutzrechtliche Fragen aufwarfen, zu denen die Datenschutzbehörde Stellung nahm. Unter den Vorschlägen waren ein Gesetzentwurf zum Erlös aus Straftaten, Novellierungen des Gesetzes zur Resozialisierung von Straftätern und des Gesetzes über Sexualstraftäter, Verhaltensregeln für den Zugang zu Kommunikationsdaten nach Maßgabe der Regelungen im Gesetz über Ermittlungsbefugnisse, Verordnungen zur Bekämpfung der Geldwäsche sowie ein Sicherheitsgesetz zur Terrorismusbekämpfung. Diese letztgenannte Rechtsvorschrift bereitet unter Datenschutzaspekten die größten Sorgen. Sie sieht nicht nur den Abbau von Barrieren für den Austausch von Informationen unter öffentlichen Organen vor, sondern erweitert die Speicherungsmöglichkeit von Telefon-, Internet- und anderen Kommunikationsdaten durch die Betreiber über deren eigene gewerbliche Nutzung hinaus und erleichtert zahlreichen Strafverfolgungsorganen den Zugang für ein breites Spektrum von strafrechtlichen Ermittlungszwecken, die weit über die Bekämpfung des Terrorismus hinausgehen.

Zu den herausragenden proaktiven Initiativen des Jahres 2001 zählt die Weiterführung der Entwicklung eines Verhaltenskodex der Datenschutzbehörde zu Beschäftigungspraktiken. Darüber hinaus veröffentlichte die Behörde Leitlinien für den Gesundheitssektor, die dazu dienen sollen, die datenschutzrechtlichen Anforderungen in einem Bereich klarzustellen, in dem der Druck zur Weitergabe von Patientendaten zunimmt und in dem hinsichtlich der bestehenden ethischen und rechtlichen Anforderungen allgemeine Verwirrung besteht.

## *C. Wichtige Rechtsprechung*

Die Datenschutzbehörde befasste sich mit 12 479 Beurteilungsanträgen, von denen sich 2 588 auf die Telekommunikationsverordnungen bezogen. In 13,8 % aller Fälle gelangte die Behörde zu dem Befund, dass die Regelungen den Rechtsvorschriften eher nicht entsprachen. Außerdem stellte die Behörde in 66 Fällen von Verstößen gegen das Datenschutzgesetz Strafantrag.

Im Jahr 2001 wurden Urteile zu sehr unterschiedlichen Fällen gesprochen, wobei es nur in einigen Fällen konkret um den Datenschutz ging, während in der Mehrzahl der Fälle in anderem Zusammenhang auf das Datenschutzgesetz, die Richtlinie 95/46/EG und das Übereinkommen 108 und die Auslegung von Artikel 8 der europäischen Menschenrechtskonvention Bezug genommen wurde. Im Fall Naomi Campbell gegen Mirror Group Newspapers wurde auf die Empfehlung 1/97 der Artikel-29-Datenschutzgruppe verwiesen, die sich mit Datenschutz und Medien befasst. In folgenden weiteren Fällen befassten sich die Gerichte mit verschiedenen Aspekten der Auslegung des Datenschutzgesetzes 1998:

**Norman Baker MP gegen den Secretary of State for the Home Department (Innenminister) – Information Tribunal (National Security Appeals) (1. Oktober 2001).**
In diesem ersten Fall, den das Tribunal zu verhandeln hatte, wurde eine vom Innenminister ausgestelltes Bescheinigung für nichtig erklärt, mit der das Recht des

Betroffenen auf Zugang aus Gründen der Verletzung der nationalen Sicherheit eingeschränkt wurde.

**R gegen City of Wakefield Metropolitan Council und andere ex parte Robertson – High Court (16. November 2001).**
In dem Fall, der die Verwendung des Wählerverzeichnisses zu gewerblichen Zwecken betraf, erkannte das Gericht, dass die geltenden Regelungen gegen das Datenschutzgesetz und das Gesetz über die Menschenrechte verstießen.

**Totalise plc gegen Motley Fool und andere – Court of Appeal (19. Dezember 2001).**
Der Fall betraf den Antrag eines Website-Betreibers auf Weitergabe von Informationen eines Teilnehmers zwecks Anstrengung einer Verleumdungsklage. Das Gericht leistete einen wertvollen Beitrag zur Auslegung der Anwendbarkeit von § 35 des Datenschutzgesetzes in Bezug auf die Weitergabe an potenzielle Prozessparteien.

## *D. Spezifische Themen*

Ausführliche Angaben zu den genannten und weiteren interessanten Fällen sowie sämtliche Informationen zur Tätigkeit der Datenschutzbehörde enthält die Website der Datenschutzbeauftragten unter

## *E. Website*

www.informationcommissioner.gov.uk

# 1.5. Aktivitäten der Europäischen Union und der Gemeinschaft

## 1.5.1. Verordnung zum Datenschutz in Organen und Einrichtungen der Gemeinschaft

Nach der Annahme der Verordnung (EG) Nr.45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr[18] legte die Kommission am 18.7.2001 einen Vorschlag für einen Beschluss des Europäischen Parlaments, des Rates und der Kommission über die Regelungen und allgemeinen Bedingungen für die Ausübung der Aufgaben des Europäischen Datenschutzbeauftragten[19] vor. Dieser Vorschlag betrifft zwei wesentliche Aspekte, die im Hinblick auf die Ernennung des Datenschutzbeauftragten und des stellvertretenden Datenschutzbeauftragten definiert werden müssen, da sie in der Verordnung nicht enthalten sind: die Bezüge des Europäischen Datenschutzbeauftragten und seines Stellvertreters und den Sitz dieses Organs.

Die Kommission schlug vor, dass der Europäische Datenschutzbeauftragte hinsichtlich seiner Bezüge einem Richter des Europäischen Gerichtshofs gleichgestellt werden sollte und der stellvertretende Datenschutzbeauftragte dem Kanzler des Gerichthofs. Als Sitz der Behörde wurde Brüssel vorgeschlagen.

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

Der im Juli 2000 durch den Vorschlag der Kommission für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation[20] angestoßene Rechtsetzungsprozess dauerte 2001 weiter an. Der Vorschlag ist Teil des Reformpakets für den Telekommunikationssektor, das verschiedene Vorschläge zur Anpassung des ordnungspolitischen Rahmens an die Anforderungen von Wettbewerb und Konvergenz enthält.

Der Entwurf für die Richtlinie zum Schutz der Privatsphäre soll die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation ablösen. Der Entwurf verfolgt das Ziel einer einheitlichen Regulierung ein und derselben Dienstleistung, unabhängig von dem Medium, mit dem sie erbracht wird.

---

18 ABl. L 8 vom 12.1.2001, S. 1.

19 ABl. C 304 E vom 30.10.2001, S. 178.

20 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 vorgeschlagenen Änderungen betreffen Begriffsbestimmungen und Terminologie (wodurch unter anderem bestätigt werden soll, dass die Richtlinie auch auf die Erbringung von E-Mail-Dienstleistungen anwendbar ist), Verkehrsdaten (um klarzustellen, dass auch Internet-Verkehrsdaten einbezogen sind), Standortdaten (Freigabe der Nutzung von Standortdaten für die Erbringung von Mehrwertdiensten mit Einwilligung des Nutzers), Verzeichnisse (freie Wahlmöglichkeit der Nutzer im Hinblick auf ihre Aufnahme und die Form ihrer Aufnahme in Telefon, Mobilfunk- und E-Mail-Verzeichnisse), unerwünschte Kommunikationen (Harmonisierung einzelstaatlicher Vorschriften durch Festschreibung der Forderung nach vorheriger Einwilligung der Empfänger von Marketingmitteilungen per E-Mail) sowie die Einhaltung der Bestimmungen zum Schutz der Privatsphäre bei der für elektronische Kommunikationsdienstleistungen genutzten Hard- und Software.

### 1.5.3. Standardisierung

Die im Auftrag der Europäischen Kommission von CEN/ISSS gegründete Initiative for Privacy Standardization in Europe (IPSE) (Initiative für die Standardisierung im Bereich des Schutzes der Privatsphäre) verfolgt im Wesentlichen zwei Ziele:

Erstens die Ermittlung von Standardisierungsmöglichkeiten als ein Mittel, um Unternehmen und andere Marktteilnehmer bei der Umsetzung der maßgeblichen Rechtsvorschriften, insbesondere der EU-Richtlinie zum Schutz personenbezogener Daten, zu unterstützen.
Zweitens – und wenn solche Möglichkeiten ermittelt werden – die Festlegung der spezifischen Anforderungen in einer Reihe von Empfehlungen auf der Grundlage einer „Pro und Contra"-Analyse und die Bestimmung der Realisierungsmöglichkeiten.

