Neunter Jahresbericht

der Art. 29

Datenschutzgruppe

EUROPÄISCHE
KOMMISSION

1830-6462

Neunter 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 2005

Angenommen am 14. Juni 2006

Dieser Bericht wurde von der Art. 29 Datenschutzgruppe erstellt. Er gibt nicht unbedingt die Überzeugungen und Ansichten der Europäischen Kommission wieder und ist nicht an ihre Weisungen gebunden.

Dieser Bericht ist ebenfalls in englischer und französischer Sprache erhältlich. Er kann auf der Internetseite der Generaldirektion für Justiz, Freiheit und Sicherheit der Europäischen Kommission in der Rubrik „Datenschutz" heruntergeladen werden: www.europa.eu.int/comm/justice_home/fsj/privacy

INHALT

VORWORT DES VORSITZENDEN DER ART. 29 DATENSCHUTZGRUPPE

Der Datenschutz in Europa wurde im Jahr 2005 vor allem durch drei Elemente geprägt:

- Die rasche Entwicklung der Informationstechnologie macht es notwendig, die Instrumente des Datenschutzes zu überprüfen und anzupassen.
- Im Interesse der EU-Bürgerinnen und -Bürger müssen weitere rechtliche und praktische Schritte zur Harmonisierung des Datenschutzes auf hohem Niveau unternommen werden.
- Die andauernde Suche Europas nach den richtigen Antworten auf die internationalen Bedrohungen der Sicherheit dürfen nicht zu unzumutbaren Beeinträchtigungen bürgerlicher Freiheitsrechte und insbesondere des Datenschutzes führen.

Der europäische Datenschutz hat sich im vergangenen Jahrzehnt zu einem weltweit attraktiven Modell entwickelt. Dieses Modell muss sich immer wieder neu bewähren, denn ansonsten gerät es in Gefahr, seine Attraktivität einzubüßen. Es muss offen sein für neue Entwicklungen und es muss dem Wandel in den technologischen, wirtschaftlichen und gesellschaftlichen Bedingungen Rechnung tragen. Im Mittelpunkt stehen dabei die mehr als 450 Millionen Bürgerinnen und Bürger der EU-Mitgliedstaaten, deren Rechte und Interessen es zu wahren gilt.

Die Artikel 29-Gruppe hat seit ihrer Gründung 1995 neue technologische Entwicklungen so früh wie möglich untersucht und auf ihre Ausgestaltung und Anwendung im Sinne des Datenschutzes Einfluss genommen. Im Berichtsjahr hat sich die Gruppe verstärkt der Radio Frequency Identification (RFID) gewidmet, die bereits jetzt in vielen Bereichen zum Einsatz kommt und weiter an Bedeutung für den Datenschutz des Einzelnen gewinnen wird. Nach Vorarbeiten in einer Arbeitsgruppe und gestützt auf die Ergebnisse einer öffentlichen Online-Konsultation hat die Gruppe erste wesentliche Orientierungen geliefert (WP 105 und WP 111).

Eines der Ergebnisse war, dass das in der Richtlinie 95/46/EG enthaltene Konzept des „personenbezogenen Datums" und die Frage der Anonymisierbarkeit und der Identifizierbarkeit einer vertieften Untersuchung bedürfen. Insbesondere muss geprüft werden, ob die derzeitigen Regelungen hinreichend berücksichtigen, dass bei der Verwendung von RFIDs als Nummerierungssysteme für Waren während ihres Lebenszyklus Phasen der Anonymität und der Identifizierbarkeit beteiligter Personen oft in rascher Folge aufeinander folgen. Es ist fraglich, in wie weit die Richtlinie diese dynamischen Prozesse und Änderungen des Zusammenhangs bestimmter Daten während ihres Lebenszyklus mit einschließt. Die Arbeitsgruppe hat deshalb diese Fragestellung in das Arbeitsprogramm des Folgejahres aufgenommen.

Weitere technologische Schwerpunkte waren Lokalisierungsdaten bei Telekommunikations- und Mehrwertdiensten (WP 115), Sicherheitsmaßnahmen in Bezug auf biometrische Merkmale in Pässen (WP 112) und das europäische Visainformationssystem (VIS) (WP 110). Gerade durch die Kombination zwischen biometrischen Merkmalen und fortgeschrittenen Techniken in der Speicher-, Übertragungs- und Softwaretechnik (Mustererkennung) entstehen qualitativ neue Risiken für das Recht auf informationelle Selbstbestimmung, denen durch angemessene Schutzmaßnahmen begegnet werden muss. Ferner beschäftigte sich die Arbeitsgruppe mit Datenschutzimplikationen bei modernen Formen der Ausübung von Urheberrechten (WP 104).

Zu den strategischen Zielen der Artikel 29-Gruppe gehört es nicht nur, die rechtlichen Regelungen des Datenschutzes auf europäischer Ebene zu harmonisieren und voranzutreiben, sondern ganz besonders auch darauf zu achten, dass die praktische Umsetzung nicht hinter der Programmatik zurückbleibt. Der Datenschutz soll im Leben der Gemeinschaftsbürger eine jederzeit präsente und greifbare Realität sein. Bei der Verfolgung dieses Ziels hat die Gruppe im abgelaufenen Jahr zwei wichtige Meilensteine setzen können. Der erste betrifft verbindliche Regelungen für den Datenschutz in internationalen Unternehmen. Die Mitglieder der Arbeitsgruppe haben sich darauf verständigt, dass dieses Instrument bei der Sicherung eines angemessenen Datenschutzniveaus bei der Übermittlung personenbezogener Daten in Drittländer ebenso anerkannt werden soll wie die in der Richtlinie ausdrücklich genannte Vertragslösung. Sie hat, nach intensiven Vorarbeiten und Kontakten mit der Industrie, einen Katalog von Anforderungen erstellt, denen diese verbindlichen internationalen Unternehmensregelungen genügen müssen.

Die Richtlinie sieht vor, dass solche Schutzgarantien von den Aufsichtsbehörden nach den Bestimmungen des jeweiligen nationalen Rechts der Mitgliedsstaaten genehmigt werden müssen, in denen sie verwendet werden sollen. Eine gegenseitige Anerkennung ist bislang nicht vorgesehen. Um dennoch Lösungen im Geiste europäischer Harmonisierung zu ermöglichen, hat sich die Arbeitsgruppe auf ein Abstimmungsverfahren geeinigt, das europaweit gültige Unternehmensregelungen erleichtert. Im Mittelpunkt steht dabei der Ansatz, dass das Unternehmen mit nur einer Aufsichtsbehörde verhandelt, die eine Abstimmung eines gemeinsamen Standpunkts mit den übrigen beteiligten Aufsichtsbehörden vornimmt. Einige internationale Unternehmen haben diesen Weg bereits beschritten; die Abstimmungsverfahren zwischen den Aufsichtsbehörden der betreffenden Mitgliedstaaten sind im Gange.

Ein Vorhaben von besonderer praktischer, aber auch strategischer Tragweite sind die geplanten abgestimmten europaweiten Datenschutzprüfungen. Die Datenschutzbehörden wollen den Effekt ihrer Kontrolltätigkeiten dadurch erhöhen, dass sie in einem gemeinsam abgesteckten zeitlichen und thematischen Rahmen bestimmte Bereiche prüfen. Dies versetzt sie nicht nur in die Lage, Unterschiede in der praktischen Umsetzung der Datenschutzrichtlinie und des nationalen Datenschutzrechts zu erkennen, sondern auch Musterlösungen auf der Basis umfassender Erfahrung gemeinsam zu erarbeiten und durchzusetzen. Hierfür hat die Arbeitsgruppe Grundsätze für ein gemeinsames Vorgehen ausgearbeitet. Die erste gemeinschaftliche Prüfung wird im Laufe des Jahres 2006 im Bereich der privaten Krankenversicherung stattfinden. Die Datenschutzbehörden wollen mit diesem Vorgehen intensiver voneinander lernen und sehen darin zugleich einen wichtigen Beitrag zur Harmonisierung ihrer praktischen Aktivitäten.

Vertreter der Artikel 29-Gruppe haben im Herbst 2005 gemeinsam mit Vertretern der Europäischen Kommission die Praxis der amerikanischen Grenzbehörden bei der Verarbeitung von Flugpassagierdaten (PNR) auf der Grundlage des zwischen der EU und den USA geschlossenen Übereinkommens[1] geprüft. Die Gruppe hat damit einen wichtigen Beitrag zur praktischen Umsetzung des Datenschutzes geleistet. Die Prüfung des Umgangs der US-Behörden mit den PNR-Daten unter Beteiligung der unabhängigen Datenschutzbehörden unterstreicht die Bedeutung, mit der Europa auch im internationalen Kontext für die Beachtung des Datenschutzes als eines zentralen Bürgerrechts eintritt. Der Besuch führte zu einer Reihe von Verbesserungen. Die Arbeitsgruppe beschäftigte sich auch mit der Übermittlung von Fluggastdaten nach Kanada und Australien, da entsprechende Abkommen durch die EU-Kommission vorbereitet wurden.

[1] Das PNR-Übereinkommen wurde am 30. Mai 2006 durch den Europäischen Gerichtshof annulliert.

Schließlich hat sich die Arbeitsgruppe im Berichtsjahr nach Erstellung einer Überprüfung durch die EU-Kommission im Jahre 2004 an einer amerikanisch-europäischen Bestandsaufnahme zum „Safe Harbor"-Abkommen[2] beteiligt. Beide Seiten, einschließlich der beteiligten Wirtschaftsvertreter, konnten eine positive Bilanz ziehen. Sie beabsichtigen, das Safe-Harbor-System weiter zu verbessern und auch für Wirtschaftssektoren zu öffnen, denen es bisher aufgrund der amerikanischen Gesetzgebung verschlossen ist.

Die Arbeit der Gruppe wurde auch im Berichtsjahr durch Diskussionen darüber geprägt, wie der Datenschutz angesichts der andauernden terroristischen Bedrohungen gewahrt bleiben kann. Entsprechende Initiativen des Rates und der Kommission veranlassten die Arbeitsgruppe wiederholt, zu entsprechenden Vorschlägen Stellung zu nehmen. Von besonderer Bedeutung war dabei die Diskussion um die Verpflichtung für Anbieter elektronischer Kommunikationsdienste zur flächendeckenden Erfassung und Aufbewahrung der Verkehrsdaten. Zu den Prinzipien des freiheitlichen Staates gehört es, dass der Staat nur dann in den Bereich des Privatlebens der Bürger eindringt, wenn es dafür einen konkreten, rechtfertigenden Grund gibt. In diesem Fall stehen die bei Unternehmen und Einzelpersonen vorhandenen Informationen grundsätzlich dem Zugriff der staatlichen Strafverfolgungs- und Sicherheitsbehörden offen. Die nach einer Einigung von Parlament und Rat beschlossenen Vorgaben haben einen qualitativ ganz anderen Charakter: Sie verpflichten die Anbieter elektronischer Kommunikationsdienste, Daten, die ansonsten gar nicht benötigt würden, allein zu dem Zweck bereitzuhalten, dass den staatlichen Organen im Bedarfsfall ein größerer Fundus an personenbezogenen Daten zur Verfügung steht. Es geht mit anderen Worten nicht mehr um Interventionen im Einzelfall, sondern um eine präventive Überwachungsstruktur.

Die Vertreter des europäischen Datenschutzes haben ihre Position mehrfach formuliert. Sie haben auf die Anforderungen der europäischen Menschenrechtskonvention hingewiesen, die eine systematische anlassfreie präventive Überwachung nicht zulässt. Sie haben – leider erfolglos – die Prüfung alternativer Ansätze eingefordert, wie sie in anderen Staaten für ausreichend gehalten werden, insbesondere des in den USA erfolgreich praktizierten „quick freeze"-Ansatzes.

Vor dem Hintergrund der Beschlusslage der europäischen Organe werden die in der Arbeitsgruppe zusammengeschlossenen Datenschutzbehörden darauf hinwirken, dass die verbleibenden Spielräume zur Umsetzung der Richtlinie in nationales Recht im Sinne eines effektiven Daten- und Grundrechtsschutzes genutzt werden. Sie werden ferner die Auswirkungen der präventiven Speicherung der Verkehrsdaten aufmerksam beobachten. Sie erklären schließlich ihre Bereitschaft, an der Evaluation der Regelung mitzuwirken. Die Leitlinie aller Beteiligten muss dabei sein, gerade angesichts terroristischer Bedrohungen die fundamentalen Grundsätze der Verhältnismäßigkeit, Klarheit und Transparenz zu wahren.

Die Artikel 29-Gruppe wird auch in Zukunft darauf hinwirken, den Datenschutz für die europäischen Bürgerinnen und Bürger weiter zu stärken und die hierfür erforderlichen Instrumente den sich wandelnden Rahmenbedingungen und Herausforderungen anzupassen. Ein effektiver Datenschutz ist zugleich ein unverzichtbarer Bestandteil einer demokratischen Informations- und Wissensgesellschaft.

Peter Schaar, Vorsitzender der Art. 29 Datenschutzgruppe

[2] http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm

[3] Alle von der Art. 29 Datenschutzgruppe angenommenen Dokumente können von folgender Website abgerufen werden: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2006_de.htm

Kapitel 1

Die Aufgaben der Art. 29 Datenschutzgruppe[3]

1.1. TRANSFER VON DATEN IN DRITTLÄNDER

1.1.1. Verbindliche unternehmensinterne Vorschriften (BCRs)

Arbeitsdokument zur Darstellung eines Verfahrens der Zusammenarbeit für die Herausgabe gemeinsamer Stellungnahmen über einen angemessenen Schutz als Ergebnis verbindlicher unternehmensinterner Vorschriften ("Binding Corporate Rules")[4]

Dieses Dokument sollte als Grundlage dienen, wenn eine Unternehmensgruppe daran interessiert ist, einen Entwurf von verbindlichen unternehmensinternen Vorschriften (BCRs) für die Anerkennung verschiedener Datenschutzbehörden vorzulegen, und deshalb eine Datenschutzbehörde (DSB) als leitende Behörde für das Verfahren der Zusammenarbeit vorschlägt; es sollte außerdem die Auswahl der leitenden Behörde anhand geeigneter Kriterien rechtfertigen und den gesamten einzuhaltenden Verfahrensablauf darstellen.

Arbeitsdokument über die Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften[5]

Da die Beteiligung von Datenschutzbehörden bei der Annahme von verbindlichen unternehmensinternen Vorschriften ausschließlich auf freiwilliger Grundlage erfolgt, können von Fall zu Fall unterschiedliche Beteiligungsentscheidungen getroffen werden. Dieses Dokument enthält eine Modellcheckliste, die einer Unternehmensgruppe dabei helfen soll, einen Antrag auf Annahme ihrer verbindlichen unternehmensinternen Vorschriften zu stellen, und die insbesondere dazu beitragen soll, zu belegen, wie die Gruppe die Auflagen des Dokuments WP74 erfüllt, das die Anforderungen an verbindliche unternehmensinterne Vorschriften zusammenfasst.

1.1.2. Artikel 26(1) der Richtlinie 95/46/EG

Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Absatz 1 der Richtlinie 95/46/EG vom 24. Oktober 1995[6]

Dieses Arbeitsdokument soll eine Anleitung dazu geben, wie Artikel 26(1) der Richtlinie 95/46 zu verstehen und von Datenschutzbeauftragten anzuwenden ist, die Datentransfers in Länder planen, die laut Artikel 25 der betreffenden Richtlinie kein angemessenes Datenschutzniveau gewährleisten. Dieses Dokument bietet Ausführungen dazu, wie Datenschutzbeauftragte die Ausnahmeregelungen von Artikel 26(1) anwenden können und in einigen Fällen anwenden sollten. Die Datenschutzgruppe (Working Party – WP) betrachtet dieses Dokument als wesentlichen Bestandteil ihrer Politik zum Datentransfer in Drittländer.

1.1.3. Kanada

Stellungnahme Nr. 1/2005 zu dem in Kanada gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdatensätzen (Passenger Name Record data – PNR) und erweiterten Passagierdaten (Advance Passenger Information – API) von Fluggesellschaften[7]

Die vorliegende Stellungnahme beruht auf der „Verpflichtungserklärung" (ein von der Kommission herausgegebenes Dokument, das eine Selbstverpflichtung der Canada Border Services Agency CBSA [kanadische Grenzschutzbehörde] bezüglich der Durchführung ihres PNR-Programms enthält). Ihre Veröffentlichung erfolgt darüber hinaus mit Hinweis auf das Schutzniveau, das von Kanada gewährleistet wird, nachdem die Fluggesellschaften die API- und PNR-Daten ihrer Passagiere und Besatzungsmitglieder entsprechend den kanadischen Gesetzen und der Verpflichtungserklärung an die CBSA übermittelt haben. Die Datenschutzgruppe

[4] WP 107
[5] WP 108
[6] WP 114
[7] WP 103

geht davon aus, dass Kanada ein im Sinne von Artikel 25(6) der Richtlinie angemessenes Schutzniveau gewährleistet.

1.2. VERBESSERTE ERFÜLLUNG DER DATENSCHUTZRICHTLINIE

Bericht der Artikel-29-Datenschutzgruppe über die Meldepflicht an die nationalen Kontrollstellen, zur bestmöglichen Nutzung der Ausnahmen und Vereinfachungen und zur Rolle von Datenschutzbeauftragten in der Europäischen Union[8]

In diesem Bericht werden vorzügliche Verfahren bezüglich der Meldepflicht in den Mitgliedstaaten einschließlich der Aufgaben der Datenschutzbeauftragten bestimmt. Er befasst sich darüber hinaus mit einem möglichen System von Vereinfachungen für Organisationen mit mehr als einer Niederlassung in der EU und enthält eine Reihe von an die Europäische Kommission gerichteten Empfehlungen, die berücksichtigt werden sollten, falls künftig weitergehende Harmonisierungsanstrengungen in Betracht gezogen werden. Dieser Bericht sollte als ein erster Beitrag zu einem besseren Verständnis der Funktion der Meldepflicht und der Aufgaben von Datenschutzbeauftragten im Rahmen des bestehenden Datenschutzsystems der Europäischen Union betrachtet werden und als ein erster Schritt bei der Verwirklichung einer weitergehenden Harmonisierung und Vereinfachung der Meldepflicht in der Gemeinschaft.

1.3. INTERNET, TELEKOMMUNIKATION UND NEUE TECHNOLOGIEN

Stellungnahme 4/2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM(2005) 438 endgültig; 21.09.2005)[9]

Im Rahmen dieser Stellungnahme wurden eine Reihe von Überlegungen angestellt, zum Beispiel, dass die Einbehaltung von Daten im Datenverkehr das uneingeschränkte Grundrecht auf vertrauliche Kommunikationen verletzt; jede Einschränkung dieses Grundrechts muss durch eine dringende Notwendigkeit gerechtfertigt sein und sollte nur in Ausnahmefällen genehmigt, und dann jeweils durch angemessene Garantien abgesichert werden. Diese Stellungnahme legt 20 spezifische Sicherheitsgarantien dar, die in Betracht gezogen werden sollten, insbesondere unter Berücksichtigung der für die Empfänger und die weitere Verarbeitung geltenden Anforderungen, der Notwendigkeit von Genehmigungen und Kontrollen, der für Dienstleistungserbringer geltenden Maßstäbe auch im Hinblick auf die Sicherheit und logische Trennung der Daten, der Ermittlung der betroffenen Datenkategorien und ihrer Aktualisierung sowie der Notwendigkeit, Nachrichten auszuschließen.

Stellungnahme 5/2005 der Gruppe 29 zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen[10]

Die Datenschutzgruppe weist darauf hin, dass es sich bei den Fragen zur Verwendung von Standortdaten um ein sehr aktuelles Thema handelt. Standortdaten, oder Ortungsdaten, werden definiert als „Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben“ (Artikel 2 der Richtlinie 2002/58/EG). In dieser Stellungnahme bringt die Datenschutzgruppe

[8] WP 106
[9] WP 113
[10] WP 115

zum Ausdruck, dass sämtliche Parteien, die an der Erbringung eines Mehrwertdienstes unter Verwendung von Ortungsdaten beteiligt sind, bei der Verarbeitung von personenbezogenen Daten ihre Verpflichtungen im Rahmen der Datenschutzgesetzgebung zum Schutz personenbezogener Daten erfüllen müssen. Dies gilt sowohl für die Betreiber elektronischer Kommunikationsnetze, die Ortungsdaten verarbeiten, als auch für Dritte, die auf Grundlage der von den Betreibern übermittelten Ortungsdaten einen Mehrwertdienst anbieten.

1.4. SCHENGEN/VISA/FREIER PERSONENVERKEHR

Stellungnahme 2/2005 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (KOM (2004) 835 endg.)[11]

In dieser Stellungnahme wurden unterschiedliche Überlegungen zur Einrichtung einer zentralen Datenbank und eines Systems für den Informationsaustausch über Visa für einen kurzfristigen Aufenthalt zum Ausdruck gebracht, die wesentliche Fragen zu Grundrechten und Freiheiten des Einzelnen aufwerfen, insbesondere zum Recht auf Privatsphäre; denn dieses Projekt wird zum einen zu einer massiven Erhebung und Verarbeitung personenbezogener Daten und biometrischer Merkmale führen, aber auch zu ihrer Speicherung in einer zentralisierten Datenbank und einem Informationsaustausch in großem Umfang, von dem eine Vielzahl von Personen betroffen sein wird. Die Stellungnahme weist außerdem auf die möglichen Risiken eines solchen Projekts hin und hebt hervor, dass der angemessenen Einhaltung der Grundsätze des Datenschutzes eine große Bedeutung zukommt. Darüber hinaus wurde die Frage der Notwendigkeit und Verhältnismäßigkeit einer so umfassenden Datenbank angesprochen, namentlich im Hinblick auf die Entscheidung der Einbeziehung biometrischer Merkmale, die in dem System gespeichert werden sollen. Die Datenschutzgruppe schlägt vor, diesen Vorschlag unter Berücksichtigung der in dieser Stellungnahme enthaltenen Anmerkungen abzuändern.

Stellungnahme Nr. 3/2005 zur Durchführung der Verordnung des Rates (EG) Nr. 2252/2004 vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten[12]

Im Anschluss an die 2004[13] ausgeführten Arbeiten unterstreicht die Stellungnahme der Datenschutzgruppe vom 30. September 2005 die von ihr bereits zum Ausdruck gebrachte Haltung hinsichtlich der Verwendung biometrischer Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, so wie in Verordnung 2252/2004 festgelegt.[14] Die Datenschutzgruppe erinnert an ihre seit langem bekannte Haltung hinsichtlich der Verarbeitung biometrischer Daten und weist darauf hin, dass die Verwendung biometrischer Angaben in Pässen und Reisedokumenten grundlegende technische, ethische und juristische Fragen aufwirft. Die Datenschutzgruppe weist insbesondere darauf hin, dass bei der Verwendung von biometrischen Daten effiziente Sicherheitsvorkehrungen getroffen werden müssen, um die spezifischen Risiken zu vermeiden, die sich aus der Verwendung dieser Daten ergeben; sie spricht sich außerdem dafür aus, die Verwendung biometrischer Daten in Pässen und Reisedokumenten auf Überprüfungszwecke zu beschränken sowie dafür Sorge zu tragen, dass nur die zuständigen Behörden Zugang zu diesen auf dem Chip gespeicherten Daten erhalten.

[11] WP 110
[12] WP 112
[13] Siehe Achter Bericht, Abschnitt 1.4
[14] Abl.EU L 385, 29.12.2004 S. 1.

Stellungnahme 6/2005 zu den Vorschlägen für eine Verordnung des Europäischen Parlaments und des Rates (KOM (2005) 236 endg.) und einer Entscheidung des Rates (KOM (2005) 230 endg.) über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) und einem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates (KOM (2005) 237 endg.) über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II).[15]

In dieser am 25. November 2005 angenommenen Stellungnahme vertritt die Datenschutzgruppe die Auffassung, dass mehrere Aspekte des von der Kommission vorgelegten Legislativpakets im Hinblick auf die Einhaltung der Datenschutzgrundsätze Anlass zur Sorge geben. Diese Stellungnahme schließt sich den Stellungnahmen des Europäischen Datenschutzbeauftragten (EDSB)[16] und der Gemeinsamen Kontrollinstanz von Schengen an.[17] Die Datenschutzgruppe hebt hervor, dass die neuen, zum Schutz von personenbezogenen Daten vorgeschlagenen Regelungen mindestens das bestehende Schutzniveau erreichen sollten, das im Rahmen des gegenwärtigen Schengener Informationssystems gewährleistet wird.

In ihrer Stellungnahme befasst sich die Datenschutzgruppe insbesondere mit Fragen, die Ziel und Zweck des SIS II betreffen; sie ist der Auffassung, dass man über das Kriterium der Beschränkung der Zweckbestimmungen hinausgehen würde, wenn neuen Behörden der Zugang zu dem System eröffnet würde; dies sollte jedoch vermieden werden, da die Bestimmungen hinsichtlich der Verbindung von in das System eingegebenen Alarmmeldungen ausführliche Sicherheitsvorkehrungen bezüglich der Verwendung solcher Verbindungen voraussetzen und von der Notwendigkeit getragen sind, die Einrichtung neuer Zugangsrechte für Behörden zu vermeiden, die Informationen betreffen, die nicht für diese Behörden bestimmt sind. Nationale Kopien sollten ebenfalls vermieden werden, da sie nicht gerechtfertigt erscheinen und zu einer Vermehrung der Zugangsstellen führen. Die Datenschutzgruppe äußerte außerdem ihre Besorgnis im Hinblick auf eine Verarbeitung biometrischer Daten im System. Entsprechend ihrer bereits mehrfach zu diesem Thema zum Ausdruck gebrachten Haltung hebt die Datenschutzgruppe hervor, dass eine Verwendung biometrischer Daten nur mit strengen Einschränkungen und unter Wahrung angemessener Sicherheitsvorkehrungen erfolgen darf. Eine Suche anhand biometrischer Kriterien sollte ausgeschlossen und die Dauer des Zeitraums geregelt werden, für den eine Aufbewahrung der verarbeiteten personenbezogenen Daten zulässig ist. Schließlich fordert die Datenschutzgruppe hinsichtlich der Kontrolle des Systems klare Regelungen in Bezug auf die Rolle und die Verpflichtungen der beteiligten Kontrollbehörden, um die Zusammenarbeit zwischen den nationalen Kontrollbehörden und dem EDPS/EDSB besser zu strukturieren und zu verbessern.

[15] WP 116
[16] Stellungnahme EDSB vom 19.10.2005
[17] Stellungnahme vom 6.10.2005

1.5. RFID

Arbeitsdokument zu Datenschutzthemen im Zusammenhang mit der RFID-Technologie[18]

In ihrer Stellungnahme bringt die Datenschutzgruppe ihre Besorgnis zum Ausdruck, dass einige Anwendungen der RFID-Technologie möglicherweise die menschliche Würde sowie Datenschutzrechte verletzen könnten. Besondere Sorgen bereitet in diesem Zusammenhang die Möglichkeit, dass Unternehmen und Regierungen RFID-Technologie verwenden könnten, um in die Privatsphäre von Einzelpersonen einzudringen. Dieses Problem wird zusätzlich durch die Tatsache erschwert, dass diese Technologie aufgrund ihrer relativ niedrigen Kosten in Zukunft nicht nur großen Organisationen, sondern auch kleineren Akteuren und einzelnen Bürgern zur Verfügung steht. Die Datenschutzgruppe setzt sich dafür ein, die technologischen Entwicklungen in diesem Bereich in Zusammenarbeit mit interessierten Parteien weiterhin zu verfolgen. Darüber hinaus könnte die Datenschutzgruppe je nach Entwicklungsstand der RFID-Technologie und ihrer Anwendungen entscheiden, sich im Einzelnen auf spezifische Bereiche/Anwendungen zu konzentrieren, indem sie für spezifische Anwendungen eine zusätzliche Anleitung bereitstellt.

Ergebnisse der öffentlichen Anhörung zum Arbeitspapier 105 der Art. 29 Arbeitsgruppe zum Thema Datenschutz und RFID-Technologie[19]

Im Anschluss an die Annahme des oben genannten Dokuments fasste die Datenschutzgruppe den Beschluss, es zum Gegenstand einer öffentlichen Anhörung zu machen. Es ist sicher nützlich, die in diesem Dokument enthaltene Zusammenfassung der wichtigsten Kommentare und einige Schlussfolgerungen allgemein an interessierte Parteien weiterzugeben.

1.6. RECHTE DES GEISTIGEN EIGENTUMS

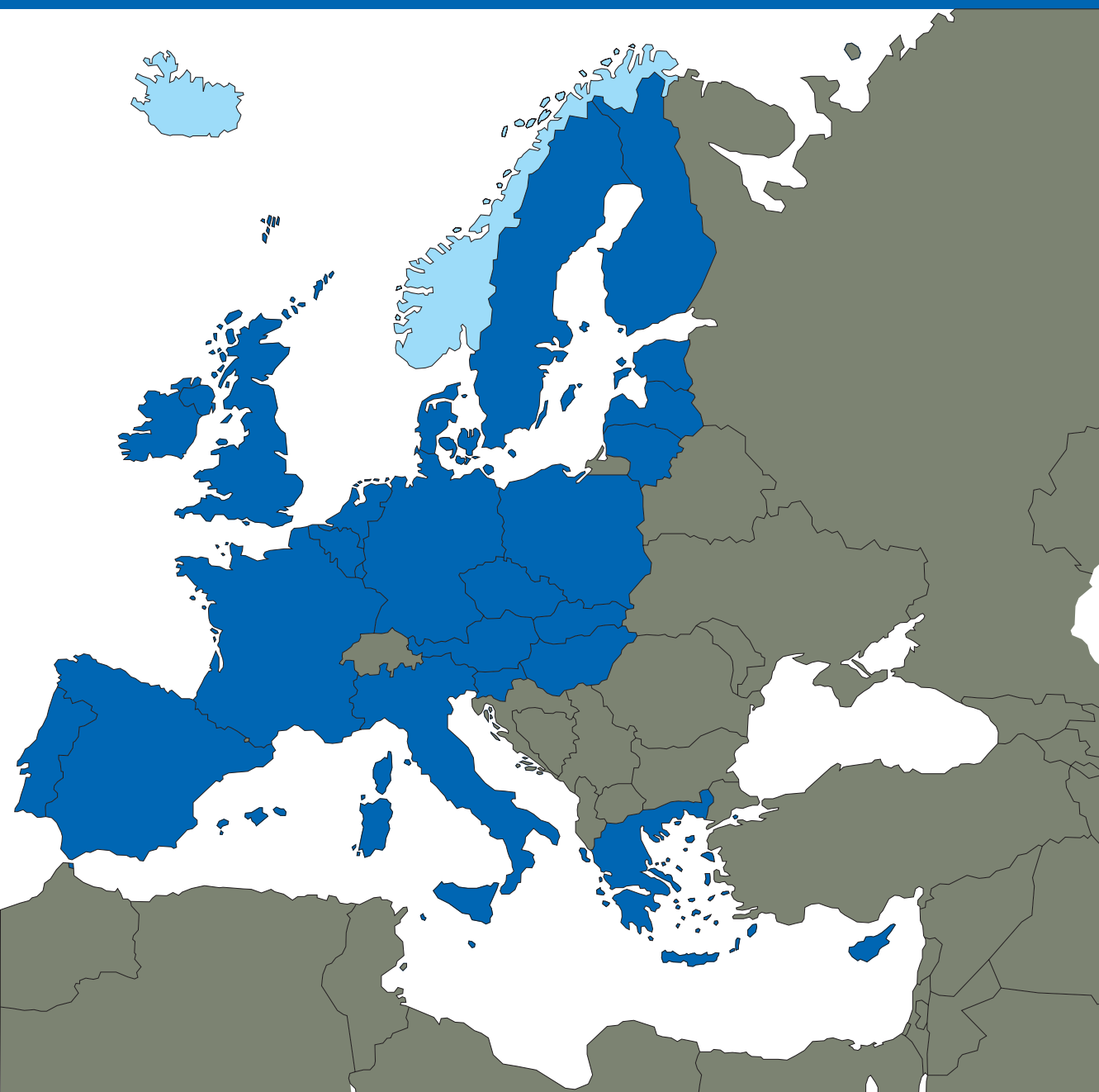
Arbeitsdokument zu Datenschutzthemen im Zusammenhang mit Rechten des geistigen Eigentums[20]

Die Datenschutzgruppe weist darauf hin, dass der wachsende Informationsaustausch im Zusammenhang mit der Entwicklung des Internets mehr und mehr die heikle Frage der Kontrolle von urheberrechtlich geschützten Informationen berührt. Dieses Dokument erinnert an die wichtigsten Rechtsgrundsätze, die von den Inhabern der Urheberrechte bei der Ausübung ihrer Rechte beachtet werden müssen, aber auch von anderen Akteuren, die sich insbesondere mit digitaler Verwaltung befassen, wie beispielsweise der Industrie und den Dienstleistungsanbietern, die Technologie zur Verwaltung digitaler Rechte anbieten. Die Datenschutzgruppe setzt sich in diesem Dokument für die Entwicklung technischer Hilfsmittel ein, die Eigenschaften aufweisen, die mit dem Schutz der Privatsphäre vereinbar sind, und ganz generell für eine transparente und begrenzte Verwendung von eindeutigen Identifikatoren, wobei dem Benutzer jeweils Wahlmöglichkeiten eingeräumt werden sollen.

[18] WP 105
[19] WP 111
[20] WP 104

Kapitel 2

Die wichtigsten Entwicklungen in den Mitgliedstaaten



Österreich

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Im Anschluss an die Tsunami-Katastrophe im Dezember 2004 wurden im Rahmen des österreichischen Datenschutzgesetzes 2000 (DSG 2000) ausführlichere Bestimmungen für die Verarbeitung personenbezogener Daten (einschließlich sensibler Daten) erlassen, die für einen Katastrophenfall gelten. Demnach ist es öffentlichen Behörden und Hilfsorganisationen von Rechts wegen gestattet, im Katastrophenfall Daten uneingeschränkt zu verarbeiten, insofern dies erforderlich ist, um den unmittelbar von der Katastrophe betroffenen Menschen Hilfe leisten zu können oder um Vermisste und Todesopfer zu lokalisieren und zu identifizieren und ihren Familienangehörigen Informationen zukommen zu lassen. Es ist zulässig, ein gemeinsames Informationssystem zu betreiben und sich daran zu beteiligen, wenn sich dies als notwendig herausstellt, um effizient auf eine Katastrophe reagieren zu können. Im Rahmen des Anwendungsbereichs der oben genannten Ziele sind darüber hinaus Datentransfers in Drittländer zulässig, einschließlich der Beteiligung an einem gemeinsamen Informationssystem mit Teilnehmern in Drittländern. Die Übertragung von polizeilichen Daten oder sensiblen Daten in ein solches gemeinsames Informationssystem ist jedoch nur dann gestattet, wenn zuverlässige Hinweise auf den Tod eines Vermissten vorliegen. Strafrechtlich relevante Informationen dürfen nicht weitergeleitet werden, es sei denn, ihre Weiterleitung ist zu Identifizierungszwecken in einem spezifischen Fall unerlässlich. Informationen über Familienangehörige (z. B. DNS-Daten zu Identifikationszwecken) dürfen nur unter Verwendung von Pseudonymen weitergeleitet werden (siehe Bundesgesetzblatt für die Republik Österreich, Teil I, Nr. 13/2005).

Darüber hinaus wurden Änderungen des Telekommunikationsgesetzes 2003 (TKG 2003) notwendig, damit es besser mit der Datenschutzrichtlinie für elektronische Kommunikation (Richtlinie 2002/58/EG) in Einklang gebracht werden kann. Die betreffende Richtlinie bezieht sich auf alle natürlichen Personen, ohne dabei Unterscheidungen zu treffen. Paragraph 107 TKG 2003 sieht jedoch vor, dass es unzulässig ist, E-Mail-Nachrichten – ohne vorherige Einwilligung des Empfängers – „an Verbraucher zu Zwecken der Direktwerbung" zu richten. In diesem Sinne war es nicht erforderlich, die vorherige Einwilligung von Unternehmern einzuholen. Diese Unterscheidung war mit dem Wortlaut der Richtlinie 2002/58/EG unvereinbar und musste aufgehoben werden. Darüber hinaus wurde in den Paragraphen 107 ein neuer Absatz aufgenommen, der die Möglichkeit eröffnet, die Nutzung der elektronischen Kontaktinformation zu Zwecken der Direktwerbung von vornherein abzulehnen.

B. Bedeutende Rechtsprechung

Eine von privater Hand geführte, öffentlich anerkannte Entwöhnungseinrichtung war daran interessiert, sich an einem mit öffentlichen Mitteln finanzierten Forschungsvorhaben zu beteiligen. Das Projekt zielte darauf ab, ein Strafaufschubsystem für Drogenabhängige zu bewerten, die sich einer Entwöhnungstherapie unterzogen hatten. Dieses „Therapie statt Strafe" genannte Strafaufschubsystem wurde erst vor wenigen Jahren in das österreichische Rechtssystem aufgenommen, und seine Auswirkungen sollten jetzt bewertet werden.

In diesem Zusammenhang hatte der wissenschaftliche Projektbetreuer des Entwöhnungszentrums eine Genehmigung beantragt, die personenbezogenen Daten von Drogenabhängigen verwenden zu dürfen, die sich einer Entwöhnungstherapie unterzogen hatten.