Die Teilnehmer der CEN/ISSS „Initiative on Privacy Standardisation in Europe" waren 2001 intensiv mit der Ausarbeitung eines Berichts befasst, der am 13. Februar 2002 veröffentlicht wurde. An den vorbereitenden Gesprächen zu diesem Bericht waren sowohl die Europäische Kommission als auch die Datenschutzgruppe beteiligt.

### 1.5.4 Beschäftigungsinitiative

Am 27. August 2001 leitete die Europäische Kommission die erste Stufe der Anhörung der Sozialpartner zum Schutz der personenbezogenen Daten von Arbeitnehmern ein, bei der die Beteiligten um ihre Meinung zu möglichen Aktionen der Gemeinschaft auf diesem Gebiet gefragt wurden.

Dabei ging es insbesondere um die Frage, ob die Sozialpartner Aktionen der Gemeinschaft zu den Themenschwerpunkten Einwilligung, Zugang und Verarbeitung medizinischer Daten im Kontext von Arbeitsverhältnissen, Drogentest und genetische Tests in der Arbeitswelt sowie Beobachtung und Überwachung am Arbeitsplatz für sinnvoll halten.

Aus den Antworten der Beteiligten wird eine eindeutige Divergenz zwischen den Arbeitgeberorganisationen einerseits und den Arbeitnehmerorganisationen andererseits ersichtlich. Während erstere generell keinen Bedarf an weiteren Rechtsvorschriften zum Datenschutz sehen, sprach sich die Arbeitnehmerseite mit

dem Argument für eine Gemeinschaftsrichtlinie zu diesem Thema aus, dass die bestehenden Richtlinien zwar durchaus nützlich, jedoch nicht hinreichend spezifisch auf den Beschäftigungskontext ausgerichtet seien.

### 1.5.5. Europol/Schengen + Eurojust

***Eurojust***

Der Europäische Rat von Tampere, Finnland, beschloss 1999 die Errichtung von Eurojust. In Artikel 31 des Vertrags über die Europäische Union in der geänderten Fassung des Vertrags von Nizza wurde ein Verweis auf Eurojust aufgenommen. Im Laufe des Jahres 2000 wurden zwei Vorschläge für einen Beschluss zur Errichtung von Eurojust vorgelegt, von denen der eine von Deutschland eingebracht worden war, während der andere von den vier Mitgliedstaaten, die in den Jahren 2000 und 2001 den Ratsvorsitz der Europäischen Union führten (Portugal, Frankreich, Schweden und Belgien), gemeinsam erarbeitet wurde.

Am 28. Februar 2002 nahm der Rat der Europäischen Union den Beschluss zur Errichtung von Eurojust an, der zahlreiche Bestimmungen zum Schutz von verarbeiteten personenbezogenen Daten enthält.

### 1.5.6. Internet und Telekommunikation (Gesundheits-Websites, ICANN „Whois"-Umfrage, Meldeverfahren 98/34/EG)

ICANN führte 2001 eine Anhörung zu den so genannten „Whois"-Verzeichnissen durch. Die Grundlage für diese Anhörung bildete eine Umfrage mit der Bezeichnung „DNSO Names Council Whois Survey", die interessierten Parteien die Möglichkeit bot, während eines Zeitraums, der am 14. August 2001 endete, Stellungnahmen abzugeben.

Die Europäische Kommission forderte die Mitglieder der Datenschutzgruppe dazu auf, sich an dieser Umfrage zu beteiligen und sammelte Stellungnahmen verschiedener Delegationen zu dem Thema. Im Anschluss daran legte die Kommission ein Arbeitspapier (Working Paper of the European Kommission, ICANN DNSO Whois Survey: Issues for consideration, vom 8. November 2001) vor, in das die Stellungnahmen der Mitglieder der Datenschutzgruppe und der verschiedenen beteiligten Kommissionsdienststellen einflossen.

In ihrem Papier hob die Kommission die praktischen und rechtlichen Schwierigkeiten hervor, die sich aus einem Interessenkonflikt zwischen den Anforderungen der Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre einerseits und dem von weiten Kreisen bekundeten Interesse an vermehrter Standardisierung, Transparenz und weltweiter Einheitlichkeit bei Verfügbarkeit und Verwendung von Identifizierungsdaten durch Whois ergeben. Dieser Themenkomplex wird im Kontext mehrerer untereinander zusammenhängender Politikfelder deutlich:

- Welche Kategorien der für die Zwecke der Registrierung von Domain-Bezeichnungen erhobenen Daten sollten öffentlich verfügbar sein und zu welchen Zwecken?

- Sind die Daten zutreffend, zuverlässig und aktuell? Es gibt Anzeichen dafür, dass dies nicht immer der Fall ist. Fehler, egal ob sie nun versehentlich oder absichtlich verursacht werden, sprechen gegen eine autorisierte Verwendung der Daten.

- Stehen Zweck und Verwendung von Registrierungsdaten, einschließlich der grenzüberschreitenden Weitergabe von Daten, mit den nationalen Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre im Einklang? ICANN ist verpflichtet, bei seinen Maßnahmen und Aktivitäten den geltenden lokalen und internationalen Rechtsvorschriften Rechnung zu tragen. Im Prinzip schließt diese Pflicht auch Register und Registrierungsstellen ein, die vertraglich an ICANN gebunden sind, und sollte ggf. auch in den vertraglichen Vereinbarungen mit diesen Stellen zum Ausdruck kommen.

- Zu welchen genau definierten Zwecken werden die Daten erhoben und wie können sie von der Öffentlichkeit verwendet werden? Diese Fragen sind nicht allein Gegenstand technischer und administrativer Vereinbarungen, sondern auch Gegenstand nationaler Rechtsvorschriften.

- Wurden die betroffenen Personen informiert und/oder haben sie ihre Einwilligung für die Zwecke gegeben, für die ihre Daten verarbeitet werden können oder können berechtigte Gründe für die Verarbeitung geltend gemacht werden?

Im europäischen Kontext treten all die genannten Fragen im Zusammenhang mit der Anwendung der EU-Richtlinie über den Datenschutz und den Schutz der Privatsphäre auf die Tätigkeiten von DNS-Verzeichnissen und den Verantwortlichen solcher Verzeichnisse auf. Vor diesem Hintergrund kommt es insbesondere darauf an, die Anforderungen der Transparenz für bestimmte vereinbarte Zwecke und die Anforderungen des Schutzes der Privatsphäre in ein ausgewogenes Verhältnis zu setzen.

Speziell unter Bezugnahme auf die ICANN DNSO-Umfrage hob die Kommission zwei generelle Fragen hervor, die von ICANN beantwortet werden müssen:

a) Welche Zielsetzung wird mit dem Whois-Suchsystem verfolgt?

b) Unter welchen Voraussetzungen können in der EU erhobene personenbezogene Daten in die USA weitergegeben werden?

## 1.5.7. Medizinische und genetische Daten

***Fiori-Bericht***

Das Europäische Parlament lehnte im November 2001 den Entschließungstext des Fiori-Berichts ab, der von dem mit der Untersuchung der „Auswirkungen neuer medizinischer und genetischer Technologien“ beauftragten nichtständigen Ausschuss vorgelegt worden war.

# 2. EUROPARAT

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

Das Zusatzprotokoll zum Übereinkommen SEV Nr. 108 über die Tätigkeit von Kontrollorganen und internationale Datenströme wurde vom Ministerkomitee angenommen und am 8. November 2001 zur Unterzeichnung durch die Mitgliedstaaten freigegeben. In derselben Sitzung nahm das Ministerkomitee auch das Übereinkommen über die Cyberkriminalität (SEV Nr. 185) an, das in der Folge zur Unterzeichnung am 23. November 2001 in Budapest freigegeben wurde.

Im Laufe des Jahres 2001 ratifizierten vier weitere Europarat-Mitgliedstaaten das Übereinkommen 108. Anlässlich des 20. Jahrestags der Unterzeichnung dieses Übereinkommens fand am 19./20. November 2001 in Warschau eine europäische Datenschutzkonferenz zum Thema „Übereinkommen 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten: Gegenwart und Zukunft“ statt.