Laut Paragraph 46, Absatz 3 des österreichischen Datenschutzgesetzes 2000 ist eine Genehmigung für die Verwendung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung

oder Statistik zu erteilen, wenn die folgenden drei Bedingungen erfüllt sind: Die Einholung der Zustimmung der Datensubjekte ist mangels ihrer Erreichbarkeit unmöglich oder würde ansonsten einen unverhältnismäßigen Aufwand bedeuten; es besteht ein öffentliches Interesse an der beantragten Verwendung; die wissenschaftliche Qualifikation des Antragstellers wurde hinreichend belegt.

Im vorliegenden Fall war die Verwendung medizinischer Daten von Personen (über die Ergebnisse der Entwöhnungstherapie) geplant, die vor dem Beginn ihrer Behandlung strafrechtlich in Erscheinung getreten sind.

Die österreichische Datenschutzkommission (DSK) lehnte den Antrag mit der Begründung ab, dass die Zustimmung des Datensubjekts eingeholt werden sollte, da nicht von vornherein davon ausgegangen werden kann, dass dies einen unverhältnismäßigen Aufwand bedeutet, insbesondere dann nicht, wenn zwei unterschiedliche Arten von äußerst sensiblen Daten bearbeitet werden sollen.

Im Falle einer „Videoüberwachung", die durchgeführt wurde, um die Intensität von Flugverkehr, der eine hohe Lärmbelastung verursacht, zu dokumentieren, wies die österreichische DSK die Beschwerde eines Piloten mit der Begründung zurück, dass Bilddaten nicht in den Anwendungsbereich der Datenschutzbestimmungen fallen, wenn sie eindeutig nicht in der Absicht aufgezeichnet wurden, die aufgenommenen Personen zu identifizieren. Darüber hinaus wurde in den Schlussfolgerungen darauf hingewiesen, dass eine analoge Videoaufzeichnung mit einer einzigen handbetriebenen Kamera in Verbindung mit handschriftlichen Aufzeichnungen kein „Speichersystem personenbezogener Daten darstellt". Analoge Videoaufzeichnungen werden im Gegensatz zu digitalen Aufzeichnungen nicht „mit automatisierten Mitteln" ausgeführt. Eine solche Dokumentation ist kein strukturierter, personenbezogener Datensatz, der einen Zugriff anhand spezifischer Kriterien ermöglichen würde.

Die österreichische DSK hat eine Notifizierung hinsichtlich der Videoüberwachung in öffentlichen Verkehrsmitteln erhalten, die zur Verhinderung von Vandalismus und für einen verstärkten Schutz der Mitarbeiter und Passagiere eingesetzt wird. Die technische Struktur des Systems ermöglicht digitale Aufzeichnungen mit einer Dauer von bis zu 48 Stunden. Die Aufnahmen werden nur gesichtet, wenn jemand den Nothaltschalter betätigt hat oder wenn Vandalismusschäden festgestellt wurden. In beiden Fällen wird der Datenträger demontiert und die Aufzeichnungen werden von eigens hierfür ausgebildeten Mitarbeitern ausgewertet.

Die österreichische DSK wies in ihren Schlussfolgerungen darauf hin, dass eine Videoüberwachung nur nach einer entsprechenden Notifizierung durchgeführt werden darf, da solche Aufzeichnungen Daten über die ethnische Herkunft und möglicherweise auch gesundheitsbezogene Daten enthalten, wobei in dem vorliegenden Fall, der Gegenstand der Untersuchung war, wahrscheinlich zusätzlich strafrechtlich relevante Daten erfasst werden.

Die österreichische DSK stellte in ihren Schlussfolgerungen darüber hinaus fest, dass die Videoüberwachung eine neue Form der Datenerfassung beinhaltet, bei der sich noch herausstellen muss, ob sie ein angemessenes Mittel zum Schutz vor Vandalismus und zur Erhöhung der Sicherheit ist. Dabei ist jedoch darauf zu achten, dass jede Einschränkung des Rechts auf eine Privatsphäre angemessen und notwendig ist, um den angestrebten Zweck zu erfüllen. Da diese Aspekte bisher nur unzureichend dokumentiert werden konnten, erteilte die österreichische DSK lediglich eine vorläufige Genehmigung und stellte besondere Anforderungen (d. h. eine ausführliche Dokumentation aller Zwischenfälle, die eine Auswertung der Aufzeichnungen nach sich gezogen haben).

Bei der österreichischen DSK wurde eine Beschwerde durch einen israelischen Bürger gegen das

französische Innenministerium auf Grundlage von Artikel 110 („das Recht, Daten löschen zu lassen") des Schengener Durchführungsübereinkommens eingereicht.

Zu Beginn der Ereignisse, die zu dieser Beschwerde geführt haben, versuchte der Beschwerdeführer, in französisches Hoheitsgebiet einzureisen. Die französische Grenzschutzpolizei verweigerte ihm jedoch die Einreise mit der Begründung, dass seine Anwesenheit auf französischem Hoheitsgebiet eine Gefährdung der öffentlichen Sicherheit bedeuten würde. Folglich wurden seine Daten im nationalen (französischen) Kontrollamt des Schengener Informationssystems (NSIS) eingetragen. Anschließend wurde dieser Eintrag an die nationalen Kontrollämter aller Mitgliedstaaten einschließlich des österreichischen NSIS weitergeleitet.

In der Folge hat der Beschwerdeführer diese Entscheidung in Frankreich angefochten und die Annullierung der Entscheidung der französischen Grenzschutzpolizei vor einem französischen Verwaltungsgericht bewirkt. Dennoch wurde der Eintrag nicht gelöscht, so dass dem Beschwerdeführer, als er in der österreichischen Botschaft in Tel Aviv einen Visumsantrag stellte, das Visum verweigert wurde.

Aufgrund des Sachverhalts fasste die österreichische DSK den Beschluss, dass das französische Innenministerium verpflichtet ist, den Eintrag im nationalen französischen Kontrollamt des Schengener Informationssystems zu löschen; die Zuständigkeit der österreichischen DSK beruht auf Artikel 111, Absatz 1 leg.cit.: „Jeder hat das Recht, im Hoheitsgebiet jeder Vertragspartei eine Klage wegen einer seine Person betreffenden Ausschreibung insbesondere auf Berichtigung, Löschung, Auskunftserteilung oder Schadenersatz vor dem nach nationalem Recht zuständigen Gericht oder der zuständigen Behörde zu erheben."

C. Wichtige spezifische Themen

Im ersten Halbjahr 2005 haben österreichische Gerichte eine Reihe von Entscheidungen gefällt, die die Verpflichtung von Internet-Dienstleistungsanbietern betreffen, die Identität von Benutzern preiszugeben, die Dateien durch sog. „Filesharing" austauschen. In diesem Zusammenhang befasste sich die Hauptfrage damit, ob eine „dynamische IP-Adresse" „Verkehrsdaten" im Sinne von Artikel 2(b) und Erwägungsgrund 15 der Richtlinie 2002/58/EG ist, was zur Folge hätte, dass sie nur unter strengen Auflagen offen gelegt werden darf (siehe Artikel 5 der Richtlinie 2002/58/EG).

Erwägungsgrund 15 der Richtlinie 2002/58/EG erklärt: „Verkehrsdaten können sich unter anderem auf [...] die Dauer, den Zeitpunkt oder die Datenmenge einer Nachricht, [...] den Beginn, das Ende oder die Dauer einer Verbindung beziehen."

Internet-Dienstleistungsanbieter weisen statische und dynamische IP-Adressen zu. Während eine statische Adresse einem einzigen Nutzer zugewiesen wird, erfolgt die Vergabe einer dynamischen IP-Adresse zu unterschiedlichen Zeitpunkten an mehrere Nutzer. Deshalb kann die Identität einer Person, die eine dynamische IP-Adresse verwendet, nur dann ermittelt werden, wenn man die Log-Dateien eines Internet-Dienstleistungsanbieters überprüft. Die Log-Dateien enthalten den spezifischen Anfang und das Ende einer Verbindung. Nur diese Informationen weisen zusammen mit einer dynamischen IP-Nummer auf einen spezifischen Teilnehmer hin.

Im Juli 2005 hat der Oberste Gerichtshof in Österreich eine Entscheidung veröffentlicht, in der er darauf hinweist, dass Name und Adresse eines Nutzers nicht unter das Kommunikationsgeheimnis fallen, da diese Informationen keine Verkehrsdaten darstellen, und deshalb offen gelegt werden müssen. Gegenwärtig ist diese Entscheidung in Österreich sehr umstritten.

Belgien

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und andere Entwicklungen in der Gesetzgebung

Richtlinie 95/46/EG

Keine Entwicklung.

Richtlinie 2002/58/EG

Der Achte Jahresbericht hat gezeigt, dass die Datenschutzkommission „Commission de la protection de la vie privée" (CPVP) zum Vorentwurf des Gesetzes zur Umsetzung der Richtlinie 2002/58/EG befragt wurde. Die Hauptkritikpunkte wurden dort dargelegt (Stellungnahme vom 14. Juni 2004, S. 21). Das Gesetz über die elektronischen Kommunikationsmittel stellte mit anderen europäischen Richtlinien die Umsetzung der Richtlinie „Privatleben und elektronische Kommunikation" vom 12. Juli 2002 in belgisches Recht dar und wurde am 13. Juni 2005 endgültig angenommen.

Es wird gezeigt, dass diese Richtlinie zwei Ausnahmen zum Abhörverbot, der Kenntnisnahme des Inhalts und der Aufzeichnung von elektronischer Kommunikation, festgeschrieben durch die Artikel 259bis und 314bis des Strafgesetzbuches, hinzufügt. So ist unbeschadet der Anwendung des Gesetzes vom 8. Dezember 1992 zum Schutz der Privatsphäre und der Verarbeitung von personenbezogenen Daten (im belgischen Bezugsrahmen) die Aufzeichnung einer elektronischen Kommunikation und der dabei anfallenden Verkehrsdaten im Rahmen der legalen kommerziellen Transaktionen wie beispielsweise als *Beweis einer kommerziellen Transaktion oder einer anderen professionellen Kommunikation erlaubt,* wenn die an der Kommunikation beteiligten Parteien im Vorfeld über die Aufzeichnung, deren Zweck und die Dauer der Speicherung der Aufzeichnung informiert werden. Weiter ist die Kenntnisnahme und die Aufzeichnung von elektronischer Kommunikation und Verkehrsdaten, die nur zum Ziel haben, die Servicequalität von Rufdiensten („Call-Centern") zu überprüfen, auch zulässig, wenn im Vorfeld die in den Call-Centern arbeitenden Personen sowohl über die Möglichkeit einer Kenntnisnahme des Inhalts und der Aufzeichnung informiert werden als auch über den genauen Zweck der Operation und die Dauer der Speicherung der Kommunikation und der aufgezeichneten Daten. Es ist nicht zulässig, die Daten länger als einen Monat zu speichern.

Der Achte Jahresbericht erwähnte weiterhin, dass der Entwurf Artikel 13 der Richtlinie nicht übertrug. Die Begründung, nach der dieser Artikel in das Gesetz über die Informationsgesellschaft vom 11. März 2003 hätte umgesetzt werden sollen, wurde von der CPVP kritisiert, da der Anwendungsbereich dieses Gesetzes sich leicht von dem der Richtlinie unterscheidet. Die CPVP hatte ebenfalls darauf hingewiesen, dass diese Umsetzung keine Faxgeräte und andere Geräte mit automatischem Abruf einschloss. Die Vorbehalte der CPVP wurden teilweise berücksichtigt, da das Gesetz vom 24. August 2005 mit dem Ziel der Umsetzung gewisser Verfügungen der Richtlinie über „Fern-Finanzdienstleistungen" und der Datenschutzrichtlinie über Privatleben und elektronische Kommunikation unter anderen europäischen Vorschriften Artikel 13 überträgt. In das Gesetz vom 14. Juli 1991 über Handelspraktiken und Aufklärung und Schutz des Verbrauchers wurde der Artikel 29bis eingefügt. Die Verwendung automatischer Anrufsysteme ohne menschlichen Eingriff und von Faxgeräten für persönliche Werbezwecke ohne vorherige, spezifische Zustimmung und ohne vorherige Information des Adressaten wird hier verboten. Beim Versand jedweder Werbung mittels dieser Art von Kommunikationstechnik ist der Sender angehalten, klare und verständliche Informationen über das Recht auf Widerspruch bei künftigem Erhalt von Werbung mitzuliefern. Daher ist es verboten, die Identität des Verkäufers, in dessen Namen die Kommunikation stattfindet, zu

verschleiern. Schließlich liegt die Beweislast dafür, dass die über diese Technik versandte Werbung erwünscht war, beim Sender der Nachricht. So kann jeder ohne Angabe von Gründen und kostenfrei einen bestimmten Sender davon in Kenntnis setzen, dass die Werbung, die über diese Technik versandt wurde, nicht mehr erwünscht ist. Diese Umsetzung von Artikel 13 ist somit unvollständig, als dass sowieso nur die über E-Mail versandte Werbung vom Gesetz vom 14. Juli 1991 erfasst wird – nicht aber kommerzielle, Spendenaufrufe enthaltende oder politische E-Mails.

Weitere Entwicklungen in der Gesetzgebung

Elektronische Verwaltung – Informatisierung des Rechtssystems

Sowohl das Gesetz vom 10. August 2005, das das System Phönix auf den Weg gebracht hat, als auch ein Gesetzentwurf über das elektronische Verfahren, das noch im Parlament debattiert wird, verfolgen das Ziel einer einheitlichen Informatisierungspolitik des belgischen Gerichtssystems. Das Gesetz vom 10. August 2005 bestimmt sechs Zwecke der Datenverarbeitung unter Zuhilfenahme des Informationssystems: a) interne Kommunikation (Verwaltung der Gerichtshöfe und Gerichte und der Prozessakten), externe Kommunikation (Benachrichtigungen, Zustellungen und Weiterleitung von Gerichtsakten), beides erforderlich für den Justizbetrieb, b) die Verwaltung und Speicherung von Gerichtsdaten, c) Bildung einer nationalen Gerichtsrolle, d) die Erstellung einer Datenbank mit Fallsammlungen, e) die Ausarbeitung von Statistiken und f) Hilfe für das Management und die Verwaltung der Justiz.

Das Gesetz sieht weiter vor, dass das Informationssystem mit einem Verwaltungsausschuss, einem Überwachungsausschuss und einem Nutzerausschuss ausgestattet wird. Der Überwachungsausschuss, ein sektoraler Ausschuss innerhalb der Datenschutzkommission, nimmt auf eigene Initiative oder auf Anfrage Stellung zu jeder Frage zur Anwendung des Datenschutzgesetzes vom 8. Dezember 1992 und behandelt Beschwerden über die Anwendung dieses Gesetzes im Rahmen des Phönix-Systems. Damit erfüllt er in diesem Rahmen die Rolle der Datenschutzkommission als Vermittler und meldet gleichzeitig Verstöße, die ihr bekannt werden, an die Staatsanwaltschaft.

Elektronische Verwaltung – das Projekt e-Gesundheit

Auch im Gesundheitswesen entwickelt die Regierung ein Projekt über die Datenverarbeitung und Informatisierung der Daten sowie über die Anwendung von Telemedizin. Das Projekt wirft viele Fragen auf, etwa hinsichtlich a) der Definition von personenbezogenen Daten im Gesundheitsbereich, b) der Einführung einer persönlichen Gesundheits-Identifikationsnummer, mit der jeder Bürger/Patient Zugriff auf seine gesamte Krankengeschichte über verschlüsselte Daten hat, und c) einer Anbindung verschiedener Institutionen untereinander. Darüber hinaus besteht die Frage nach dem Zweck und den Zugriffsmodalitäten solcher Datenbanken sowie ihrer engen Verbindung mit der Sozialversicherung.

B. Rechtssprechung

Es gibt keine erwähnenswerte bedeutende Rechtssprechung, außer dem Urteil des Kassationshofes vom 2. März 2005, das im Achten Jahresbericht zum Jahr 2004 (S. 21 ff) bereits kommentiert wurde.

C. Wichtige spezifische Themen

Allgemeines

Im Allgemeinen schließt sich das Jahr 2005 an die bereits in den letzten Jahren festgestellte Tendenz

zur Zentralisierung und Vernetzung der Dateien mit personenbezogenen Daten an. Diese Tendenz ist in einen Kontext eingebunden, in dem die Sicherheit – sowohl die öffentliche als auch die finanzielle und geschäftliche – eine immer größere Bedeutung erlangt. In ihren Stellungnahmen und Positionen von 2005 hat die Datenschutzkommission immer den Akzent auf die Einhaltung des Prinzips der Kompatibilität zwischen den Dateien zwecks Vermeidung einer systematischen Datenvermehrung sowie auf die Transparenz der Datenverarbeitung gegenüber dem Bürger gesetzt.

Polizei und Sicherheit

Ein Entwurf der Behörden, zu dem sich die Datenschutzkommission geäußert hat, zielt auf die Gründung eines Föderalorgans (OCAM), das damit beauftragt wird, terroristische und extremistische Bedrohungen zu evaluieren, die die Sicherheit des Staates und der belgischen Interessen gefährden können. Die Sammlung von Informationen seitens dieses Organs beruht auf einer Beteiligung der Polizei, schließt aber ebenso Kontaktstellen in gewissen föderalen Behörden mit ein. Die Datenschutzkommission hat bei dieser Gelegenheit und speziell angesichts der Zusammenlegung von Informationen aus verschiedenen Quellen auf der Notwendigkeit beharrt, die bei diesem Projekt verfolgten Zwecke präzise zu bestimmen. Weiter erachtet sie es als sehr wichtig, die Relevanz der gelieferten Daten sowie die Harmonisierung der Schutzgarantien für Daten, die im Rahmen der Polizeiarbeit an Stellen außerhalb der Europäischen Union gegeben werden, exakt zu evaluieren.

Identifikatoren

Im Hinblick auf eine Eingrenzung des Risikos einer Überschneidung oder Kopplung von Daten hat die CPVP einige Grundsätze über die Tragweite von einmaligen Identifikatoren hingewiesen. Im Gesundheitswesen hat sie dafür plädiert, dass die behandelten Daten des Krebsregisters durch einen eigenen sektorspezifischen Identifikator und nicht durch die Nummer im Nationalregister identifiziert werden.

Weiter hat sie ihren starken Vorbehalten Ausdruck verliehen, in den elektronischen Personalausweis Informationen etwa zu einer Organspendebereitschaft mit einzuschließen oder den Personalausweis als Schlüssel für den Zugang zur persönlichen Krankengeschichte zu verwenden. Die CPVP hat besonders darauf hingewiesen, dass das Einbinden von ausländischen Daten in die Identifizierung und Überprüfung der betreffenden Person im elektronischen Personalausweis einen gefährlichen Präzedenzfall darstellen würde.

Weiter entstand eine gewisse Verwirrung im Banksektor, da dieser berechtigt ist, gespeicherte Daten im Personalausweis zum Kampf gegen die Geldwäsche zu verwenden, nicht aber zu anderen Zwecken wie zum Beispiel für die damit nicht in Zusammenhang stehende Kundenverwaltung. Im Allgemeinen ist das Sammeln von Daten seitens der Finanzinstitute aufgrund von nationalen und internationalen Regeln im Namen des Kampfes gegen die Geldwäsche und den Terrorismus mit einer Anzahl von Fragen verknüpft, die die Datenschutzkommission zusammen mit der Bank- und Finanzkommission (CBF, Bankenaufsicht) untersuchen wird.

Schwarze Listen

Auf Anfrage der Regierung hat die Datenschutzkommission Maßnahmen entwickelt, die einen gesetzlichen Rahmen für schwarze Listen vorsehen. Risikomanagement und der Wille, sich gegen einen Ausfall eines Vertragspartners abzusichern, haben dazu geführt, dass sich diese Listen stark vermehren (siehe auch das Arbeitspapier der Artikel-29-Gruppe (WP 65) vom 3. Oktober 2002 über schwarze Listen). Die Datenschutzkommission

weist weiter darauf hin, dass das Erstellen dieser Listen ein Grundrecht gefährden kann (siehe die Liste von säumigen Mietern – Recht auf Wohnung; Liste von gefährlichen Patienten – Zugang zur Gesundheitsfürsorge). Sie beschreibt die Bestandteile, die in der Definition enthalten sein müssen, und tritt dann für Garantien ein, die ihre Verarbeitung vorsehen. In Bezug auf sonstige Garantien ist die Datenschutzkommission der Meinung, dass das Sammeln von sensiblen Daten (wie etwa Daten zur Gesundheit, Gerichtsdaten sowie Daten, die Aufschluss über die ethnische oder religiöse Zugehörigkeit geben) einer spezifischen gesetzlichen Genehmigung bedarf.

Schutz der Privatsphäre im Berufsleben

Die CPVP hat sich ebenfalls über verschiedene Aspekte des Privatlebens am Arbeitsplatz geäußert, sowohl in Bezug auf Daten der Arbeitnehmer als auch der Mitglieder des Verwaltungsrates und Führungskräfte. Sie hat somit eine Stellungnahme zu verschiedenen Gesetzesentwürfen abgegeben, die im Namen der guten Regierungsführung („Good Governance") eine Veröffentlichung von Finanzdaten von Personen anstreben, die in Führungspositionen von börsennotierten Gesellschaften, öffentlichen Unternehmen oder Vereinigungen, die von öffentlicher Hand gefördert werden, arbeiten. Ohne das Prinzip einer gezielten Veröffentlichung in Frage zu stellen, hat die Datenschutzkommission, indem sie sich auf die Rechtsprechung des europäischen Gerichtshofs stützt, auf dem Anspruch eines Gleichgewichts (Verhältnismäßigkeit) hingewiesen, das zwischen einer legitimen Kontrolle einerseits und dem Schutz des Privatlebens der betroffenen Personen andererseits zu finden ist.

Ein weiteres Thema der Datenschutzkommission war die Verwendung von Mitarbeiterausweismarken und die Lokalisierung von Arbeitnehmern über ein GPS-Lokalisierungssystem. Im Zuge der Anwendung des Grundsatzes der Verhältnismäßigkeit bei dieser Art der Datenverarbeitung wies die Datenschutzkommission darauf hin, dass eine kontinuierliche Überwachung von Mitarbeitern als unverhältnismäßig und nicht notwendig anzusehen ist. Dies wurde auch im Zusammenhang mit der Verwendung biometrischer Daten im Rahmen eines Systems von Mitarbeiterausweismarken erörtert, mit dem die Anwesenheit von Arbeitnehmern am Arbeitsplatz überprüft werden soll. Im Rahmen einer geographischen Lokalisierung wie der Sammlung von biometrischen Identifikatoren muss dieser tiefe Eingriff in die Privatsphäre der Personen unbedingt mit dem verfolgten Ziel in Einklang gesetzt werden.

Die CPVP hat zahlreiche Fragen, Informationsanfragen und auch eine Beschwerde bezüglich der Einführung von ethischen Arbeitsrichtlinien zur Weitergabe von Unternehmensinterna erhalten (siehe auch die Stellungnahme 1/2006 der Arbeitsgruppe (WP 117) vom 1. Februar 2006 über die Anwendung von EU-Datenschutzvorschriften auf innerbetriebliche Maßnahmen zur Unterstützung von Hinweisgebern („whistleblowing") in den Bereichen Buchhaltung, Rechnungsprüfung, Buchprüfung und Kampf gegen Bestechung sowie Bank- und Finanzkriminalität).

Marketing

Des Weiteren richtete die CPVP ein besonderes Augenmerk auf Marketingpraktiken, sowohl mittels einer aktiven Verfolgung der Beschwerden Einzelner als auch durch die Zusammenarbeit mit anderen nationalen oder internationalen Behörden. Der Großteil der Beschwerden, die vom Sekretariat des CPVP bearbeitet wurden, betrifft die Schwierigkeiten der Betroffenen, ihr Recht auf Widerspruch gegen eine Verarbeitung ihrer Daten für Marketingzwecke auszuüben.

Zypern

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Im Rahmen des „strukturierten Dialogs" zwischen der Europäischen Kommission und dem Büro der Datenschutzbehörde in Zypern wurde darauf hingewiesen, dass einige der Bestimmungen des Gesetzes über die Verarbeitung personenbezogener Daten (Schutz der Privatsphäre) der Republik Zypern aus dem Jahr 2001 nicht vollständig den Anforderungen der Richtlinie 95/46/EG entsprechen. Diese Bestimmungen beziehen sich in erster Linie auf den Datentransfer in Drittländer, das Recht auf Information und andere verfahrenstechnische Fragen. Das Büro der Datenschutzbehörde hat diese Punkte berücksichtigt und bereitet gegenwärtig eine Änderung des Gesetzes vor.

Das Büro richtete einen Änderungsvorschlag an die Regulierungsbehörde für elektronische Kommunikation und Postdienstleistungen bezüglich Teil 14 des Gesetzes über die Regulierung der elektronischen Kommunikation und Postdienstleistungen aus dem Jahr 2004, in dem die Bestimmungen der Richtlinie 2002/58/EG enthalten sind. Teil der vorgeschlagenen Änderungen war unter anderem die Aufnahme der Bestimmungen von Artikel 16 der Richtlinie 2002/58/EG (Übergangsbestimmungen) in dieses Gesetz.

Die Behörde machte außerdem den Vorschlag, in das Änderungsgesetz Verweise auf Anordnungen für juristische Persönlichkeiten bezüglich unerbetener Nachrichten und Daten in öffentlichen Verzeichnissen aufzunehmen, die von der Regulierungsbehörde für elektronische Kommunikation und Postdienstleistungen im Jahr 2005 in dem Abschnitt, der sich mit dem Gesetz über Telefonbücher befasst, abgefasst worden sind.

Das Gesetz über die Verletzung der Straßenverkehrsordnung aus dem Jahr 2001 wurde 2005 in Kraft gesetzt (Verwendung automatischer Kontrollgeräte und sonstige relevante Fragen). Das Gesetz sieht vor, dass gewisse Verletzungen der Straßenverkehrsordnung aufgezeichnet werden dürfen. Im Rahmen der Verfügungen dieses Gesetzes wurde der stellvertretende Polizeichef als Verantwortlicher für den Betrieb und die Verwendung dieser Geräte benannt.

Das Gesetz zum Schutz und zur Wahrung von Patientenrechten wurde 2005 in Kraft gesetzt. Dieses Gesetz regelt unter anderem die Auflagen, an die Erbringer von Gesundheitsdienstleistungen bei der Verarbeitung von medizinischen Daten gebunden sind, sowie die Rechte der Patienten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten.

B. Bedeutende Rechtsprechung

Im Rahmen der Überprüfung einer dem Büro vorgelegten Beschwerde über unverlangte SMS-Werbenachrichten (Dienst für Kurznachrichten – Textnachrichten) wurde eine Prüfung des Datendienstes, der die SMS-Nachrichten verschickt hatte, durchgeführt. Die Prüfung führte zu dem Ergebnis, dass das Unternehmen die Bestimmungen des Gesetzes über elektronische Kommunikation und Postdienstleistungen aus dem Jahr 2004 verletzt hatte, woraufhin der Datenschutzbeauftragte eine Entscheidung traf, in der dem Unternehmen die Zahlung einer Geldbuße in Höhe von 1 500 CYP auferlegt wurde.

Ein Ehepaar beschwerte sich bei der Behörde darüber, dass ihr Hochzeitsfotograf ohne ihre Einwilligung ihre Hochzeitsfotos in einem von ihm veröffentlichten Werbeprospekt verwendet hätte. Nachdem sich der Fotograf geweigert hatte, den Anweisungen der Behörde Folge zu leisten und die Fotos zu entfernen, traf der Datenschutzbeauftragte eine Entscheidung, in der dem Fotografen eine Geldbuße in Höhe von 1 000 CYP auferlegt wurde.

Die Behörde hat eine Reihe von Beschwerden über Praktiken in mehreren Ministerien erhalten, wonach

Stellenbewerber nicht über die Ergebnisse ihrer schriftlichen oder mündlichen Prüfungen informiert worden seien, die sie bei ihrer Bewerbung um eine Anstellung im öffentlichen Dienst abgelegt hatten. Die Behörde forderte in der Folge alle Ministerien in einem Rundschreiben dazu auf, die diesbezüglichen Bestimmungen des Gesetzes einzuhalten, in denen das Recht der Bewerber auf Zugang zu ihren Daten geregelt wird.

C. Wichtige spezifische Themen

Öffentliches Bewusstsein

Die zypriotische Datenschutzbehörde organisierte in Zusammenarbeit mit der Abteilung für Informationsaustausch und technische Unterstützung (TAIEX) ein Seminar in Nikosia über Kontrollen am Arbeitsplatz, das sich an Arbeitgeber und Arbeitnehmer sowohl des öffentlichen als auch des privaten Sektors richtete. Das Seminar befasste sich im Wesentlichen mit den Rechtsgrundlagen der Kontrollen, den Rechten der Beschäftigten und den Verpflichtungen der Arbeitgeber auf der Grundlage der Bestimmungen des Datenschutzgesetzes.

Der Europäische Datenschutzbeauftragte Peter Hustinx wurde eingeladen, um auf einer Veranstaltung, die das Büro in Limassol organisiert hatte, einen Vortrag über die rechtmäßige Verarbeitung personenbezogener Daten zu halten. Der Vortrag wurde vor Mitgliedern der Vereinigungen der Richterschaft und Anwaltschaft aus Limassol und Paphos gehalten.

Der Datenschutzbeauftragte veröffentlichte Leitlinien über die Verarbeitung von personenbezogenen Daten im Beschäftigungssektor. Diese Leitlinien wurden in Form einer Broschüre veröffentlicht, die im Rahmen einer ersten Initiative von der zypriotischen Handelskammer, dem Verband der Arbeitgeber und der Industrie sowie mehreren großen Gewerkschaften an Arbeitgeber und Arbeitnehmer verteilt wurde.

Auf einen Vorschlag des Datenschutzbeauftragten hin haben die zypriotische Akademie für öffentliche Verwaltung und die Polizeiakademie Zyperns das Thema des Schutzes personenbezogener Daten in Teilbereiche ihres Lehrplans aufgenommen. Die Mitarbeiter des Datenschutzbeauftragten wurden von den Akademien eingeladen, Vorträge über die Verpflichtungen von Polizei und öffentlichem Dienst bei der Verarbeitung personenbezogener Daten vor Beamten und Vertretern der Polizei zu halten.

Prüfungen und Felduntersuchungen

Die Mitarbeiter des Datenschutzbeauftragten führten eine Prüfung in der zentralen automatisierten Datenbank der Polizei, der (im Aufbau befindlichen) Datenbank des Schengener Informationssystems (SIS) und der Eurodac-Datenbank durch, um zu bewerten, inwieweit die Polizei ihre Verpflichtungen bei der Verarbeitung von Daten erfüllt. Als Ergebnis dieses Audits konnte festgestellt werden, dass die Polizei ihren Verpflichtungen insgesamt in zufrieden stellender Weise nachkommt; dennoch sprach die Behörde einige Empfehlungen aus und machte Vorschläge, um zu gewährleisten, dass die Verarbeitung den gesetzlichen Bestimmungen in jeder Hinsicht gerecht wird.

Die Notifizierungen, die eine Fluggesellschaft dem Büro vorlegte, enthielten keine angemessene Beschreibung der Datenverwaltungssysteme des Unternehmens. Aus dem anschließenden Briefwechsel ergab sich eine Reihe von Fragen. Die Mitarbeiter des Datenschutzbeauftragten besuchten das Unternehmen, um Informationen zu sammeln und zu überprüfen, ob die in den vorgelegten Notifizierungen beschriebene Datenverarbeitung mit den Verfahren übereinstimmt, die das Unternehmen im Rahmen seiner Datenverwaltungssysteme verwendet.

Die Behörde erhielt eine Reihe von Beschwerden bezüglich unerbetener SMS-Nachrichten, die von einem Unternehmen ohne vorherige Einwilligung der Empfänger versandt wurden. Daraufhin wurde in den Räumen des Unternehmens eine Prüfung durchgeführt, bei der aufgrund erster Feststellungen ermittelt werden konnte, dass das Unternehmen mit seiner Handlungsweise gesetzliche Bestimmungen verletzt

hat. Eine abschließende Entscheidung wird erst dann getroffen, wenn das Unternehmen Gelegenheit erhalten hat, seinen Standpunkt darzulegen.

Stellungnahmen und Leitlinien

Der Datenschutzbeauftragte hat eine Reihe von Stellungnahmen und Leitlinien veröffentlicht, die die rechtmäßige Verarbeitung von persönlichen Daten im privaten Sektor und in erster Linie im öffentlichen Sektor betreffen.

In drei Stellungnahmen bezüglich der von für den Datenschutz Verantwortlichen im öffentlichen Sektor verarbeiteten Daten hat der Datenschutzbeauftragte die Änderung des entsprechenden Gesetzes oder der Verordnungen empfohlen, um zu gewährleisten, dass die Datenverarbeitung den Auflagen des nationalen Datenschutzgesetzes entspricht. Diese Stellungnahmen bezogen sich auf:

(a) die Löschung überflüssiger Informationen, die anhand von Stellenbewerbungsformularen im öffentlichen Sektor erfasst wurden,

(b) die Änderung einiger Gesetze, in denen vorgesehen war, dass die jeweils zuständigen Behörden vor der Vergabe gewisser Genehmigungen die Polizei beauftragen sollten, den „guten Leumund" der Antragsteller zu überprüfen, und

(c) die Änderung einer Verordnung, die Autoverleihunternehmen dazu verpflichtete, der Datenverarbeitungsstelle der Polizei täglich die Identität aller Personen mitzuteilen, die Autos gemietet hatten.

In den beiden ersten Fällen reagierten die für den Datenschutz Verantwortlichen positiv auf die Empfehlungen des Datenschutzbeauftragten, während im dritten Fall noch keine endgültige Antwort vorliegt.

In einer Stellungnahme bezüglich der Verpflichtung der Ministerien, dem Abgeordnetenhaus im Rahmen der Ausübung seiner parlamentarischen Vollmachten personenbezogene Daten mitzuteilen, hat der Datenschutzbeauftragte die Empfehlung ausgesprochen, dass die Ministerien dem Abgeordnetenhaus die angeforderten personenbezogenen Daten unter der Voraussetzung zur Verfügung stellen, dass diese Daten für die in Betracht kommende Person von Belang sind.

Meldepflicht

Im Jahr 2005 wurden dem Büro des Datenschutzbeauftragten insgesamt 108 Notifizierungen vorgelegt, die meisten darunter von für Datenverarbeitung Verantwortlichen aus dem privaten Sektor. Es wird jedoch davon ausgegangen, dass nach wie vor eine Reihe von für die Datenverarbeitung Verantwortlichen ihre Verpflichtungen hinsichtlich der Vorlage von Notifizierungen noch nicht erfüllt haben.

Beschwerden

Im Jahr 2005 wurden dem Büro 153 schriftliche Beschwerden vorgelegt. Darüber hinaus wurden viele telefonische Beschwerden entgegengenommen, von denen die meisten Spam- und unerbetene SMS-Nachrichten betrafen.

Eine geringere Anzahl von Beschwerden bezog sich auf die Ausübung der Zugangsrechte.

Lizenzen

Im Jahr 2005 erhielt der Datenschutzbeauftragte 16 Lizenzanträge zur Übertragung von Daten in Drittländer. In zwei Fällen wurde eine Lizenz gewährt, während in drei anderen Fällen Lizenzen verweigert wurden. Über die restlichen Fälle wurde noch nicht entschieden.

Der Datenschutzbeauftragte hat außerdem neun Anträge auf eine Verbindung von Registrierungssystemen erhalten und fünf Lizenzen ausgestellt, die solche Verbindungen zulassen.

Tschechische Republik

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Die Basisverordnung, die den Schutz personenbezogener Daten regelt, ist das Gesetz Nr. 101/2000 Coll. zum Schutz personenbezogener Daten und zur Änderung einiger damit zusammenhängender Gesetze (nachstehend als Gesetz 101 bezeichnet), das am 1. Juni 2000 in Kraft getreten ist. Dieses Gesetz richtete das Amt für den Schutz personenbezogener Daten ein und stattete es mit allen notwendigen Befugnissen aus, einschließlich des Rechts, unmittelbar Geldbußen zu verhängen. Das Gesetz sorgte darüber hinaus für die Umsetzung der Richtlinie 95/46/EG in tschechisches Recht. Mit Wirkung vom 26. Juli 2004 wurde das Gesetz 101 durch das Gesetz Nr. 439/2004 Coll. geändert und so mit der oben genannten Richtlinie in Einklang gebracht.