Der Beratende Ausschuss (T-PD) für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 108) setzte seine Arbeit an einem Leitfaden für die Ausarbeitung von Vertragsklauseln über den Datenschutz bei der Weitergabe personenbezogener Daten an Dritte, die nicht an ein angemessenes Datenschutzniveau gebunden sind, fort. Die Projektgruppe Datenschutz (CJ-PD) führte ihre Beratungen über Leitlinien für den Schutz natürlicher Personen bei der Erhebung und Verarbeitung von Daten mittels Videoüberwachung fort. Nach der Annahme durch die Projektgruppe genehmigte der Europäische Ausschuss zur Zusammenarbeit in Rechtsfragen (CD-CJ) den Entwurf für eine Empfehlung zum Schutz personenbezogener Daten, die für Versicherungszwecke erfasst und verarbeitet werden, und leitete die Empfehlung zur Genehmigung an das Ministerkomitee weiter.

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

### - Island

Am 1. Januar 2001 trat das Gesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Nr. 77/2000 in Kraft, welches das Gesetz über die Erfassung personenbezogener Daten Nr. 121/1989 ablöst. Mit dem neuen Gesetz wurde die Richtlinie 95/46/EG umgesetzt. Es sieht die Einsetzung einer unabhängigen staatlichen Datenschutzbehörde (Personuvernd, Website: www.personuvernd.is) mit einem fünfköpfigen Vorstand vor. Entsprechend dem Gesetz übernahm Personuvernd die Aufgaben der vormaligen Datenschutzkommission. An der Spitze der Datenschutzbehörde steht derzeit die Datenschutzkommissarin Sigrún Jóhannesdóttir.

Hauptaufgabe der Datenschutzbehörde im ersten Jahr ihrer Tätigkeit war es, das neue Gesetz und die dadurch bedingten Änderungen publik zu machen. Hierzu wurden Plakate und Broschüren erstellt und Seminare und Vorträge gehalten. Eine weitere wichtige Aufgabe bestand im Aufbau der neuen Einrichtung und der Ausarbeitung der Regelungen für ihre Tätigkeit. In diesem Sinne wurden die Verwaltungsvorschriften für die Meldung und vorherige Überprüfung von Datenverarbeitungen (Nr. 90/2001) verabschiedet, außerdem Vorschriften über Sicherheitsverfahren (Nr. 299/2001), Vorschriften über die Einholung der in Kenntnis der Sachlage gegebenen Einwilligung zur Verarbeitung personenbezogener Daten für wissenschaftliche Zwecke (Nr. 170/2001), Vorschriften über die Sicherheit personenbezogener Daten in Biobanken (Nr. 918/2001) sowie Leitlinien für Unternehmer für die Überwachung der Nutzung von Computern und Internet durch ihre Mitarbeiter (Nr. 1001/2001). Daneben wurde mit der Ausarbeitung von Sicherheitsstandards für die zentrale Datenbank für den Gesundheitssektor gemäß Artikel 2 des Gesetzes Nr. 139/1998 über eine Datenbank für den isländischen Gesundheitssektor begonnen.

Neben den vorgenannten traten 2001 verschiedene weitere Legislativmaßnahmen mit Bezug zur Verarbeitung personenbezogener Daten in Kraft. Die wichtigsten diesbezüglichen Rechtsakte:

1. Gesetz Nr. 90/2001. Mit diesem Gesetz wurde das Gesetz über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten Nr. 77/2000 geändert. Erstens wurden zusätzliche Bestimmungen über die Einhaltung von Beschlüssen des Ausschusses nach Artikel 25 der Richtlinie 95/46/EG aufgenommen. Zweitens wurden die Bestimmungen von Artikel 4 der Richtlinie über die Anwendbarkeit einzelstaatlichen Rechts ausführlicher formuliert. Drittens wurden die Bestimmungen über die Sicherheit personenbezogener Daten geändert, um sie verständlicher zu machen und den Bestimmungen der Richtlinie, insbesondere der Artikel 16 und 17, besser Rechnung zu tragen. Als letzter Punkt wurde eine Bestimmung aufgenommen, die die Einhaltung von Artikel 14 der Richtlinie über das Widerspruchsrecht der betroffenen Person gewährleisten soll.

2. Gesetz über Biobanken Nr. 110/2000. Mit dem Gesetz wird ein Rechtsrahmen für den Aufbau und den Betrieb von Biobanken, also „Banken“, die biologische Proben von Menschen enthalten, aufgestellt. Entsprechend dem Gesetz legt die Datenschutzbehörde die Sicherheitsmaßnahmen fest, die von den Biobanken eingehalten werden müssen. Die Datenschutzbehörde hat bereits Vorschriften für die Sicherheit personenbezogener Daten bei der Verarbeitung und Aufbewahrung biologischer Proben in derartigen Biobanken erlassen.

3. Gesetz über elektronische Signaturen Nr. 28/2001. Mit diesem Gesetz wurde die Richtlinie 99/93/EG über einen gemeinschaftlichen Rahmen für elektronische Signaturen umgesetzt. Mit dem Gesetz wird die Verarbeitung personenbezogener Daten im Zusammenhang mit elektronischen Signaturen der Zuständigkeit der Datenschutzbehörde unterstellt.

4. Gesetz Nr. 29/2001. Dieses Gesetz ändert die Bestimmungen des Telekommunikationsgesetzes Nr. 107/1999 über das Verbot der Aufzeichnung von Telefongesprächen durch Gesprächsteilnehmer ohne Wissen des Gesprächspartners. Hier wurden zwei Ausnahmen zugelassen, die nach Auffassung des Gesetzgebers mit Artikel 5 der Richtlinie 97/66/EG vereinbar sind. Die erste Ausnahme betrifft Fälle, in denen mit Sicherheit davon auszugehen ist, dass dem Gesprächspartner bewusst ist, dass das Gespräch aufgezeichnet wird. Die zweite betrifft Fälle, in denen die Aufzeichnung von Gesprächen als Teil der üblichen Verfahrensweise einer Verwaltungsbehörde zu betrachten und für die nationale und die öffentliche Sicherheit notwendig ist, vorausgesetzt, die Umstände der Aufzeichnung entsprechen den Auflagen der Datenschutzbehörde.

5. Gesetz über das Verzeichnis genetischer Daten der Polizei Nr. 88/2001. Dieses Gesetz überträgt dem Datenschutzbeauftragten der isländischen Polizeibehörde die Verantwortung für ein digitales Verzeichnis genetischer Daten. Das Verzeichnis soll die Ermittlungen bei schweren Straftatbeständen wie Mord, Vergewaltigung, Körperverletzung und sexuellem Missbrauch von Kindern erleichtern. Maßgeblich für die Verarbeitung der Daten ist das Gesetz Nr. 77/2000, die Verarbeitung unterliegt der Aufsicht der Datenschutzbehörde.

6. Verordnung über die Erhebung und Verbreitung von Daten über finanzielle Angelegenheiten und Kreditwürdigkeit Nr. 246/2001. Diese Verwaltungsverordnung wurde vom Justizminister entsprechend einer Bestimmung im Gesetz Nr. 77/2000 angenommen. Sie regelt die Verarbeitung von Daten über finanzielle Angelegenheiten sowohl natürlicher als auch juristischer Personen. Nach Maßgabe der Verordnung wird für die Verarbeitung entsprechender Daten eine Genehmigung der Datenschutzbehörde benötigt, wenn diese zur Weitergabe an Dritte bestimmt sind.

7. Verordnung über die Verarbeitung von Daten für polizeiliche Zwecke Nr. 322/2001. Diese Verwaltungsverordnung wurde vom Justizminister entsprechend den Bestimmungen der Strafprozessordnung Nr. 19/1991, des Polizeigesetzes Nr. 90/1996 und des Gesetzes Nr. 77/2000 angenommen. Die Verordnung überträgt der Datenschutzbehörde verschiedene Aufgaben bei der Überwachung der Datenverarbeitung für polizeiliche Zwecke.

## - Norwegen

Die norwegische Datenschutzbehörde befasste sich 2001 vorrangig mit folgenden Aufgaben:

- Exekutiven Tätigkeiten und Anhörungen
- Anpassung an das Gesetz über personenbezogene Daten 2000
- Entwicklung und Durchsetzung von neuen Verfahren zur Durchführung von Kontrollen
- Management von Informationsressourcen einschließlich beratender Tätigkeiten und Seminarveranstaltungen
- Entwicklung von Selbstregulierungsmaßnahmen in verschiedenen Wirtschaftszweigen

Zu den Hauptaufgaben der Datenschutzbehörde zählen: die Bearbeitung von Anträgen auf Genehmigung der Verarbeitung sensibler personenbezogener Daten, die Erstellung einer systematischen, öffentlich zugänglichen Aufstellung der Meldungen über die Verarbeitung nicht-sensibler personenbezogener Daten, die vermehrte Durchführung von Kontrollen sowie die Beratung und Betreuung von Leitlinien zu Sachverhalten, die für den Schutz der Privatsphäre von Belang sind. Die Datenschutzbehörde soll auch an der Errichtung von ergänzenden Systemen zum Schutz der Privatsphäre in der Privatwirtschaft und in der öffentlichen Verwaltung nach Maßgabe von Artikel 18 Absatz 2 der Richtlinie 95/46/EG mitwirken. Die Aktivitäten zur Einsetzung von Datenschutzbeauftragten und zur Entwicklung von Selbstregulierungsbestimmungen für die Verarbeitung personenbezogener Daten in verschiedenen Wirtschaftszweigen stehen noch relativ am Anfang.