Im Jahr 2004, als die Tschechische Republik der EU beigetreten ist, war die Umsetzung der Richtlinie 2002/58/EG nur ein Teilerfolg. Das Gesetz 480/2004 Coll. über gewisse Dienste der Informationsgesellschaft, das am 7. September 2004 in Kraft getreten ist, enthält spezifische Bestimmungen über unerbetene Nachrichten. Dieses Gesetz verlieh der Behörde für den Schutz personenbezogener Daten neue, weitreichende Befugnisse bei der Bekämpfung unerbetener Werbenachrichten, einschließlich des Rechts, bei Gesetzesübertretungen schwere Strafen zu verhängen. Die Richtlinie 2002/58/EC wurde anschließend im Wesentlichen durch das Gesetz über elektronische Kommunikation Nr. 127/2005 Coll. umgesetzt, das am 1. Mai 2005 in Kraft getreten ist. Dieses Gesetz setzt gleichzeitig eine ganze Reihe anderer Richtlinien des so genannten „Telekommunikationspakets" um. Der schwierige legislative Prozess der Umsetzung der Richtlinie 2002/58/EG in nationales Recht führte zu geringfügigen Unstimmigkeiten in Artikel 7 des Gesetzes Nr. 480/2004, was von der Europäischen Kommission kritisiert wurde. Diese Unstimmigkeiten werden durch einen schnell durchführbaren Änderungsantrag im ersten Halbjahr 2006 behoben.

In Übereinstimmung mit den für die Regierung der Tschechischen Republik geltenden gesetzlichen Bestimmungen ist die Behörde die erste Stelle, der Entwürfe von in ihren Zuständigkeitsbereich fallenden Rechtsakten im Rahmen interministerieller Verfahren zur Stellungnahme zusammen mit anderen Verordnungen vorgelegt werden müssen – also noch bevor die Entwürfe beim Parlament zur Vorlage kommen. Im Jahr 2005 gab die Behörde ihre Stellungnahmen zu einer Reihe von Verordnungen ab. Zu den entscheidendsten Stellungnahmen zählten Vorschläge zu einem Entwurf des Gesetzes zur Änderung einiger Gesetze im Bereich der Reisedokumente, um den EU-Verordnungen Rechnung zu tragen, die die Einbeziehung von biometrischen Daten in Reisedokumente verlangen. Die Behörde verfolgte in erster Linie das Ziel, eine Ausweitung des Anwendungsbereichs gescannter Fingerabdrücke über den in der Ratsverordnung 2252/2004 beantragten notwendigen Anwendungsbereich hinaus zu vermeiden und darüber hinaus bei der Ausstellung von Reisedokumenten den betroffenen Personen die korrekte Vornahme der Datenüberprüfung zu gewährleisten.

B. Bedeutende Rechtsprechung

Im Jahr 2005 wurden in zwei Fällen von der Behörde getroffene Entscheidungen durch Verwaltungsklagen angefochten; diese Fälle wurden bisher noch nicht entschieden. Zwei Fälle aus dem Jahr 2004 und ein Fall aus dem Jahr 2002 wurden noch nicht abgeschlossen. Der oben genannte älteste noch nicht geklärte Fall betrifft ein Finanzinstitut, dem es nicht gelungen ist, die personenbezogenen Daten seiner Kunden

wirksam zu schützen und dessen elektronische Ausrüstungen mit Aufzeichnungen der personenbezogenen Daten von mehreren hunderttausend Kunden gestohlen wurden. Die Entscheidung der Behörde, eine Geldbuße zu verhängen, wurde im Jahr 2003 durch eine Klage angefochten, die im Jahr 2004 vom Verwaltungsgericht der Stadt Prag abgewiesen wurde, womit die Entscheidung der Behörde erneut wirksam war. Anschließend hat sich das Finanzinstitut mit einer Beschwerde gegen die Entscheidung gewehrt, über die jedoch bis heute vom obersten Verwaltungsgericht noch nicht entschieden wurde.

Ein weiterer Fall, der gegenwärtig noch von den Gerichten verhandelt wird, betrifft eine Entscheidung der Behörde, in der sie es abgelehnt hat, einer natürlichen Person den Status eines Beteiligten an Verwaltungsverfahren zu gewähren, die im Jahr 2004 durchgeführt wurden. Die betroffene Person hat gegen diese Entscheidung Verwaltungsklage eingelegt, die dazu geführt hat, dass die Entscheidung Anfang 2005 vom Verwaltungsgericht abgelehnt wurde, womit wie im vorangegangenen Fall ein Aufschub bei der Ausführung der Entscheidung der Behörde erreicht wurde. Gegen diese Entscheidung wurde ebenfalls eine Beschwerde eingelegt, über die vom obersten Verwaltungsgericht bis heute noch nicht entschieden wurde.

Der andere Fall aus dem Jahr 2004 betrifft ebenfalls eine Entscheidung der Behörde, eine Geldbuße wegen einer unzulässigen Verarbeitung personenbezogener Daten im Zusammenhang mit Entschließungen der Kommunalbehörden einer Stadt zu verhängen, die in vollem Wortlaut auf der Website der Stadtverwaltung veröffentlicht wurden (d. h. ohne die Verpflichtung zum Schutz personenbezogener Daten einzuhalten). Im Oktober 2004 wurde die Entscheidung des Amts durch eine Verwaltungsklage angefochten, über die das Prager Verwaltungsgericht bis heute noch nicht entschieden hat.

C. Wichtige spezifische Themen

Die von der Behörde im Jahr 2005 ausgeführten Kontrollen umfassten in erster Linie Ad-hoc-Kontrollen, d.h. die Überprüfung von Beschwerden. Insgesamt wurden 80 Ad-hoc-Kontrollen ausgeführt, von denen 68 abgeschlossen wurden. So konnten 133 Beschwerden beantwortet werden. Andere Beschwerden wurden von den Inspektoren in anderer Form gehandhabt als durch Kontrollen, d. h. indem der Anlass für die Beschwerde beseitigt werden konnte. Kontrollen wurden in Banken, Leasingunternehmen, Handels- und Bauunternehmen, Gesundheitsversorgungseinrichtungen und pharmazeutischen Unternehmen durchgeführt, aber auch in Regierungsstellen und selbstverwalteten Einrichtungen. Außerdem konnten mehrere umfassende Kontrollen auf der Grundlage des Kontrollplans ausgeführt werden:

Die im Jahr 2005 festgestellten Gesetzesübertretungen betrafen im Wesentlichen

- die unzulässige Verarbeitung von unrichtigen oder überschüssigen Daten

- den unzulässigen Transfer von Daten an einen anderen für die Datenverarbeitung Verantwortlichen

- unzureichende oder unrichtige Informationen über die von der Datenverarbeitung betroffenen Personen

- die Verarbeitung von sensiblen Daten ohne ausdrückliche Einwilligung der betroffenen Personen

- die ungenügende Absicherung von personenbezogenen Daten, z. B. als eine Folge unangemessener Zugangsbestimmungen in einem Informationssystem, das Unbefugten Zugang zu personenbezogenen Daten eröffnet.

Die bei der Behörde im vergangenen Jahr eingetroffenen Aufforderungen und Beschwerden betrafen im Wesentlichen folgende Bereiche:

1) Öffentliche Verzeichnisse. Die Mehrzahl der Aufforderungen und Beschwerden richtete sich gegen übermäßige Veröffentlichungen oder Bereitstellungen von personenbezogenen Daten und Kopien von Urkunden, die solche Daten enthalten. Dies trifft z. B. auf die Fälle zu, in denen der kommerziell verwaltete Datenbestand aufgrund des Zwecks, zu dem er eingerichtet wurde, nach wie vor hinsichtlich der Begründung einer Veröffentlichung von bestimmten Auszügen aus dem Bestand an personenbezogenen Daten einschließlich Geburtsdaten diskutiert wird.

2) Die Veröffentlichung von Daten aus Sitzungen der kommunalen Verwaltungen und Gemeinderäte, insbesondere im Internet. Die Anzahl der Beschwerden in diesem Bereich ist im Verhältnis zum Jahr 2004 zurückgegangen, nachdem die Behörde eine aktualisierte Stellungnahme und Leitlinien herausgegeben hat und von den zuständigen Einrichtungen die notwendigen Maßnahmen ergriffen wurden und die betreffenden personenbezogenen Daten aus den Dokumenten der kommunalen Verwaltungen aufgrund der Bestimmungen einer spezifischen Gesetzgebung, die die Zuständigkeiten dieser kommunalen Verwaltungen regelt, verfügbar gemacht werden konnten.

3) Verarbeitung von personenbezogenen Daten im Bereich der kommunalen Dienstleistungen. Aufgrund von Beschwerden, die bei der Behörde eingereicht wurden, kann festgestellt werden, dass die Bürger in diesem Bereich nicht immer ausreichend über die Aktivitäten privater Einrichtungen informiert sind, die über Genehmigungen von öffentlichen, selbstverwalteten Organen verfügen. Hierdurch wird deutlich, dass die Erbringung von Dienstleistungen durch öffentliche Einrichtungen notwendigerweise beinhaltet, dass die Bürger Informationen über ihre Rechte und Pflichten erhalten; dabei muss das Recht der Datenverarbeitung eng mit der Verpflichtung verbunden sein, die betroffene Person über die Verarbeitung ihrer personenbezogenen Daten zu informieren.

4) Die Verwaltung von personenbezogenen Daten von Mitarbeitern. Vermutungen deuten oft darauf hin, dass die Verwaltung von personenbezogenen Daten unter anderem bei der Beilegung von arbeitsrechtlichen Auseinandersetzungen als ein Druckmittel eingesetzt werden könnte. Solche Anregungen werden in Zusammenarbeit mit Vertretungen der Arbeitnehmerinteressen und gegebenenfalls mit den seit dem 1. Juli 2005 neu eingerichteten Arbeitsaufsichtsbehörden besprochen.

5) Kopien persönlicher Dokumente. Änderungsanträge zu den Gesetzen über Personalausweise und Pässe (die ab dem 1. Januar in Kraft treten) haben sich in diesem Zusammenhang eindeutig als sehr nützlich erwiesen; Übertretungen, bei denen Dokumente ohne die Einwilligung der Bürger kopiert werden, führen jetzt zu einer Verfolgung durch die kommunalen Behörden. Die Behörde kümmert sich jedoch weiterhin um die Fälle, in denen eine Kopie des persönlichen Dokuments insbesondere für die Aufnahme einer Vertragsbeziehung erforderlich ist, und überprüft auch in den Fällen, in denen besonders deutlich wird, dass eine unnötige Erhebung persönlicher Daten stattfinden könnte, die Notwendigkeit der Erhebung und Form der Verwendung aller persönlichen Daten, die auf der Kopie eines Dokuments in Erscheinung treten.

Auf Grundlage von Kontrollergebnissen der Inspekteure des Amts wurde eine Reihe von Geldbußen verhängt, wie die folgenden Beispiele verdeutlichen:

In Verbindung mit der Ausübung ihrer Befugnisse auf Grundlage des Gesetzes über den Schutz personenbezogener Daten verhängte die Behörde im

vergangenen Jahr ihre höchste Geldbuße gegen eine Bürgervereinigung, die in dem Bestreben, auf das Thema der regulierten Mieten aufmerksam zu machen, persönliche Daten spezifischer Mieter von Wohnungen herausgesucht, zusammengestellt und auf ihrer Website veröffentlicht hatte, die ihrer Auffassung nach nicht auf Mieterleichterungen in Form von regulierten Mieten angewiesen sind. Auf diesem Weg wurden Daten verarbeitet, die eine Identifizierung der betroffenen Personen ermöglichen, einschließlich ihres Geburtsdatums, sowie sensible personenbezogene Daten, die auf ihre politischen Orientierungen hinweisen, zusammen mit Informationen über in ihrem Besitz befindliche Immobilien und Aufstellungen ihrer Eigentumstitel, neben Auszügen aus Katastereintragungen.

Das Amt verhängte außerdem eine schwere Geldbuße gegen eine Wohngenossenschaft, die im Zusammenhang mit der Ausübung ihrer Rechte und Pflichten bei der Verwaltung eines Mietshauses in diesem Mietshaus ein kameragestütztes Überwachungssystem installiert und betrieben hat, mit dem personenbezogene Daten von Wohnungsmietern in diesem Gebäude ohne ihre Einwilligung verarbeitet wurden. Die dort montierten Kameras wurden im Dauerbetrieb eingesetzt und zeichneten die Vorkommnisse in den Gemeinschaftsräumen des Gebäudes dergestalt auf, dass jede Person, die ihre Wohnung betrat oder verließ, in den Gemeinschaftsräumen erfasst werden konnte; die Auflösung der Kameras reichte aus, um Personen und ihre Aktivitäten identifizieren zu können. Zusätzlich wurden elektronische Schlösser in dem Gebäude installiert, für die jeder Bewohner einen passenden persönlichen und spezifisch identifizierbaren Chip erhielt. Die mit den elektronischen Schlössern ausgestatteten Räume wurden ebenfalls von Kameras überwacht. Die Aufzeichnungen der Kameras und der elektronischen Schlösser bildeten ein umfassendes Informationssystem, mit dessen Verwendung die Möglichkeit eröffnet wurde, in den Gemeinschaftsräumen des Gebäudes Informationen über die Bewegungen und Aktivitäten von natürlichen Personen, d. h. Mietern, Mitgliedern der Genossenschaft und anderen Besuchern, zu erhalten.

Eine weitere Geldbuße wurde gegen eine staatliche Einrichtung im Zusammenhang mit dem Scannen von biometrischen Daten und Bildern von Fingerabdrücken verhängt. Die Erfassung von Fingerabdruckdaten erfolgte dort routinemäßig, womit die spezifischen, für diese Einrichtung geltenden Bestimmungen verletzt wurden, namentlich im Hinblick auf Personen, die die Voraussetzungen für eine zulässige Abnahme der Fingerabdrücke nicht erfüllten, so wie sie aus den spezifischen Gesetzen hervorgehen; außerdem wurden die Fingerabdruckdaten im Rahmen der Ausführung unterschiedlicher Aufgaben dieser Einrichtung nicht von anderen Daten getrennt verarbeitet.

Die Behörde verhängte darüber hinaus hohe Geldbußen im Rahmen der Ausübung ihrer neuen Zuständigkeit auf Grundlage des Gesetzes über bestimmte Dienstleistungen der Informationsgesellschaft. Diese Zuständigkeit deckt den Bereich der Verschickung unerbetener kommerzieller Nachrichten bzw. kommerziellen E-Mülls („Spams“) ab.

Dänemark

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

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 dieses Gesetzes kann auf folgender Website abgerufen werden: http://www.datatilsynet.dk/eng/index.html

Das Gesetz setzt die Umsetzung der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr um.

Die Richtlinie 2002/58/EG wurde ins nationale dänische Recht übertragen durch:

- die dänische Verfassung
- Gesetz über Marketingpraktiken, Paragraph 6 (siehe Gesetz Nr. 1389 vom 21. Dezember 2005)
- Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten
- Gesetz über die Wettbewerbsbedingungen und den Verbraucherschutz auf dem Telekommunikationsmarkt (vgl. Durchführungsverordnung Nr. 784 vom 28. Juli 2005)
- Durchführungsverordnung Nr. 638 vom 20. Juni 2005 über die Bereitstellung elektronischer Kommunikationsnetze und Dienstleistungen
- Kapitel 71 des Gesetzes über Rechtspflege (Law on Administration of Justice), vgl. Durchführungsverordnung Nr. 777 vom 16. September 2002
- Paragraph 263 des Strafgesetzbuches, vgl. Durchführungsverordnung Nr. 779 vom 16. September 2002.

Gemäß Artikel 57 des dänischen Gesetzes über die Verarbeitung personenbezogener Daten wird um eine Stellungnahme der dänischen Datenschutzbehörde Datatilsynet ersucht, wenn Verordnungen, Rundschreiben oder ähnliche allgemeine Richtlinien für den Schutz der Privatsphäre in Zusammenhang mit der Datenverarbeitung herausgegeben werden. Dies gilt auch für Gesetzentwürfe. Die Datenschutzbehörde (DB) hat zu verschiedenen Gesetzen und Regelungen, die Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz haben, Stellung bezogen.

1. Im Jahr 2005 hat sich die DB genau wie im Jahr 2004 sehr ausführlich mit der anstehenden Reform der Struktur des öffentlichen Sektors befasst.

Die DB wurde gebeten, zu einem Regierungserlass Stellung zu nehmen, der in Steuerangelegenheiten die Verarbeitung personenbezogener Daten durch kommunale Einwohnerdienste im Auftrag der nationalen Steuerbehörden vorsah. Dieser Vereinbarung zufolge würden die Kommunalbehörden Zugang zu allen Daten erhalten, die im System der Steuerbehörden gespeichert sind.

Die DB wies darauf hin, dass der Transfer von Daten an einen Datenverarbeiter auf einer schriftlichen Vereinbarung zwischen den Parteien beruhen muss. Die DB war der Auffassung, dass ein solcher Zugang den Einsatz zusätzlicher Sicherheiten erneut notwendig macht und dass der Zugang zu den Daten aufgrund geografischer und organisatorischer Voraussetzungen gewährt werden sollte.

2. Die DB wurde gebeten, zu einem Gesetzentwurf Stellung zu nehmen, der die Einrichtung eines elektronischen Einkommensverzeichnisses betraf, in dem Informationen über das monatliche Einkommen und den Beschäftigungsstatus enthalten sein sollten. Dieses Verzeichnis verfolgte den Zweck, die Kommunikation zwischen Bürgern und Unternehmen zu vereinfachen, indem sichergestellt werden sollte, dass niemand dieselben Informationen zweimal mitteilen muss.

Die DB wies darauf hin, dass das Verzeichnis neben einer effizienteren Kommunikation auch die Kontrolle der Bürger vereinfacht hat, und vertrat die Auffassung, dass in dem Gesetz deutlich gemacht werden sollte, in welchem Umfang beabsichtigt wird, den Behörden Gelegenheit zu geben, die Daten von Bürgern anhand des Verzeichnisses zu überprüfen.

Die DB stellte fest, dass ein Zugang zu dem Verzeichnis nur dann erfolgen kann, wenn dies ausdrücklich im Rahmen einer anderen Gesetzgebung vorgesehen ist, und machte deutlich, dass es ganz

wesentlich ist, in jedem Fall zu beurteilen, ob ein Zugang zu dem Verzeichnis erforderlich ist.

3. Im Juli 2005 wurde ein neues dänisches Gesetz über Internet-Domänen angenommen. Dem neuen Gesetz zufolge können nur Eintragende im Whois-Verzeichnis anonym geführt werden und nur unter der Voraussetzung, dass die betreffende Person im dänischen Bürgerregister (CPR) und/oder im Telefonverzeichnis anonym geführt wird. Die DB erklärte, dass grundsätzlich alle Bürger die Möglichkeit haben sollten, in öffentlichen Verzeichnissen anonym geführt zu werden.

B. Bedeutende Rechtsprechung

1. Im Anschluss an eine Notifizierung über die Verarbeitung personenbezogener Daten, die jugendliche Sexualtäter, ihre Familien und Opfer betreffen, erklärte die DB, dass die Sexualtäter und ihre Familien einer Verarbeitung der Daten zustimmen müssten. Hinsichtlich einer die Opfer betreffenden Datenverarbeitung erklärte die DB, dass es unter Umständen nicht immer möglich sei, die Zustimmung des Opfers zu erhalten, und dass Informationen ohne dessen Zustimmung verarbeitet werden dürften, wenn dies notwendig sei, um dem jugendlichen Sexualtäter die bestmögliche Therapie anzubieten.

Da keine Notifizierungen erfolgten und angemessene Sicherheiten fehlten, teilte die DB dem zuständigen Ministerium mit, dass das Gesetz über die Verarbeitung personenbezogener Daten nicht befolgt worden sei.

2. Die dänischen Bibliotheken forderten die DB auf, sie zu informieren, ob es mit dem Datenschutzgesetz vereinbar ist, Bürgern per E-Mail unverschlüsselte Informationen über die Reservierung von Büchern zu schicken.

Die DB war der Auffassung, dass Daten über eine persönliche Auswahl von Bibliotheksbüchern vertraulich seien und nicht unverschlüsselt über das Internet mitgeteilt werden sollten. Dennoch hat die DB angesichts der geringen Anzahl von Bürgern, die in der Lage sind, verschlüsselte E-Mails zu empfangen, ausnahmsweise eingewilligt, dass Bibliotheken während eines Fünfjahreszeitraums weiterhin diese E-Mail-Nachrichten unverschlüsselt versenden dürfen. Die DB forderte die Bibliotheken auf, den Fünfjahreszeitraum zu nutzen, um Systeme einzuführen, die das Sicherheitsniveau bei der Übermittlung von Informationen über das Internet erhöhen.

3. Die DB wurde aufgefordert, die das Recht auf Information betreffenden Bestimmungen im Hinblick auf die Situationen zu interpretieren, in denen die von den Daten betroffene Person ein Minderjähriger ist.

Die DB vertrat die Auffassung, dass Minderjährige auf Grundlage derselben Regeln Informationen erhalten sollten wie alle anderen Betroffenen, wenn sie älter als 15 Jahre sind. In diesen Fällen sollten die Informationen auch den Eltern oder dem Vormund des Kindes mitgeteilt werden, es sei denn, dass es sich um so persönliche Informationen handelt, dass dies als eine Verletzung der Privatsphäre ausgelegt werden könnte. Wenn das Kind jünger als 15 Jahre ist, sollten die Informationen einem Elternteil oder dem Vormund mitgeteilt werden.

C. Wichtige spezifische Themen

Im Jahr 2005 fasste der Justizminister den Beschluss, eine Expertengruppe einzurichten, um die bestehende Gesetzgebung zum Thema CCTV-Überwachung (Closed Circuit Television) zu evaluieren und eine Bewertungsgrundlage zu bilden, anhand der ermittelt werden kann, wo die Trennungslinie zwischen der Notwendigkeit für Sicherheit und Verbrechensprävention und dem Anrecht eines Bürgers auf seine Privatsphäre gezogen werden muss.

Die Entscheidung beruhte unter anderem auf einer vor kurzem veröffentlichten Stellungnahme der Datenschutzbehörde, die auf eine Reihe offener Fragen im Zusammenhang mit der gemeinsamen Umsetzung des Gesetzes über CCTV-Überwachung und des Gesetzes über die Verarbeitung personenbezogener Daten hinwies.

Die Expertengruppe will ihre Evaluierung vor dem 1. September 2006 abschließen.

Estland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Es haben sich keine wesentlichen Weiterentwicklungen ereignet, aber die Arbeitsgruppe arbeitet intensiv an den Änderungen des estländischen Datenschutzgesetzes.

B. Bedeutende Rechtsprechung

Bürger gegen die estländische Datenschutzbehörde (EDPI)

Zwei Bürger reichten Beschwerden bei der estländischen Datenschutzbehörde (EDPI) über die Grenzschutzverwaltung (BGA) und die Staatsanwaltschaft (PPO) ein, weil diese Stellen es versäumt hätten, die EDPI über die Verarbeitung sensibler, personenbezogener Daten zu informieren. Die Datenschutzbehörde leitete ein Verfahren wegen Amtsvergehens hinsichtlich der versäumten Mitteilung ein, aber die EDPI gab dem Antrag der Antragsteller nicht statt, der Verarbeitung sensibler, personenbezogener Daten auf Ebene der BGA und des PPO ein Ende zu setzen und die sensiblen Daten, die die Antragsteller betreffen, zu löschen. In diesem Fall vertrat die EDPI die Auffassung, dass das Recht der von der Datenverarbeitung betroffenen Person, eine Löschung ihrer personenbezogenen Daten zu beantragen und die Verarbeitung von sensiblen Daten durch die Behörde zu unterbinden, nicht uneingeschränkt gilt. Zunächst besteht für die betroffenen Behörden eine gesetzliche Verpflichtung, diese Daten zu verarbeiten. Die Tatsache, dass die Behörden die Verarbeitung sensibler Daten nicht mitgeteilt haben, ist sekundär und sollte kein Grund sein, diese Behörden an ihrer Weiterarbeit zu hindern.

Die Antragsteller waren mit der Entscheidung des EDPI nicht einverstanden und legten vor dem Verwaltungsgericht Berufung ein. Das Gericht verwarf den Einspruch der Antragsteller und bestätigte die Entscheidung des EDPI.

Anschließend gingen die Antragsteller vor dem für mehrere Bezirke zuständigen erstinstanzlichen Gericht in die Berufung, die erneut abgewiesen wurde.

C. Wichtige spezifische Themen

Im Verlauf der Jahre stellte sich heraus, dass sich die meisten Schwierigkeiten im Zusammenhang mit der Verarbeitung von Daten zu wissenschaftlichen und statistischen Zwecken ergeben.

Die neuste Fassung des Gesetzes über den Schutz personenbezogener Daten ist im Oktober 2003 in Kraft getreten. Diesem Gesetz zufolge muss für die zu statistischen, historischen und wissenschaftlichen Zwecken ausgeübte Datenverarbeitung die Einwilligung des Betroffenen eingeholt werden. Außerdem ist es zur Erfüllung der gesetzlichen Auflagen notwendig, die Verarbeitung der sensiblen Daten der EDPI mitzuteilen.

Die Uneinigkeiten mit Wissenschaftlern und Statistikern beziehen sich auf das Gesetz, und gegenwärtig werden nach wie vor Anstrengungen unternommen, um Lösungen zu finden (Änderungsanträge zu den Gesetzen, eine Zusammenarbeit zwischen der EDPI und den statistischen/wissenschaftlichen Behörden usw.).

Finnland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Die Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) wurde in Finnland durch das Gesetz zum Schutz personenbezogener Daten (523/1999) durchgeführt, das am 1. Juni 1999 in Kraft getreten ist. Dieses Gesetz wurde am 1. Dezember 2000 durch die Aufnahme von Bestimmungen über die Entscheidungsfindung der Kommission und durch die Festlegung überarbeitet, wie verbindlich diese Entscheidungen in Fragen des Transfers personenbezogener Daten in Länder außerhalb der Europäischen Union unter der Datenschutzrichtlinie sind.

Der Schutz der Privatsphäre gehört in Finnland seit dem 1. August 1995 zu den Grundrechten. Im Rahmen der finnischen Verfassung wird der Schutz personenbezogener Daten durch einen eigenständigen Gesetzestext geregelt.

Das am 1. September 2004 in Kraft getretene Gesetz über den Datenschutz in der elektronischen Kommunikation (516/2004) setzte die Datenschutzrichtlinie (2002/58/EG) für die elektronische Kommunikation um. Das Gesetz über den Datenschutz in der elektronischen Kommunikation (516/2004), das am 1. September 2004 in Kraft trat, setzte die Datenschutzrichtlinie für die elektronische Kommunikation (2002/58/EG) um. Zweck dieses Gesetzes ist die Gewährleistung der Vertraulichkeit und der Schutz der Privatsphäre in der elektronischen Kommunikation, die Verbesserung der Sicherheit in der elektronischen Kommunikation sowie die ausgewogene Entwicklung der elektronischen Kommunikationsdienste. Die Verantwortung für die Durchsetzung des Gesetzes ist geteilt, so dass der Auftrag des Büros des Datenschutzbeauftragten folgende Aufgaben umfasst:

- Regulierung der Verarbeitung von Ortungsdaten,
- Regulierung des Direktmarketing,
- Regulierung der Katalogisierungsdienste und
- Regulierung des Informationsrechtes der Benutzer.

In diesem Zusammenhang muss erwähnt werden, dass der Staatsanwalt laut dem Strafgesetzbuch zur Rücksprache mit dem Datenschutzbeauftragten verpflichtet ist, bevor er im Fall einer Verletzung der Vertraulichkeit in der elektronischen Kommunikation Anklage erhebt.

B. Bedeutende Rechtsprechung

Im internationalen Vergleich ist die in Finnland in den Haushalten anfallende Menge an Werbemüll relativ unbedeutend. Es wird davon ausgegangen, dass die von finnischen Betreibern verbreitete Menge an Werbemüll deutlich zurückgegangen ist. Dennoch führte im Jahr 2005 die Interpretation von Paragraph 26 des Gesetzes über den Datenschutz in der elektronischen Kommunikation zu großen Schwierigkeiten. Diesem Paragraphen zufolge ist ein Verkäufer, der die E-Mail-Adresse eines Kunden im Rahmen eines Verkaufs erhalten hat, berechtigt, diese Adresse ohne die vorherige Einwilligung des Kunden, die ansonsten vorausgesetzt wird, für die Verschickung von Werbenachrichten bezüglich eigener identischer oder ähnlicher Produkte oder Dienstleistungen zu verwenden. Das Problem bestand darin, zu definieren, was unter „ähnlich" zu verstehen ist. In den meisten Fällen wurde allem Anschein nach deutlich, dass die von der Datenverarbeitung betroffenen Personen, die Beschwerden eingereicht hatten, sich noch

nicht einmal dessen bewusst waren, dass sie eine Kundenbeziehung zu dem Unternehmen unterhielten, das die Werbenachrichten verschickt hatte, obwohl das Gesetz über die Verarbeitung personenbezogener Daten die Verpflichtung beinhaltet, sie über die Verarbeitung von Daten zu informieren.

Hinsichtlich der Telefonverzeichnisse und Nummerndienste veröffentlichte die Behörde des Datenschutzbeauftragten im Sommer 2005 einen Bericht, aus dem hervorging, dass Betreiber die Teilnehmer nicht umfassend und genau genug über ihre Rechte und die Verzeichnisdienste, in denen die Teilnehmerinformationen gespeichert werden, informiert hatten. Andererseits geht aus dem Bericht hervor, dass die Teilnehmer von den Betreibern allem Anschein nach angemessen über die Verwendung von Ortungsdaten informiert wurden.

Gegenwärtig befinden sich in Finnland mehrere Gesetze in Vorbereitung, die wesentliche Bestimmungen über die Verarbeitung von personenbezogenen Daten enthalten. Zu diesen Gesetzen zählen unter anderem das neue Gesetz über Kreditinformationen, das Gesetz über Einwohnerinformationen und das Gesetz über die elektronische Verarbeitung von Kundendaten in Sozial- und Gesundheitsversorgungsdiensten.

Das vorgeschlagene Gesetz über Kreditinformationen ist als umfassendes Gesetz vorgesehen, das alle Aktivitäten und Verarbeitungstätigkeiten im Bereich der Kreditinformationen umfasst. Es würde bei der Verarbeitung von Kreditinformationen im Zusammenhang mit Verbrauchern, Unternehmen und den auf Unternehmensebene hierfür zuständigen Personen zur Anwendung kommen. Das Gesetz würde das Verzeichnis für Kreditinformationen und die dort eingetragenen Daten sowie die Dauer der Aufbewahrung der Informationen in dem Verzeichnis regeln. Die Datenqualität der Kreditinformationsverzeichnisse würde unter anderem dadurch erhöht, dass die Dauer der Speicherung von Zahlungsversäumnissen in diesen Verzeichnissen gestaffelt wird, je nachdem ob der Betroffene erneut Zahlungsaufforderungen nicht nachgekommen ist oder auch unter Berücksichtigung von Eintragungen mit Hintergrundinformationen über Zahlungsverzögerungen, beispielsweise bezüglich ihrer Verbindung mit einer Garantiehaftung. Das neue Gesetz würde die Bestimmungen über persönliche Kreditinformationen ersetzen, die heute in dem Gesetz über personenbezogene Daten enthalten sind. Der Datenschutzbeauftragte wäre für die Kontrolle und Umsetzung des neuen Gesetzes zuständig.

Das Gesetz über die elektronische Verarbeitung von Benutzerdaten in Sozialdiensten und Gesundheitsdiensten würde sich sowohl auf die interne elektronische Datenverarbeitung durch die Datenkontrolleure beziehen als auch auf den elektronischen Datentransfer zwischen verschiedenen für die Verarbeitung personenbezogener Daten Verantwortlichen.

Die Änderung des Gesetzes über das Einwohnerverzeichnis zielt darauf ab, eine Gesetzgebung zu verwirklichen, die die Pflege, Verwendung und Systeme sowie die Entwicklung der Dienste im Zusammenhang mit den Daten, die in dem Einwoh nerinformationssystem enthalten sind, und die zertifizierten elektronischen Transaktionen besser und genauer regelt. Die überarbeitete Gesetzgebung ist darauf ausgerichtet, die Grundrechte der Bürger besser zu berücksichtigen, insbesondere den Schutz der Privatsphäre und der personenbezogenen Daten und den Rechtsschutz und eine verantwortungsbewusste Regierungsführung.

C. Wichtige spezifische Themen

Die Anzahl der von der Behörde des Datenschutzbeauftragten bearbeiteten Fälle ist in dem Zeitraum von 2004 bis 2005 um etwa 20 Prozent gestiegen. Im Jahr 1998 betrug das Verhältnis der Beschwerden, die sich an den privaten Sektor richteten, im Vergleich zu den an den öffentlichen Sektor gerichteten Beschwerden 1:1,17, während es im Jahr 2005 1:1,74 erreichte. Damit entsprachen jeder an den öffentlichen Sektor gerichteten Beschwerde fast zwei Beschwerden, die an den privaten Sektor gerichtet wurden.

Der Grund für diese Entwicklung liegt wahrscheinlich darin, dass in Übereinstimmung mit Paragraph 10 der finnischen Verfassung die Verarbeitung personenbezogener Daten durch öffentliche Behörden in der Regel gesetzlich geregelt ist. Darüber hinaus verfügt der öffentliche Sektor über zentrale Kontrollen auf nationaler Ebene. Sie werden im Rahmen von Entwicklungsprogrammen auf der Ebene der nationalen Regierung und der Gebietskörperschaften organisiert. Die Zahlen machen jedoch deutlich, dass die Veränderung des Verhältnisses nicht im Wesentlichen auf eine Verbesserung im öffentlichen Sektor zurückzuführen ist, sondern auf eine Verschlechterung im privaten Sektor. Tatsächlich versuchen private Unternehmen, Grenzbereiche der Gesetze auszuloten.

Ein Vertreter der Behörde hat an etwa 30 verschiedenen Arbeitsgruppen oder vergleichbaren Einrichtungen teilgenommen, die von unterschiedlichen Behörden eingesetzt wurden. In diesem Zusammenhang kam der Zusammenarbeit mit dem Lenkungsausschuss für Datensicherheit in der öffentlichen Verwaltung (VAHTI) besondere Bedeutung zu. Außerdem fand eine regelmäßige, informelle Zusammenarbeit mit einer Reihe anderer Interessengruppen statt. Im Jahr 2005 wurden 45 Erklärungen zu legislativen Fragen und 20 Erklärungen zu Verwaltungsreformprojekten abgegeben. Ein Vertreter der Behörde wurde während des Jahres 29 Mal im Parlament angehört.

In der Informationsgesellschaft hat sich die gesellschaftliche Bedeutung der Daten und ihrer Verarbeitung geändert, da die Datenverarbeitung mehr und mehr als fester Bestandteil der Durchführung aller grundlegenden Prozesse verstanden wird. Heute werden Datenschutz und -sicherheit in die Prozesse integriert. Gleichzeitig wächst das Bewusstsein dafür, dass Daten ein Kapital darstellen, das geschützt und verwaltet werden muss. Die Datenverarbeitung muss darüber hinaus an Regeln gebunden sein. Seit kurzem wird die Datensicherheit als Mittel verstanden, um die Rechtswirksamkeit von Diensten und anderen Prozessen zu sichern. Glücklicherweise wird die Datensicherheit nicht länger ausschließlich als technische Aktivität betrachtet. Es entsteht vielmehr ein Bewusstsein dafür, dass Anleitungen, Ausbildung und Planung auch Mittel zur Verwirklichung der Datensicherheit darstellen.

Mehr und mehr wird deutlich, dass die Hervorhebung der Bedeutung des Datenschutzes und seiner Förderung einen wesentlichen Beitrag dazu leistet, das Vertrauen der Menschen zu stärken. Das Bewusstsein setzt sich durch, dass jede Datensystemlösung auch eine Maßnahme zum Schutz der Grundrechte der Bürger darstellt. Bei der Einsetzung neuer Technologien wird immer stärker berücksichtigt, welche Datenschutz- und Sicherheitsrisiken sie nicht nur für die Bürger, sondern auch für das gesamte System beinhalten.

Datenschutzanliegen ließen sich bisher relativ gut mit den Schwierigkeiten vereinbaren, die sich aus der Verwendung des Internets ergeben. Im Gegensatz zu anderen Ländern hat sich Identitätsdiebstahl in Finnland bis heute nicht zu einem sehr verbreiteten Problem

entwickelt. Dennoch deuteten vermehrte Online-Transaktionen, die das Internet und mobile Dienste verwendeten, darauf hin, dass dieses Problem auch in Finnland besteht. Deshalb veröffentlichte die Behörde des Datenschutzbeauftragten mehrere Leitlinien zu diesem und zu angrenzenden Themen.

Im Hinblick auf die öffentlichen Verwaltungen gab das Innenministerium Ende 2005 einen Bericht über öffentliche Onlinedienste in Auftrag. Der Bericht ergab, dass die Verbraucher heute bei der Verwendung ihrer Bank- oder Kreditkarteninformationen oder ihrer persönlichen Daten im Internet vorsichtiger sind. Die Kenntnisse der Verbraucher im sicheren Umgang mit Daten wurden beispielsweise durch die Organisation einer nationalen Datensicherheitskampagne und eines Datensicherheitstages verbessert, die sogar im Ausland Interesse geweckt haben. Ende 2005 organisierte der Rat für die Informationsgesellschaft darüber hinaus eine Kampagne zur Steigerung des öffentlichen Bewusstseins. Die Dokumentation und Themen beider Kampagnen umfassten Bereiche und Leitlinien, die die Verarbeitung personenbezogener Daten zum Gegenstand hatten.

Die Verbreitung von Informationen über das Internet durch die Stadtverwaltungen und die damit zusammenhängende Verarbeitung personenbezogener Daten führten dazu, dass sich die Bürger eine Vielzahl von Fragen gestellt haben. Deshalb war es wichtig, dass die Vereinigung lokaler und regionaler finnischer Behörden im Jahr 2005 neue Leitlinien für die Verbreitung von Informationen über das Internet veröffentlicht hat.

Das Ministerium für Transport und Kommunikation richtete im Jahr 2005 ein zweijähriges, „LUOTI" genanntes Programm ein. Das Programm befasst sich damit, festzustellen, welche Herausforderungen sich in der nächsten Zeit auf dem Gebiet der Datensicherheit im Rahmen der Entwicklung elektronischer Dienste ergeben, wie man sich darauf vorbereiten kann, welche Lösungen sich anbieten und wie sie entwickelt werden sollten. Zu den Teilnehmern an diesem Programm zählen sowohl Vertreter des öffentlichen als auch des privaten Sektors. Das grundlegende Ziel des Programms besteht darin, das Vertrauen der Verbraucher in die neuen elektronischen Dienstleistungen zu stärken. Ein entscheidendes Mittel zur Verwirklichung dieses Vertrauens besteht darin, sich mit der Anwendung von Datenschutz- und Sicherheitsregeln vertraut zu machen.

Frankreich

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und andere Entwicklungen in der Gesetzgebung

Das geänderte Gesetz vom 6. Januar 1978 und seine Durchführungsverordnung vom 20. Oktober 2005

Frankreich hat die europäische Richtlinie vom 24. Oktober 1995 durch das Gesetz vom 6. August 2004 umgesetzt, das das Gesetz vom 6. Januar 1978 geändert hat. Die Durchführungsverordnung des neuen „Gesetzes über Informatik und persönliche Freiheit", des französischen Datenschutzgesetzes, wurde am 20. Oktober 2005 angenommen. Diese Texte haben zu wichtigen Veränderungen geführt.

1. Der Datenschutzbeauftragte
Seit dem Gesetz vom 6. August 2004 können Unternehmen, kommunale Körperschaften, öffentliche Einrichtungen und Vereinigungen einen Datenschutzbeauftragten ernennen. Im Gegenzug dazu müssen diese Träger von der Pflicht befreit werden, Angaben bei der französischen Datenschutzkommission CNIL zu machen. Diese große Neuerung stellte eine Wende in der Anwendung des Gesetzes dar. Der Akzent wird auf Pädagogik und auf Beratung im Vorfeld gelegt. Durch die Ernennung eines Datenschutzbeauftragten werden zwar die Formalitäten zur Abgabe von Erklärungen erleichtert, vor allem aber können die für die Datenverarbeitung Verantwortlichen ihren gesetzlichen Verpflichtungen besser nachkommen: Sicherheit, Transparenz, Verhältnismäßigkeit und Einhaltung des Ziels der Datenverarbeitung und der Personenrechte. Verletzungen werden streng geahndet. Mit der Ernennung eines Datenschutzbeauftragten wird dem für die Datenverarbeitung Verantwortlichen ein spezialisierter Partner zur Seite gestellt, der ihn berät, Empfehlungen ausspricht, der pädagogisch vorgeht und ihn sogar bei gravierenden Missständen alarmiert. Per 31. Dezember 2005 hatten 73 Einrichtungen einen Datenschutzbeauftragten ernannt.

2. Maßnahmen zur Vereinfachung
Eine der Hauptachsen des neuen Gesetzes ist die Vereinfachung der Formalitäten im Vorfeld. Im Einklang mit der Absicht des Gesetzgebers und seiner europäischen Verpflichtungen hat die CNIL die Möglichkeiten der Vereinfachung wie Befreiung von Erklärungen, Annahme von vereinfachten Normen, Entscheidungen über Einzelbevollmächtigungen sowie Stellungnahmen über einfache Rechtsverordnungen genutzt. Die Vereinfachung der Formalitäten im Vorfeld ist immer noch ein Schwerpunkt der Arbeit der CNIL für 2006.

3. Die Anerkennung der Ehrenkodizes
Das geänderte Gesetz von 1978 gibt der CNIL die Möglichkeit, ihre Stellungnahme über die Übereinstimmung der Vorschriften mit den französischen Datenschutzbestimmungen in den Entwürfen „Regeln im Arbeitsumfeld zum Schutz von personenbezogenen Daten" abzugeben. Die CNIL hat so 2006 zwei Entwürfe der „Ehrenkodizes für den Versand von elektronischer Post" anerkannt, die mit den jeweiligen Branchen ausgehandelt wurden.

4. Kontrollaufgaben
Das neue Gesetz hat der CNIL erweiterte Aufgaben zur Kontrolle übertragen. Die CNIL hat so Hunderte von Kontrollen im Jahr 2005 (ein Anstieg von 235 Prozent gegenüber 2004) durchgeführt. Diese Zahl soll in den nächsten Jahren noch leicht ansteigen. Die Hauptfelder, in denen Kontrollen durchgeführt wurden, sind:
- Großhandel
- Direktmarketing
- Biometrie

- Videoüberwachung von privaten Orten
- Maklerprovision bei Versicherungen über das Internet

Weiter wurde im ersten Halbjahr 2005 eine Überprüfung des Internet-Bankings bei zehn Banken mittels eines Standardfragebogens durchgeführt. Dadurch war die CNIL in der Lage, sowohl den Banken als auch den Nutzern Empfehlungen auszusprechen. Diese Empfehlungen sind auf ihrer Website zu finden.

5. Die Sanktionen der reduzierten Kommission
Das neue Gesetz hat innerhalb der CNIL ein spezielles Organ geschaffen: ein in Personenzahl reduziertes Gremium (la „formation restreinte"), das zur Aufgabe hat, Sanktionen zu verhängen. Im ersten Arbeitsjahr dieses Gremiums wurden neue Sanktionsmechanismen bei den Verfahrensweisen sowie den zu untersuchenden Vorgängen ausprobiert. Im Jahr 2005 hat sich das Gremium achtmal getroffen und 50 Vorgänge untersucht.

Diese Dossiers behandelten u. a. folgende Themen:
- Nichteinhaltung der Einschreibebedingungen in einer Datei der Banque de France
- Schwierigkeiten bei der Ausübung eines Zugangsrechts oder eines Einspruchsrechts gegen den Erhalt von Werbung
- Illegale Blog-Zonen
- Erstellung von Dateien mit gesetzeswidrigem Inhalt
- Zugriff von Dritten, nicht autorisierten Personen auf Daten

Das Gremium sanktioniert gleichsam Verfahrensverstöße wie das Fehlen einer Genehmigungsanfrage vor der Erstellung bestimmter Dateien oder eine fehlende Reaktion auf das Ersuchen um Ergänzungen per Post z. B. im Rahmen von Verfahren. Um finanzielle Sanktionen gegen einen Träger verhängen zu können, ist die CNIL gehalten, im Vorfeld durch eine Aufforderung zur Beendigung des Verletzungen zuzustellen. Die CNIL kann erst finanzielle Sanktionen verhängen, wenn die Aufforderung ergebnislos verstrichen ist. Im Jahr 2005 wurden 36 Aufforderungen an die angemahnten Einrichtungen versandt. Dies hatte einen extremen allgemeinen Abschreckungseffekt zur Folge, da mehr als 85 Prozent von ihnen die Gesetzesverletzungen regelten. Die finanzielle Sanktion ist nicht das alleinige Mittel. Das Gremium konnte beobachten, dass die Unterlassungsaufforderungen bezüglich der Verarbeitung oder das Aussprechen von öffentlichen Verwarnungen manchmal mehr Erfolg hatten.

6. Internationaler Datentransfer
Das Gesetz vom 6. August 2004 gibt der CNIL die Befugnis, in bestimmten Fällen internationale Datentransfers in ein der EU nicht zugehöriges Land zu genehmigen. Die CNIL ist in ständiger Sorge, dass verschiedene Bedingungen, unter denen diese internationalen Datentransfers möglich werden, auch wirklich auf kohärente und effiziente Weise artikuliert werden. So hat die CNIL am 30. Juni 2005 akzeptiert, dass „interne Regeln" (BCR) im Unternehmen General Electric rechtmäßig dazu benutzt werden können, um zahlreiche gruppeninterne, internationale Datentransfers zum Personalmanagement durchzuführen. Sie hat im Allgemeinen mit ihren europäischen Kollegen zusammengearbeitet, um mehrere ähnliche Vorgänge voranzubringen und um die Legitimität der internen Regeln auf europäischer Ebene zu festigen und sie bei betreffenden Unternehmen zu fördern. Darüber hinaus war die CNIL Verfasser eines wichtigen Arbeitsdokuments der Artikel-29-Gruppe über eine allgemeine Interpretation „der Abweichungen von Artikel 26-1 von der Richtlinie 95/46/EG vom 24. Oktober 1995". Zudem arbeitet sie an einer Vereinfachung und größeren Effizienz der Verfahren und Formalitäten, die bei internationalen Datentransfers auf nationaler Ebene anwendbar sind.

Die Umsetzung der Richtlinie 2002/58/EG

Die europäische Richtlinie 2002/58/EG wurde durch das Gesetz vom 21. Juni 2004 „über das Vertrauen in die digitale Wirtschaft" („loi pour la confiance dans l'économie numérique", LCEN) umgesetzt. Dieses Gesetz unterstützt den Kampf gegen E-Müll („Spam"), indem es den Schutz des Nutzers von E-Mail verstärkt. Es führt ebenfalls eine vorherige Zustimmung *(opt-in)* für die Zusendung von SMS- oder MMS-Werbenachrichten ein. Die Zustimmung des Nutzers sollte in voller Kenntnis der Sache erfolgen. Die CNIL ist dennoch der Meinung, dass natürliche Personen mittels E-Mail an ihre Büro-E-Mail-Adresse beworben werden können, ohne dass ihre vorherige Zustimmung erfolgt ist, wenn die Nachricht in Zusammenhang mit ihrer Funktion in der privatrechtlichen oder öffentlichen Einrichtung steht, in der sie arbeiten und die ihnen diese Adresse zugeteilt hat. Für nicht-kommerzielle Werbung (wie politische, Vereinigungen betreffende, religiöse oder gemeinnützige E-Mails), gelten die allgemeinen Datenschutzregeln: vorherige Informationen darüber, dass die E-Mail-Adresse zu diesen Zwecken genutzt werden kann, und kostenloses Recht auf Widerspruch gegen diese Nutzung *(opt-out)*.

Andere Entwicklungen in der Gesetzgebung, die den Datenschutz betreffen

1. Gesetzgebung zum Kampf gegen den Terrorismus (Gesetz Nr. 2006-64 vom 23. Januar 2006 über den Kampf gegen den Terrorismus)
Im Jahr 2005 wurde die CNIL offiziell vom Innenministerium über seinen Gesetzesentwurf bezüglich des Kampfes gegen den Terrorismus konsultiert, der eine neue Verarbeitung von personenbezogenen Daten in verschiedenen Bereichen vorsah (Videoüberwachung, Übertragung von personenbezogenen Daten an die Polizei über in die EU ein- oder ausreisende Passagiere, Bereitstellung von Vorrichtungen zum Einlesen von Autokennzeichen und Aufnahmen der Autoinsassen an „allen geeigneten Punkten" des Straßennetzes, Zugriff auf Internet- und Telefonie-Daten sowie Konsultieren von bestimmten Verwaltungsdateien des Innenministeriums durch die Anti-Terrordienste.

In ihrer Stellungnahme vom 10. Oktober 2005 hat die CNIL darauf hingewiesen, dass die verfolgten Ziele legitim wären, aber einige besondere Garantien erforderten, um ein Gleichgewicht zwischen den nationalen Sicherheitsanforderungen und dem Schutz der Freiheiten zu gewährleisten. Die CNIL ist vor allem darüber besorgt, dass unter dem Deckmantel des Kampfes gegen den Terrorismus Dateien und Videoaufzeichnungen der Polizei und Gendarmerie zur Verfügung gestellt werden können, mit denen man systematisch und permanent die Mobilität und bestimmte alltägliche Handlungen eines großen Teils der Bevölkerung mitverfolgen kann. Der Gesetzgeber hat hierbei nicht alle Forderungen der CNIL berücksichtigt, er hat auch zugestimmt, dass die Informationen, die der CNIL zugetragen werden, limitiert werden, wenn sie eine Stellungnahme über Dateien abgeben muss, die die Staatssicherheit, die Verteidigung oder die öffentliche Sicherheit betreffen.

Es gibt mehrere Vorschriften im Gesetz von 23. Januar 2006, die das Recht zur Nutzung von Verbindungsdaten der Anbieter elektronischer Kommunikation erweitern, die diese seit dem Gesetz vom 15. November 2001 über die Alltagssicherheit aufbewahren müssen. Das Gesetz erweitert die Definition eines Online-Kommunikationsanbieters, um vor allem die klassischen Anbieter in die Verpflichtung zur Datenaufbewahrung einzubinden, aber auch Internet-Cafés sowie Hotels und Flughäfen, seit diese auch Zugang zum Internet anbieten. Die CNIL wies darauf hin, dass diese Verpflichtung die Internet-Cafés zum Beispiel nicht dazu zwang, ihre Nutzer von elektronischer Kommunikation preiszugeben, und forderte (erfolglos), dass die betroffenen

Personengruppen näher beschrieben werden sollten, damit die Bibliotheken, Rathäuser, Universitäten etc., die einen Internet-Zugang anbieten, in die Lage versetzt würden, abschätzen zu können, ob sie zur Datenaufbewahrung verpflichtet sind. Das Gesetz erlaubt in Zukunft den Zugang außerhalb der Kontrolle der Gerichtshoheit von unterschiedlichen, hierzu befugten Beamten aus Polizei und nationaler Gendarmerie, die mit der Bekämpfung des Terrorismus beauftragt sind, zu technischen Daten, die von den Anbietern elektronischer Kommunikation aufbewahrt worden sind.

2. Das Gesetz von 12. Dezember 2005 über den Rückfall von Straftätern und der elektronischen Fußfessel
Die elektronische mobile Überwachung (PSEM) ist eine der Hauptvorschriften des Gesetzes vom 12. Dezember 2005 über den Umgang mit rückfälligen Straftätern. Konkret heißt das, dass durch die PSEM eine Person mit elektronischer Fußfessel permanent über die GPS- oder GSM-Technologie lokalisiert werden kann. Die PSEM kann in drei verschiedenen rechtlichen Situationen verwendet werden: im offenen Vollzug, in der Bewährungszeit und während der gerichtlichen Überwachung. In diesem Fall muss die Person ihre vorherige Zustimmung geben.

3. Die Verordnung vom 6. Juni 2005 und die Verbreitung und Wiederverwendung von öffentlichen Daten
Der Beschluss vom 6. Juni 2005 sieht den Schutz von personenbezogenen Daten in vielen Dokumenten vor, die von allen öffentlichen Stellen erstellt wurden (Wahllisten, Daten über die Verwaltung von Leistungsempfängern, Katasteramt, Steuerdaten etc.) Künftig unterliegt jedwede Wiederverwendung von öffentlichen Informationen, die personenbezogene Daten enthalten, dem Gesetz vom 6. Januar 1978. Dies führt insbesondere dazu, dass eine Verarbeitung mit dem Ziel einer Datenwiederverwertung eine Meldepflicht des Datenlieferanten oder Datenadressaten gegenüber der CNIL mit sich bringt.

4. Die Verordnung über öffentliche Online-Dienste vom 8. Dezember 2005
Die Verordnung vom 8. Dezember 2005 gab der Schaffung der öffentlichen Online-Dienste („Téléservices") einen juristischen Rahmen. Sie definiert die Bedingungen für den papierlosen Verkehr zwischen den Verwaltungen und den Bürgern sowie zwischen den Verwaltungen untereinander. Die CNIL hat den Online-Dienst für Adressänderungen, das Portal für die Anforderung eines Auszugs aus dem Geburtenregister und eine nicht offizielle Version des Portals „monservicepublic" bereits untersucht.

5. Die Folgen des Gesetzes Nr. 2004-1486 vom 30. Dezember 2004 und die Bemessung der Vielfalt
Durch das Gesetz vom 30. Dezember 2004 wurde die Hohe Behörde zur Bekämpfung der Diskriminierung und zur Förderung der Gleichbehandlung, zur Bekämpfung von Diskriminierung im Beschäftigungssektor, vor allem derjenigen mit ethnischen, nationalen oder rassistischen Hintergrund, geschaffen. Sie war in den letzten Monaten Gegenstand einer Vielzahl von Berichten und Initiativen.

Die Werkzeuge zur Bemessung der Vielfalt haben zum Ziel, dem Arbeitgeber Aufschluss über die ethnische oder soziale Herkunft seiner Arbeitnehmer oder von Stellenbewerbern zu geben. Diese Werkzeuge können auf einer Datensammlung und -verarbeitung beruhen, die sogar eine augenblickliche Identifizierung der betroffenen Personen ermöglichen. Daten über die rassische oder ethnische Herkunft einer Person sind jedoch sensible Daten, deren Sammlung und Verwendung besonderen Auflagen unterliegen.

Die CNIL hat eine Anzahl von Empfehlungen über dieses Thema am 5. Juli 2005 ausgesprochen. Sie glaubt, dass der Einsatz von statistischen Werkzeugen zur Bemessung der Vielfalt zum Kampf gegen Diskriminierungen am Arbeitsplatz völlig legitim ist. Dennoch gibt es ihrer Meinung nach

keine vertrauensvolle aktuelle Vergleichsgrundlage in Frankreich, da es keine nationale Bezugsquelle zu ethno-rassischer Typologie für die öffentliche Statistik gibt und deren Erstellung vom Gesetzgeber genehmigt werden müsste. Somit empfiehlt die CNIL momentan den Arbeitgebern, keine Daten zur tatsächlichen oder mutmaßlichen rassischen oder ethnischen Herkunft ihrer Arbeitnehmer oder Bewerber zu sammeln. Sie bevorzugt die Verarbeitung von Informationen über die nationale Herkunft von Personen, die bereits in den öffentlichen Statistiken erfasst sind (Staatsangehörigkeit, ggf. ursprüngliche Staatsangehörigkeit, Geburtsort, Staatsangehörigkeit oder Geburtsort der Eltern) und empfiehlt, dass die Nutzung dieser Daten anonym geschehen soll. Sie empfiehlt den Arbeitgebern, vorher in Übereinstimmung mit den Personalvertretern über die Ziele einer Politik der Vielfalt nachzudenken.

6. Die Folgen des amerikanischen Sarbanes-Oxley-Gesetzes

Am 26. Mai 2005 weigerte sich die CNIL, zwei Warnungen von „Whistleblowern" freizugeben. Beide Warnungen wurden ausgesprochen, um es Angestellten und Mitarbeitern der Unternehmen zu erlauben, mutmaßlich falsches Verhalten von Kollegen zu melden. Die CNIL hat diese Entscheidungen so begründet, dass die Genehmigung genau dieser beiden Warnungen zu einem „organisierten System des Denunziantentums am Arbeitsplatz" hätte führen können. Diese beiden Genehmigungsverweigerungen hatten große Auswirkungen in Frankreich und im Ausland, da die Unternehmen befürchteten, dass sie sich einerseits nicht mit den Datenschutzregeln arrangieren konnten, andererseits genauso wenig mit dem amerikanischen Sarbanes-Oxley-Gesetz (SOX). Das SOX-Gesetz lässt die Warnungen auch in den Bereichen Finanzwesen, Buchhaltung und Kontenkontrolle zu. Die französischen Unternehmen, die diesem Gesetz unterliegen, weil sie an US-Börsen notiert sind oder weil sie französische Tochtergesellschaften von amerikanischen börsennotierten Unternehmen sind, müssen den jeweiligen Märkten vorweisen, dass sie die Verpflichtung einhalten, eine derartige Warnung auszusprechen, ansonsten verlören sie ihre Aktiennotierung. Die CNIL ist sich dieser Schwierigkeiten bewusst und möchte die Unternehmen nicht in dieser Unsicherheit belassen. Deshalb hat sie mehrere Schritte im Sinne einer weiteren Verfolgung der Entscheidungen vom 26. Mai 2006 unternommen. So hat sie am 8. Dezember 2005 eine Entscheidung zur einmaligen Genehmigung der Warnungen der „Whistleblower" getroffen, die den Orientierungen entsprechen, die sie im Rahmendokument vom 10. November 2005 festgehalten hatte. Die CNIL empfiehlt vor allem, die Möglichkeit des Aussprechens der Warnungen auf bestimmte Bereiche zu begrenzen, wie zum Beispiel auf die Buchhaltung, das Bankwesen, die Kontenüberwachung und die Korruptionsbekämpfung, zu keinen anonymen Denunziationen zu ermutigen und ein besondere Organisation zu schaffen, die Warnungen sammeln und bearbeiten sowie die betroffene Person hierüber informieren soll.

7. Die Verordnung vom 27. Mai 2005 über Universaldienstverzeichnisse und Universalauskunftsdienste

Bereits im Jahr 1996 hat das Telekommunikationsregulierungsgesetz die Umsetzung des Universaldienstverzeichnisses vorgesehen. Allerdings wurde diese durch die Entwicklung des rechtlichen Rahmens immer weiter verzögert. Die Veröffentlichung der Verordnung vom 27. Mai 2005 hat den rechtlichen Rahmen bezüglich der Universaldienstverzeichnisse und Verzeichnisabfragedienste komplettiert, die die Koordinaten aller Telefonnutzer zusammenfassen sollen, egal welchen Anbieter sie nutzen. Die Mitteilungen der Kunden der Betreiber setzten Ende 2005 ein, um Abonnenten- oder Nutzerlisten zu erstellen und darin gewisse Optionen zum Schutz von personenbezogenen Daten aufzu-

nehmen. Die Anbieter müssen diese Listen jedem zur Verfügung stellen, der auf nationaler oder lokaler Ebene das Universaldienstverzeichnis verlegen oder einen Universalauskunftsdienst anbieten will.

B. Bedeutende Rechtsprechung

Arbeitszeitenkontrolle durch Fingerabdruck

Das „tribunal de grande instance" (~ Oberlandesgericht) in Paris hat in einem Urteil vom 19. April 2005 die Unverhältnismäßigkeit einer Arbeitszeitenkontrolle durch Fingerabdruck festgestellt. Dennoch war der Arbeitgeber seinen Verpflichtungen der individuellen Information seiner Arbeitnehmer und der vorherigen Konsultation der Arbeitnehmer nachgekommen und hatte die Maßnahme gegenüber der CNIL angegeben. Bei den Kontrollmitteln des Arbeitgebers ist hinsichtlich der verfolgten Ziele ausdrücklich die Vorgabe der Verhältnismäßigkeit zu achten (gemäß Art. L. 120-2 Arbeitsrecht); dennoch verbietet das Gericht der Gesellschaft, biometrische Mitarbeiterausweise mit Fingerabdruck einzuführen. Der Richter befindet, dass ein Arbeitgeber nicht befugt sei, ein Kontrollsystem der Arbeitszeiten über Fingerabdruck einzuführen, da es nicht erwiesen sei, dass die Verwendung eines klassischen Systems mit Mitarbeiterausweisen nicht eine ebenso effiziente Kontrolle ermögliche Das Gericht unterstützt die diesbezüglich getroffenen Entscheidungen der CNIL, laut denen jedes biometrische System zur Kontrolle des Zugangs oder der Arbeitszeit im Vorfeld der Einführung genehmigt werden muss.

Der Zugriff des Arbeitgebers auf die Festplatte des Arbeitnehmers ist unter bestimmten Bedingungen genehmigt

Der Kassationshof hat durch sein „Nikon"-Urteil vom 2. Oktober 2001 das absolute Recht der Arbeitnehmer auf die Wahrung der Intimsphäre und des Privatlebens im Rahmen der Nutzung ihres E-Mail-Nachrichtensystems betont. Durch sein Urteil vom 17. Mail 2005 erkannte es das Recht des Arbeitgebers an, unter gewissen Umständen auf die persönlichen Dateien auf der Festplatte des Arbeitnehmers zuzugreifen. Der Gerichtshof betonte jedoch auch, dass der Arbeitgeber ohne einen besonderen Grund persönliche Dateien des Arbeitnehmers auf der Festplatte des zur Verfügung gestellten Computers nur in dessen Anwesenheit öffnen darf. Diese Entscheidung gefährdet jedoch nicht den Grundsatz der Verhältnismäßigkeit bei Kontrollen von „persönlichen" Dateien der Arbeitnehmer. Der Arbeitgeber ist in jedem Fall verpflichtet, eine präzise Rechtfertigung für jeden angestrebten Zugriff auf persönliche Daten in Einklang mit dem Arbeitsrecht und den Gesetzen zum Schutz des Privatlebens abzugeben.

Die Verurteilung eines Spammers

Durch ein Urteil vom 18. Mai 2005 hat der Appelationshof in Paris einen Versender von Spam-Nachrichten zu einem Bußgeld von 3 000 € verurteilt, nachdem dieser von der CNIL angezeigt wurde. Diese Entscheidung bestätigt die Analyse der CNIL, nach der das Sammeln von E-Mail-Adressen, die direkt oder indirekt eine physische Person identifizieren können, ohne Wissen der betroffenen Personen im öffentlichen Raum des Internet, gegen das Datenschutzgesetz verstößt. Gegen diese Entscheidung wurde Revision eingelegt.

C. Wichtige spezifische Themen

Elektronische Identität

Die CNIL hat am 22. November 2005 ihre Stellungnahme zum Erlass zur Einführung des elektronischen Passes und der Modalitäten für dessen sichere Produktion abgegeben. Der Pass enthält einen kontaktlos auslesbaren Chip und ein digi-

tales Foto seines Inhabers. Das Foto ist bereits Teil der personenbezogenen Daten des Passes, aber der Erlass sieht zudem vor, dass das Foto in Zukunft digital im kontaktlos auslesbaren Chip integriert werden soll. Die CNIL hat zur Vermeidung von Betrug bei der Datenerfassung des elektronischen Chips sowie zur besseren Zugriffskontrolle auf die Datei mit den nationalen Passdaten Empfehlungen herausgegeben.

Parallel dazu wird das Projekt des elektronischen und biometrischen Personalausweises INES im Jahr 2008 abgeschlossen werden. Dieser kompatible elektronische Personalausweis ist in jedem Land mit kontaktlosen Chipkartenlesegeräten einlesbar, insbesondere in Europa. Der Personalausweis dürfte auch für die Nutzung von Telediensten durch die Identifizierung seines Inhabers benutzt werden können. Der Besitz dieses Ausweisdokuments sollte weiterhin freiwillig bleiben. Die im Chip gespeicherten Daten enthalten insbesondere die Fingerabdrücke und ein Foto des Inhabers. Das INES-Projekt wird seit Jahren von der CNIL verfolgt. Die Thematik der Identifizierung über biometrische Daten ist in der Tat eine Frage der mündigen Gesellschaft der gesamten französischen Bevölkerung.

Die Geolokalisierung von Fahrzeugen der Arbeitnehmer

Die CNIL hat eine Vielzahl von Anfragen und Beschwerden von Arbeitgebern und Arbeitnehmern erhalten, die den anwendbaren rechtlichen Rahmen bei der Lokalisierung von Fahrzeugen hinterfragen. Die betreffenden Mittel stützen sich hauptsächlich auf die Verwendung der GSM/GPS-Technologie, die es beispielsweise möglich macht, die Position eines Fahrzeugs zu einem gegebenen Zeitpunkt auf einer Karte wiederzugeben. So kann jede Aktivität des Arbeitnehmers und Nutzers des Fahrzeugs kontrolliert werden. Die Einführung der Geolokalisation stellt gewisse Risiken sowohl für die Kollektivrechte (Gewerkschaftsrecht, Streikrecht) als auch für die individuellen Freiheiten (Recht auf Fortbewegung in der Anonymität, Recht auf Privatleben) dar. Bei der Bearbeitung werden zwei Fragen aufgeworfen: die Frage nach der Grenze zwischen Arbeit und Privatleben und die Frage nach dem Niveau einer zulässigen Dauerkontrolle, die man dem Arbeitnehmer zumuten kann. Die CNIL hat Problematiken der Verwendung von Geolokalisationstechniken im beruflichen Umfeld bestimmt. In der ersten Hälfte des Jahres 2006 wird sie so eine Empfehlung zu den Bedingungen, in denen diese Maßnahmen verwendet werden können, annehmen.

Parallele Strafregister

Im Jahr 2006, wie auch zuvor 2005, stellen die sozialen Folgen der Abfrage von Daten der Kriminalpolizei für administrative Zwecke eine der Hauptbedenken der CNIL dar. Die CNIL führt im Rahmen des indirekten Zugriffsrechts auf die Dateien von Polizei und Gendarmerie zahlreiche Kontrollen durch. Hierbei stellt sie auch so manches Mal fest, dass der Zugriff auf Daten der Kriminalpolizei im Rahmen von administrativen Untersuchungen zum Zwecke des Zugangs zu bestimmten sicherheitskritischen Positionen oder der Beeidigung zu bestimmten Funktionen dramatische Konsequenzen für die Personen haben kann. Allein aufgrund der Konsultation dieser Dateien und auf der Basis von manchmal ungerechtfertigten, fälschlichen oder abgelaufenen falschen Personenbeschreibungen wurden Personen nicht eingestellt oder gekündigt. Diese administrative Nutzung der Dateien der Kriminalpolizei verleiht ihnen die Rolle eines parallelen Strafregisters, allerdings ohne jegliche Garantie, die in der Strafprozessordnung für das nationale Strafregister vorgesehen ist.

Diese Situation kann sich verschlimmern. Ein Erlass vom 6. September 2005 hält in der Tat eine große Erweiterung der Liste dieser Untersuchungen bereit, was zu einer Konsultation der Dateien der Kriminalpolizei führt. Außerdem ist es vorhersehbar, dass das Anwendungsfeld der Dateien der Kriminalpolizei (STIC) ausgedehnt wird, da in diesen Dateien gegenwärtig nur schwere Verstöße („Verbrechen") oder relativ schwere Verstöße („Vergehen") aufgezeichnet werden. Folglich erscheint diese Erweiterung nicht gerechtfertigt.

Die CNIL bestreitet nicht die Legitimität des vom Staat verfolgten Ziels, der eine engere Kontrolle der sogenannten „sensiblen Aktivitäten" erwünscht. Sie erachtet es als nützlich, die abartigen Auswirkungen einer Maßnahme zu korrigieren, die nicht für diesen Zweck geschaffen wurde. Die CNIL hat der Regierung bereits eine Vielzahl von Vorschlägen zur Abhilfe gemacht.

Gewalt in den Stadien

Das Thema der Sicherheit in den Stadien ist in Frankreich gerade 2006 durch die Vielzahl von Sportveranstaltungen rund um den Fußball und die hin und wieder auftretenden Ausschreitungen sehr aktuell. Die Organisatoren dieser Veranstaltungen sind manchmal zu Recht versucht, eine EDV-basierte Erfassung zur Auswahl der Zuschauer vorzunehmen. So wurde die Aufmerksamkeit der CNIL auf die Bedingungen gelenkt, in denen die Französische Fußballvereinigung (FFF) beim Spiel Frankreich-Deutschland am 12. November 2005 Daten wie Name, Vorname, Adresse und Personalausweisnummer der französischen Zuschauer aufgezeichnet hat. Diese Operation wurde im Zeichen der Sicherheit durchgeführt, hielt allerdings, so wie sie organisiert war, nicht die Gesetzesvorschriften ein – vor allem, weil die Verwendung dieser Daten nicht klar definiert war und weil dieses Sammeln von Daten nicht der CNIL gemeldet worden war. Nach dem Einschreiten der CNIL hat die FFF sich jedoch dazu entschieden, diese Operation zu stoppen und eine Abstimmung mit der CNIL anzusteuern, damit diese verschiedenen Praktiken in Einklang mit den Regeln des Datenschutzes stehen.

Deutschland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

- Die Richtlinie 02/58/EG wurde im Rahmen der 2004 vorgenommenen Änderung des Telekommunikationsgesetzes teilweise in deutsches Recht umgesetzt. Ihre Umsetzung in den Bereichen der Tele- und Mediendienste steht noch aus.

- Gesetz vom 24. Juni 2005 (BGBl. I S.1841) über die Durchführung der Entscheidung des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung).

- Gesetz zur Novellierung der forensischen DNA-Analyse vom 12. August 2005 (BGBl. I S. 2360).

B. Bedeutende Rechtsprechung

In seiner Entscheidung vom 18. Juli 2005 (2 BvR 2236/04) entschied das Bundesverfassungsgericht, dass das Gesetz zur Umsetzung des Ratsbeschlusses über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten der Europäischen Union (Amtsblatt Nr. L 190 vom 18. Juli 2002 S. 1) gegen das Grundgesetz verstößt und nichtig ist. Deshalb wird es nicht möglich sein, deutsche Staatsbürger in andere EU-Mitgliedstaaten auszuliefern, solange kein neues Gesetz über den Europäischen Haftbefehl angenommen wurde. Gegenwärtig wird ein neuer Gesetzentwurf diskutiert.

In seiner Entscheidung vom 27. Juli 2005 entschied das Bundesverfassungsgericht, dass die Bestimmung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) zur Überwachung der Telekommunikation zur Vorsorge für die Verfolgung oder zur Verhütung von Straftaten nichtig ist, weil sie eine Verletzung der Vertraulichkeit der Kommunikationen bedeutet, die von der Verfassung geschützt wird (Art. 10 Grundgesetz). Das Gericht kritisierte unter anderem, dass es in den jeweiligen Gesetzesbestimmungen an Definitionen und an Klarheit mangelte. Außerdem verstoßen diese Bestimmungen gegen den Grundsatz der Verhältnismäßigkeit. Abschließend bestätigte das Bundesverfassungsgericht seine im Rahmen vergangener Entscheidungen zum Ausdruck gebrachte Haltung, indem es darauf hinwies, dass der unantastbare Grundsatz einer unversehrten Privatsphäre, der im Rahmen des Schutzes der Menschenwürde garantiert wird, ohne jede Einschränkung aufrechterhalten werden muss, wenn Sicherheitsdienste verdeckte Datenaufzeichnungen vornehmen. Wenn in einem konkreten Fall Hinweise darauf vorliegen, dass Inhalte einer Überwachungsmaßnahme Informationen aus dem Bereich dieser Privatsphäre einschließen, kann diese Maßnahme nicht gerechtfertigt werden und muss deshalb abgebrochen werden. Darüber hinaus müssen Sicherheitsvorkehrungen getroffen werden, die garantieren, dass die Inhalte von Mitteilungen aus einem so persönlichen Bereich nicht verwendet und unmittelbar gelöscht werden, wenn ihre Aufzeichnung im Rahmen von Ausnahmeumständen zuvor erfolgt ist.

C. Wichtige spezifische Themen

Zusammenarbeit der Polizeikräfte in Europa

Am 27. Mai 2005 unterzeichneten Belgien, Frankreich, Luxemburg, die Niederlande, Österreich, Spanien und die Bundesrepublik Deutschland in Prüm, Deutschland, einen Vertrag über die Intensivierung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung von Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration.

Dieser Vertrag bildet einen Meilenstein auf dem Gebiet der grenzüberschreitenden Zusammenarbeit zur Bekämpfung der Kriminalität und in anderen Aufgabenbereichen. Unter anderem zu diesem

Zweck wurde vorgesehen, dass die Vertragsparteien ihre zentralen DNA- und Fingerabdruckdatenbanken den zentralen Kontaktstellen der anderen Vertragsparteien im Rahmen eines Abgleichungsverfahrens zur Verfügung stellen. Wenn bei dieser Abgleichung ein Treffer erzielt wurde, wird der anschließende Informationsaustausch durch die gesetzlichen Bestimmungen der gegenseitigen Rechtshilfe geregelt.

Darüber hinaus sieht der Vertrag einen automatischen Zugang zu dem jeweiligen Kfz-Register vor. Außerdem sind in diesem umfassenden Vertrag Maßnahmen zur Verhinderung terroristischer Straftaten und zur Bekämpfung illegaler Migration enthalten.

Um die Interessen der Bürger zu wahren, die beim Austausch/Abrufen personenbezogener Daten geschützt werden müssen, wurden umfassende Datenschutzbestimmungen in den Vertrag aufgenommen. Neben dem allgemeinen, obligatorischen hohen Datenschutzniveau umfassen sie auch den garantierten Grundsatz der Zweckbindung bei der Übertragung personenbezogener Daten und Regelungen hinsichtlich der Aufrechterhaltung der Datenqualität. Darüber hinaus sieht der Vertrag umfassende technische und organisatorische Maßnahmen im Zusammenhang mit dem Datenschutz und der Datensicherheit vor, die das obligatorische Dokumentieren und Einloggen bei einem Datentransfer mit einschließen. Schließlich sorgen alle Vertragsparteien für eine unabhängige Kontrolle während des Datentransfers durch die zuständigen Behörden, an die sich die Betroffenen wenden können, um ihre Rechte geltend zu machen, unter anderem das Recht auf Information. In Deutschland haben die vorbereitenden Arbeiten für die Ratifizierung dieses Vertrags bereits im Jahr 2005 begonnen; sie konnten jedoch bis zum Jahresende noch nicht abgeschlossen werden.