Die Übergangsregelungen brachten 2001 Arbeiten mit Bezug sowohl zu dem neuen Gesetz als auch zum bisher geltenden Gesetz über den Schutz der Privatsphäre und personenbezogener Daten mit sich. Die Datenschutzbehörde erteilte 2001 drei Genehmigungen nach dem bisherigen Gesetz und 163 Genehmigungen nach dem jetzt geltenden Gesetz. Die Übergangsfrist endet am 1. Januar 2003.

2001 gingen bei der Datenschutzbehörde 2494 Meldungen ein, die überwiegend wissenschaftliche Studien betrafen.

Die Beschwerdekammer gab im November 2001 ihre erste Entscheidung bekannt. Eine natürliche Person hatte die Datenschutzbehörde um Hilfestellung in Bezug auf die Löschung von Informationen aus dem Zugangskontrollsystem ihres Arbeitgebers ersucht. Die Daten waren mit einer Vereinbarung gekoppelt, die der Betroffene im Zusammenhang mit seinem Ausscheiden aus dem Unternehmen mit dem Arbeitgeber getroffen hatte. Die Beschwerdekammer bestätigte die Entscheidung der Datenschutzbehörde, dass die betreffenden Daten nicht gelöscht werden mussten.

### *A. Angenommene legislative Maßnahmen im Bereich der ersten Säule*

**Gesetz (2000-04-14 Nr. 31) über personenbezogene Daten** und Verordnungen – in Kraft getreten am 1. Januar 2001. Mit dem Gesetz wurde die Richtlinie 95/46/EG umgesetzt; es tritt an die Stelle älterer Rechtsvorschriften zu diesem Thema. Das neue Gesetz hebt das Recht natürlicher Personen auf Einwilligung zu bzw. Widerspruch gegen verschiedene Formen der Verarbeitung personenbezogener Daten hervor. Nach

einer Meldung an die Datenschutzbehörde können verschiedene Arten der Verarbeitung personenbezogener Daten erfolgen. Für die Verarbeitung sensibler personenbezogener Daten ist allerdings weiterhin eine Genehmigung erforderlich.

**Gesetz (2001-05-18 Nr. 24) über Systeme zur Archivierung personenbezogener Gesundheitsdaten und die Verarbeitung personenbezogener Gesundheitsdaten**
Das Gesetz, das am 1. Januar 2002 in Kraft tritt, bezieht sich auf die ganz oder teilweise automatisierte Verarbeitung personenbezogener Gesundheitsdaten in der öffentlichen Gesundheitsverwaltung und öffentlichen Gesundheitsdiensten. Das Gesetz geht von den gleichen Grundsätzen aus wie das Gesetz über personenbezogene Daten und verlangt somit als Voraussetzung für die Verarbeitung grundsätzlich die Einwilligung der betroffenen Person.

**Gesetzesvorlage zu Biobanken**
Die Datenschutzbehörde wies darauf hin, dass die Gesetzesvorlage nicht mit den wesentlichen Grundsätzen des Gesetzes über personenbezogene Daten und des Gesetzes über Systeme zur Archivierung personenbezogener Gesundheitsdaten im Einklang stehe, da es nicht die gleichen Anforderungen in Bezug auf die Information und die Form der Einwilligung der betroffenen Personen beinhalte.

### *B. Durchgeführte Änderungen im Bereich der zweiten und dritten Säule*

**Gesetz (1999-07-16 Nr. 66) über das Schengener Informationssystem** (SIS) und Verordnungen – in Kraft getreten am 1. Januar 2001. Mit dem Gesetz wird das SIS-Übereinkommen umgesetzt, es enthält die maßgeblichen Regelungen für die norwegische Abteilung des Verzeichnisses.

### *C. Wichtige Rechtsprechung*

**Ablaufprotokoll**
Ein Arbeitnehmer wurde wegen Herunterladens von umfangreichen MP3-Dateien aus dem Internet mithilfe der Computeranlagen an seinem Arbeitsplatz während der Arbeitszeit entlassen. Er verklagte daraufhin seinen ehemaligen Arbeitgeber wegen unfairer Entlassung, das Oberste Gericht schloss sich jedoch der Auffassung des Arbeitgebers an. Es stellte fest, dass das Unternehmen für die Nutzung seiner Geräte Einschränkungen verhängt hatte, die allen Mitarbeitern bekannt waren. Außerdem wurde hervorgehoben, dass aufgrund seiner Position bei der Verwaltung der Geräte vorausgesetzt werden konnte, dass dem Arbeitnehmer das System genau bekannt war und ihm deshalb auch bewusst war, welchen Schaden Downloads von umfangreichen MP3-Dateien verursachen würden. Der Arbeitgeber ermittelte anhand des Ablaufprotokolls, wer das System missbräuchlich verwendete. Das Gericht entschied, dass die Verwendung des Protokolls durch den Arbeitgeber in den Bereich der in den Bestimmungen des Gesetzes über personenbezogene Daten festgelegten Zwecke fiel und die Entlassung des Arbeitnehmers somit nicht unfair war.

**Videoüberwachung**
Ein Arbeitgeber überwachte sein Ladengeschäft wegen des Verdachts der Veruntreuung gegen einen seiner Mitarbeiter. Weder die Kunden noch die Beschäftigten waren – wie in § 40 des Gesetzes über personenbezogene Daten

vorgeschrieben – über die Videoüberwachung informiert. Das Oberste Gericht sprach den Arbeitgeber schuldig.

## *D. Spezifische Themen*

### 1. Schutz der Privatsphäre nach den Ereignissen des 11. September

Das letzte Vierteljahr des Jahres 2001 wurde von den dramatischen Ereignissen des 11. September in New York überschattet.
Es wurden verschiedene Vorschläge für das Vorgehen bei der Bekämpfung des Terrorismus eingebracht, von denen viele, wenn sie angenommen würden, in der einen oder anderen Weise Auswirkungen auf das Recht auf Schutz der Privatsphäre hätten. Das Recht auf Schutz der Privatsphäre und der Kampf gegen den Terror haben durchaus beide ihre Berechtigung, doch lassen sie sich nicht ohne weiteres vereinbaren. Auf die Datenschutzbehörde kommt mit der Beurteilung der verschiedenen nach dem 11. September vorgeschlagenen Initiativen, die nicht immer mit den in der Richtlinie 95/46/EG formulierten Grundsätzen und damit auch mit dem Gesetz über personenbezogene Daten 2000 in Einklang stehen, beträchtliches Maß an Mehrarbeit zu, wobei die Initiativen ihren Ursprung sowohl in Norwegen als im Ausland haben.

Die Datenschutzbehörde stellte in einer Übersicht zusammen, welche grundsätzlichen Anforderungen erfüllt sein müssen, damit eine Initiative mit dem geltenden Gesetz über personenbezogene Daten und somit mit dem Recht auf Schutz der Privatsphäre vereinbar ist:

- Die Initiative muss auf einer gesetzlichen Bestimmung beruhen und in einer solchen Bestimmung beschrieben sein.
- Die Initiative muss dem Grundsatz der Verhältnismäßigkeit entsprechen, d. h. die Mittel müssen zum Zweck in einem angemessenen Verhältnis stehen.
- Die Grenzen zwischen Ermittlung und Überwachung müssen klar erkennbar sein.
- Es darf ohne gerichtliche Entscheidung nicht möglich sein, personenbezogene Daten, die für einen bestimmten Zweck erhoben wurden, für einen anderen Zweck zu verwenden. Dieser Grundsatz muss auch bei Informationsüberschuss angewandt werden.
- Datenarchive mit personenbezogenen Daten dürfen nur mit Einwilligung der Betroffenen errichtet werden.

Bei einer solchen Beurteilung sind jedoch in jedem Fall die Grundsätze von Artikel 8 der Menschenrechtskonvention zu beachten.