Griechenland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Richtlinie 95/46/EG

Die Richtlinie 95/46/EG wurde durch das Gesetz 2472/97 *über den Schutz von Einzelpersonen bei der Verarbeitung von personenbezogenen Daten* (Amtsblatt Nr. A50/10-4-1997) in nationales Recht übertragen. Zu diesem Gesetz wurde im Rahmen von Art. 8 des Gesetzes 2819/2000 (Amtsblatt Nr. 84/15-3-2000) ein begrenzter Änderungsantrag angenommen, der für gewisse Kategorien von für die Datensicherheit Verantwortlichen Ausnahmen von der Notifizierungsverpflichtung vorsieht.

Eine englische Fassung des geänderten Textes ist unter www.dpa.gr verfügbar.

Richtlinie 97/66/EG

Die Richtlinie 97/66/EG wurde durch das Gesetz 2774/99 *über den Schutz von personenbezogenen Daten im Bereich der Telekommunikation* (Amtsblatt Nr. A287/22-12-1999) in nationales Recht umgesetzt.

Eine englische Fassung des Textes ist unter www.dpa.gr verfügbar.

Richtlinie 2002/58/EG

Die Richtlinie 2002/58/EG wurde bisher noch nicht in nationales Recht umgesetzt. Ein Sonderausschuss, der 2004 durch einen Erlass des Justizministers eingerichtet wurde, legte dem Minister im September 2005 einen Textentwurf vor. Im März 2006 legte der Justizminister dem Parlament einen Gesetzentwurf für (a) die Umsetzung der Richtlinie 2002/58/EG in nationales Recht und (b) die Revision des Gesetzes 2472/97 über den Datenschutz vor, um es mit dem ersten Bericht des Europaausschusses bezüglich der Umsetzung der Datenschutzrichtlinie in Einklang zu bringen.

Die wichtigsten Entwicklungen

Unter der ersten Säule haben sich keine nennenswerten Entwicklungen ergeben.

Unter der dritten Säule wurde Griechenland im Februar 2005 im Rahmen der Kompetenzen der Schengener Evaluierungsgruppe des Europäischen Rates bewertet. Die Evaluierung der griechischen Datenschutzbehörde (HDPA) als Kontrollbehörde des griechischen SIRENE-Büros wurde am 8. und 9. Februar 2005 von einer gemischten Gruppe von Experten der Datenschutzbehörde und Polizeiexperten aus Luxemburg (Präsidentschaft), Belgien, Norwegen, Zypern, Estland und Schweden mit positiven Ergebnissen durchgeführt.

B. Bedeutende Rechtsprechung

Leitlinien für die sichere Löschung und Vernichtung personenbezogener Daten (1/2005)

Die griechische Datenschutzbehörde veröffentlichte einen Text über Leitlinien für die sichere Löschung und Vernichtung von personenbezogenen Daten nach dem Verstreichen des Speicherungszeitraums, der zum Zweck der Datenverarbeitung eingehalten werden muss.

Den oben stehenden Leitlinien zufolge müssen Daten unmittelbar unter der Verantwortung des für den Datenschutz Verantwortlichen gelöscht und vernichtet werden, nachdem der notwendige Speicherungszeitraum abgelaufen ist. Um die Löschung und Vernichtung vornehmen zu können, muss der für den Datenschutz Verantwortliche

ein spezifisches schriftliches Löschungs- und Vernichtungsverfahren einschließlich Mechanismen zur Überprüfung der Durchführung der vorgeschriebenen Verfahrensschritte einhalten. In jedem Fall muss ein Löschungs- und Vernichtungsprotokoll erstellt werden.

Auf die jeweiligen Vorgänge wird spezifisch Bezug genommen, beispielsweise mit dem Hinweis „Durch den für den Datenschutz Verantwortlichen vorgenommene Vernichtung" oder „Vernichtung von Daten, die durch besondere Vertraulichkeitsauflagen geschützt sind", usw.

Verarbeitung von sensiblen Daten in Fernsehsendungen

Im Jahr 2005 wurden zwei wesentliche Fälle vor den Gerichten verhandelt. Der erste betraf eine Reihe von Richtern, die in Korruptionsaffären verwickelt waren. Der zweite bezog sich auf Kirchenvertreter, einschließlich Bischhöfen, die von Korruptionsaffären und Sex-Skandalen betroffen waren. Diese Fälle wurden im Rahmen journalistischer Fernsehsendungen offenbart. Die Journalisten hatten entweder versteckte Kameras verwendet oder illegal Telefongespräche abgehört und verwiesen auf die personenbezogenen Daten der Betroffenen oder von Dritten. Einige dieser Personen reichten Beschwerden wegen illegaler Verarbeitung ihrer personenbezogenen Daten ein.

Die Datenverarbeitungsbehörde vertrat die Auffassung, dass die Verarbeitung von sensiblen, personenbezogenen Daten (Offenlegung im Rahmen von Fernsehsendungen) aufgrund des großen öffentlichen Interesses an der Ausübung öffentlicher Tätigkeiten durch Personen in öffentlichen Ämtern gerechtfertigt werden kann, wenn diese Offenlegung erforderlich ist, um die Öffentlichkeit zu informieren, und somit im öffentlichen Interesse liegt, wobei jedoch der Gleichbehandlungsgrundsatz gewahrt bleiben muss. Diese Verarbeitung ist jedoch nicht gerechtfertigt, wenn sie Dritte betrifft, die nicht an den Skandalen beteiligt waren. Die wiederholte Offenlegung dieser Informationen kann ebenfalls unter gewissen Umständen gerechtfertigt sein, aber dies muss im Einzelfall entschieden werden, auch unter Berücksichtigung des Gleichbehandlungsgrundsatzes.

Die Datenschutzbehörde verhängte gegen die Fernsehsender und die Journalisten eine Geldbuße wegen der Nichtachtung des Gleichbehandlungsgrundsatzes in einigen der oben genannten Fälle und der Offenlegung personenbezogener Daten von Dritten.

Veröffentlichung eines parlamentarischen Berichts über Börsentransaktionen von Parlamentsmitgliedern

Im Anschluss an eine Anfrage, die der Datenschutzbehörde durch den Präsidenten des Parlaments vorgelegt wurde und in der er sich erkundigt, ob die Veröffentlichung des parlamentarischen Berichts über die Ausführung von Börsentransaktionen durch Mitglieder des Parlaments, die gesetzlich nicht zulässig ist, mit den geltenden Datenschutzbestimmungen vereinbar ist, erklärte die Datenschutzbehörde, dass die Veröffentlichung eine Form der Verarbeitung darstelle, die ohne die vorherige Einwilligung der Betroffenen (Mitglieder des Parlaments) erfolgen könne, weil sie für die Durchführung eines Vorhabens von öffentlichem Interesse erforderlich sei, das von einer öffentlichen Behörde betrieben werde und offensichtlich darauf ausgerichtet sei, Transparenz im öffentlichen Leben zu verwirklichen.

Veröffentlichung der Namen von Personen, die gesetzeswidrig als für den Wehrdienst untauglich eingestuft wurden

Der Verteidigungsminister erkundigte sich danach, ob die Veröffentlichung der Namen von Personen zulässig ist, die gesetzeswidrig als für den Wehrdienst untauglich eingestuft wurden, um sie als öffentliches Beispiel zum Zwecke der zukünftigen Vermeidung dieses Phänomens zu verwenden.

Die Datenschutzbehörde erklärte, dass die Veröffentlichung nicht mit dem Datenschutzgesetz vereinbar sei, weil sie nicht dem Zweck der Maßnahme des Ministeriums entspräche, der darin besteht, gegenüber der Öffentlichkeit deutlich zu machen, dass solche Vorgehensweisen in Zukunft nicht mehr toleriert würden. Die Datenschutzbehörde wies darauf hin, dass der angestrebte Zweck durch Mittel erreicht werden könne, die vom Standpunkt des Datenschutzes aus betrachtet unbedenklich seien und darin bestünden, Statistiken über die Anzahl der geprüften und geahndeten Fälle zu veröffentlichen.

Der Fall ist vor dem Staatsrat anhängig, bei dem der Minister gegen die Entscheidung Berufung eingelegt hat.

Verwendung von CCTV (Closed Circuit Television) in der Stadt Athen

Durch die Entscheidung 28/2004 gab die HDPA die Bedingungen an, unter denen die griechische Polizei berechtigt ist, ein CCTV-System in öffentlichen Bereichen der Stadt Athen und in ihren Vorstädten zu montieren, um die Sicherheit der Olympischen Spiele 2004 bis zum Ende der Spiele zu garantieren.

In ihrer Entscheidung 63/2004 gab die HDPA dem Antrag der griechischen Polizei statt, den Zeitraum der rechtmäßigen Nutzung des CCTV-Systems, der mit dem Ende der Olympischen Spiele abgelaufen war, allein zum Zwecke der Verkehrsüberwachung unter strengen Auflagen um sechs Monate zu verlängern, darunter die Entfernung der Mikrofone sowie aller Kameras, die in Bereichen montiert waren, die sich nicht zur Verkehrsüberwachung eignen, und unter der Verpflichtung, das System während Demonstrationen usw. abzuschalten.

Nach Ablauf der sechsmonatigen Frist beantragte die griechische Polizei die Verlängerung des CCTV-Betriebszeitraums und eine Ausweitung der Verwendungsmöglichkeiten, um den Schutz von Personen und Gütern gegen strafbare und terroristische Handlungen (öffentliche Sicherheit) mit aufzunehmen. In der Entscheidung 58/2005 (12-8-2005) lehnte die HDPA den Antrag auf eine Ausweitung der Verwendungsmöglichkeiten mit der Begründung ab, dass der Einsatz eines globalen elektronischen Überwachungssystems nicht mit dem Grundsatz der Verhältnismäßigkeit vereinbart werden kann, da er eine schwerwiegende Verletzung der Rechte des Einzelnen auf eine Privatsphäre und Datenschutz darstellt, ohne bei der Wahrung des Anrechts der Bürger auf Sicherheit nennenswerte Fortschritte zu erzielen.

Der für die öffentliche Ordnung zuständige Minister legte gegen diese Entscheidung Berufung ein, die gegenwärtig vor dem Staatsrat anhängig ist.

C. Wichtige spezifische Themen

Aufgrund des Personalmangels bei der Datenschutzbehörde, die ihre wichtigsten Aufgaben nicht ordnungsgemäß erfüllen konnte (sieben Anwälte und fünf IT-Experten), nahm das Justizministerium die vorgeschlagene Einstellung von 14 weiteren Prüfern (acht Anwälte und sechs IT-Experten) sowie von fünf weiteren Verwaltungskräften an. Das Verfahren wurde im Januar 2006 abgeschlossen.

Ungarn

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Das Gesetz über den Schutz von personenbezogenen Daten und den öffentlichen Zugang zu Daten von öffentlichem Interesse wurde im Jahr 2005 geändert und weiterentwickelt. Die meisten Änderungen hatten Auswirkungen auf die Informationsfreiheit. Eine der Änderungen bezog sich auf die Verordnung über Daten für eine interne Verwendung und Daten im Zusammenhang mit der Vorbereitung einer Entscheidungsfindung, die als ungenügend definiert angesehen wurde und deren Verwendung laut einer im Jahr 2004 vom Verfassungsgericht gefällten Entscheidung eine unnötige und unverhältnismäßige Einschränkung der Informationsfreiheit bedeutete.

In dem Gesetz wurde die Definition von Daten von öffentlichem Interesse mit dem Hinweis präzisiert, dass jede Aufzeichnung von Informationen als Daten von öffentlichem Interesse betrachtet werden muss, unabhängig davon, in welcher Form die Daten verarbeitet wurden oder ob es sich um unabhängige oder erfasste Daten handelt. Gleichzeitig kann das Recht auf Zugang zu Daten von öffentlichem Interesse nicht nur im Interesse von Gerichtsverfahren, sondern auch behördliche Verwaltungsvorgänge eingeschränkt werden.

Jeder ist berechtigt, die Offenlegung von Daten, an denen ein öffentliches Interesse besteht, in einer beliebigen Form zu beantragen (mündlich, in schriftlicher Form oder auch auf elektronischem Wege). Der Zugang zu Daten von öffentlichem Interesse, die auf elektronischem Wege veröffentlicht werden, kann nicht von einer Registrierung abhängig gemacht werden. Dabei besteht nur die Möglichkeit, so viele personenbezogene Daten zu verarbeiten, wie dies für die beantragte Offenlegung erforderlich ist und den entrichteten Gebühren entspricht.

Das vom Parlament im Jahr 2005 angenommene Gesetz über die Freiheit elektronischer Informationen sieht die Verpflichtung vor, Daten von öffentlichem Interesse und öffentlich verwaltete Daten von öffentlichem Interesse zu veröffentlichen, wodurch sich das Gesetzgebungsverfahren offener gestaltet und die digitale Fassung von Rechtsnormen und die bisher anonymisierten Entscheidungen des Obersten Gerichtshofes leichter zugänglich werden.

Der Aufgabenbereich des Datenschutzbeauftragten wurde erweitert. Ab dem 1. Juni 2005 vertritt der Datenschutzbeauftragte die Republik Ungarn in den gemeinsamen Kontrollgremien der Europäischen Union.

B. Bedeutende Rechtsprechung

In einer Empfehlung über die Datenschutzimplikationen des Verfahrens der Steuererklärungen, das in Übereinstimmung mit den Regelungen des Gesetzes über Bedienstete im öffentlichen Dienst durchgeführt wird, erklärte der Datenschutzbeauftragte, dass das Ziel der Einführung der obligatorischen Steuererklärung, d. h. die Gewährleistung der Transparenz des öffentlichen Lebens, nicht dadurch verwirklicht werden kann, dass die Steuererklärungen von öffentlichen Bediensteten und ihren Familienangehörigen abgespeichert werden. Die Speicherung von fast 300 000 Steuererklärungen verstößt gegen die Grundsätze des Datenschutzes, d. h. gegen den Grundsatz der Verhältnismäßigkeit, und die Abspeicherung kann als Lagerung betrachtet werden, die im Rahmen einer früheren Entscheidung des Verfassungsgerichts als verfassungswidrig erklärt wurde. Außerdem ist es fraglich, ob jedes Familienmitglied, das seine eigene Steuererklärung

ausfüllen muss, hierzu aus freien Stücken seine Einwilligung gegeben hat.

C. Wichtige spezifische Themen

Die Ergebnisse einer Untersuchung bezüglich der Drogenkontrollen am Arbeitsplatz haben ergeben, dass Drogenkontrollen am Arbeitsplatz und die damit verbundenen Datenkontrollen aus folgenden Gründen **nicht generell zulässig** sind:

- Der freiwillige Charakter der Einwilligung des Mitarbeiters ist aufgrund des unausgewogenen Kräfteverhältnisses zwischen Arbeitgebern und Arbeitnehmern sehr fraglich.
- Die Kontrollen können zu Praktiken führen, die einen schwerwiegenden Eingriff in die Privatsphäre und die persönlichen Rechte darstellen.
- Die Effizienz der mobilen Tests ist nicht überzeugend, weil die Testergebnisse Informationen über den Verbrauch liefern – oder über einen physischen Kontakt mit der Substanz – aber nicht über die Arbeitsfähigkeit.

Der Datenschutzbeauftragte fasste einige Punkte zusammen, die im Rahmen des Legislativverfahrens berücksichtigt werden sollen.

Ein Thema, das in vielen zentral- und osteuropäischen Ländern immer wieder diskutiert wird, betrifft die Aufdeckung der Vergangenheit früherer Sicherheitsagenten. Viele Parlamentsmitglieder legten Gesetzentwürfe über die Änderung des Archivgesetzes vor – wobei die Stellungnahme des Datenschutzbeauftragten eingeholt, aber gleichzeitig nicht berücksichtigt wurde. Sie verfolgten das Ziel, über eine schrittweise Erweiterung des Datenbestandes, der ohne eine Anonymisierung der Daten verfügbar gemacht werden kann, und durch eine Veröffentlichung der Dokumente im Internet, die aus Gründen der nationalen Sicherheit zu schützen sind, die Möglichkeit zu schaffen, dass die Identitäten von all denjenigen offengelegt werden, die mit den nationalen Sicherheitsorganen zusammengearbeitet hatten oder von diesen Organen beschäftigt worden waren. Der Datenschutzbeauftragte wies ausdrücklich darauf hin, dass der Änderungsantrag die Verfassungsgrundsätze des Datenschutzes nicht erfüllt und darüber hinaus eine schwerwiegende Verletzung des Rechts von Einzelpersonen auf eine Privatsphäre darstellt.

Im Rahmen einer anderen Eingabe beschwerte sich ein Bürger darüber, dass er von seinem Arbeitgeber dazu verpflichtet worden sei, den Grundsätzen der Scientology-Kirche zu folgen, wobei von ihm verlangt würde, Dokumente und Fragebögen auszufüllen, in denen ein großes Maß an persönlichen Daten, die ihn selbst und andere Personen betreffen, abgefragt worden sei. Der Datenschutzbeauftragte der Republik Ungarn ist berechtigt, jede Erfassung personenbezogener Daten in Ungarn zu kontrollieren. Dieses Recht bezieht sich auch auf die Datenerhebungen der eingetragenen Kirchen. In seiner Antwort machte der Datenschutzbeauftragte auf folgende Punkte aufmerksam:

- Jeder übt die Kontrolle über seine eigenen personenbezogenen Daten aus und entscheidet selbst, ob er spezifische personenbezogene Daten einer anderen Person zugänglich machen will.
- Wenn jemand seine personenbezogenen Daten der Kirche oder einem beliebigen Kirchenorgan zur Verfügung stellt, kann er Einblick in die von ihm erhobenen personenbezogenen Daten verlangen, und auch ihre Löschung.
- Die Person, die mit der Kirche oder einem beliebigen Kirchenorgan in Verbindung tritt, darf nur über ihre eigenen personenbezogenen Daten eine Kontrolle ausüben. Sie ist berechtigt, über die personenbezogenen Daten anderer eine Kontrolle auszuüben, wenn die Datensubjekte aufgrund von Informationen, die vor der Datenerhebung mitgeteilt wurden,

ihre Einwilligung dazu gegeben haben. Wenn personenbezogene Daten einer anderen Person ohne vorherige Einwilligung des Betroffenen der Kirche oder einem beliebigen Kirchenorgan mitgeteilt werden, kann die Person, die die Daten übermittelt, zivilrechtlich und strafrechtlich hierfür haftbar gemacht werden.

- Wenn die Datensubjekte Informationen über die von ihnen erhobenen personenbezogenen Daten beantragen, ist jeder für den Datenschutz Verantwortliche dazu verpflichtet, die angeforderten Informationen so schnell wie möglich in einer leicht verständlichen Form und in keinem Fall später als innerhalb von 30 Tagen nach Antragstellung zur Verfügung zu stellen.
- Abgesehen von gesetzlich angeordneten Datenerhebungen ist jeder für den Datenschutz Verantwortliche auf Antrag des Datensubjekts dazu verpflichtet, von ihm erhobene personenbezogene Daten zu löschen.
- Die Bereitstellung der beantragten Informationen oder Löschung personenbezogener Daten (abgesehen von gesetzlich angeordneten Restriktionen) können nicht unter dem Hinweis auf eine in welcher Form auch immer abgegebene Erklärung abgelehnt werden, die entweder vom Datensubjekt oder einer beliebigen anderen Person unterzeichnet wurde.

Der Generaldirektor eines Bezirkskrankenhauses leitete eine Untersuchung über die medizinischen Unterlagen von Adoptivkindern ein. Diese Untersuchung befasste sich damit, dass alle persönlichen Identitätsdaten des Kindes im Anschluss an die Adoption geändert werden, wodurch der Zugang zu den Daten früherer Behandlungen im Rahmen einer späteren medizinischen Betreuung unmöglich gemacht wird. Tatsächlich lassen die gesetzlichen Bestimmungen eine Verbindung zwischen den Datenbanken zum gegenwärtigen Zeitpunkt nicht zu, aber das verfassungsmäßige Anrecht auf eine gute Gesundheit ist für das jeweils betroffene Kind von so großer Bedeutung, dass es den Zugang zu Daten, die von dem jeweiligen Gesundheitsdienst verwaltet werden und sich auf frühere Behandlungen und Krankheiten beziehen, dennoch rechtfertigen kann. Die Situation wird zusätzlich dadurch verkompliziert, dass jede Änderung von Daten in medizinischen Eintragungen so ausgeführt werden muss, dass die geänderten Daten lesbar bleiben. Der Datenschutzbeauftragte regte in seinem an den Gesundheitsminister und den Minister für Familienangelegenheiten gerichteten Vorschlag eine Änderung der gesetzlichen Bestimmungen an, die im Wesentlichen beinhaltet, dass sich die Kontrollbehörde unter Verwendung der Eintragungen des nationalen Gesundheitsversicherungsfonds (National Health Insurance Fund – NHIF, eine Finanzierungseinrichtung) an alle Erbringer von Gesundheitsdienstleistungen wenden kann, die an der medizinischen Betreuung des Kindes vor seiner Adoption beteiligt waren, mit der Aufforderung, alte, personenbezogene Identitätsdaten, die Teil der medizinischen Unterlagen sind, zu löschen und gleichzeitig die Eintragungen durch Aufnahme der neuen personenbezogenen Identitätsdaten zu ändern.

Irland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Beide Richtlinien wurden vollständig in irisches Recht umgesetzt. Im Jahr 2005 wurden keine Gesetzesänderungen vorgenommen.

B. Bedeutende Rechtsprechung

Der Datenschutzbeauftragte verklagte mit Erfolg ein Unternehmen wegen eines Spam-Delikts im Rahmen einer Rechtsverordnung, mittels der die Richtlinie 2002/58/EG in irisches Recht umgesetzt worden ist.

Das Unternehmen wurde vom Dubliner Bezirksgericht in fünf Fällen für schuldig befunden, da es Werbeachrichten ohne die Einwilligung der Empfänger an fünf Mobiltelefone gerichtet hatte. Das Unternehmen musste mit einer Geldbuße von bis zu 3 000 Euro je verschickter Werbenachricht rechnen. Das Gericht verhängte eine Geldbuße von 300 Euro für jeden festgestellten Fall (insgesamt 1 500 Euro). Das Unternehmen wurde darüber hinaus verpflichtet, Verfahrenskosten in Höhe von 1 000 Euro zu übernehmen.

Die gerichtliche Verfolgung wurde im Anschluss an eine Reihe von Beschwerden eingeleitet, die im März 2004 an den Datenschutzbeauftragten gerichtet worden waren und sich auf ein Unternehmen bezogen, das Werbung für ein Glücksspiel machte, indem es Anrufe an Mobiltelefone richtete. In allen Fällen klingelte das Mobiltelefon nur kurz, ohne den Beschwerdeführern ausreichend Zeit zu lassen, den Anruf noch vor dessen Beendigung zu beantworten. Das Mobiltelefon der Empfänger registrierte einen „versäumten Anruf" und wies die Nummer eines Dubliner Festanschlusses als Anrufer aus. Sobald diese Nummer angerufen wurde, ertönte eine aufgezeichnete Nachricht, mit der an den Anrufer gerichteten Aufforderung, eine Mehrwertnummer anzurufen, um ein Angebot wahrzunehmen, bei dem ein Guthaben von 50 Euro zur Nutzung in einem Glücksspiel abgerufen werden soll.

Der Datenschutzbeauftragte traf außerdem eine Reihe von Einzelentscheidungen zu Beschwerden, die aufgrund der Datenschutzgesetze eingereicht wurden und gegen die vor den Gerichten kein Einspruch erhoben wurde. Die wesentlichsten darunter waren:

- Ein Einwohner beschwerte sich darüber, dass eine CCTV-Kamera (Closed Circuit Television), die von dem Betreiberunternehmen des Dubliner Straßenbahnnetzes eingesetzt wird, den Garten hinter seinem Haus filmte, wodurch das Gefühl entstand, dass die Familie laufend überwacht wird. Das Unternehmen erklärte, dass seine Politik im Zusammenhang mit der Verwendung von CCTV darin bestünde, die Kameras so einzusetzen, dass sie öffentliche Bereiche überwachen, wobei vermieden werden solle, private Bereiche zu filmen. Es gestand ein, dass die betreffende Kamera tatsächlich Teile des Gartens hinter dem Haus des Beschwerdeführers aufzeichnen könnte. Der Datenschutzbeauftragte wies darauf hin, dass die Datenschutzbestimmungen voraussetzen, dass die Erhebung personenbezogener Daten relevant ist und im Rahmen der Zweckbegründung ihrer Durchführung den Grundsatz der Verhältnismäßigkeit wahrt. Im Hinblick auf die CCTV-Kameras bedeutete dies, dass die Kamera so ausgerichtet werden müsse, dass sie keine irrelevanten Bilder in ihrer näheren Umgebung aufzeichnen kann. Das Unternehmen änderte das System so, dass der Bildschirm schwarz wird, sobald die CCTV-Kamera das Privatgrundstück in ihrem Einzugsbereich filmt. Das Unternehmen erklärte, dass die entsprechenden Einstellungen nicht von seinen Mitarbeitern geändert werden können, die die Kameras in seinem zentralen Kontrollraum überwachen.

- Ein Reisebüro leitete die Anschriften seiner Kunden an ein Kreditkartenunternehmen weiter, das anschließend mit einigen dieser Kunden Verbindung aufnahm, um ihnen eine Kreditkarte unter einer gemeinsamen Marke (Reisebüro/Kreditkartenunternehmen) anzubieten. Die Buchungsunterlagen des Reisebüros enthielten den Hinweis, dass die in den Formularen enthaltenen Informationen zur Erfüllung seiner vertraglichen Verpflichtungen gegenüber dem Kunden dienen und dass Informationen von Zeit zu Zeit an andere Unternehmen innerhalb derselben Gruppe weitergegeben werden dürfen. Da das Kreditkartenunternehmen nicht der Unternehmensgruppe des Reisebüros angehörte und die Vermarktung einer Kreditkarte nicht dasselbe wie Urlaubsvermarktung ist, erklärte der Datenschutzbeauftragte, dass vor der Vermarktung der Kreditkarte unter einer gemeinsamen Marke die Einwilligung der Kunden erforderlich gewesen wäre. Das Unternehmen erklärte sich bereit, seine Marketingpraktiken zu ändern, um der Entscheidung des Datenschutzbeauftragten Folge zu leisten.

- Eine Reihe von Angestellten einer öffentlichen Einrichtung legten Beschwerden vor, in denen sie darauf hinwiesen, dass das auf biometrischen Kriterien beruhende Arbeitszeit- und Anwesenheitssystem, das eine zentrale Datenspeicherung und die Auswertung von Fingerabdruckdaten umfasste, eine unverhältnismäßige Einschränkung ihres Rechts auf eine Privatsphäre bedeute. Die Einrichtung erklärte, dass das System im Rahmen einer Sicherheitsüberprüfung eingeführt wurde, bei der der Verpflichtung Rechnung getragen worden sei, die in öffentlichem Besitz befindlichen Wertsachen, die in dem Gebäude untergebracht sind, zu schützen. Sie wies außerdem auf die systemeigenen Sicherheitscharakteristiken hin, dass gespeicherte Daten verwendet werden können, um einen Fingerabdruck zu reproduzieren, sowie auf die Tatsache, dass das System im Rahmen eines Tarifvertrages mit den Mitarbeitern eingeführt wurde. Der Datenschutzbeauftragte fasste den Beschluss, dass das System unter den gegebenen Umständen dem Grundsatz der Verhältnismäßigkeit entspricht und keine ungerechtfertigte Verletzung des Rechts von Einzelpersonen auf eine Privatsphäre darstellt.

C. Wichtige spezifische Themen

CCTV-Nutzungsplan für Gemeinden

Der Datenschutzbeauftragte wurde von der Abteilung Gleichbehandlung und Gesetzesreform des Justizministeriums zu den Datenschutzimplikationen befragt, die sich aus der vorgeschlagenen Einführung der CCTV-Nutzungsplänen für Gemeinden ergeben, die zur Abschreckung kriminellen Verhaltens dienen. Die an das Ministerium gerichtete Stellungnahme wies darauf hin, dass persönliche Daten, die durch solche Systeme erhoben werden, unter die Datenschutzgesetzgebung fallen: Es wäre wünschenswert, solche Systeme auf gesetzlicher Grundlage zu betreiben, und hilfreich, ihren Betrieb durch einen Verhaltenskodex abzudecken. Im Verlauf des Jahres wurde eine Gesetzgebung, die solche Systeme zulässt, vom Oireachtas (Parlament) angenommen und ein Kodex guter Praktiken, der Datenschutzthemen mit einschließt, auf der Website des Ministeriums (www.justice.ie) veröffentlicht.

Italien

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Kodex über digitale Verwaltung (Code of Digital Administration)

Im März 2005 wurde der sogenannte Kodex über digitale Verwaltung in Kraft gesetzt, in dem eine Reihe von Verordnungen konsolidiert werden, darunter diejenigen, die sich auf elektronische Personalausweise beziehen. Der Kodex, bei dessen Ausarbeitung auch die Stellungnahme der italienischen Datenschutzbehörde berücksichtigt wurde, weist darauf hin, welche Daten in den elektronischen Personalausweis aufgenommen werden müssen (Name des Karteninhabers + Steuernummer) und welche Informationen in den Personalausweis aufgenommen werden dürfen.

Sensible Daten dürfen nur auf Antrag des Karteninhabers aufgenommen werden. Abgesehen von DNS-Daten, die audrücklich ausgenommen sind, bezieht sich die Liste auf biometrische Daten, Daten über Blutgruppen und Daten über die Bereitschaft, im Todesfall Organe zu spenden.

Der Personalausweis kann außerdem andere, für Verwaltungszwecke nützliche Daten enthalten, insbesondere im Hinblick auf die Verwendung elektronischer Signaturen. Zusätzliche Spezifikationen müssen in Ad-hoc-Verordnungen festgelegt werden, namentlich im Bezug auf biometrische Daten.

Es besteht für die Bürger keine Verpflichtung, ihre Ausweispapiere gegen die neuen, elektronischen Karten zu tauschen, d. h. der Einstieg in das System ist gegenwärtig freiwillig.

Besondere Sorgfalt wurde darauf verwendet, die Normen festzulegen, die bei der Herstellung der neuen elektronischen Personalausweise eingehalten werden müssen, einschließlich der Verschlüsselung und anderer Sicherheitsmaßnahmen, die für die Speicherung von biometrischen Daten auf dem Chip der Karte verwendet werden.

Dringende Maßnahmen im Kampf gegen den internationalen Terrorismus (Gesetz Nr. 155/2005)

Im Anschluss an die Londoner Terroranschläge im Juli 2005 ergriff die italienische Regierung Eilmaßnahmen, um die Prävention und Bekämpfung des internationalen Terrorismus zu verstärken. Einige Bestimmungen haben erhebliche Auswirkungen auf die Grundrechte und -freiheiten, insbesondere auf das Recht auf den Schutz personenbezogener Daten:

a) *Speicherung von Daten über Telefon- und Internetverbindungen.* Die Anwendung der Bestimmungen des Datenschutzgesetzes bezüglich der Löschung von Telefon- und Internetverbindungsdaten wurde bis zum 31. Dezember 2007 außer Kraft gesetzt, unter anderem für nicht entgegengenommene Anrufe.

Die Speicherungsverpflichtungen wurden für zwölf Monate auf Internetverkehrsdaten ausgedehnt (sechs Monate allgemeingültige Frist zuzüglich sechs Monaten für Zwecke, die mit der Bekämpfung von Terrorismus und Kapitalverbrechen in Verbindung stehen). Die Datenschutzbehörde wird aufgefordert, vorab zu den Maßnahmen, die für die Durchführung dieser Bestimmungen erforderlich sind, eine Stellungnahme abzugeben.

b) *Verpflichtungen, die für öffentlich zugängliche Telefon- und Internetanschlüsse gelten.* Jeder, der beabsichtigt, für Kommunikationszwecke einschließlich internetgestützter Kommunikation bestimmte Endgeräte der Öffentlichkeit und/oder Verbrauchern und/oder Mitgliedern (z. B. eines privaten Klubs/einer Vereinigung) zugänglich zu machen, muss eine Lizenz von öffentlichen Sicherheitsbehörden erwerben. Die Eigentümer und/oder Verwalter der genannten Zugangsstellen müssen außerdem die Aktivitäten ihrer Kunden überwachen und relevante Daten einschließlich Angaben zur Identität der Kunden aufbewahren. Ein Erlass des Ministers für Innere Angelegenheiten, der im Anschluss

an Beratungen mit der Datenschutzbehörde veröffentlicht wurde, legte die spezifischen Durchführungsmaßnahmen fest.

c) *Zwangsentnahme von Gen-Proben zu Identifikationszwecken.* Im Rahmen einer Änderung der Strafprozessordnung wurde für die Polizei die Möglichkeit geschaffen, im Rahmen einer Zwangsmaßnahme aufgrund einer durch den zuständigen Staatsanwalt erteilten schriftlichen Genehmigung Haar- und/oder Speichelproben zu entnehmen, wenn der Betroffene seine Einwilligung verwehrt und wenn sich dieses Verfahren als notwendig erweist, um eine beliebige Person zu identifizieren, gegen die spezifische Ermittlungen laufen.

Vermeidung von Zahlkartenbetrug

Zur Vermeidung von Zahlkartenbetrug sah das Gesetz Nr. 166/2005 vor, eine Datenbank im Wirtschaftsministerium einzurichten. Diese Datenbank – die bisher noch nicht in Betrieb genommen worden ist – soll unter anderem die Identifikationsdaten der Geschäftsleute und der jeweiligen gesetzlichen Vertreter enthalten, die von einer Teilnahme an den Vereinbarungen mit dem Aussteller der Kredit-/Zahlkarten ausgeschlossen wurden; darüber hinaus werden die Daten aller von den Karteninhabern angefochtenen Transaktionen und andere Informationen im Zusammenhang mit einem Betrugsrisiko in die betreffende Datenbank eingegeben. Durchführungsbestimmungen müssen im Einzelnen festlegen, welche spezifischen Informationen und Daten eingegeben werden, und die Stellen benennen, die über eine Zugangsberechtigung zu den Informationen verfügen; ferner sollten sie die Zugangsmechanismen zu den in der Datenbank enthaltenen Informationen und die Mechanismen des Datenaustauschs regeln.

Elektronischer Reisepass

Im Anschluss an die EU-Verordnung, die die Anforderungen für elektronische Reisepässe festlegt, veröffentlichte das italienische Außenministerium nach Rücksprache mit der Datenschutzbehörde am 29. Dezember 2005 einen Erlass über elektronische Reisepässe. Der Erlass sieht die Aufnahme eines RFID-Chips in die Deckseite des Passes vor, um das Passbild des Inhabers und die Fingerabdrücke seiner beiden Zeigefinger zusätzlich zu den bereits in dem Papierdokument enthaltenen Informationen (den Inhaber betreffende Informationen usw.) in einem interoperablen Datenformat zu speichern. Die auf dem Chip gespeicherten biometrischen Angaben dürfen nur zur Überprüfung der Echtheit des Dokuments und der Identität seines Inhabers anhand von Vergleichsangaben verwendet werden, die unmittelbar in den Fällen verfügbar sein müssen, in denen das Gesetz die Vorlage eines Passes und/oder beliebiger anderer Reisedokumente vorschreibt. Die für die Ausstellung des Passes erfassten biometrischen Daten werden nicht in einer zentralisierten Datenbank gespeichert.

B. Bedeutende Rechtsprechung

Verfassungsgericht – Entscheidung Nr. 271 vom 17. Juli 2005 – Gesetzgebungsbefugnisse der Regionen

In einer wichtigen Entscheidung, die im Anschluss an eine Beschwerde des Amtssitzes des Premierministers gegen Teile eines regionalen Gesetzes getroffen wurde, die Maßnahmen zur Förderung der Entwicklung der „Informationsgesellschaft" enthalten, entschied das Verfassungsgericht, dass die betreffenden Bestimmungen eine Übertretung der Verfassungsgrundsätze darstellten. Das Gericht urteilte, dass die betreffenden Maßnahmen das Recht auf den Schutz personenbezogener Daten verletzen, und machte deutlich, dass die Gesetzgebung über den Umgang mit personenbezogenen Daten eine Reihe von persönlichen Rechten regelt, die für jedes Datensubjekt gelten, und einen Anspruch beinhaltet, eine Kontrolle über die Daten zur eigenen Person und die Mechanismen zur Verarbeitung dieser Daten auszuüben. Deshalb fällt dieser Regelungsbereich entsprechend der Definition von Artikel 117 der italienischen Verfassung in die alleinige Zuständigkeit des Staates. Die Regionen sind nur berechtigt, ergänzende Maßnahmen zu ergreifen, insofern dies im Rahmen der vom Staat verabschiedeten Gesetze vorgesehen ist – sie können beispielsweise Zuständigkeiten im Rahmen der Verfahrensregelung oder organisatori-

scher Mechanismen zur Verarbeitung personenbezogener Daten auf regionaler/lokaler Ebene ausüben, namentlich dann, wenn sie die Einrichtung eines Informationsnetzes über regionale Einrichtungen und Strukturen betreffen.