### 2. Dauerhafte oder verlängerte Speicherung von Verkehrsdaten

Die *Nationale Behörde für die Untersuchung und strafrechtliche Verfolgung von Wirtschafts- und Umweltstraftaten in Norwegen* stellte fest, dass der uneingeschränkte Zugang zu Verkehrsdaten für die norwegische Polizei unverzichtbar sei. Nach Auffassung der Behörde müssen derartige Daten vom Telekommunikationsbetreiber mindestens ein Jahr gespeichert werden. Die Datenschutzbehörde vertrat demgegenüber ausdrücklich den Standpunkt, dass personenbezogene Daten, die für einen bestimmten Zweck erhoben werden, grundsätzlich nicht für einen anderen Zweck verwendet werden und insbesondere nicht gespeichert werden dürfen, wenn

sie für den ursprünglichen Zweck nicht benötigt werden, sondern zu einem späteren Zeitpunkt und für einen anderen als den ursprünglichen Zweck von Nutzen sein könnten.

### 3. Personenbezogene Gesundheitsdaten

*Nationale DNA-Datenbank und Verarbeitung genetischer Daten*
Im vergangenen Jahr machte die Staatsanwaltschaft einen Vorschlag zur Errichtung einer nationalen Datenbank, in der die DNA-Profile der gesamten norwegischen Bevölkerung gespeichert werden sollten. Ihrer Auffassung nach würde eine solche Datenbank in Kriminalfällen wertvolle Hilfe bei der Ermittlung der Täter leisten.

Ein privates Unternehmen beantragte bei der Datenschutzbehörde die Genehmigung für die Sammlung von 600 000 Blutproben norwegischer Bürger für wissenschaftliche Studien und die Entwicklung neuer Medikamente. Die Datenschutzbehörde entschied in diesem Fall, dass die Verarbeitung von Gesundheitsdaten für die betroffenen Personen erhebliche Nachteile mit sich bringen würde, die mit dem Gesetz nicht vereinbar seien. Die Datenschutzbehörde wies insbesondere darauf hin, dass derartige Verarbeitungen personenbezogener Gesundheitsdaten in der Zuständigkeit staatlicher Behörden erfolgen müssten und nicht privatwirtschaftlichen Unternehmen übertragen werden dürften. Die Aufsichtsbehörde wird für die Verwendung genetischer Informationen eigene Leitlinien erlassen, um zu verhindern, dass ethische Grundsätze und das Recht auf Schutz der Privatsphäre in Konkurrenz zu kommerziellen Interessen treten.

*Verwendung personenbezogener Gesundheitsdaten im Arbeitsumfeld*
Ein mit der Beurteilung einer derartigen Verwendung befasster Ausschuss stellte in seinem Bericht fest, dass Arbeitgeber generell zu wenig über ihre Rechte wissen, nach denen sie von Arbeitnehmern Informationen über deren Gesundheit verlangen können.

Vor dem Hintergrund, dass die Datenschutzbehörde in ihrer Arbeit seit jeher hervorhebt, wie wichtig es ist, die Verwendung von Gesundheitsdaten im Arbeitsumfeld auf Situationen zu beschränken, in denen eine Rechtsgrundlage für die Kenntnis dieser Daten besteht, kommt dem Aufzeigen dieser Kenntnislücke große Bedeutung zu.

## *E. Website*

www.datatilsynet.no
Der Großteil der Website ist nur in norwegischer Sprache verfügbar, eine englische Fassung des Gesetzes über personenbezogene Daten kann jedoch abgerufen werden.

## 3.2. Beitrittsländer

Die intensivierte Heranführungsstrategie zielt bei allen Beitrittsländern darauf ab, diesen Ländern die Übernahme 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, zur Umsetzung von EU-Recht und zum anderen auf der Schaffung der für die wirksame Einführung des gemeinschaftlichen Besitzstandes erforderlichen Verwaltungsstrukturen, beispielsweise unabhängiger Datenschutzbehörden.

In einer Reihe von Beitrittsländern sind entsprechende Entwicklungen auf diesem Gebiet zu verzeichnen. In Slowenien wurde im Juni und in Bulgarien, Malta, Rumänien und Zypern wurden im Dezember neue Rechtsvorschriften zum Datenschutz angenommen. Änderungen des bestehenden Datenschutzrechts wurden im Mai in der Tschechischen Republik und im August in Polen eingeführt.

## 3.3. Vereinigte Staaten von Amerika

Am 26. Juli 2000 nahm die Kommission die Entscheidung 520/2000/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens“ und der diesbezüglichen „Häufig gestellten Fragen“ (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, an. Die Mitgliedstaaten waren somit verpflichtet, bis zum 25. Oktober 2000, also binnen 90 Tagen, nachdem sie von der Entscheidung in Kenntnis gesetzt worden waren, alle notwendigen Vorkehrungen zu treffen, um die Weitergabe von Daten an die in der „Safe Harbor“-Liste verzeichneten US-Organisationen zu ermöglichen.

Die Vereinbarung über den sicheren Hafen ist seit dem 1. November 2000 mit der Freigabe des Online-Selbstzertifizierungsverfahrens für US-Organisationen, die sich der Vereinbarung über den sicheren Hafen anschließen wollen, durch das US-Handelsministerium in Kraft.

Im Jahr 2001 traten die ersten Unternehmen der Vereinbarung über den sicheren Hafen bei. Zunächst waren dies nur wenige Unternehmen, doch muss hierbei berücksichtigt werden, dass die Unternehmen einige Zeit brauchen, bis sie die erforderlichen Vorbereitungen für den Beitritt zu der Vereinbarung getroffen haben.

## 3.4. Andere Drittländer

### - Kanada

Die Europäische Kommission erließ im Dezember 2001 eine positive Entscheidung über die Angemessenheit des Datenschutzes, den das kanadische Personal Information Protection and Electronic Documents Act bietet (Entscheidung 2002/2/EG vom 20.12.2001, ABl. L 2/13vom 4.1.2002).

In ihrer Entscheidung gelangt die Kommission zu dem Schluss, dass Kanada für die Zwecke von Artikel 25 Absatz 2 der Richtlinie 95/46/EG als ein Land angesehen wird, das ein angemessenes Schutzniveau bei der Übermittlung personenbezogener

Daten aus der Gemeinschaft an Empfänger garantiert, die der Personal Information Protection and Electronic Documents Act unterliegen.

Diese Entscheidung betrifft ausschließlich die Angemessenheit des Schutzes, den das kanadische Gesetz in Kanada im Hinblick auf die Anforderungen des Artikels 25 Absatz 1 der Richtlinie 95/46/EG gewährleistet, andere zur Umsetzung sonstiger Vorschriften der Richtlinie festgelegte Bestimmungen und Einschränkungen hinsichtlich der Verarbeitung personenbezogener Daten in den Mitgliedstaaten bleiben davon unberührt.

Das kanadische Gesetz gilt für privatwirtschaftliche Organisationen, die im Rahmen kommerzieller Tätigkeiten personenbezogene Daten erheben, verarbeiten oder weitergeben. Zunächst ist es nur für Organisationen anwendbar, die als Betrieb oder Unternehmen des Bundes tätig sind wie z. B. Fluggesellschaften, Banken, Rundfunkgesellschaften, provinzübergreifende Verkehrsbetriebe und Telekommunikationsunternehmen, sowie für sämtliche Organisationen – unabhängig davon, ob es sich um eine unter Bundesrecht fallende Organisation handelt oder nicht –, die personenbezogene Daten gegen Entgelt an Empfänger außerhalb einer Provinz oder außerhalb Kanadas weitergeben. Außerdem ist das Gesetz anwendbar auf alle Unternehmen in den Territorien, da diese als Betriebe des Bundes gelten. Die betreffenden Daten selbst müssen Gegenstand der Transaktion sein, die Vergütung erfolgt für die Daten.

# 4. SONSTIGE ENTWICKLUNGEN AUF INTERNATIONALER EBENE

## Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

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.

Am 8. Oktober 2001 war die OECD Gastgeber einer Forumveranstaltung über „Privacy-Enhancing Technologies“ (PET). Im Anschluss an den Meinungsaustausch in der WPISP wurde die Geheimhaltungspflicht für eine PET-Bestandsliste aufgehoben.

Gemeinsam mit den Mitgliedstaaten leitete die OECD 2001 verschiedene Initiativen ein, mit denen der Bekanntheitsgrad des Tools „Privacy Policy Statement Generator“ erhöht werden sollte (z. B. durch Einrichtung von Hyperlinks von nationalen Websites zur OECD-Website, Übersetzung des Generator in die Sprachen der Mitgliedstaaten usw.).