Kassationshof – 1. Abteilung, zivilrechtliche Angelegenheiten – Entscheidung Nr. 14390/2005

Der Kassationshof – der im italienischen Justizsystem das Gericht der letzten Instanz darstellt – hat der von einem Polizeibeamten eingereichten Beschwerde entsprochen, der vom Dienst suspendiert wurde, nachdem er in einem Hardcorefilm erkannt worden war, der auf einer Website mit „homosexuellen und fetischistischen Inhalten" gezeigt wurde. Der Polizeibeamte hatte sich gegenüber der Datenschutzbehörde über die Verwendung der sensiblen Daten beschwert, die den Bildern entnommen worden waren und die anschließend im Internet veröffentlicht wurden. Er erklärte, dass sich die Polizei ungesetzlich verhalten habe, insbesondere weil seine Kollegen (die die von dem Polizeibeamten besuchten Websites in dessen Haus gefunden, und daraufhin Informationen über ihn angeboten hatten) außerhalb ihrer gesetzlichen Befugnisse gehandelt hätten. Der Kassationshof entschied – nachdem die Polizeiverwaltung (Ministerium für Innere Angelegenheiten) die Entscheidung der Datenschutzbehörde angefochten hatte –, dass die Verbreitung von Daten über das Internet nicht bedeutet, dass die Daten uneingeschränkt verwendet werden dürften. Tatsächlich werden öffentlich verfügbare und/oder veröffentlichte personenbezogene Daten ebenfalls durch das Datenschutzgesetz gerade deswegen geschützt, weil jede Einrichtung, die solche Daten verarbeitet, ihnen einen „Informationsmehrwert" entnehmen kann, der möglicherweise dazu führt, dass die Würde des Datensubjekts verletzt wird. Deshalb dürfen die Daten nicht in dem Ausmaß verarbeitet werden, in dem sie der Öffentlichkeit zur Verfügung stehen, sondern nur in dem Umfang, in dem eine Veröffentlichung gesetzlich zulässig ist. Diese Anforderungen wurden in dem vorliegenden Fall vom Ministerium für Innere Angelegenheiten allem Anschein nach nicht erfüllt, insbesondere dann nicht, wenn davon ausgegangen werden kann, dass von öffentlichen Einrichtungen erwartet wird, dass sie bei der Verarbeitung von Daten, die im Rahmen der geltenden Gesetzesbestimmungen als sensible Daten eingestuft werden, strengere Sicherheitsvorkehrungen einhalten. Deshalb entschied der Kassationshof, dass die vom Ministerium für Innere Angelegenheiten gegen den Polizeibeamten eingeleiteten Maßnahmen nichtig sind, und verwies den Fall zurück an das zuständige Gericht, das zu entscheiden hatte, ob das Ministerium über die gesetzlichen Voraussetzungen verfügt, die hochsensiblen, den Beschwerdeführer betreffenden personenbezogenen Daten zu verarbeiten.

Staatsrat – Entscheidungen Nr. 4471/2005 und 5879/2005

Der Staatsrat – der in verwaltungsrechtlichen Fragen das Gericht der letzten Instanz bildet – fällte zwei Entscheidungen, in denen er Mitglieder einer Gemeindeverwaltung dazu berechtigte, sich Zugang zu allen Daten zu verschaffen, die ihnen bei der Ausübung ihres Amtes behilflich sein können. Dieses Zugangsrecht gilt insbesondere auch für Dokumente und Aufzeichnungen (die personenbezogene Daten über Dritte enthalten), die auf die Zeit vor der Amtszeit des Antragstellers zurückgehen, weil es ein inhärenter Bestandteil der Ausübung seines Amtes mit all seinen möglichen Implikationen ist.

C. Wichtige spezifische Themen

Im März 2005 wurden die Mitglieder des kollegialen Gremiums „Garante per la protezione dei dati personali" (Bevollmächtigte für den Schutz personenbezogener Daten) vom Parlament (für eine Mandatsperiode von vier Jahren) ernannt; es handelt sich um Prof. Franco Pizzetti (Präsident), Herrn Giuseppe Chiaravalloti (Vizepräsident), Herrn Mauro Paissan und Herrn Giuseppe Fortunato. Herr Giovanni Buttarelli wurde von dem neuen Panel als Generalsekretär der Behörde bestätigt.

Öffentliche Konsultationen: angenommene Bestimmungen

Zusätzlich zu den Ergebnissen der öffentlichen Konsultationen, auf die im Achten Jahresbericht

hingewiesen wird, nahm die Behörde vier allgemeine Bestimmungen an, die Sicherheitsmechanismen und Anforderungen im Zusammenhang mit Paybackkarten, interaktivem Fernsehen, RFID-Geräten und Videophonen festlegen.

Paybackkarten und Sicherheitsmechanismen für Verbraucher

Die Datenschutzbehörde legte die Maßnahmen fest, die die für den Datenschutz Verantwortlichen ergreifen müssen, um zu gewährleisten, dass sie sich bei der Durchführung der von ihnen ausgeführten Datenverarbeitung im Rahmen der gesetzlichen Grenzen bewegen.

Die Grundsätze können wie folgt zusammengefasst werden:

a) Minimale Datenmengen und Verhältnismäßigkeit: Informationssysteme und Programme müssen von Anfang an in einer Form konfiguriert werden, bei der die Verwendung von Informationen, die identifizierbare Kunden betreffen, soweit wie möglich eingeschränkt wird. Personenbezogene Daten, die die Kunden betreffen, dürfen nicht verarbeitet werden, wenn die Möglichkeit besteht, den Verarbeitungszweck – unter besonderer Berücksichtigung der Ermittlung von Kundenprofilen – entweder anhand von anonymisierten Daten oder unter Verwendung von indirekt identifizierenden Daten zu erreichen; es dürfen insbesondere nur die Daten im Zusammenhang mit dem eigentlichen Kundenprogramm verarbeitet werden, die notwendig sind, um die Kunden in den Genuss der Vorzüge zu bringen, die sich aus der Verwendung ihrer Paybackkarte ergeben.

b) Verwendung zum Zwecke des Direktmarketings: Relevante Daten dürfen in angemessener Menge erhoben und verwendet werden, um Werbematerial und kommerzielle Nachrichten zu verschicken oder Waren im Direktverkauf anzubieten. Grundsätzlich gilt dies nur für die Daten, die sich unmittelbar auf die Identifizierung entweder des Karteninhabers oder seiner Familienangehörigen oder auch vom Karteninhaber benannter Personen beziehen. Falls personenbezogene Daten bei der Ermittlung von Kundenprofilen gewonnen werden, muss ihre Verwendung in einer separaten Zustimmungserklärung der Betroffenen genehmigt werden.

c) Informierung von Datensubjekten: Die Kunden müssen eindeutig und vollständig (in einem knappen, umgangssprachlichen Stil) informiert werden, bevor die Offenlegung ihrer Daten und die Ausstellung ihrer Paybackkarte erfolgt, um ihre uneingeschränkte Einwilligung zu den vorgeschlagenen Initiativen und der Erstellung von Kundenprofilen und/oder Marketingaktivitäten zu gewährleisten.

d) Einwilligung zur Datenverarbeitung: Die Einwilligung ist „eine Voraussetzung für die Erfüllung der Verpflichtungen aus einem Vertrag, den das Datensubjekt als Vertragspartei abgeschlossen hat"; deshalb ist ihre Beantragung, als ob es sich dabei um eine Option handele, unangemessen. Andererseits setzt jeder andere Verarbeitungszweck, der mit der Möglichkeit verbunden ist, Datensubjekte zu identifizieren – bei der Erstellung von Kundenprofilen und Marktstudien, oder im Rahmen von Marketingtätigkeiten – die spezifische Einwilligung der Datensubjekte voraus, die in Kenntnis des jeweiligen Sachverhalts, für jeden Verwendungszweck unabhängig voneinander und bei sensiblen Daten schriftlich erteilt werden muss. Die Aufnahme in das Paybackkartenprogramm darf nicht von dieser Einwilligung abhängig gemacht werden.

e) Aufbewahrungsfristen: Der für diesen Bereich geltende Grundsatz besagt, dass alle persönlichen Daten, deren Aufbewahrung zur Erfüllung des Zwecks ihrer Verarbeitung nicht erforderlich ist, entweder gelöscht und vernichtet oder anonymisiert werden müssen. In jedem Fall dürfen ausführliche Daten über von identifizierbaren Kunden gekaufte Waren zu Zwecken der Kundenprofilierung oder des Marketing nicht länger als jeweils 12 oder 24 Monate aufbewahrt werden, je nachdem, ob die Daten bereits in einer Weise anonymisiert wurden, die eine selbst indirekte Identifizierung und/oder eine Identifizierung der Datensubjekte durch Vernetzung mit anderen Datenbanken unmöglich macht.

Datenschutz und interaktives (digitales) Fernsehen

Mit dieser Bestimmung wurde erneut der Grundsatz hervorgehoben, demzufolge die Notwendigkeit besteht, die Verwendung von Informationen über identifizierbare Nutzer und Abonnenten auf ein Minimum zu beschränken und grundsätzlich anonymen Daten den Vorzug zu geben; darüber hinaus ist es notwendig, auf die Erhebung von Informationen zu verzichten, die nicht unbedingt notwendig sind – z. B. sollten Titel gekaufter Filme nicht auf den entsprechenden Rechnungen in Erscheinung treten.

Die Verwendung von im Voraus bezahlten Karten wird bevorzugt, um die Anonymität der Benutzer zu gewährleisten. Bei der Inrechnungstellung ihrer Einkäufe muss den Abonnenten, unabhängig davon, ob Sportveranstaltungen oder Filme gekauft wurden, die Möglichkeit eingeräumt werden, keine aufgeschlüsselten Rechnungen zu erhalten – die nur auf ausdrücklichen Wunsch ausgestellt werden sollten.

Die Bestimmung hebt hervor, dass es ungesetzmäßig ist, personenbezogene Daten im Zusammenhang mit der Einschaltdauer, den verfolgten Programmen und Ereignissen, den Fernseheinschaltzeiten, Einschaltunterbrechungen, dem Umschalten auf andere Sender, und Verhaltensanalysen bezüglich der Fernsehwerbung zu verarbeiten.

Wenn eine Fernabstimmung durchgeführt wird, was bei Fernsehsendungen oft der Fall ist, müssen Vorkehrungen getroffen werden, um die abgegebenen Stimmen von den Namen der Teilnehmer an der Abstimmung getrennt zu verwalten. Dasselbe gilt für Marktforschungsuntersuchungen und andere repräsentative Umfragen, bei denen ausgeschlossen werden muss, dass personenbezogene Daten unter welchen Umständen auch immer Dritten mitgeteilt werden.

Eindeutige und vollständige Anleitungen sind erforderlich, auch im Hinblick auf die Möglichkeit, dass sich andere Mitglieder des Haushalts Zugang zu den digitalen Fernsehdiensten verschaffen, und Informationen über die Art der Verarbeitung der Daten nach ihrer Eingabe durch den Benutzer müssen über eine Bildschirmmaske mitgeteilt werden, bevor ein Kauf und/oder die Einrichtung einer interaktiven Verbindung vorgenommen werden kann.

Die Einwilligung des Datensubjekts ist notwendig, um seine Präferenzen festzuhalten und/oder sein Abonnentenprofil zu erstellen; diese Einwilligung darf jedoch nicht zu einer Voraussetzung gemacht werden, um Zugang zu anderen, vertraglich geregelten Fernsehdiensten zu erhalten.

In der Regel gilt der Grundsatz, demzufolge sensible Daten nicht verarbeitet werden dürfen. Dabei ist darauf hinzuweisen, dass die Zustimmung des Datensubjekts in einigen Fällen mit Hilfe der Fernbedienung abgeschickt werden kann, während ein spezifischer, durch ein Passwort geschützter Zugang notwendig ist, wenn die Einwilligung zur Verarbeitung von sensiblen Daten gewährt werden soll.

Sämtliche die Abonnenten betreffenden Informationen dürfen nur über einen begrenzten Zeitraum hinweg aufbewahrt werden, der vertraglich geregelt werden muss – in diesem Zusammenhang besteht die grundlegende Verpflichtung, alle Daten grundsätzlich so schnell wie möglich entweder zu löschen oder zu anonymisieren. Detaillierte, einen Kauf betreffende Daten dürfen nicht länger als zwölf Monate aufbewahrt werden; wenn der betreffende Vertrag beendet ist, müssen alle diesbezüglichen Informationen innerhalb von drei Monaten gelöscht werden.

Sicherheitsvorkehrungen, die für die Verwendung von RFID-Geräten gelten

Die Anforderungen, die für eine Verwendung von RFID-Geräten gelten, wurden auch unter Berücksichtigung des im Jahr 2005 veröffentlichten Arbeitsdokuments der Art. 29 Datenschutzgruppe festgelegt.

Diese Bestimmungen sehen im Wesentlichen vor, dass die für die Datensicherheit Verantwortlichen sowohl des öffentlichen Dienstes als auch des privaten Sektors die gesetzlich vorgegebenen Datenschutzgrundsätze einhalten.

Minimale Datenmengen: Grundsätzlich sollten RFID-gestützte Systeme so ausgelegt sein, dass eine Erhebung personenbezogener Daten vermieden und/oder die Identifizierung der Datensubjekte abgesehen von den Fällen unmöglich gemacht wird, in denen dies unbedingt erforderlich ist, um die Funktion der Systeme zu erfüllen.

Gebrauchsanleitung: Die Betroffenen müssen über das Vorhandensein und die Verwendung von RFID-Kennzeichnungen einschließlich der Verwendung von RFID-Lesegeräten angemessen informiert werden. In diesem Zusammenhang kann es erforderlich werden, an Orten, an denen RFID-Kennzeichnungen verwendet werden, entsprechende Informationsmitteilungen bekannt zu geben; in jedem Fall sollten die Informationen aber auch auf einzelnen Produkten angebracht werden, die eine RFID-Kennzeichnung tragen.

Einwilligung: Einrichtungen des privaten Sektors müssen über eine Einwilligung der Datensubjekte verfügen, bevor sie RFID-Kennzeichnungen verwenden, wenn eine solche Verwendung mit einer Verarbeitung personenbezogener Daten verbunden ist; die Einwilligung muss aus freien Stücken und aufgrund angemessener Informationen gewährt werden. Wenn die Kennzeichnungen nur zu Zahlungszwecken verwendet werden und keine Verbindung zu identifizierten und/oder identifizierbaren Käufern hergestellt werden kann, ist eine Einwilligung nicht erforderlich.

Zweckbindung: Die mit Hilfe der RFID-Kennzeichnungen gesammelten Daten dürfen nur für die Zwecke verwendet werden, zu denen sie erhoben wurden, und ihre Aufbewahrung darf nur solange erfolgen, wie dies unbedingt erforderlich ist. Einzelpersonen sind berechtigt, RFID-Kennzeichnungen nach dem Erwerb eines mit einer solchen Kennzeichnung ausgestatteten Produkts zu entfernen, zu deaktivieren und/oder außer Betrieb zu setzen. Hierfür müssen verbraucherfreundliche Verfahren zur Verfügung stehen. Grundsätzlich sollten RFID-Kennzeichnungen ihre Wirksamkeit verlieren, sobald der Kunde die Verkaufsstelle verlässt.

Darüber hinaus wurden spezifische Bestimmungen hinsichtlich der Verwendung von RFID-Kennzeichnungen im Beschäftigungsbereich oder in Form von subkutanen Implantaten erlassen. Im Hinblick auf den Beschäftigungsbereich sollte daran erinnert werden, dass es in Italien unzulässig ist, Kennzeichnungen einzusetzen, die eine Fernkontrolle der Beschäftigten zulassen; wenn RFID-Kennzeichnungen bei Zugangskontrollen zu gewissen Bereichen für notwendig erachtet werden, müssen die Sicherheitsmechanismen der diesbezüglichen arbeitsrechtlichen Bestimmungen und geltende Datenschutzregelungen eingehalten werden.

Subkutane Implantate dürfen nur unter außergewöhnlichen Umständen bewilligt werden (wenn beispielsweise belegt werden kann, dass sie für die Aufrechterhaltung der Gesundheit eines Patienten erforderlich sind), weil sie die Würde des Einzelnen verletzen (Paragraph 2 des Datenschutzgesetzes), namentlich auch in Bezug auf die Grundrechtecharta der EU. Für die Datensubjekte muss die Möglichkeit bestehen, die RFID-Implantate jederzeit kostenlos entfernen zu lassen. Der Einsatz sukutaner RFID-Kennzeichnungen ist grundsätzlich eine Frage, die eine Vorabüberprüfung durch die Datenschutzbehörde notwendig macht.

Videophone

Die Datenschutzbehörde legte die Bestimmungen fest, die eingehalten werden müssen, um bei der Verwendung von Videophonen die Privatsphäre zu schützen und den Datenschutzanforderungen gerecht zu werden.

In diesem Zusammenhang wurde darauf hingewiesen, dass die Bestimmungen der Datenschutzgesetzgebung nicht zur Anwendung kommen, wenn die Videophonanrufe für eine persönliche Verwendung bestimmt sind und die aufgezeichneten Bilder nicht außerhalb des persönlichen Bekanntenkreises des Benutzers gezeigt werden.

Wenn die Bilder jedoch verbreitet werden, einschließlich einer Verbreitung über das Internet, gelten die Bestimmungen der Datenschutzgesetzgebung – was bedeutet, dass die Einwilligung des

Datensubjekts auf Grundlage seiner vorherigen Inkenntnissetzung eingeholt werden muss. Dies betrifft auch Dritte, die auf den für eine Verbreitung bestimmten Bildern gezeigt werden. Außerdem müssen die Beschränkungen beachtet werden, die möglicherweise für Videoaufzeichnungen in öffentlichen und/oder privaten Gebäuden gelten, da eine Verarbeitung der Daten ansonsten ungesetzlich ist.

Darüber hinaus appellierte die Datenschutzbehörde an die Hersteller von Videophonen und die Entwickler passender Programme, den Einbau von Ad-hoc-Signalfunktionen vorzusehen (z. B. in Form von Leuchtsignalen), die darauf hinweisen, dass sich das Videophon in Betrieb befindet.

Parteienwerbung und Information der Datensubjekte

Anlässlich der Gemeindewahlen und Referenden, die in den ersten sechs Monaten des Jahres 2005 in Italien durchgeführt wurden, und im Hinblick auf die nationalen Wahlen, die im Jahr 2006 stattfinden, wies die Datenschutzbehörde in zwei Ad-hoc-Entscheidungen auf mehrere Fragen hin, die die Parteienwerbung und Datenschutzanforderungen betreffen. Grundsätzlich waren politische Parteien und Bewegungen, Förderkomitees, Anhänger und Kandidaten von der Verpflichtung, die Datensubjekte im Voraus über die Verwendung ihrer Daten durch Informationsmitteilungen zu informieren, befreit, insofern sie personenbezogene Daten aus öffentlich zugänglichen Registern, Verzeichnissen, Aufzeichnungen und/oder Dokumenten ausschließlich zu Zwecken der Parteienwerbung und damit zusammenhängender politischer Mitteilungen verarbeitet hatten und die Datensubjekte vom Verwender der Daten nicht zuvor hierüber informiert worden waren oder Werbematerial erhielten, das die Aufnahme entsprechender Hinweise nicht ohne weiteres zuließ (beispielsweise kleine Broschüren oder Handzettel, wie sie oft von politischen Kandidaten verwendet werden).

Zusätzlich zu dieser Maßnahme bekräftigten die Entscheidungen erneut den Dekalog, der in einer 2004 angenommenen Entschließung veröffentlicht wurde und die Grundsätze und Kriterien zusammenfasst, die generell im Rahmen politischer Werbung und politischer Mitteilungen gelten sollen. Diese Entschließung trifft folgende Unterscheidungen:

a) Die Fälle, in denen eine Kontaktaufnahme mit den Datensubjekten (d. h. Bürgern, die politische Mitteilungen und Nachrichten erhalten) ohne ihre vorherige Einwilligung möglich ist – wenn die Daten wirklich aus „öffentlichen" Quellen stammen, was bedeutet, dass sie von jedem uneingeschränkt eingesehen werden können, z. B. Register, Verzeichnisse, Aufzeichnungen und/oder Dokumente, die von einer öffentlichen Einrichtung verwaltet werden und frei und ohne Einschränkungen zugänglich sind, insofern dies ausdrücklich durch Gesetze und/oder Verordnungen bestätigt wird. In diese Kategorie fallen im Wesentlichen die so genannten Wählerverzeichnisse, d. h. die Listen der wahlberechtigten Bürger, die in den Gemeindeverwaltungen aufbewahrt werden, die Mitgliederlisten von Berufsverzeichnissen und -vertretungen und die in einigen Verzeichnissen der Handelskammern und anderen Formen von Wählerverzeichnissen (z. B. für im Ausland wohnhafte italienische Bürger) enthaltenen Informationen. Dies umfasst jedoch insbesondere nicht bei Volkszählungen verwendete Verzeichnisse sowie das Geburten-, Heirats- und Sterberegister, die nicht zu Zwecken der Wählerwerbung an private Stellen weitergegeben werden dürfen – auch dann nicht, wenn der Antragsteller ein Mitglied der Gemeindeverwaltung und/oder Volksvertreter ist.

b) Die Fälle, in denen nur mit Einwilligung der Datensubjekte mit ihnen Kontakt aufgenommen werden kann – was alle anderen Fälle betrifft, in denen Daten aus nicht „öffentlichen" Quellen im Sinne der oben genannten Definition erhoben werden, unabhängig davon, ob SMS-Nachrichten, MMS-Systeme, E-Mail-Systeme oder andere Kommunikationsmittel verwendet werden.

Die Datenschutzbehörde wies außerdem darauf hin, dass die Verpflichtung, über die Datenerhebung zu informieren, auch dann besteht, wenn die Daten unmittelbar beim Datensubjekt erhoben werden

und nicht aus öffentlichen, frei verfügbaren Quellen stammen. In diesem Zusammenhang wurde der Entwurf einer Informationsmitteilung ausgearbeitet, die in solchen Fällen verwendet werden kann.

Öffentliche Verwaltung

Verarbeitung sensibler Daten durch öffentliche Verwaltungen

Im Zusammenhang mit der Verarbeitung personenbezogener Daten durch öffentliche Behörden kann auf die im April 2005 vom Minister für die öffentliche Verwaltung veröffentlichten Leitlinien hingewiesen werden, in denen daran erinnert wurde, dass öffentliche Einrichtungen dazu verpflichtet sind, Ad-hoc-Bestimmungen zum Schutz der Privatsphäre bei der Verarbeitung sensibler und justizieller Daten zu erlassen. Das italienische Datenschutzgesetz (196/2003) räumt öffentlichen Einrichtungen nur dann die Möglichkeit ein, sensible und gerichtliche Daten zu verarbeiten, wenn spezifische Gesetze und/oder Verordnungen dies zulassen; wenn Letztere aber – was in der Regel der Fall ist – die spezifischen Verarbeitungsschritte und betroffenen Datenkategorien nicht im Einzelnen angeben, sind die jeweiligen öffentlichen Einrichtungen verpflichtet, sie im Rahmen von Ad-hoc-Verordnungen selbst zu regeln. Bisher ist es nicht dazu gekommen, und die Leitlinien des Ministers haben den Rahmen gebildet, in dem die öffentlichen Einrichtungen entsprechende Maßnahmen verabschieden – die auf einer sorgfältigen Bewertung des Zwecks, der im Rahmen der unterschiedlichen Datenverarbeitungsschritte verfolgt wurde, sowie der Menge an personenbezogenen Daten, die tatsächlich erforderlich („unerlässlich") ist, beruhen müssen.

Darüber hinaus veröffentlichte die Datenschutzbehörde (im Amtsblatt Nr. 170 vom 23. Juli 2005) eine Bestimmung, in der notwendige als auch angemessene Maßnahmen beschrieben werden, die für den Datenschutz öffentlich Verantwortliche auf Grundlage des Datenschutzgesetzes bei der Verarbeitung von sensiblen Daten einhalten müssen. Die öffentlichen Verwaltungen werden ebenfalls aufgefordert, die von ihnen erhobenen personenbezogenen Informationen im Einzelnen zu rechtfertigen und zu präzisieren, wie solche Informationen für das wesentliche öffentliche Interesse verwendet werden, auf die das Gesetz Bezug nimmt. Zur Unterstützung der Erfüllung dieser Anforderungen wurde die Zusammenarbeit mit dem Amt des Premierministers, dem Ministerium für den öffentlichen Dienst und den Organisationen, die die Regionen, Gemeinden und Universitäten vertreten, intensiviert, um Modellverordnungen zu entwickeln, die dazu beitragen können, die Sicherheitsmechanismen zu vereinheitlichen, die von anderen Verwaltungen eingesetzt werden, und die so die Verfahren zur Annahme entsprechender Verordnungen erleichtern. Tatsächlich bildet die Annahme dieser Sicherheitsbestimmungen eine Voraussetzung, um die Stellungnahme der Datenschutzbehörde einholen zu können, die innerhalb von 45 Tagen nach Eingang eines entsprechenden Antrags abgegeben werden muss.

Die Datenschutzbehörde erläuterte den Inhalt dieser Bestimmungen und wies dabei insbesondere auf folgende Punkte hin:

a) die Angabe der unbedingt erforderlichen Daten (nach Kategorien) unter dem Hinweis auf entsprechende Aufgaben, die von der Behörde erfüllt werden müssen

b) die Angabe der Verarbeitungsschritte, die unerlässlich sind, um in einem wesentlichen, öffentlichen Interesse handeln zu können, das gesetzlich vorausgesetzt wird

c) die Bereitstellung einer Übersicht über die von der betreffenden öffentlichen Einrichtung ausgeführten Tätigkeiten, unter besonderer Berücksichtigung der Aufgabenbereiche, die sich am nachhaltigsten auf die Bürgerrechte auswirken. In diesem Zusammenhang sollten die öffentlichen Einrichtungen angemessene Maßnahmen ergreifen, um zu gewährleisten, dass die bei der Verarbeitung sensibler und/oder justizieller Daten getroffenen Entscheidungen angemessen veröffentlicht werden, wobei sie sich nicht nur ihrer institutionellen Websites, sondern auch gezielter institutioneller Veröffentlichungsinitiativen bedienen können.

Bisher wurden insgesamt 33 Verordnungen von öffentlich-rechtlichen Körperschaften veröffentlicht – namentlich, unter anderem, vom Ministerium für Umwelt und Kulturerbe, dem Verteidigungsministerium, dem Bildungsministerium und dem nationalen Forschungsrat sowie von mehreren Handelskammern, Regionen, Gemeindeverwaltungen und unabhängigen Verwaltungsbehörden.

Steuerbehörden

Die Datenschutzbehörde befasste sich mit einer Reihe von Fragen, die die Erhebung und Verwendung von personenbezogenen Daten im Rahmen der gesetzlich vorgesehenen Untersuchungen betreffen, die von den Steuerbehörden durchgeführt werden. Angesichts der Neuerungen, die durch das Haushaltsgesetz aus dem Jahr 2005 eingeführt wurden, um die Datenerhebungsbefugnisse der zuständigen Behörden zu erweitern, wurde auf folgende Punkte hingewiesen:

a) Der Austausch von personenbezogenen Daten über elektronische Netze im Rahmen der Einholung von Bankauskünften sollte unter Berücksichtigung der Grundsätze der Erhebung minimaler Datenmengen und der Verhältnismäßigkeit erfolgen, d. h. unter Bezugnahme auf spezifische Fälle und mit dem Hinweis auf bestimmte Vorgänge (eine Pauschalerhebung von Daten ist nicht zulässig).

b) Anstelle der Erstellung von Kopien von Datenbeständen der Steuerbehörden sollten diese Behörden Maßnahmen ergreifen, um sicherzustellen, dass die notwendigen personenbezogenen Informationen im Rahmen einer elektronischen Erhebung aus den vorhandenen öffentlichen und privaten Datenbeständen, die bereits entsprechende Informationen enthalten, gewonnen werden können.

c) Besondere Sicherheitsvorkehrungen müssen bei der Verwendung und Aufbewahrung von personenbezogenen Daten angewendet werden, die Bank- und Spareinlagen betreffen oder ihnen entnommen wurden, beziehungsweise außergerichtliche Erklärungen und Kataster- sowie Hypothekeneintragungen (insbesondere dann, wenn es sich um kommerziell genutzte Informationen handelt) oder auch bei der elektronischen Übertragung von Krankmeldungen an Sozialversicherungsträger.

Studenten-Portfolio

Im Rahmen der in Italien vor kurzem umgesetzten Lehrplanreform wurde ein neues Bewertungs- und Orientierungsinstrument unter der Bezeichnung „Studenten-Portfolio" eingeführt, das von den Lehrkräften unter Berücksichtigung der individuellen Situation des Schülers/Studenten zusammengestellt wird. Neben Zeugnissen und Ausbildungsberichten soll dieses Portfolio Informationen über Haltungen, Erwartungen und Verhaltensweisen enthalten, die ein Schüler/Student während seiner gesamten Bildungslaufbahn zum Ausdruck gebracht hat.

Die Datenschutzbehörde wies auf die Notwendigkeit hin, nur solche personenbezogenen Daten aufzunehmen, die relevant und notwendig sind, um einen Studenten zu beurteilen und ihm Orientierungshilfen zu geben; sensible Daten (medizinische Daten, Daten über psychologische Eigenschaften usw.) dürfen nur dann in das Portfolio aufgenommen werden, wenn sie für eine Bewertung des einzelnen Schülers/Studenten unbedingt erforderlich sind. Jede Schule/Bildungseinrichtung wird aufgefordert, Ad-hoc-Maßnahmen zu ergreifen, um die Eltern und Schüler/Studenten in angemessener Weise über das Portfolio und die darin enthaltenen Daten zu informieren, damit die Eltern Gelegenheit erhalten, alle ihnen im Rahmen der Datenschutzgesetzgebung gewährten Rechte auszuüben (Recht auf Zugang, Berichtigung usw.), und angemessene Sicherheitsvorkehrungen zu treffen.

Die Erbringung von Gesundheitsversorgungsleistungen unter Gewährleistung der menschlichen Würde

In einer im November 2005 angenommenen Regelung wurden die Maßnahmen festgelegt, die von öffentlichen und privaten Einrichtungen

ergriffen werden müssen, um den Betrieb und die Organisation von Gesundheitsversorgungseinrichtungen mit den geltenden Bestimmungen des Datenschutzgesetzes in Einklang zu bringen, damit die Rechte der Einzelpersonen möglichst umfassend geschützt werden können. Ihre wesentlichen Inhalte können wie folgt zusammengefasst werden:

- Schutz der menschlichen Würde
  Es ist notwendig, stets den Schutz der Würde jedes Einzelnen zu gewährleisten. Dies bezieht sich insbesondere auf Behinderte, Kinder und ältere Menschen sowie auf Patienten, an denen invasive medizinische Eingriffe vorgenommen werden und/oder die auf eine besondere Betreuung angewiesen sind (z. B. Patientinnen, die eine Schwangerschaftsunterbrechung vornehmen lassen).

- Schutz der Vertraulichkeit von Kommunikationen
  Die Mitarbeiter der Gesundheitsdienste müssen eine Offenlegung medizinischer Informationen gegenüber Dritten insbesondere dann verhindern, wenn sie Rezepte oder Bescheinigungen ausstellen. Dies gilt auch in den Fällen, in denen medizinische Unterlagen (Laborergebnisse, Krankengeschichten, Verschreibungen) von Einrichtungen abgegeben werden, die nicht spezifisch für diesen Zweck eingerichtet wurden (z. B. Einrichtungen, in denen unterschiedliche Diensteistungen erbracht werden, Informationsstellen usw.).

- Warteabstand
  Krankenhäuser und Gesundheitsversorgun gseinrichtungen müssen für Gespräche am Schalter (z. B. Terminvereinbarungen) sowie die Entgegennahme von medizinischen Angaben einen angemessenen Warteabstand vorsehen.

- Informationen durch Notaufnahmen/Krankenhausabteilungen
  Notaufnahmen und Krankenhausabteilungen sind berechtigt, unter anderem auch telefonische Auskünfte darüber zu erteilen, ob eine bestimmte Person in ihren Räumen anwesend war/ist; diese Auskunftsberechtigung gilt jedoch nur gegenüber Dritten, die einen Rechtsanspruch auf diese Informationen haben (Familienangehörige, Freunde und Mitbewohner). Wenn das Datensubjekt bei Bewusstsein und nicht handlungsunfähig ist, muss es im Voraus (z. B. zum Zeitpunkt seiner Krankenhausaufnahme) informiert werden und Gelegenheit erhalten, zu entscheiden, wer über seinen Aufenthalt in der Notaufnahme/Krankenhausabteilung informiert werden soll.

- Wartesäle
  Die Patienten sollten nicht mit ihrem Namen aufgerufen werden, wenn sie auf eine Dienstleistung warten und/oder Dokumente in Empfang nehmen (z. B. Labortests). Alternativlösungen sollten angewendet werden, z. B. die Vergabe fortlaufender Nummern, sobald eine Anmeldung erfolgt und/oder ein Antrag eines Patienten registriert wird.

- Patientenlisten
  Die Veröffentlichung von Wartelisten von Patienten in für die Öffentlichkeit zugänglichen Bereichen der chirurgischen Abteilung ist unabhängig davon nicht zulässig, ob außerdem individuelle Krankheiten genannt werden.

- Informationen über den Gesundheitszustand
  Informationen über die Gesundheit eines Datensubjekts dürfen Dritten nur dann mitgeteilt werden, wenn das Datensubjekt (oder ein Familienangehöriger, wenn das Datensubjekt körperlich behindert oder rechtsunfähig ist) hierzu seine ausdrückliche Einwilligung gegeben hat. Im Einzelfall können andere Personen aufgefordert werden, im Namen des Datensubjekts eine entsprechende Einwilligung zu erteilen (Familienangehörige, Mitbewohner usw.).

- Die Abholung von Labortests
  Klinische Berichte, Labortests und von Labors und/oder anderen Gesundheitsversorgungseinrichtungen ausgestellte Bescheinigungen können von anderen Einzelpersonen als den Datensubjekten unter der Voraussetzung abgeholt werden, dass sie über eine entspechende schriftliche Vollmacht verfügen und die Informationen in einem verschlossenen Umschlag ausgehändigt werden.

Hausärzte, private Krankenhäuser und Fachärzte sind nicht verpflichtet, die oben stehenden Maßnahmen zu ergreifen; sie müssen jedoch die Würde des Datensubjekts gewährleisten und ihren beruflichen Verpflichtungen zur Wahrung der Vertraulichkeit nachkommen.

Öffentliche Ordnung

Nummerierte Tickets und Videoüberwachung in Stadien

Die Datenschutzbehörde wurde im Zusammenhang mit zwei vom Ministerium für Innere Angelegenheiten vorgelegten Erlassentwürfen konsultiert, die sich mit der Bekämpfung von Gewalt bei Sportveranstaltungen in Stadien befassten, und den Einsatz von Videoüberwachungssystemen verbunden mit der Ausgabe nummerierter Tickets vorsahen.

Im Hinblick auf die Videoüberwachung kam sie zu dem Ergebnis, dass ihr Einsatz angesichts der in Fußballstadien oft stattfindenden gewalttätigen Ausschreitungen sowohl rechtmäßig als auch notwendig sei. Die für die Bilddaten vorgeschlagene Aufbewahrungszeit von einer Woche wurde im Verhältnis zu dem verfolgten Zweck als angemessen betrachtet; wenn jedoch besondere Formen und Techniken der Verfilmung eingesetzt werden sollen, müssen sie zuvor der Datenschutzbehörde zur Überprüfung mitgeteilt werden.

Die vorliegenden Informationen gaben angesichts der gewaltigen Mengen an zu verarbeitenden personenbezogenen Daten und des im Hinblick auf den angestrebten Zweck zweifelhaften Nutzens dieser Maßnahme keinen Anlass zu der Annahme, dass die vorgeschlagene Einführung namentlich zugeordneter Tickets dem Grundsatz der Verhältnismäßigkeit entspricht – zumal andere Kontrollmaßnahmen zur Verfügung stehen, um gewalttätige Fans zu identifizieren und ihnen den Zugang zu Stadien zu verwehren. Diesbezüglich wurde darauf hingewiesen, dass die zuständigen Behörden, wenn sie sich für die Einführung namentlich zugeordneter Tickets entscheiden, festlegen müssen, welche für die Datensicherheit Verantwortlichen/Verarbeiter dafür zuständig sind, wie lange die personenbezogenen Daten aufbewahrt werden, welche Einrichtungen eine Zugangsberechtigung zu den personenbezogenen Daten erhalten und ob die so erhobenen Daten mit den Daten einzelner Fußballvereine abgeglichen werden sollen.