# 5. ARTIKEL-29-DATENSCHUTZGRUPPE

## Mitglieder und Beobachter 2001[21]

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE

| ÖSTERREICH | BELGIEN |
|---|---|
| Frau Dr. Waltraut KOTSCHY<br>Das geschäftsführende Mitglied<br>Österreichische Datenschutzkommission<br>Bundeskanzleramt<br>Ballhausplatz, 1<br>A – 1014 WIEN<br>Tel. 43/1/531.15.26.79 | Monsieur Paul THOMAS<br>Président<br>Commission de la protection de la vie privée<br>Ministère de la Justice<br>Boulevard de Waterloo, 115<br>B - 1000 BRUXELLES<br>Tel. 32/2/542.72.00 |
| **DÄNEMARK** | **FINNLAND** |
| Mr Henrik WAABEN<br>Director<br>Datatilsynet<br>Borgergade 28, 5. sal.<br>DK – 1300 KOEBENHAVN K<br>Tel .: 45/33.19.32.33 | Mr Reijo AARNIO Stellv. Vorsitzender<br>Data Protection Ombudsman<br>Office of the Data Protection Ombudsman<br>Ministry of Justice<br>P.O. Box 315<br>FIN - 00181 HELSINKI<br>Tel. 358/9/18251 |
| **FRANKREICH** | **DEUTSCHLAND** |
| Monsieur Marcel PINET<br>Conseiller d'Etat honoraire<br>Commission Nationale de l'Informatique et des Libertés (CNIL)<br>Rue Saint Guillaume, 21<br>F - 75340 PARIS CEDEX 7<br>Tel. 33/1/53.73.22.22 | Dr. Joachim JACOB<br>Der Bundesbeauftragte<br>für den Datenschutz<br>Friedrich-Ebert-Str. 1<br>D - 53173 BONN (Bad Godesberg)<br>Tel. 49/228/819.95.0 |
| **GRIECHENLAND** | **IRLAND** |
| Mr Constantin DAFERMOS<br>President<br>Hellenic Data Protection Authority<br>Ministry of Justice<br>8 Omirou Street<br>10564 Athens, Greece<br>Tel. 30-210/33.52.602 | Mr Joe MEADE<br>Data Protection Commissioner<br>Irish Life Centre, Block 4<br>Talbot Street, 40<br>IRL - DUBLIN 1<br>Tel. 353/1/874.85.44 |

[21] Regelmäßig aktualisierte Lebensläufer der Mitglieder sowie die Anschriften der Stellvertreter können auf der Datenschutz-Webseite der GD Binnenmarkt auf dem Europa-Server eingesehen werden unter: http://europa.eu.int/comm/internal_market/privacy/workingroup/members_de.htm http://europa.eu.int/comm/internal_market/privacy/workingroup/contact-members_de.htm

| ITALIEN | LUXEMBURG |
|---|---|
| Prof. Stefano RODOTA Vorsitzender<br>President<br>Garante per la protezione dei<br>dati personali<br>Piazza di Monte Citorio, 121<br>I – 00186 ROMA<br>Tel. 39/06/69.67.77.03 | Monsieur René FABER<br>Président<br>Commission à la protection des<br>données nominatives<br>Ministère de la Justice<br>Boulevard Royal 15<br>L – 2934 Luxembourg<br>Tel. 352/487.180 |
| **NIEDERLANDE** | **PORTUGAL** |
| Mr Peter HUSTINX<br>President<br>College Bescherming persoonsgegevens (CBP)<br>Prins Clauslaan 20<br>P.O. Box 93374<br>NL – 2509 AJ 's-GRAVENHAGE<br>Tel. 3170/381.13.00 | Mr João LABESCAT (bis 9/2001)<br>Mr Luís da SILVEIRA (ab 9/2001)<br>Président<br>Comissão Nacional de Protecção de Dados<br>Rua de S. Bento, 148<br>P – 1 200-821 Lisboa Codex<br>Tel. 351/21/392.84.00 |
| **SPANIEN** | **SCHWEDEN** |
| Mr Juan Manuel FERNANDEZ LOPEZ<br>Director<br>Agencia de Protección de Datos<br>C/ Sagasta, 22<br>E – 28004 MADRID<br>Tel. 34/91/399.62.20 | Mr Ulf WIDEBÄCK<br>Director General<br>Datainspektionen<br>Fleminggatan, 14<br>9th Floor<br>Box 8114<br>S - 104 20 STOCKHOLM<br>Tel. 46/8/657.61.00 |
| **VEREINIGTES KÖNIGREICH** | |
| Ms Elisabeth FRANCE<br>Information Commissioner<br>The Office of the Information Commissioner<br>Executive Department<br>Water Lane<br>Wycliffe House<br>UK - WILMSLOW - CHESHIRE SK9 5AF<br>Tel. 44/1625/54.57.00 (Zentrale) | |

BEOBACHTER BEI DER ARTIKEL-29-DATENSCHUTZGRUPPE

| ISLAND | NORWEGEN |
|---|---|
| Ms Sigrun JOHANNESDOTTIR<br>Director<br>Icelandic Data Protection Authority<br>Raudararstigur 10<br>IS – 105 REYKJAVIK<br>Tel. 354/560.90.10 | Mr Georg APENES<br>Director General<br>Datatilsynet<br>The Data Inspectorate<br>P.B. 8177 Dep<br>N - 0034 OSLO<br>Tel. 47/22/39.69.00 |

# Die Aufgaben der Datenschutzgruppe nach Artikel 29

Mit der Einsetzung der Datenschutzgruppe sollen die folgenden vorrangigen Ziele erreicht werden:

- Zu Fragen des Datenschutzes in der Gemeinschaft gegenüber der Kommission in Form von Sachverständigenbeiträgen der Mitgliedstaaten Stellung zu nehmen.

- Die einheitliche Anwendung der allgemeinen Grundsätze der Richtlinien in allen Mitgliedstaaten durch die Zusammenarbeit der Aufsichtsbehörden für den Datenschutz zu fördern.

- Die Kommission hinsichtlich aller Gemeinschaftsmaßnahmen zu beraten, die sich auf die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre auswirken.

- Gegenüber der Allgemeinheit und insbesondere gegenüber den Organen der Gemeinschaft Empfehlungen zu Angelegenheiten auszusprechen, die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie den Schutz der Privatsphäre in der Europäischen Gemeinschaft betreffen.

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

**Artikel 29 und 30 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[22]**
*Amtsblatt L 281 vom 23.11.1995 S. 0031 - 0050*

*„Artikel-29- Datenschutzgruppe*

1. *Es wird eine Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten eingesetzt (nachstehend „Gruppe" genannt).*
   *Die Gruppe ist unabhängig und hat beratende Funktion.*

2. *Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestellten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission.*
   *Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, benannt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Institutionen und die Organe der Gemeinschaft eingerichtet sind.*

3. *Die Gruppe beschließt mit der einfachen Mehrheit der Vertreter der Kontrollstellen.*

4. *Die Gruppe wählt ihren Vorsitzenden. Die Dauer der Amtszeit des Vorsitzenden beträgt zwei Jahre. Wiederwahl ist möglich.*

5. *Die Sekretariatsgeschäfte der Gruppe werden von der Kommission wahrgenommen.*

6. *Die Gruppe gibt sich eine Geschäftsordnung.*

7. *Die Gruppe prüft die Fragen, die der Vorsitzende von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission auf die Tagesordnung gesetzt hat.*

*Artikel 30*

*1. Die Gruppe hat die Aufgabe,*

- *a) alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;*
- *b) zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;*
- *c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischer Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;*

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

*d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben.*

*2. Stellt die Gruppe fest, dass sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigten könnten, so teilt sie dies der Kommission mit.*

*3. Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen.*

*4. Die Stellungnahme und Empfehlungen der Gruppe werden der Kommission und dem in Artikel 31 genannten Ausschuss übermittelt.*

*5. Die Kommission teilt der Gruppe mit, welche Konsequenzen sie aus den Stellungnahmen und Empfehlungen gezogen hat. Sie erstellt hierzu einen Bericht, der auch dem Europäischen Parlament und dem Rat übermittelt wird. Dieser Bericht wird veröffentlicht.*

*6. Die Gruppe erstellt jährlich einen Bericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, den sie der Kommission dem Europäischen Parlament und dem Rat übermittelt. Dieser Bericht wird veröffentlicht."*

**Artikel 14 der Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation**
*Amtsblatt L 024 vom 30.01.1998 S. 0001 – 0008*

*„Artikel 14*

*Ausweitung des Geltungsbereichs bestimmter Vorschriften der Richtlinie 95/46/EG*

*(…)3. Die gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzte Datenschutzgruppe nimmt die in Artikel 30 der genannten Richtlinie festgelegten Aufgaben auch im Hinblick auf den Schutz der Grundrechte und der Grundfreiheiten und der berechtigten Interessen im Bereich der Telekommunikation, der Gegenstand der vorliegenden Richtlinie ist, wahr."*

# Geschäftsordnung

KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN
GENERALDIREKTION XV
Binnenmarkt und Finanzdienstleistungen
Freier Verkehr von Informationen, Gesellschaftsrecht und finanzielle Informationen
**Freier Verkehr von Informationen; Datenschutz und damit zusammenhängende internationale Aspekte**

XV/D/5031/96 DE

**GRUPPE FÜR DEN SCHUTZ VON PERSONEN**
**BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN**

G E S C H Ä F T S O R D N U N G

verabschiedet
auf der dritten Sitzung der Gruppe am
11. September 1996

---

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[23], hat in Anwendung von Artikel 29 und 30 der vorgenannten Richtlinie ihre Geschäftsordnung wie folgt festgelegt[24]:

Artikel 1

1. Die Gruppe ist unabhängig und hat beratende Funktion.[Artikel 29 Absatz 1]
2. Die Gruppe hat die Aufgabe:
   a) Alle Fragen im Zusammenhang mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften zu prüfen, um zu einer einheitlichen Anwendung beizutragen;
   b) Zum Schutzniveau in der Gemeinschaft und in Drittländern gegenüber der Kommission Stellung zu nehmen;
   c) die Kommission bei jeder Vorlage zur Änderung dieser Richtlinie, zu allen Entwürfen zusätzlicher oder spezifischere Maßnahmen zur Wahrung der Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zu allen anderen Entwürfen von Gemeinschaftsmaßnahmen zu beraten, die sich auf diese Rechte und Freiheiten auswirken;
   d) Stellungnahmen zu den auf Gemeinschaftsebene erarbeiteten Verhaltensregeln abzugeben [Artikel 30 Absatz 1]
3. Stellt die Gruppe fest, dass sich im Bereich des Schutzes von Personen bei der Verarbeitung personenbezogener Daten zwischen den Rechtsvorschriften oder der Praxis der Mitgliedstaaten Unterschiede ergeben, die die Gleichwertigkeit des Schutzes in der Gemeinschaft beeinträchtigen könnten, so teilt sie dies der Kommission mit. [Artikel 30 Absatz 2]
4. Die Gruppe kann von sich aus Empfehlungen zu allen Fragen abgeben, die den Schutz von Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft betreffen. [Artikel 30 Absatz 3]

Mitglieder der Gruppe

Artikel 2

1. Die Gruppe besteht aus je einem Vertreter der von den einzelnen Mitgliedstaaten bestimmten Kontrollstellen und einem Vertreter der Stelle bzw. der Stellen, die für die Institutionen und Organe der Gemeinschaft eingerichtet sind, sowie einem Vertreter der Kommission. [Artikel 29 Absatz 2]
2. Jedes Mitglied der Gruppe wird von der Institution, der Stelle oder den Stellen, die es vertritt, bestimmt. Hat ein Mitgliedstaat mehrere Kontrollstellen bestimmt, so ernennen diese einen gemeinsamen Vertreter. Gleiches gilt für die Stellen, die für die Organe und Einrichtungen der Gemeinschaft eingerichtet sind. [Artikel 29 Absatz 2]

---

23 ABl. L 281 vom 23.11.95, S. 31.

24 Die vorliegende Fassung enthält die entsprechenden Verfügungen der Richtlinie 95/46/EG. Ein Verweis auf die betreffenden Artikel der Richtlinie erscheint zwischen Klammern.

3. Die Stellen und Institutionen der vorgenannten Absätze bestimmen nach dem gleichen Verfahren einen Stellvertreter. Bei Bedarf kann ein zweiter Stellvertreter bestimmt werden.
4. Die in den vorstehenden Absätzen genannten Stellen und Institutionen teilen dem Sekretariat die Namen ihrer Vertreter mit.
5. Werden durch einen Mitgliedstaat die in Absatz 1 genannten Stellen nicht ernannt, lädt der Vorsitzende gemäß Artikel 9 den betroffenen Mitgliedstaat ein, einen Beobachter zu bestimmen. Dieser Beobachter besitzt Rederecht, jedoch kein Stimmrecht.

Vorsitz der Gruppe

Artikel 3

1. Die Gruppe wählt den Vorsitzenden und den stellvertretenden Vorsitzenden in geheimer Abstimmung.
2. Der Vorsitzende sowie der stellvertretende Vorsitzende der Gruppe werden von den gemäß Artikel 17 stimmberechtigten Mitgliedern der Gruppe mit absoluter Mehrheit gewählt.
3. Die Dauer Amtszeit des Vorsitzenden und des stellvertretenden Vorsitzenden beträgt zwei Jahre. Das Mandat des Vorsitzenden und des stellvertretenden Vorsitzenden kann einmal erneuert werden. [Artikel 29 Absatz 4]

Sekretariat

Artikel 4

1. Die Sekretariatsgeschäfte der Gruppe werden von den Dienststellen der Kommission wahrgenommen.(*)
2. Das Sekretariat bereitet die Arbeiten der Gruppe unter Mitwirkung ihres Vorsitzenden vor. Es unterstützt die Gruppe bei der Anfertigung der Entwürfe von Stellungnahmen und Empfehlungen.
3. Die für die Gruppe bestimmten Informationen sind an das Sekretariat zu übermitteln.

Einberufung der Gruppe und Sitzungsort

Artikel 5

1. Die Gruppe wird auf Veranlassung ihres Vorsitzenden oder des Sekretariats einberufen. Sie kann ebenfalls durch den Vorsitzenden auf Antrag von wenigstens einem Drittel der ordentlichen Mitglieder einberufen werden.

---

(*)Anschrift: Sekretariat der Gruppe für den Schutz von Personen
bei der Verarbeitung personenbezogener Daten
Generaldirektion für Binnenmarkt und Finanzdienstleistungen
Kommission der Europäischen Gemeinschaften
Rue de la Loi 200
B - 1049 Brüssel

2. Der Vorsitzende beruft die Gruppe unter Mitwirkung des Sekretariats ein.
3. Das Sekretariat der Gruppe unterrichtet jedes Mitglied der Gruppe von der anberaumten Sitzung und der Tagesordnung mindestens vier Wochen vor der vorgesehen Sitzung; gleichzeitig werden die Stellvertreter benachrichtigt.
4. In dringenden Fällen kann die vorgenannte Frist von vier Wochen abgekürzt werden; jedoch ist eine Mindestfrist von zwei Wochen einzuhalten.

Artikel 6

Die Sitzungen der Gruppe finden im Allgemeinen am Sitz der Kommission statt.

Tagesordnung

Artikel 7

1. Die vorläufige Tagesordnung wird aufgestellt entweder auf Vorschlag des Vorsitzenden von sich aus oder auf Antrag eines Vertreters der Kontrollstellen oder auf Antrag der Kommission.[Artikel 29 Absatz 7]
2. Der Vorsitzende kann auf Antrag eines Gruppenmitglieds einen zusätzlichen Tagesordnungspunkt aufnehmen oder einen Punkt von der vorläufigen Tagesordnung streichen.
3. Zu Beginn der Sitzung nimmt die Gruppe die Tagesordnung an.

Artikel 8

Jedes Gruppenmitglied, das verhindert ist, an einer Sitzung teilzunehmen, hat seinen Stellvertreter und das Sekretariat der Gruppe hiervon möglichst schnell zu benachrichtigen.

Teilnahme an den Sitzungen

Artikel 9

1. Außer den Mitgliedern und den Stellvertretern können an den Sitzungen die vom Vorsitzenden auf Beschluss der Gruppe eingeladenen Sachverständigen oder Beobachter teilnehmen.
2. Der Vorsitzende ermächtigt auf Beschluss der Gruppe die Gruppenmitglieder, sich bei einer oder mehreren Sitzungen durch Sachverständige ihres Vertrauens assistieren zu lassen. Die Mitglieder teilen dem Sekretariat die Namen dieser Sachverständigen mit.

Beschlussfähigkeit

Artikel 10

Die Gruppe ist beschlussfähig, wenn mehr als die Hälfte der gemäß Artikel 17 stimmberechtigten Personen anwesend sind.

Durchführung der Beratungen

Artikel 11

1. Unbeschadet des Artikels 214 des EG -Vertrages müssen die Sachverständigen und die Beobachter Stillschweigen über die Debatten der Gruppe bewahren.
   Die Sitzungsberichte sowie Dokumentenentwürfe der Gruppe sind nur für den Dienstgebrauch bestimmt, sofern die Gruppe nicht anders entscheidet.
   Die Stellungnahmen, Empfehlungen und alle anderen von der Gruppe angenommenen Dokumente sind, sofern die Gruppe nicht anders entscheidet, nicht nur für den Dienstgebrauch bestimmt.
2. Der Vorsitzende leitet die Beratungen. Ist der Vorsitzende verhindert, so vertritt ihn der stellvertretende Vorsitzende.
3. Ist auch dieser verhindert, wird er durch ein von der relativen Mehrheit der gemäß Artikel 17 stimmberechtigten Personen bestimmtes Mitglied vertreten.