Hotelreservierungsinformationen

Hinsichtlich eines Erlassentwurfs zur Neuregelung der Verpflichtung für Hotels und andere Unterkünfte, die besagt, dass lokalen Polizeibehörden Angaben zur Identität aller ihrer Gäste zu machen sind, richtete die Datenschutzbehörde eine begründete Stellungnahme an das Ministerium für Innere Angelegenheiten. In diesem Zusammenhang wies sie insbesondere auf folgende Punkte hin:

a) Für Hotels und vergleichbare Einrichtungen besteht keine Notwendigkeit, die Formulare, die sie zur Erhebung der personenbezogenen Daten ihrer Gäste verwendet haben, weiterhin aufzubewahren, nachdem die darin enthaltenen Daten den Polizeibehörden mitgeteilt wurden, mit Ausnahme der Informationen, die zur Erfüllung ihrer Buchhaltungs- und Steuerverpflichtungen erforderlich sind.

b) Die Daten können den Polizeibehörden entweder in Papierform oder elektronisch mitgeteilt werden; bei Verwendung eines elektronischen Formats müssen jedoch zusätzliche Sicherheitsvorkehrungen getroffen werden, um die digitale Identität des Empfängers (d. h. der Polizeibehörde) zu bestätigen.

c) Die Daten dürfen nicht in eine zentralisierte Datenbank aufgenommen werden, da nur die lokalen Polizeibehörden zu ihrer Aufbewahrung berechtigt sind; außerdem müssen sie getrennt von anderen Formen personenbezogener Daten aufbewahrt werden, die von der Polizei im Rahmen ihrer Tätigkeiten zur Aufrechterhaltung der öffentlichen Ordnung und zur Verbrechensbekämpfung verwendet werden, wobei eine kurze Aufbewahrungszeit sichergestellt werden muss; generell ist es erforderlich, die Notwendigkeit

und Verhältnismäßigkeit dieser Maßnahme auf Grundlage des Datenschutzgesetzes neu zu prüfen. Diesbezüglich wäre ebenfalls zu berücksichtigen, dass das Schengener Durchführungsübereinkommen entsprechende Maßnahmen nur in Verbindung mit ausländischen Gästen in Betracht zieht und dabei ausdrücklich ausschließt, dass Informationen über Gäste, die die Staatsangehörigkeit des Landes besitzen, in dem sie sich aufhalten, von Hotels und vergleichbaren Einrichtungen an die Polizeibehörden weitergeleitet werden. Außerdem darf eine Weiterleitung auf Grundlage des Durchführungsübereinkommens nur dann erfolgen, wenn die darin enthaltenen Daten zum Zweck der Verhütung oder Aufdeckung krimineller Handlungen erforderlich sind.

Telekommunikation

Im Jahr 2005 wurden die im Jahr 2004 angenommenen Bestimmungen über Telefonverzeichnisse (siehe Achter Jahresbericht) umgesetzt; demzufolge erhielten 22 Millionen Abonnenten fester Telefonanschlüsse Formulare, auf denen sie angeben konnten, ob und wie ihre personenbezogenen Daten und Präferenzen in den gedruckten oder elektronischen Verzeichnissen in Erscheinung treten sollten. Hierauf antworteten in etwa fünf Millionen Telefonkunden, von denen ungefähr zehn Prozent erklärten, dass sie ihre Einwilligung dazu geben, zu Marketing- und Werbezwecken angesprochen zu werden. Die Abonnenten, die nicht geantwortet haben, werden weiterhin im Rahmen des bisherigen, vertraglich festgelegten Kundenverhältnisses betreut.

„Gelbe Seiten": Branchenverzeichnisse

In einer im Juli 2005 veröffentlichten Bestimmung wurden die Kriterien für die Zusammenstellung von Unternehmens- und Geschäftsverzeichnissen wie den „Gelben Seiten" oder vergleichbarer Verzeichnisse festgelegt. Insbesondere sind Unternehmen, die diese Verzeichnisse zusammenstellen und veröffentlichen, nicht verpflichtet, zuvor die Einwilligung der dort eingetragenen Unternehmen und Geschäfte einzuholen, da die zu verarbeitenden Informationen deren kommerzielle Tätigkeiten betreffen und deshalb von der gesetzlichen Verpflichtung zur Einholung einer Einwilligung ausgenommen sind. Hierbei müssen jedoch insofern die Anforderungen an die Datenqualität erfüllt werden, als korrekte, vollständige und aktuelle Daten zu verarbeiten sind. Wenn die Daten der vor kurzem eingerichteten „einheitlichen Datenbank" (einschließlich aller Daten über Teilnehmer mit Festnetz- und Mobilfunkanschlüssen sowie der Verwender von Telefonen mit Prepaid-Karten) entnommen werden, müssen alle eingetragenen Präferenzen, so wie sie der Datenbank entnommen wurden, berücksichtigt werden (z. B. ist es nicht möglich, die Namen der Kunden mit aufzunehmen, die sich dafür entschieden haben, nicht in Telefonverzeichnissen in Erscheinung zu treten). In diesem Zusammenhang wurde auch eine vereinfachte Fassung einer Informationsmitteilung entworfen, die von den Unternehmen, die diese Verzeichnisse veröffentlichen, verwendet werden kann.

Das Abhören von Gesprächen

Im Anschluss an eine umfassende und ausführliche, in der Zeit zwischen August und Dezember 2005 von der Datenschutzbehörde durchgeführte Untersuchung über die Mechanismen, mit denen Betreiber von Telefongesellschaften auf gerichtliche Anordnungen zum Abhören von Telefongesprächen reagieren, zeigten die Ergebnisse, dass die Betreibergesellschaften keinen Zugang zum Inhalt der Gespräche erhalten und sich darauf beschränken, die Telefonleitung der von der gerichtlichen Untersuchung betroffenen Person zu verdoppeln und diese Parallelverbindung in das von der zuständigen Justizbehörde benannte Abhörzentrum freizuschalten. Dennoch wurde zum Teil aufgrund der Verarbeitung von personenbezogenen Daten, die sowohl die abgehörte Person als auch Dritte betrifft, sowie der zusätzlichen Dienstleistungen, die die Telefongesellschaften in diesen Fällen erbringen (z. B. geografische Ortung des Teilnehmers, Entnahme von Daten aus dem Einwohnerverzeichnis) auf einige spezifische Sicherheitsvorkehrungen hingewiesen, die bei der Durchführung solcher Maßnahmen beachtet werden müssen. Hierunter fallen organisatorische Maßnahmen (Reduzierung der Anzahl der Personen, die für die Verarbeitung der abgehörten Daten

zuständig sind, Trennung der Rechnungsdaten von anderen Daten, die im Rahmen des Abhörvorgangs anfallen), verstärkte Sicherheitsvorkehrungen (strenge Ausweisauflagen für die Mitarbeiter, die den Zugriff auf die betreffenden Daten vornehmen, Verwendung von Technologien auf dem neusten Stand der Verfahrenstechnik bei der Kommunikation mit den Justizbehörden, wobei beispielsweise Fax-Mitteilungen vermieden werden, und die Umsetzung komplexer Verschlüsselungssysteme, solange sich die Daten in den Datenbanken der Telefongesellschaft befinden), sowie erhöhter Datenschutz (durch sofortige Löschung der Daten, sobald sie den Justizbehörden mitgeteilt wurden). Den Telefonbetreibergesellschaften wurde sechs Monate Zeit gewährt, um diese Auflagen zu erfüllen.

Biometrik

Biometrik am Arbeitsplatz

Im Anschluss an einen vorangegangenen Antrag auf Überprüfung der Verwendung von biometrischen Daten zur Kontrolle der Gewissenhaftigkeit der Mitarbeiter eines privaten Unternehmens stellte die Datenschutzbehörde fest, dass die geplante Datenverarbeitung ungesetzlich ist, und verbot ihre Anwendung. Diese Entscheidung bezog sich auf ein Bauunternehmen mit etwa 300 Mitarbeitern, das geplant hatte, Fingerabdruckdaten zu verwenden, um die Gewissenhaftigkeit seiner Mitarbeiter zu kontrollieren, einigen Formen des Missbrauchs vorzubeugen und die Probleme zu vermeiden, die sich aus dem Verlust von Magnetkarten ergeben; es hatte daran gedacht, die Erhebung von Fingerabdruckdaten als obligatorische Anforderung an alle Mitarbeiter vorzuschreiben, wobei die Daten anschließend in einer zentralisierten Datenbank gespeichert würden.

Unter Berücksichtigung der im Hinblick auf die Datenqualität geltenden Grundsätze wurde festgestellt, dass die in Betracht gezogenen Mechanismen die Verlässlichkeit und Integrität der Daten nicht in angemessener Weise gewährleisten konnten, vor allem nicht bei der zuverlässigen Feststellung sowohl „falscher Identifikationen als nicht autorisierte Person" als auch „falscher Identifikationen als autorisierte Person". Mit Hinweis auf den Verhältnismäßigkeitsgrundsatz wurde entschieden, dass diese Art der Pauschalverwendung biometrischer Daten ungesetzlich sei – unter anderem, weil Alternativmechanismen zur Verfügung stehen, mit denen die persönliche Identität festgestellt werden kann, die die Privatsphäre weniger stark beeinträchtigen, persönliche Freiheiten nicht einschränken und nicht dazu führen, dass der Körper eines Mitarbeiters instrumentalisiert wird. Diesbezüglich wurde darauf hingewiesen, dass es – soweit möglich – besser gewesen wäre, einen Identifikationskode auf einem Datenträger zu speichern, der zur alleinigen Verfügung des Datensubjekts gehalten wird, anstelle diesen Kode zentralisiert im Informationssystem des Unternehmens zu speichern.

Umgekehrt wurde in einer Bestimmung vom 23. November 2005 die Verwendung von biometrischen Daten (Fingerabdruckdaten) zugelassen, um den Zutritt zu einem zugangsbeschränkten Hochsicherheitstrakt eines Unternehmen, das Verteidigungstechnologien in den Bereichen Luftfahrt und Elektronik produziert, zu kontrollieren und zu regeln. Das betroffene Unternehmen hatte einen Antrag auf vorherige Überprüfung dieser Maßnahme gestellt, woraufhin die Datenschutzbehörde den Beschluss fasste, dass diese zur vorherigen Überprüfung vorgelegte Form der Datenverarbeitung gesetzeskonform sei; in ihrer Schlussfolgerung stützte sie sich dabei auf die Bewertung der unterschiedlichen in diesem Zusammenhang verfolgten Zweckbestimmungen sowie auf einige Sicherheitsvorkehrungen, die das Unternehmen zusätzlich zu denen ergreifen wollte, die von der Datenschutzbehörde im Hinblick auf die konkreten Mechanismen für eine biometrische Identifikation genannt wurden.

Sonstige Themen

Anspruch auf Löschung

Eine wesentliche Entscheidung wurde von der Datenschutzbehörde im Zusammenhang mit einer im Jahr 2004 eingereichten Beschwerde getroffen. Dieser Fall bezog sich auf das Abrufen einer

Entscheidung über das Internet, die von der italienischen Kartellbehörde (die keine Justizbehörde ist) wegen irreführender Werbung gegen ein Unternehmen verhängt worden war; die betreffende Entscheidung wurde 1996 getroffen und anschließend auf der Website der Behörde veröffentlicht. Der Beschwerdeführer machte geltend, dass die Tatsache, dass die Entscheidung immer noch bei jeder Internet-Suche zu den laufenden Tätigkeiten des Unternehmens auf der Trefferliste steht, seinen Anspruch auf Löschung verletzt.

Die Datenschutzbehörde wies in ihrer Entscheidung darauf hin, dass die von der Kartellbehörde vorgenommene Veröffentlichung rechtmäßig und im Rahmen der geltenden gesetzlichen Bestimmungen vorgesehen sei, wobei das Gesetz jedoch keinen Aufschluss darüber gäbe, welche spezifischen Verfahren im Rahmen einer solchen Veröffentlichung angewendet werden sollten; hierbei müssen jedoch die beiden folgenden Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung der Daten im Internet nicht zu einer Übertretung der Datenschutzbestimmungen führt:

a) Einrichtung eines Bereichs mit Zugangsbeschränkung auf der Website der Kartellbehörde, in dem ähnliche Entscheidungen wie die oben genannte (die auf 1996 zurückgeht), veröffentlicht werden können, ohne dass die Möglichkeit besteht, sie mit Hilfe der gängigen externen Suchmaschinen abzurufen

b) Festlegung eines angemessenen Zeitraums durch die Kartellbehörde, während dessen die Veröffentlichung und freie Verfügbarkeit einer Entscheidung auf der Website der Kartellbehörde im Hinblick auf die Erreichung des Zwecks dieser Entscheidung als mit dem Grundsatz der Verhältnismäßigkeit vereinbar betrachtet werden kann.

In diesem Zusammenhang kann hervorgehoben werden, dass die Kartellbehörde die Leitlinien der Datenschutzbehörde befolgt hat; sie verhinderte, insbondere durch den Einsatz so genannter „Robot-Meta-Tags", dass gewisse Seiten (einschließlich der Seite, die auf die betreffende Entscheidung hinweist) durch Suchmaschinen abgerufen werden können. Darüber hinaus wurde der angemessene Zeitraum für eine uneingeschränkte Veröffentlichung von Informationen über die Website der Behörde – so wie sie in dem oben genannten Fall erfolgt ist – in Anlehnung an die geltenden kartellrechtlichen Bestimmungen, die vorsehen, dass nach Ablauf einer Fünfjahresfrist für einen Wiederholungsfall geltende Sanktionen nicht mehr angewendet werden können, auf fünf Jahre festgelegt.

Im Zusammenhang mit den die Suchmaschinen und Anrechte auf Löschung betreffenden Fragen hat die Datenschutzbehörde im November 2005 eine andere Entscheidung angenommen, die sich insbesondere mit der Aufbewahrung und Verfügbarkeit von Zeitungsartikeln im Internet befasst, die mehrere Jahre zuvor veröffentlicht wurden. Die betreffenden Artikel waren über die Website der Zeitung, die sie veröffentlicht hatte, nicht mehr erhältlich; dennoch konnten sie nach wie vor über Google abgerufen werden – womit interessanterweise die von Google eingesetzte parallele Datenverarbeitung deutlich wurde, bei der Cache-Kopien und die entsprechenden Zusammenfassungen verwendet werden.

Abfalltrennung

Im Anschluss an eine Reihe von Berichten und Behauptungen bezüglich der Nichteinhaltung des grundsätzlichen Schutzes der Privatsphäre bei der Anwendung von Verfahren einiger Gemeindeverwaltungen im Zusammenhang mit der Trennung fester Abfälle und/oder der Aufdeckung von Übertretungen der maßgeblichen Verwaltungsbestimmungen wies die Datenschutzbehörde in einer allgemeinen Entscheidung auf die Maßnahmen hin, die Datenverarbeiter insbesondere unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit ergreifen müssen. Hierzu gehören:

a) Der zur Abholung bereitstehende Hausmüll sollte nicht in durchsichtigen Müllsäcken vor die Tür gestellt werden.

b) Abfallcontainer sollten nicht mit Klebeetiketten versehen werden – auf denen Name und Anschrift des Datensubjekts eingetragen sind – insbesondere dann nicht, wenn diese Großbehälter öffentlich zugänglich auf die Straße gestellt werden.

c) Müllsäcke können mit einem Strichcode gekennzeichnet werden, der den Identifikationsdaten des Inhabers entspricht; ersatzweise ist auch eine Kennzeichnung mit Chip- oder RFID-Etiketten möglich.

d) Die zuständigen Kontrollbehörden sind nicht berechtigt, Pauschalüberprüfungen von Müllsäcken durchzuführen; solche Überprüfungen sollten auf einer selektiven Grundlage vorgenommen werden und nur dann, wenn Grund zu der Annahme besteht, dass der Müll unter Missachtung der geltenden Gesetze/Bestimmungen entsorgt wurde und keine anderen Möglichkeiten zur Verfügung stehen, um den/die mutmaßlichen Verursacher zu ermitteln.

e) Den gesetzlichen Bestimmungen zufolge dürfen die Namen und Adressen von Bürgern, die ihren Müll zwecks Mülltrennung an so genannten Ecopiazzole (umweltfreundliche Abfallentsorgungsstellen) entsorgen, festgehalten werden – wenn auch nur vorübergehend.

Taxis und Kundendaten

Die Anforderungen, die von Unternehmen erfüllt werden müssen, die Taxi-Reservierungsdienste führen (so genannte Taxi-Rufdienste), wurden festgelegt. Diese Unternehmen erheben in der Regel zum Zeitpunkt der Reservierung Kundendaten, um ihre Dienstleistungen anbieten zu können, und die Datenschutzbehörde erinnerte im Anschluss an eine Reihe von Beschwerden, die auch von Verbraucherverbänden eingereicht wurden – in denen behauptet wurde, dass einige Unternehmen unter anderem weiterführende Daten aufbewahren, die das Verhalten der Kunden betreffen (z.B.: „Kunde nicht erschienen"„falsche Adresse"„hat sich geweigert, eine Fahrt zu bezahlen") und über deren Vorhandensein die Kunden nicht informiert werden – an die Kriterien, die in diesem Zusammenhang eingehalten werden müssen. Den Behauptungen zufolge wurden solche Informationen von den Taxi-Diensten verwendet, um zu entscheiden, ob sie ihre Dienste in Zukunft einem solchen Kunden zur Verfügung stellen sollen.

Diesbezüglich wurde hervorgehoben, dass diese Dienste solche zusätzlichen Informationen nicht erfassen und speichern dürfen und sich darauf beschränken sollten, nur solche Daten aufzubewahren, die notwendig sind, um mit dem Kunden Verbindung aufzunehmen und dessen Identität als diejenige Person festzustellen, die die jeweilige Reservierung vornimmt (z. B. Adresse oder Telefonnummer). Diese Daten müssen nach Beendigung der Fahrt abgesehen von spezifischen Ausnahmen (z. B. Uneinigkeit über den für die Fahrt zu bezahlenden Preis, Rückgabe von Fundsachen) gelöscht werden – wobei die maximale Aufbewahrungszeit 30 Tage nicht überschreiten sollte. Die Taxi-Dienste müssen ihre Kunden über Verfahren und Zweck der von ihnen durchgeführten Datenerhebung informieren, bevor sie das Reservierungsverfahren weiterführen (z. B. in Form einer im Voraus aufgezeichneten Standardmitteilung), und die ausdrückliche Einwilligung der Kunden einholen, wenn sie ihre Daten für Werbezwecke und/oder Marktstudien verwenden.

Abtretung von Kreditforderungen (durch Kredit-Factoring): die Notwendigkeit, die Würde der Person zu achten

Diesbezüglich wurde auf die notwendigen, von den jeweiligen für die Datenverarbeitung Verantwortlichen (oder von in ihrem Auftrag handelnden Dritten) zu ergreifenden Maßnahmen hingewiesen, um die in Verbindung mit dem Kredit-Factoring durchgeführten Datenverarbeitungsverfahren mit den geltenden Bestimmungen zum Schutz personenbezogener Daten in Einklang zu bringen. Insbesondere wurde an die Verpflichtung erinnert, die Verarbeitung auf eine gesetzliche Grundlage zu stellen (keine ungerechtfertigte Offenlegung der Daten des Schuldners gegenüber Dritten, z. B. um ihn unter Druck zu setzen; keine

Verwendung von im Voraus aufgezeichneten Telefonansagen ohne den Eingriff des Betreibers, um auf die Begleichung von Außenständen drängen) und angemessene Verfahren zu verwenden (keine Verschickung von Postkarten mit einer „Kredit-Factoring"-Kennzeichnung und keine Verbreitung von Daten an Dritte unter Verwendung ähnlich gekennzeichneter Briefumschläge); darüber hinaus dürfen nur die Daten verarbeitet werden, die für die jeweiligen Factoring-Aufgaben erforderlich sind (z. B. Name, Geburtsort und Geburtsdatum, Steuernummer, Höhe der Außenstände), wobei die Daten nach Abschluss der Factoring-Tätigkeiten gelöscht werden müssen (d. h. bei Einzug der Forderungen). Außerdem wurde darauf hingewiesen, dass sich Datensubjekte an die zuständigen Justizbehörden wenden können, wenn im Rahmen des Kredit-Factoring eingesetzte Verfahren zivilrechtliche (wie die Forderung einer Entschädigung für gegebenenfalls erlittene Schäden) oder strafrechtliche Verletzungen (wenn das Verhalten einen strafrechtlichen Tatbestand darstellt, wie beispielsweise Belästigung oder Drohungen) beinhalten.

Durchführung

Während des Jahres 2005 wurde der Durchführung der geltenden Bestimmungen besondere Aufmerksamkeit geschenkt. Dies betrifft insbesondere die verstärkte Durchführung von Kontrollen und Untersuchungen in einer Reihe von Bereichen, die sich von der Verwendung von Paybackkarten bis zu Kreditauskunftsunternehmen, der Aufbewahrung von Telefonverkehrsdaten, der Einstellung von Mitarbeitern und der Verarbeitung von personenbezogenen und sensiblen Daten durch Gesundheitsversorgungseinrichtungen erstrecken.

Im Jahr 2005 wurden in ganz Italien 250 Kontrollen vor Ort durchgeführt. Dabei konnten etwa 100 Übertretungen von Datenschutzgesetzen festgestellt werden, die mit entsprechenden Geldbußen geahndet wurden. Dies war unter anderem durch eine gemeinsame Ad-hoc-Absichtserklärung möglich geworden, die von dem Garante und der italienischen Finanzpolizei angenommen wurde – einer Polizeieinheit, die in Italien für die Überwachung der Einhaltung der Steuer- und Finanzgesetzgebung zuständig ist. Auf Grundlage dieser Absichtserklärung kann sich die Datenschutzbehörde bei der Durchführung von (selbstverwalteten) Kontrollen von der Finanzpolizei insbesondere in abgelegenen Gebieten unterstützen lassen.

Bei den wichtigsten Überprüfungen kann auf die Untersuchungen hingewiesen werden, welche aufgrund von Behauptungen von gesetzeswidrigen Zugriffen auf die EDV-Verzeichnisse der Römischen Stadtverwaltung (Einwohnerverzeichnis, Geburten- , Sterbe- und Heiratsregister usw.), die von einem von der Region Latium (mit der Hauptstadt Rom) geleiteten Unternehmen verwaltet werden, durchgeführt wurden. Diese Überprüfung hat gezeigt, dass Mitarbeiter dieses Unternehmens Datenschutzauflagen verletzt hatten (insbesondere durch unrechtmäßige Zugriffe auf die personenbezogenen Daten von Kandidaten bei den Regionalwahlen und Missachtung der gesetzlich vorgeschriebenen Aufgabenverteilung). Im Übrigen wies die Datenschutzbehörde auf die Notwendigkeit hin, die gemeinsame Absichtserklärung, die die Beziehungen zwischen der Region Latium und der Stadtverwaltung von Rom regelt, zu ändern, um einen unmittelbaren Onlinezugang zu den Verzeichnissen der Stadtverwaltung über regionale Organe und Behörden zu verhindern, wobei die Stadtverwaltung ihrerseits die Sicherheitsmaßnahmen und technischen Voraussetzungen für den Zugang zu diesen Verzeichnissen erweitern, und ein proaktives „Push-System" entwickeln muss, um die Daten an die Antragsteller weiterzuleiten. Die Anweisungen der Datenschutzbehörde wurden im Amtsblatt der italienischen Republik veröffentlicht, da die für diesen spezifischen Fall geltenden Anforderungen grundsätzlich auch auf alle anderen Stadtverwaltungen übertragbar sind.

Lettland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Änderungen des Gesetzes zum Schutz personenbezogener Daten

Zur Gewährleistung der Übereinstimmung der lettischen Gesetze mit den Anforderungen der Richtlinie 95/46/EG und um die Grundprinzipien für die Arbeiten der Einrichtung, die für den Schutz personenbezogener Daten zuständig ist, festzulegen, richtete der Premierminister am 10. Januar 2005 eine Arbeitsgruppe ein, deren Aufgabe darin bestand, entsprechende Gesetzesentwürfe vorzubereiten. Die Gesetzesentwürfe zur Änderung des Gesetzes über den Schutz personenbezogener Daten wurden seitdem vorgelegt. Sie sollen umreißen, welche Systeme zur Verarbeitung personenbezogener Daten notifiziert werden müssen, die Notifizierungsverfahren erläutern, die gesetzlichen Normen nennen, die bei der Anwendung des Gesetzes Schwierigkeiten bereitet haben, und die Anforderungen der Richtlinie 95/46/EG, die in dem Gesetz zum Schutz personenbezogener Daten umgesetzt werden, einschließlich derjenigen Anforderungen benennen, die die rechtliche Stellung der staatlichen Datenkontrollbehörde (State Data Inspectorate) regeln.

Gleichzeitig wurden Änderungen der Satversme (Verfassung) der Republik Lettland ausgearbeitet, deren Annahme den rechtlichen Status der staatlichen Datenkontrollbehörde betrifft.

Im Verlauf der Diskussionen konnte eine Einigung über einen Gesetzentwurf erzielt werden, in dem darauf hingewiesen wird, dass auf Ebene der Verfassung eine Ausnahme von dem allgemeinen Grundsatz vorgesehen werden muss, demzufolge alle staatlichen Behörden dem Ministerkabinett unterstehen. Dadurch bietet die Verfassung die Möglichkeit der Bestimmung, dass eine Behörde nicht der Hierarchie des staatlichen Verwaltungssystems untergeordnet wird. In § 58, Absatz 2 wird Folgendes festgelegt: „Das Saeima (Parlament) kann zur Gewährleistung angemessener Verwaltungsstrukturen festlegen, welche Behörden nicht dem Kabinett unterstehen. Die Zuständigkeiten und Strukturen dieser Behörden werden in einem separaten Gesetz geregelt." Der erste Satz in Absatz 2 weist darauf hin, dass das Saeima auf Grundlage geltender gesetzlicher Bestimmungen Behörden benennen kann, die bei der Ausübung ihrer Funktionen und/oder im Rahmen ihrer institutionellen Zuordnung nicht dem Kabinett unterstehen. Die Formulierung „... die ... nicht dem Kabinett unterstehen" umfasst somit zwei Möglichkeiten:

1) Zu erklären, dass eine Behörde bei der Ausübung ihrer Funktionen nicht dem Kabinett untersteht, d. h. im Rahmen ihrer Entscheidungsfindung, während sie institutionell an das Kabinett gebunden bleibt, z. B. in Bezug auf die Disziplinarhaftung, Finanzen, Arbeitsorganisation usw. In diesem Fall wird die Behörde von einem Ministerium verwaltet. Die Inhalte dieser Verwaltung werden gesetzlich geregelt.
2) Zu erklären, dass eine Behörde weder bei der Ausübung ihrer Funktionen noch institutionell dem Kabinett untersteht.

Der zweite Satz von § 58, Absatz 2 legt Folgendes fest: „Die Zuständigkeiten und Strukturen dieser Behörden werden in einem separaten Gesetz geregelt." Wenn im Rahmen einer Entscheidung beschlossen wird, gewisse Kompetenzen aus dem Zuständigkeitsbereich des Kabinetts abzugeben, wird das Saeima für jeden spezifischen Fall in einem separaten Gesetz entsprechende Vorkehrungen treffen und darin Struktur und Zuständigkeiten der Behörde festlegen. Je nach Art der Behörde können hierbei für jeden einzelnen Fall unterschiedliche Lösungen vorgesehen werden.

Es ist nicht geplant, ein gemeinsames „Globalgesetz" anzunehmen, das für alle unabhängigen Behörden gilt. Für jede Behörde wird ein separates Gesetz angenommen. Dies ist deshalb gerechtfertigt, weil die Behörden, die aus dem Zuständigkeitsbereich des Kabinetts ausgegliedert werden sollen, sehr

unterschiedlich sind und somit ein separates und spezifisches Gesetz erforderlich wird, das der jeweiligen Situation gerecht wird. Der Gesetzgeber ist weder berechtigt, einer Behörde eine „geringere Unabhängigkeit" als das Ausmaß an eigenverantwortlicher Verwaltung einzuräumen, das für eine angemessene Erfüllung ihrer Aufgaben in dem jeweiligen staatlichen Verwaltungsbereich notwendig ist, noch darf er „unnötige Kompetenzen" an eine Behörde in Bereichen abtreten, in denen dies nicht erforderlich ist (was bedeutet, dass die Behörde ihre Aufgaben bei untergeordneter Stellung gegenüber dem Kabinett erfüllen kann) oder in denen die Behörde keine angemessene Verwaltung gewährleisten würde.

Hierbei regelt ein separates Gesetz den rechtlichen Status der Behörde, ihre Anbindung an eine Kontrollbehörde, das Verfahren ihrer Einrichtung, ihre Aufgaben und Finanzierung, und sonstige Fragen. § 58 der Verfassung weist außerdem auf eine Reihe spezifischer Maßnahmen hin:

1) Unabhängigkeitsgarantien für die leitenden Beamten der Behörden
2) Ex-ante- und Ex-post-Kontrollen der angenommenen Durchführungsgesetze und anderer Verwaltungsakte, um ihre Rechtmäßigkeit und Nützlichkeit zu gewährleisten
3) die Genehmigung, eigene externe behördliche Regelungen zu veröffentlichen

Am 23. Februar wurde der Gesetzentwurf über die Änderungen der Satversme der Republik Lettland dem Ministerkabinett vorgelegt. Im Anschluss an die Annahme des Gesetzes über die Änderungen der Satversme der Republik Lettland durch das Parlament wird das Justizministerium die Vorbereitung anderer notwendiger Durchführungsgesetze koordinieren. Darüber hinaus werden die Gesetzentwürfe „Änderungen des Verwaltungsverfahrensrechts" und „Änderungen des Gesetzes über das Verfahren der Ankündigung, Veröffentlichung, Inkraftsetzung und Gültigkeit von Gesetzen und anderen Rechtsakten, die vom Saeima, dem Präsidenten und dem Ministerkabinett angenommen wurden", vorbereitet.

Änderungen des Strafrechts

Gegenwärtig gilt die Verwaltungshaftung für Übertretungen, die die Verarbeitung personenbezogener Daten betreffen – Verwarnungen, Geldbußen, vorübergehende Stilllegung von Systemen zur Verarbeitung personenbezogener Daten und Beschlagnahme der eingesetzten technischen Mittel.

Zur Erleichterung des Schutzes der Verarbeitung von personenbezogenen Daten und zur Verhinderung einer rechtswidrigen Verarbeitung dieser Daten wurden im Jahr 2005 die Arbeiten zur Begründung einer strafrechtlichen Haftung für Übertretungen bei der Verarbeitung von personenbezogenen Daten aufgenommen. Der Gesetzentwurf wird dem Ministerkabinett in der ersten Hälfte des Jahres 2006 vorgelegt. Er sieht eine strafrechtliche Haftung für die illegale Verarbeitung personenbezogener Daten in folgenden Fällen vor: wenn sie mehrmals innerhalb eines Jahres ausgeführt wurde oder auch wenn sie von einer Gruppe von Personen auf Grundlage einer vorausgehenden Vereinbarung ausgeführt wurde, sowie für entsprechende Aktivitäten, insofern diese darauf abzielten, sich an einer Person zu rächen, sie zu erpressen, oder aus anderen Gründen vorgenommen wurden oder falls diese Aktivitäten mit Gewalt, Betrug oder Drohungen verbunden waren; bei Nichtverwendung der erforderlichen technischen und organisatorischen Mittel, um personenbezogene Daten zu schützen und ihre rechtswidrige Verarbeitung zu verhindern, wodurch erheblicher Schaden verursacht wurde und bei der illegalen Verarbeitung personenbezogener Daten, wenn sie einen erheblichen Schaden verursacht.

Änderungen des Gesetzes über elektronische Kommunikationen

Dieses Gesetz wurde am 12. Mai 2005 vom Parlament angenommen. Es enthält die Anforderungen der Richtlinie 2002/58/EG, beispielsweise im Hinblick auf die Verarbeitung von Verkehrsdaten, Ortungsdaten und öffentlich zugängliche Teilnehmerverzeichnisse.

Änderungen des Gesetzes über die Dienstleistungen in der Informationsgesellschaft

Dieses Gesetz wurde am 10. November 2005 vom Parlament angenommen. Es fasst im Rahmen der Umsetzung von Artikel 13 der Richtlinie 2002/58/EG die Rechtsnormen für ein Verbot der Verschickung kommerzieller Nachrichten zusammen und nennt die im Zusammenhang mit der Verbreitung von Diensten der Informationsgesellschaft zuständigen Kontrollbehörden, unter anderem die staatliche Datenkontrollbehörde, die im Rahmen ihrer Zuständigkeiten für seine Durchführung verantwortlich ist.

B. Bedeutende Rechtsprechung

Die Beschwerden, die bei der staatlichen Datenkontrollbehörde eingegangen sind und die von ihr durchgeführten Untersuchungen machen deutlich, dass die Mehrheit der Gesetzesübertetungen im Jahr 2005 darauf zurückzuführen waren, dass personenbezogene Daten ohne jede Rechtsgrundlage verarbeitet wurden.

Typische Übertretungen im Rahmen der Verarbeitung personenbezogener Daten umfassten folgende Fälle:

1) die Verarbeitung unrichtiger und oft eindeutig falscher personenbezogener Daten bei der Erhebung von Kreditdaten und Daten über Zahlungsaußenstände (schwarze Listen)
2) keine Informierung der Datensubjekte und Verweigerung der Aushändigung von Informationen an die Datensujekte (insbesondere auf Ebene der Gesundheitsdienste)
3) unverhältnismäßige Verarbeitung von personenbezogenen Daten, bei der der ursprünglich vorgesehene Rahmen der Datenverarbeitung überschritten und ausgeweitet wird

C. Wichtige spezifische Themen

Zugänglichkeit von Gerichtsentscheidungen

Die Zugänglichkeit von Gerichtsentscheidungen wurde in Lettland ausführlich im Zusammenhang mit dem Aufbau der Datenbank gemeinsamer Gerichtsurteile (und dem Portal www.tiesas.lv) sowie der Datenverfügbarkeit im Internet diskutiert.

Informationsfreiheit und Datenschutz

Verfügbarkeit von Daten zu Erklärungen von Beamten im Internet. Veröffentlichung des Einkommens und von Prämien, die Beamte erhalten haben. Veröffentlichung von Daten über Empfänger von Fördermitteln für den ländlichen Raum. Veröffentlichung von Namen von Verkehrssündern.

Forschung am menschlichen Genom

Da gegenwärtig eine Forschungsdatenbank über das menschliche Genom in Lettland eingerichtet wird, die Daten zu wissenschaftlichen Zwecken verarbeiten soll, führte die Datenkontrollbehörde eine Inspektion der Genomdatenbank des biomedizinischen Forschungs- und Studienzentrums der Universität von Lettland durch. Diese Überprüfung und die Erklärung der staatlichen Kontrollbehörde sind eine Vorbedingung, um in Lettland Arbeiten am menschlichen Genom durchführen zu dürfen.

Schutz von Patientenrechten im Zusammenhang mit der Wahrung der Rechte von Datensubjekten

Das Gesetz über den Schutz der Patientenrechte wurde ausgearbeitet; es enthält eine Reihe von Bestimmungen, die die Rechte der Datensubjekte im Bereich der Medizin präzisieren.

Datenschutz im Rahmen von Arbeitsverhältnissen

Die staatliche Datenkontrollbehörde bereitete Empfehlungen über den Schutz personenbezogener Daten bei Arbeitsverhältnissen vor. Das Handbuch richtet sich sowohl an Arbeitgeber als auch Arbeitnehmer und es erklärt, welche personenbezogenen Daten von Arbeitgebern verarbeitet werden dürfen und ob sie ihre Beschäftigten über die Datenverarbeitung informieren müssen.

Litauen

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

1. Das Gesetz über elektronische Kommunikationen der Republik Litauen beauftragt die staatliche Kontrollbehörde, die Kontrolle über Unternehmen auszuüben, die elektronische Kommunikationsnetze und/oder -dienste anbieten, im Zusammenhang mit ihrer Erfüllung der Anforderungen von Paragraph 1 von Artikel 63 des oben genannten Gesetzes bezüglich der Vertraulichkeit von Kommunikationen. Unternehmen, die elektronische Kommunikationsnetze und/oder -dienste anbieten, sind entsprechend der Bestimmungen von Paragraph 2 des oben genannten Gesetzes verpflichtet, der staatlichen Datenkontrollbehörde die Durchführung von Kontrollen in Übereinstimmung mit den von der Regierung hierfür festgelegten Verfahren zu ermöglichen. Auf dieser Grundlage verabschiedete die Regierung von Litauen am 20. Juli 2005 die Entschließung Nr. 807, in der die Regeln für die Durchführung von Überprüfungen der Vertraulichkeit von Kommunikationen festgelegt wurden. Diese Entschließung legt fest, welche Überprüfungsverfahren von der staatlichen Datenkontrollbehörde in Übereinstimmung mit den Anforderungen in Paragraph 1 von Artikel 63 durchgeführt werden sollen, der sich mit der Vertraulichkeit von Kommunikationen und der Vorlage von Inspektionsergebnissen befasst.

2. Auf Grundlage des Gesetzes über elektronische Kommunikationen bereitete die staatliche Kontrollbehörde die Anforderungen für detaillierte Rechnungen vor, die durch die Entscheidung Nr. 1T-95 vom 5. Juli 2005 des Direktors der staatlichen Datenkontrollbehörde angenommen wurden. Die Entscheidung verwies auf die Anforderungen bei der Festlegung der Inhalte von detaillierten Rechnungen, die von den Betreibern öffentlich zugänglicher Kommunikationsdienste ausgestellt werden, und deren Formen für Teilnehmern an diesen Dienste.

3. Am 7. Dezember 2005 verabschiedete die Regierung die Entschließung Nr. 1317 „über die Änderung der Entschließung Nr. 262 der Republik Litauen vom 20. Februar 2002" „über die Neuorganisation des staatlichen Verzeichnisses von für die Verarbeitung personenbezogener Daten Verantwortlichen, die Annahme dieses Verzeichnisses betreffenden Bestimmungen und des Notifizierungsverfahrens, das von für die Datenverarbeitung Verantwortliche bei der Verarbeitung von personenbezogenen Daten befolgen müssen". Diese Entschließung führt ein vereinfachtes Notifizierungsverfahren für die Verarbeitung von personenbezogenen Daten ein und nimmt auf das Verfahren der Durchführung von Vorabkontrollen Bezug, das im Gesetz über den Schutz personenbezogener Daten verankert ist, sowie auf das Verfahren für die Registrierung von für die Datenverarbeitung Verantwortlichen.