Entscheidungen der Gruppe

Artikel 12

1. Die Gruppe entscheidet mit der Mehrheit der gültig abgegebenen Stimmen. Stimmenthaltungen werden als gültig abgegebene Stimmen bewertet. Auf Antrag der Gruppenmitglieder können in den Entscheidungen die von ihnen vertretenen Auffassungen angegeben werden.
2. Bei Stimmengleichheit gilt der Vorschlag als abgelehnt.

Artikel 13

1. Die Gruppe entscheidet einstimmig darüber, ob über eine bestimmte Frage schriftlich abgestimmt werden soll.
2. In dringenden Fällen kann der Vorsitzende entscheiden, dass über eine Frage schriftlich abgestimmt wird.
3. Der der Gruppe zur Abstimmung unterbreitete Entwurf wird den nach Artikel 17 stimmberechtigten Mitgliedern vom Sekretariat zugesandt. Die stimmberechtigten Mitglieder teilen dem Sekretariat schriftlich innerhalb der vom Vorsitzenden gesetzten Frist, die auf keinen Fall kürzer als 14 Tage sein darf, ihren Beschluss mit. Erfolgt keine solche Mitteilung an das Sekretariat innerhalb dieser Frist, gilt dies als Stimmenthaltung. Das Sekretariat teilt den Mitgliedern das Ergebnis der Abstimmung mit. Das Ergebnis der Abstimmung wird in das Protokoll der folgenden Sitzung aufgenommen.
4. Die schriftliche Abstimmung im Sinne von Absatz 2 wird ausgesetzt, wenn eines der nach Artikel 17 stimmberechtigten Mitglieder innerhalb von 5 Tagen nach Erhalt des Entwurfs die Diskussion des Entwurfs auf einer Sitzung der Gruppe beantragt.

Artikel 14

1. Die Stellungnahmen und Empfehlungen der Gruppe müssen mit einer Begründung versehen sein.
2. Die Stellungnahmen und Empfehlungen werden der Kommission und dem in Artikel 31 der Richtlinie 95/46/EG vorgesehenen Ausschuss übermittelt. [Artikel 30 Absatz 4] Die Stellvertreter erhalten davon eine Abschrift.

Artikel 15

1. Die Gruppe erstellt einen Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Gemeinschaft und in Drittländern, der der Kommission, dem Europäischen Parlament und dem Rat übermittelt wird. Der Bericht wird veröffentlicht. [Artikel 30 Absatz 6]
2. Der im Absatz 1 genannte Bericht wird von der Gruppe angenommen, vom Vorsitzenden an die im Absatz 1 genannten Institutionen weitergeleitet und vom Sekretariat veröffentlicht.

Artikel 16

Die Gruppe kann einen oder mehrere Berichterstatter für bestimmte Fragen und für den gemäß Artikel 15 jährlich zu erstellenden Bericht ernennen.

Stimmrecht

Artikel 17

1. Das Stimmrecht steht ausschließlich den Mitgliedern zu, die die Kontrollstellen vertreten. [Artikel 29 Absatz 3]
2. Vertritt ein Stellvertreter ein stimmberechtigtes Mitglied, zu dessen Stellvertreter er ernannt wurde, so übt er dessen Stimmrecht aus.

Niederschrift über die Sitzungen

Artikel 18

1. Das Sekretariat fertigt über jede Sitzung eine Niederschrift an.
   Dieser Sitzungsbericht enthält:
   a) die Anwesenheitsliste
   b) einen Kurzbericht über die Beratungen
   c) die von der Gruppe beschlossenen Stellungnahmen und Empfehlungen unter Angabe der Verteilung der Stimmen bei den erfolgten Abstimmungen und gegebenenfalls der abweichenden Stellungnahmen.
2. Die Gruppe nimmt den Sitzungsbericht an.
3. Der Sitzungsbericht wird der Gruppe nur dann zur Beschlussfassung vorgelegt, wenn er den Mitgliedern und Stellvertretern im Entwurf mindestens 15 Tage vor der Sitzung übersandt worden ist; wird diese Arbeitsunterlage nicht rechtzeitig zugeleitet, so wird der Beschluss erst in der folgenden Sitzung der Gruppe gefasst.
4. Änderungsvorschläge zum Entwurf des Sitzungsberichts müssen soweit wie möglich schriftlich vor der Sitzung, in der er angenommen werden soll, eingereicht werden.

Änderungen der Geschäftsordnung

Artikel 19

Die vorliegende Geschäftsordnung kann unter den in Artikel 12 vorgesehenen Bedingungen geändert werden.

# Im Jahr 2000 angenommene Dokumente mit Angabe der Website

**WP 38 (5102/00):** Stellungnahme 1/2001 zum Entwurf einer Entscheidung der Kommission betreffend die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach Artikel 26 Absatz 4 der Richtlinie 95/46. Angenommen am 26. Januar 2001.

**WP 39 (5109/00):** Stellungnahme 2/2001 zum Datenschutzniveau des kanadischen Personal Information and Electronic Documents Act. Angenommen am 26. Januar 2001.

**WP 40 (5095/00):** Stellungnahme 3/2001 zum Datenschutzniveau des australischen Privacy Amendment (Private Sector) Act 2000. Angenommen am 26. Januar 2001.

**WP 41 (5001/01):** Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarats über Cyberkriminalität. Angenommen am 22. März 2001.

**WP 42 (5008/01):** Empfehlung 1/2001 Beurteilungsdaten von Beschäftigten. Angenommen am 22. März 2001.

**WP 43 (5020/01):** Empfehlung 2/2001 zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union. Angenommen am 17. Mai 2001.

**WP 44 (5003/01):** Stellungnahme 5/2001 zum Sonderbericht des Europäischen Bürgerbeauftragten an das Europäische Parlament im Anschluss an den Empfehlungsentwurf an die Europäische Kommission in der Beschwerde 713/98/IJH. Angenommen am 17. Mai 2001.

**WP 45 (5029/01):** NICHT ÖFFENTLICH - Opinion 6/2001 on the working paper submitted by DG Employment with regard to the processing of personal data in employer/employee relationships (Stellungnahme 6/2001 zum Arbeitspapier der GD Beschäftigung zur Verarbeitung personenbezogener Daten in Arbeitgeber-Arbeitnehmerverhältnissen). Angenommen am 17. Mai 2001.

**WP 46 (5019/01):** Vierter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Gemeinschaft und in Drittländern, Berichtsjahr 1999. Angenommen am 17. Mai 2001.

**WP 47 (5061/01):** Stellungnahme 7/2001 zum Entwurf der Entscheidung der Kommission in der Fassung vom 31. August 2001 über Standardvertragsklauseln zur Übermittlung personenbezogener Daten an Datenverarbeiter in Drittländern nach Artikel 26 Absatz 4 der Richtlinie 95/46. Angenommen am 13. September 2001.

**WP 48 (5062/01)** Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten. Angenommen am 13. September 2001.

**WP 49 (5032/01):** Arbeitsdokument über die empfohlene Praktik 1774 der IATA zum Schutz der Privatsphäre und grenzüberschreitende Flüsse personenbezogener Daten, die im internationalen Luftverkehr bei der Beförderung von Personen und Fracht verwendet werden. Angenommen am 14. September 2001.

**WP 50 (5085/01):** **NICHT ÖFFENTLICH!**
Working document. Progress report of the subgroup on the FEDMA Draft European Code of Practice for the Use of Personal Data in Direct Marketing (Arbeitspapier. Zwischenbericht der Untergruppe zum Entwurf von Verhaltensregeln für Europa der FEDMA für die Verwendung personenbezogener Daten im Direktmarketing).
Angenommen am 14 September 2001.

**WP 51 (5074/01):** Stellungnahme 9/2001 zur Mitteilung der Kommission über die „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität". Angenommen am 5. November 2001.

**WP 52 (5080/01):** Beschluss 1/2001 über die Teilnahme von Vertretern der Kontrollstellen in den Beitrittsländern an Sitzungen der Artikel-29-Datenschutzgruppe. Angenommen am 13. Dezember 2001.

**WP 53 (5403/01):** Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus. Angenommen am 14. Dezember 2001.

**Die von der 29 angenommenen Papiere stehen auf der Datenschutz-Website der Generaldirektion Binnenmarkt auf dem Europa-Server der Europäischen Kommission zur Verfügung unter:**
http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_de.htm

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