B. Bedeutende Rechtsprechung

Die staatliche Datenkontrollbehörde führte eine Überprüfung in einer Einrichtung durch, die ein feststehendes System für die Messung von Geschwindigkeiten und die Registrierung von Geschwindigkeitsübertretungen verwendete (TraffiPhot), um die Effizienz des Systems unter Betriebsbedingungen zu testen. Bei Auslösung fotografierte das System Fahrer, die die Geschwindigkeitsbegrenzung nicht beachteten oder bei Rot über die Kreuzung fuhren. Diese Daten wurden automatisch an den litauischen Verkehrsüberwachungsdienst weitergeleitet. Anschließend war es möglich, die Fahrer anhand einer Video-Datenbank mit Verkehrsteilnehmern zu identifizieren. Danach wurden diese Fotos im Fernsehen veröffentlicht. Die staatliche Datenkontrollbehörde stellte fest, dass insofern eine Ordnungswidrigkeit stattgefunden hat, als die Verkehrsüberwachungseinrichtung ohne vorherige Notifizierung der staatlichen Kontrollbehörde personenbezogene Daten mit automatisierten

Mitteln verarbeitet und die Datensubjekte nicht über die Verarbeitung ihrer personenbezogenen Daten informiert hatte. In seiner Entscheidung erklärte das Gericht, dass die mit Kameras und Video-Überwachung aufgezeichneten Informationen, die eine Identifizierung der Person ermöglichen, als personenbezogene Daten betrachtet würden. Deshalb würden die Bestimmungen des Gesetzes über den Schutz personenbezogener Daten auch für die Verarbeitung dieser Video-Aufzeichnungen gelten. Das Gericht verhängte kein Bußgeld gegen den Direktor der Verkehrsüberwachungsdienst, da diese Einrichtung legal Daten erhoben hätte, um sie in das TraffiPhot-System einzugeben. Das Gericht wies in seiner Entscheidung darauf hin, dass das Verhalten der Verkehrsteilnehmer in Litauen gegenwärtig zu wünschen übrig ließe. Aufgrund einer Verletzung geltender Verkehrsregeln träten viele Unfälle auf, die wiederum viele Tote und Verletzte mit sich brächten. Deshalb sei es notwendig, Maßnahmen zu ergreifen, um die Verkehrsteilnehmer zu disziplinieren, da dies einerseits einen Beitrag dazu leisten könnte, Übertretungen der Verkehrsregeln zu vermeiden, und andererseits einen Beitrag zu einer zügigen Untersuchung von Verkehrsunfällen leisten würde. Technische Maßnahmen wie das TraffiPhot-System sollten eingerichtet werden, um diese Ziele zu erreichen. Im Hinblick auf die Überprüfung des TraffiPhot-Systems wurde festgestellt, dass die Verkehrssünder aufgezeichnet werden, wenn sie eine Verletzung der Straßenverkehrsordnung begehen, die schwerwiegende Folgen haben könnte, was bedeutet, dass die Übertretung im Datenschutzbereich unter dem Verhältnismäßigkeitsgrundsatz nicht so schwer wiegt wie die folgenschwere Verkehrsübertretung, die vom TraffiPhot-System festgehalten wurde.

C. Wichtige spezifische Themen

Probleme, die sich aus der Verarbeitung von personenbezogenen Daten für geschichtliche Zwecke ergeben

Da am 1. Januar das Gesetz über Dokumente und Archive verabschiedet wurde, stellte sich für Personen, die historische Nachforschungen anstellen, das Problem des Zugangs zu Dokumenten. Aufgrund des Gesetzes über Dokumente und Archive wird der Zugang zu Dokumenten des nationalen Dokumentenfonds, der Informationen aus dem Privatleben von Personen enthält, sowie zu strukturierten Zusammenstellungen personenbezogener Daten, die in staatliche Archive übertragen werden, für einen Zeitraum von 50 Jahren nach dem Tod einer Person und, falls der Tod nicht nachgewiesen werden kann, für einen Zeitraum von 100 Jahren nach dem Erstellungsdatum der jeweiligen Dokumente beschränkt. Daraus ergaben sich einige Schwierigkeiten hinsichtlich der Frage, wie geschichtliche Nachforschungen beurteilt werden sollen, da das Gesetz über den Schutz personenbezogener Daten keine spezifischen Bestimmungen hinsichtlich der Durchführung historischer Nachforschungen enthält, obwohl es sich in seinen Verfügungen mit der Durchführung wissenschaftlicher Forschungen befasst.

Den Bestimmungen des Gesetzes zum Schutz personenbezogener Daten zufolge dürfen personenbezogene Daten verarbeitet werden, wenn die Personen, die die wissenschaftliche Forschung durchführen, die Zustimmung des Datensubjekts erhalten haben. Ohne Zustimmung des Datensubjekts dürfen personenbezogene Daten zum Zwecke wissenschaftlicher Forschung nur dann verarbeitet werden, wenn die staatliche Datenkontrollbehörde zuvor angemessen notifiziert wurde und eine vorherige Kontrolle durchgeführt hat. Um die sich hierbei ergebenden Probleme zu lösen, wurde eine Reihe von Sitzungen mit Vertretern des Ministeriums für Archive und verschiedenen Historikern durchgeführt. Als Ergebnis dieser Sitzungen bereitete die staatliche Datenkontrollbehörde eine Empfehlung über die Verarbeitung von personenbezogenen Daten zu Zwecken der geschichtlichen Forschung vor. Das Ziel dieser Empfehlung besteht darin, die Grundsätze darüber darzulegen, wie personenbezogene Daten im Rahmen der geschichtlichen Forschung verarbeitet werden können, um das Recht des Datensubjekts auf eine Privatsphäre nicht zu verletzen und eine sichere und rechtmäßige Verarbeitung personen-

bezogener Daten zu gewährleisten. Darüber hinaus bereitete die staatliche Datenkontrollbehörde eine Empfehlung zur Verwendung des Vorabnotifizierungsformulars zum Zwecke einer Vorabprüfung für den Fall einer Verarbeitung personenbezogener Daten aus geschichtlichen Gründen vor.

Die Sicherheit der Daten bei der Verschickung von Rechnungen für Dienstleistungen

Ein in Litauen eingetragener Lobbyist wendete sich mit dem Hinweis an die staatliche Datenkontrollbehörde, dass ein öffentliches Versorgungsunternehmen Notifizierungen über gegenüber Kunden erbrachte Dienstleistungen verschickt hätte, die Informationen im ungekürzten Wortlaut über erbrachte Leistungen enthielten. Daraufhin sprach die staatliche Datenkontrollbehörde, um den Datenverarbeitern die Überwachung der Einhaltung der gesetzlichen Bestimmungen zu erleichtern, die Empfehlung aus, personenbezogene Daten bei der Verschickung von Rechnungen für erbrachte Dienstleistungen zu schützen. In der Empfehlung wird erklärt, dass Rechnungen für Dienstleistungen nicht öffentlich gemacht werden dürfen (indem sie beispielsweise ausgehängt werden); außerdem müssen die für die Datenverarbeitung Verantwortlichen dafür sorgen, dass die Rechnungen in verschlossenen Umschlägen verschickt werden.

Fälle der Verwendung der persönlichen Identifikationsnummer

Die persönliche Identifikationsnummer (PIN) ist eine spezifische Reihe von Zahlen, die für die Identifikation einer Person vergeben wird; mit ihrer Hilfe können Daten über die betreffende Person erhoben werden und sie ermöglicht die Gewährleistung der Interaktionen zwischen den staatlichen Verzeichnissen und Informationssystemen. Die einer Person zugewiesene PIN-Nummer kennzeichnet diese Person individuell und kann nicht gefälscht werden. Oft holen für die Datenverarbeitung Verantwortliche PIN-Nummern von Datensubjekten ein – nicht zu Identifikationszwecken, sondern, um diese Daten aufzubewahren, obwohl sie anschließend nicht für andere Zwecke verwendet werden. Die Datenkontrollbehörde erhält beispielsweise mehr und mehr Beschwerden von Personen, die von Geschäften zur Abgabe ihrer PIN-Nummer gezwungen werden, wenn sie Waren umtauschen oder Waren schlechter Qualität zurückgeben möchten. Nach einer Überprüfung der Beschwerden stellte die staatliche Datenkontrollbehörde fest, dass die für die Datenverarbeitung Verantwortlichen zu viele personenbezogene Daten in Form von PIN-Nummern verarbeitet hätten, weil diese Informationen nicht für die Zwecke erforderlich seien, zu denen sie erhoben wurden, und nicht für andere Zwecke verwendet würden.

Nachdem die staatliche Datenkontrollbehörde Überprüfungen bezüglich der Verarbeitung von PIN-Nummern zu Zwecken der Direktwerbung durchgeführt hatte, teilte sie den für die Datenverarbeitung Verantwortlichen wie Kreditvereinigungen und Banken mit, dass sie die PIN-Nummern von Datensubjekten im Rahmen der Direktwerbung nicht mehr erfassen und weiterverarbeiten und auch für andere Verarbeitungszwecke keine PIN-Nummern mehr erfragen dürften.

Die Regierung lenkte die Aufmerksamkeit der staatlichen Datenkontrollbehörde auf in der Presse erschienene Informationen über anstehende öffentliche Versteigerungen. Die Behörde überprüfte diese im Internet verfügbaren Informationen und stellte fest, dass die Amtswalter im Rahmen ihrer Verkaufsankündigungen zu viele Daten über die Besitzer offenlegten (wie beispielsweise ihre persönliche Identifikationsnummer, Geburtsdatum, Adresse). Die Amtswalter wurden aufgefordert, diese übermäßige Offenlegung von persönlichen Daten über Eigentümer bei öffentlichen Versteigerungen in Zukunft zu unterlassen.

Staatliche Verzeichnisse und Verzeichnisse der Ministerien

Im Jahr 2005 führte die staatliche Kontrollbehörde Kontrollen auf Ebene staatlicher Einrichtungen durch, die über staatliche Verzeichnisse oder Verzeichnisse der Ministerien mit personenbezogenen Daten verfügten, um festzustellen, welche Informationen den Verzeichnissen entnommen wurden, wem gegenüber sie offengelegt wurden und ob die Vereinbarungen zur Offenlegung der Daten rechtmäßig geschlossen wurden. Nach einer Überprüfung der meisten dieser Verzeichnisse konnten keine Übertretungen des Gesetzes zum Schutz personenbezogener Daten festgestellt werden. In zwei Fällen wurden die Institutionen jedoch aufgefordert, auf die Einhaltung der Bestimmungen des oben genannten Gesetzes zu achten.

Konferenz „Elektronischer Handel und Datenschutz"

Angesichts der Entwicklung der Informationsgesellschaft in Litauen gewinnt der Schutz personenbezogener Daten eine wachsende Bedeutung. Das Internet und die damit verbundenen Chancen betreffen mehr und mehr Bereiche des öffentlichen Lebens und führen dazu, dass der Anwendungsbereich für im Internet zu erfassende und zu verarbeitende personenbezogene Daten ständig wächst. Im elektronischen Raum ist man in der Regel besonders sichtbar, womit persönliche Daten leichter missbraucht werden können.

Durch die schnelle Entwicklung der Informationstechnologien ergeben sich spezifische Probleme: Wie kann erreicht werden, günstige Bedingungen für die Entwicklung des elektronischen Handels zu schaffen und gleichzeitig das Recht auf den Schutz der Privatsphäre zu gewährleisten? Auf der Konferenz „Elektronischer Handel und Datenschutz", die vom 14. bis 15. November in Wilna stattfand, wurden Wege und Mittel in Betracht gezogen, um eine solche Kompatibilität zu erreichen, das öffentliche Vertrauen in die Datenverarbeiter zu stärken, sichere Räume im Internet zu schaffen und die Gefahren in Angriff zu nehmen, auf die die Konferenz hingewiesen hatte. Andere, im Rahmen der Konferenz angesprochene Themen befassten sich mit elektronischem Handel und der Politik zur Sicherung einer Privatsphäre; Direktvertrieb und Datenschutz; der Organisation des Datenschutzes innerhalb der Unternehmen; guten Praktiken bei der Verarbeitung von Daten auf Ebene internationaler Unternehmen; Identifikation im Internet; der Bekämpfung von Spam; Cyberkriminalität und E-Banking und Betrug.

PHARE-Projekt

Vom 29. März 2004 bis Ende Juni 2005 führte die staatliche Datenkontrollbehörde gemeinsam mit dem Ludwig-Boltzman-Institut für Menschenrechte (Österreich) das PHARE-Twinningprojekt LT02/IB-JH-02/03 mit dem Thema „Stärkung der Verwaltungskapazitäten und technischen Kapazitäten für den Schutz personenbezogener Daten" durch.

Am 30. Juni 2005 wurde das PHARE-Projekt abgeschlossen. Im Rahmen dieses Projektes beteiligten sich Spezialisten der staatlichen Datenschutzbehörde an Ausbildungsmaßnahmen auf Ebene des Unabhängigen Zentrums für Datenschutz Schleswig-Holstein, des Amts des Datenschutzbeauftragten in Bonn in Deutschland und des Büros der Datenschutzkommission in Wien, Österreich. Im Rahmen dieser Ausbildungsmaßnahmen wurden die Experten der staatlichen Datenschutzbehörde über die Verfahren erprobter Kontrollformen unterrichtet sowie über den Umgang mit Beschwerden; darüber hinaus hatten sie Gelegenheit, an Kontrollen vor Ort teilzunehmen. Schließlich kann darauf hingewiesen werden, dass im Rahmen des Twinning-Projekts des PHARE-Programms ein Kommentar zum Gesetz über den gesetzlichen Schutz personenbezogener Daten in der Republik Litauen vorbereitet wurde. Dieser Kommentar kann dabei sehr hilfreich sein, dass Datensubjekte, für die Datenverarbeitung Verantwortliche, staatliche und kommunale Einrichtungen und Unternehmen die Bestimmungen des Gesetzes leichter verstehen (er könnte beispielsweise Richtern besonders behilflich sein, wenn sie versuchen, die Bestimmungen des Gesetzes über den gesetzlichen Schutz personenbezogener Daten der Republik Litauen fair zu interpretieren und anzuwenden), und er kann privaten Einrichtungen (Unternehmen) helfen.

Luxemburg

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Gesetz vom 2. August 2002 über den Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten

Die nationale Datenschutzkommission *(Commission nationale pour la protection des données – CNPD)* hat die Regierung im Hinblick auf die geplante Änderung gewisser Bestimmungen des Datenschutz-Rahmengesetzes beraten (Gesetzentwurf Nr. 5554 vom 16. März 2006), insbesondere im Hinblick auf die Vereinfachung der formalen Anforderungen, die für den Schutz der Freiheiten und Grundrechte der Bürger nicht als wesentlich betrachtet werden. Darüber hinaus wurden einige weniger entscheidende Punkte präzisiert und der Anwendungsbereich des Gesetzes auf natürliche Personen beschränkt.

Nach seiner Annahme durch das Parlament im Jahr 2007 wird das künftige, geänderte Gesetz umfassendere Ausnahmen von der Notifizierungsverpflichtung vorsehen, und einige Formen der Datenverarbeitung werden nicht länger von einer Vorabüberprüfung (Genehmigung durch die CNPD) abhängen.

Gesetz vom 30. Mai über die spezifischen Bestimmungen zum Schutz der Privatsphäre im Bereich der elektronischen Kommunikationen (Umsetzung der Richtlinie 2002/58/EG)

Dieses Gesetz wurde am 30. Mai 2005 vom Parlament angenommen und trat am 1. Juli 2005 in Kraft.

Im Anschluss an eine Empfehlung der *Commission nationale pour la protection des données* beabsichtigt die Regierung, die Dauer der obligatorischen Aufbewahrung der Daten und die für Verkehrsdaten elektronischer Kommunikationsdienste geltenden Aufbewahrungszeiten von zwölf Monaten auf sechs Monate zu reduzieren.

Gesetz vom 8. Juni 2004 über die Freiheit der Meinungsäußerung in den Medien

Das oben genannte Gesetz vom 16. März 2006 wird ebenfalls die Formulierung des Gesetzes vom 8. Juni 2004 bezüglich der Wahrung der Pressefreiheit und der Haftung und Verpflichtungen von Herausgebern und Journalisten hinsichtlich der geänderten Bestimmungen des Datenschutzgesetzes des Jahres 2002 übernehmen, da der Presserat und die repräsentativen Verbände der Journalisten und Herausgeber die Datenschutzbestimmungen in ihren Verhaltenskodex aufnehmen müssen. Anschließend muss die Durchführung dieser Bestimmungen laufend durch den Ausschuss für Pressebeschwerden als einem Selbstregulierungsorgan des Presse- und Mediensektors überwacht werden.

Erlässe und untergeordnete Gesetze

In Übereinstimmung mit dem Datenschutzgesetz wurde (am 30. September 2005) eine Verordnung angenommen, in der festgelegt wird, welche natürlichen oder juristischen Personen berechtigt sind, gesundheitsbezogene Daten zu Zwecken der Präventivmedizin, medizinischer Diagnosen, der Bereitstellung von Pflege oder Behandlungen oder der Verwaltung von Gesundheitsdiensten oder wissenschaftlicher Forschung in den Bereichen der Biologie und der Medizin zu verarbeiten.

Andere Entwicklungen in der Gesetzgebung

Im April 2005 holte die Regierung eine Stellungnahme der CNPD bezüglich eines Gesetzentwurfs ein, der den Zugang von Justiz-

und Polizeibehörden zu personenbezogenen Daten regelt, die von staatlichen Verwaltungen und öffentlichen Behörden verarbeitet werden.

Die CNPD forderte die Regierung auf, eine restriktivere Haltung anzunehmen und die Rechte der betroffenen Personen besser zu schützen.

Die CNPD brachte darüber hinaus ihre Haltung zu einem Verordnungsvorschlag über ein automatisiertes System zur Kontrolle von Reisenden in Hotels und anderen Unterkünften zum Ausdruck und gab einige Hinweise dazu, wie dieser Entwurf verbessert werden könnte.

Am 15. November 2005 wurde dem Parlament ein Gesetzentwurf für die Annahme des Vertrags von Prüm vorgelegt, der am 27. Mai 2005 von den Mitgliedstaaten unterzeichnet wurde und die grenzübergreifende Polizeizusammenarbeit fördert, insbesondere den Kampf gegen Terrorismus, grenzübergreifende Kriminalität und illegale Einwanderung. Er ändert darüber hinaus das Gesetz vom 21. Dezember 2004, mit dem der am 8. Juni 2004 in Luxemburg unterzeichnete Vertrag über grenzüberschreitende Polizeieinsätze angenommen wurde.

B. Bedeutende Rechtsprechung

Zivilrechtliche und strafrechtliche Rechtsprechung

Nach wie vor wurden sowohl im zivilrechtlichen als auch im strafrechtlichen Bereich keine wesentlichen Gerichtsentscheidungen im Zusammenhang mit allgemeinen Fragen des Datenschutzes gefällt. Da jedoch Entscheidungen der Datenschutzbehörde bezüglich der Genehmigung einer Datenverarbeitung auf Grundlage einer vorherigen Überprüfung vor den Verwaltungsgerichten angefochten werden können, wurden dennoch einige fallrechtliche Entscheidungen in diesem Bereich getroffen.

Verwaltungsrechtliche Entscheidungen

Am 23. Februar 2005 verwarf das Verwaltungsgericht von Luxemburg eine Entscheidung der *Commission nationale*, die den Zeitraum, während dessen ein Juweliergeschäft mit Genehmigung der CNPD Videoaufzeichnungen seines unter Videoüberwachung stehenden Juweliergeschäfts aufbewahren darf, auf zwei Wochen beschränkt hatte. Das Gericht vertrat die Auffassung, dass dieser Zeitraum zu kurz sei, insbesondere um eine angemessene Untersuchung durch die Polizei zu ermöglichen, wenn beispielsweise die Vorbereitungsphase eines später erfolgten Überfalls untersucht werden soll.

Am 9. Mai 2005 verwarf das Verwaltungsgericht eine Entscheidung der *Commission nationale*, in der erklärt wurde, dass öffentliche Verwaltungen im Sinne von Artikel 11 nicht als „Unternehmen" betrachtet werden können. Das Gesetz beschränkt die Zwecke, zu denen eine Überwachung der Arbeitnehmer durch den Arbeitgeber erfolgen kann, auf die Fälle, die im Gesetz genannt werden, darunter die Fälle, die Artikel 11, Paragraph (1), b) anführt, in denen der Schutz von Gütern und Eigentum des Unternehmens im Vordergrund steht. Dies bedeutet, dass auch Verwaltungen eine Überwachung am Arbeitsplatz vornehmen können, um ihr Eigentum zu schützen.

Am 12. Juli 2005 bestätigte die Berufungsinstanz des Verwaltungsgerichts ein Urteil des Verwaltungsgerichts vom 15. Dezember 2004, das den Antrag auf Löschung einer Entscheidung der *Commission nationale* abgelehnt hatte, in der die Videoüberwachung eines Schuhgeschäfts verboten worden war.

Am 8. November 2005 bestätigte die Berufungsinstanz des Verwaltungsgerichts die oben genannte Entscheidung des Verwaltungsgerichts der ersten Instanz vom 23. Februar 2005.

C. Wichtige spezifische Themen

Die *Commission nationale pour la protection des données* veröffentlichte ihre erste Entscheidung in einem Fall, der sich mit der Biometrik befasste. Die CNPD weigerte sich, die Verwendung eines biometrischen Systems für die Zugangskontrolle in einem Wellness- und Fitness-Center zu genehmigen. Sie begründete ihre Entscheidung damit, dass die von dem Betreiber vorgenommene Speicherung biometrischer Daten in einer zentralen Datenbank im Hinblick auf den verfolgten Zweck der Zugangskontrolle eingetragener Besucher eines Wellness- und Fitness-Centers unverhältnismäßig sei.

In einem anderen Fall gewährte die *Commission nationale* keine Genehmigung für die Mitteilung personenbezogener Daten der nationalen Sozialversicherungsverwaltung an eine Einrichtung, die öffentliche Meinungsumfragen durchführt und die diese Daten verwenden wollte, um eine Gruppe von Personen auszuwählen, die als repräsentative Gruppe der Bevölkerung befragt werden kann. In dem vorliegenden Fall wurde allem Anschein nach der wissenschaftliche Hintergrund der Befragung nicht mitgeteilt, dessen Erläuterung notwendig gewesen wäre, um die Anwendung von Artikel 6, § (1), Buchstabe b, zweiter Satz, zu rechtfertigen, der eine Weiterverarbeitung zulässt, wenn sie aus wissenschaftlichen, statistischen oder geschichtlichen Gründen notwendig ist.

Die *Commission nationale* hat sich gemeinsam mit den zuständigen öffentlichen Behörden an den Vorbereitungsarbeiten (bezüglich sowohl technischer als auch praktischer Aspekte) im Hinblick auf die bevorstehende Einführung des biometrischen Passes in Luxemburg beteiligt (die für August 2006 geplant ist).

Darüber hinaus führte die *Commission nationale* mit den zuständigen Regierungsstellen Diskussionen durch und arbeitete mit ihnen im Rahmen der gegenwärtigen Vorbereitung von Aktionsplänen über E-Gesundheit und E-Commerce sowie eines Berichts über eine Strategie zur Vereinfachung von Verwaltungsverfahren und zur Erleichterung der Auflagen, die für private Unternehmen gelten, zusammen. In den beiden kommenden Jahren werden sich die Aktivitäten der *Commission nationale* weitgehend auf diese Fragen konzentrieren.

Eine ganze Reihe von Experten haben Anträge eingereicht, in denen die CNPD aufgefordert wird, die von für die Darenverarbeitung Verantwortlichen vorgenommene Ernennung dieser Experten als Datenschutzbeauftragte anzuerkennen. Die *Commission nationale* teilte ihnen nützliche Hinweise mit und bot ihnen Ausbildungsmaßnahmen in Form von Workshops an.

Die *Commission nationale* setzte ihre Informations- und Bewusstseinsbildungskampagne fort, indem sie gemeinsam mit einer Verbraucherschutzvereinigung einen Kalender veröffentlichte.

Eine mit Unterstützung der Informations- und Presseabteilung der Regierung bereits im Jahr 2004 auf Deutsch, Französisch und Englisch herausgegebene Broschüre wurde im Jahr 2005 auch auf Portugiesisch veröffentlicht.

Die Website der Datenschutzbehörde wurde mit Erfolg neu eingerichtet und bietet jetzt ein verbessertes Layout und zusätzliche Inhalte (Unterlagen). Ein bekanntes Wirtschafts- und Finanzmagazin hat sie sogar als „Website des Monats" ausgezeichnet.

Von der Polizei in öffentlichen Bereichen durchgeführte Video-Überwachungen und die Verwendung von genetischen Daten für die Identifikation von Personen auf dem Gebiet der Verbrechensbekämpfung und in strafrechtlichen Verfahren waren die Hauptthemen, die im vergangenen Jahr von der Presse kommentiert wurden.

Malta

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Die Datenschutzrichtlinie 95/46/EG der EU wurde im Rahmen von Kapitel 440 durch das Gesetz XXVI von 2001, geändert durch das Gesetz XXXI aus dem Jahr 2002 und das Gesetz IX aus dem Jahr 2003, in maltesisches Recht umgesetzt. Das Datenschutzgesetz wurde im Juli 2003 in allen seinen Teilen in Kraft gesetzt, wobei im Juli 2004 die Notifizierungsverpflichtung eingeführt wurde. Einige Bestimmungen hinsichtlich manueller Systeme der Datenverwaltung treten im Oktober 2007 in Kraft.

Die Richtlinie 2002/58/EG bezüglich der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre im Bereich elektronischer Kommunikationen wurde durch die gesetzliche Mitteilung (Legal Notice - L.N.) 16 aus dem Jahr 2003 und L.N. 19, ebenfalls aus dem Jahr 2003, umgesetzt, die beide im Juli 2003 in Kraft getreten sind.

Weitere Entwicklungen der Gesetzgebung:

Im Jahr 2005 wurde die L.N. 16 aus dem Jahr 2003 geändert, um den Anwendungsbereich der Bestimmungen, die unerbetene Mitteilungen betreffen, sowohl auf juristische als auch auf natürliche Personen auszudehnen.

B. Bedeutende Rechtsprechung

Es wurden keine Entscheidungen getroffen.

C. Wichtige spezifische Themen

Entwicklung von Leitlinien

Auf Grundlage von Artikel 40 des Datenschutzgesetzes setzt sich der Datenschutzbeauftragte regelmäßig mit Vertretern der unterschiedlichen Sektoren in Verbindung, um die sich aus dem Gesetz ergebenden Grundsätze zu diskutieren, entsprechende Vereinbarungen zu treffen und sie anschließend in Form von Leitlinien und Verhaltenskodizes zu formulieren.

➔ Bildung
Im Oktober wurden Datenschutzleitlinien für die Verarbeitung von Bildern in Schulen veröffentlicht.

Diese Leitlinien, deren Veröffentlichung der Auftakt zu einer Reihe weiterer geplanter Leitlinien war, wurden gemeinsam von dem Datenschutzbeauftragten und einem Komitee von Schulvertretern herausgegeben, das Vertreter staatlicher Schulen, unabhängiger Schulen, kirchlicher Schulen, der Bildungsbehörden und des Amtes des Premierministers umfasste. Die Leitlinien verfolgen den Zweck, gute Praktiken zu definieren, die in den Schulen umgesetzt werden sollen.

➔ Versicherungen
Eine Arbeitsgruppe, die sich aus Vertretern der Vereinigung der maltesischen Versicherer (Malta Insurance Association), der maltesischen Behörde für Finanzdienstleistungen (Malta Financial Services Authority) und des Amtes des Datenschutzbeauftragten zusammensetzt, kam regelmäßig zusammen, um innerhalb dieses Bereichs Datenschutzfragen zu besprechen.

Zu den diskutierten Themen zählten die Erholung der Einwilligung, die Informierungsverpflichtung, Zugangsrechte und die gemeinsame Nutzung von Informationen zur Verhinderung von Versicherungsbetrug. Zu jedem der Themen wurden beste Praktiken mit dem Ziel festgehalten, sie bei der Veröffentlichung von Leitlinien mit aufzunehmen.

Die Arbeitsgruppe wird in Zukunft weitere Sitzungen abhalten, um zusätzliche Themen, die

den Versicherungssektor betreffen, zu besprechen, wie beispielsweise die Erhebung und die Aufbewahrungszeiträume medizinischer Daten zu den Erbanlagen der Familienangehörigen der Antragsteller.

➔ Banken
In Zusammenarbeit mit der maltesischen Bankenvereinigung (Malta Bankers Association) wurden Leitlinien-Mitteilungen für eine interne Verwendung durch die Banken entwickelt. Die Inhalte dieser Leitlinien-Mitteilungen bilden anschließend die Grundlage für Leitlinien, die künftig vom Datenschutzbeauftragten veröffentlicht werden, und sich unmittelbar an die Datensubjekte richten.

➔ Sicherheit
Überwachungsmethoden, die die Erhebung und Verarbeitung personenbezogener Daten umfassen, sind ein weiterer Bereich, in dem Leitlinien durch das Amt veröffentlicht werden. Sitzungen mit Vertretern dieses Bereichs konzentrierten sich auf CCTV-Anlagen (Closed Circuit Television).

Twinning-light-Projekt (kürzere Partnerschaften)

Im Oktober 2005 wurde eine Twinning-light-Vereinbarung mit dem deutschen Bundesbeauftragten für Datenschutz unterzeichnet. Auf dieser Grundlage können sowohl dessen Behörde als auch die zentrale Direktion für Datenschutz der Behörde des Premierministers den Sachverstand der Experten nutzen, die im Rahmen von Kurzaufenthalten ihre Aufgaben in unterschiedlichen Bereichen wahrnehmen.

Das Hauptziel dieses Projekts besteht darin, den Datenschutzbeauftragten darin zu unterstützen, die Ressourcen und den Sachverstand zu stärken und zu konsolidieren, die erforderlich sind, um seine Aufgaben und Verpflichtungen bei der Verwaltung und Durchsetzung des Datenschutzgesetzes zu erfüllen.

Niederlande

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie andere Entwicklungen in der Gesetzgebung

Die Richtlinie 95/46/EG wurde durch ein Gesetz vom 6. Juli 2000[21] in nationales Recht umgesetzt und trat am 1. September 2001 in Kraft; sie löste dabei das alte Datenschutzgesetz, *Wet persoonsregistraties (Wpr),* vom 28. Dezember 1988 ab.

Die Richtlinie 2002/58/EG wurde im Wesentlichen durch das geänderte *Telecommunicatiewet* (Telekommunikationsgesetz), das am 19. Mai 2004[22] in Kraft getreten ist, in niederländisches Recht umgesetzt. Andere Gesetzgebungen, die Teile dieser Richtlinie übernommen haben, sind unter anderem das *Wet op de Economische Delicten* (Gesetz über Wirtschaftsvergehen), das den Artikel 13(4) der Richtlinie 2002/58/EG umsetzt.

Polizeidaten

Das *Wet Bijzondere Opsporingsbevoegdheden* (Gesetz über besondere Ermittlungsbefugnisse) für die Untersuchung und Verfolgung von Schwerverbrechen und organisierten Verbrechen trat am 1. Februar 2000 in Kraft. Im Rahmen dieses Gesetzes wird der Staatsanwaltschaft eine Reihe besonderer Ermittlungsbefugnisse einschließlich systematischer Beobachtungen, kriminaltechnischer Infiltrationsmaßnahmen und des Abhörens mit Telefonabhöranlagen eingeräumt. Ein wesentlicher Bestandteil der Gesetzgebung betrifft die Regelungen zur Überwachung dieser Ermittlungsbefugnisse. Einzelpersonen, gegen die diese besonderen Ermittlungsbefugnisse eingesetzt wurden, müssen aufgrund der gesetzlichen Vorschriften zu einem bestimmten Zeitpunkt hierüber informiert werden, es sei denn, sie sind sich im Anschluss an die Durchführung der strafrechtlichen Ermittlungen bereits dessen bewusst.

Am 13. Dezember 2004 richtete der Justizminister einen Evaluierungsbericht zum Gesetz über besondere Ermittlungsbefugnisse an das Parlament, in dem er darauf hinwies, dass die Verpflichtung zur Informierung (die als Notifizierungsverpflichtung bezeichnet wird) nur in sehr wenigen Fällen erfüllt wurde (siehe WODC-Bericht *Das Gesetz über besondere Ermittlungsbefugnisse: Abschlussbewertung 2004*, www.wodc.nl). Die hierfür genannten Gründe waren unter anderem, dass die Notifizierung erst dann erforderlich wird, wenn die Ermittlungen dies zulassen, die Tatsache, dass Notifizierungsversäumnisse nicht geahndet werden, und der Umstand, dass die Notifizierungsverpflichtung für die Staatsanwaltschaft keine Priorität darstellt. In seinem Begleitschreiben vom 13. Dezember 2004 kündigte der Justizminister Maßnahmen an, um für die Erfüllung dieser Verpflichtung zu sorgen.

Die besonderen Ermittlungsbefugnisse stellen eine schwere Verletzung der Privatsphäre von Einzelpersonen dar, da sie die heimliche Erfassung von Daten und die Einrichtung von Abhöranlagen in einem privaten Umfeld umfassen. Nachdem die besonderen Ermittlungsbefugnisse eingeführt wurden, betrachtete die Staatsanwaltschaft über Jahre hinweg eine der Garantien nicht als Priorität, die die Gesetzgeber offensichtlich als notwendig erachteten, um das Privatleben von Einzelpersonen und personenbezogene Daten zu schützen. Der niederländischen Datenschutzbehörde zufolge ergibt sich daraus ein alarmierendes Bild bezüglich der Missachtung von Garantien zum Schutz der Privatsphäre.

Am 17. Oktober 2005 wurde dem Parlament ein Gesetz über die Verarbeitung von Polizeiberichten vorgelegt. Dieses Gesetz führt zu einer grund-

[21] Gesetz vom 6. Juli 2000 über Regelungen zum Schutz personenbezogener Daten *(Wet bescherming persoonsgegevens)*, Amtsblatt der Gesetze, Gesetzesverordnungen und Erlässe 2000, 302. Eine nicht offizielle englische Übersetzung ist auf der Website der niederländischen Datenschutzbehörde verfügbar, www.dutchDPA.nl oder www.DutchDPAweb.nl

[22] Gesetz vom 19. Oktober 1998 bezüglich der im Telekommunikationsbereich geltenden Regelungen (Telekommunikationsgesetz), Amtsblatt der Gesetze, Gesetzesverordnungen und Erlässe 2004, 189.

legenden Überarbeitung der heutigen Fassung des Gesetzes über Polizeiregister *(Wet politieregisters)*. Wesentliche Aspekte der Stellungnahmen, die der niederländische Datenschutzbeauftragte zu einem Vorentwurf abgegeben hatte, wurden nicht berücksichtigt: Daten werden nicht mit einer Kennzeichnung versehen, die über ihre Zuverlässigkeit Auskunft gibt (der Unterschied zwischen harten und weichen Fakten) und Irrtumsrisiken anzeigt; gegen die Weitergabe von Daten an nur begrenzt zuverlässige Dritte werden unzureichende Garantien gewährt, und es werden keine zusätzlichen Garantien für Daten unverdächtiger Personen gegeben oder gegen eine übermäßige Erfassung von Daten unverdächtiger Personen.

Die Terrorismusbekämpfung und Geheimdienstaktivitäten

Das Gesetz über besondere Ermittlungsbefugnisse zur Terrorismusbekämpfung *(Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven)* wurde am 17. Juni 2005 vorgelegt. Im Rahmen dieses Gesetzes sind Polizei- und Justizbehörden berechtigt, Telekommunikationen abzuhören und vertrauliche Mitteilungen mit Telefonabhöranlagen aufzuzeichnen, systematische Beobachtungen vorzunehmen, und Infiltrationsmaßnahmen zu ergreifen, wenn Hinweise auf terroristische Aktivitäten vorliegen. Darüber hinaus bietet es die Möglichkeit, die Prüfung von Dokumenten in Gerichtsverfahren für lange Zeiträume zurückzustellen. Als Kriterium ist „Hinweise" weniger streng gefasst als das gängige Kriterium „Verdachtsmomente", um den Einsatz der Ermittlungsbefugnisse zu begründen.

In seiner Stellungnahme vom 26. Mai 2005 wies der Staatsrat darauf hin, dass in dem Gesetz über terroristische Straftaten *(Wet terroristische misdrijven)*, das am 1. September 2004 in Kraft getreten ist, bereits Vergehen geahndet werden, die im Rahmen der Vorbereitungsphase zu terroristischen Straftaten begangen werden, womit die Anwendung von erweiterten Ermittlungsbefugnissen und verstärkten Zwangsmaßnahmen bereits in einer frühen Phase der Ermittlungen möglich wird. Dieses neue Gesetz bietet eine Reihe von Möglichkeiten, um bereits in einer frühen Phase vorbeugende Maßnahmen gegen terroristische Aktivitäten zu ergreifen. Diese Optionen stellen eine erhebliche Weiterentwicklung des bisherigen Systems der Befugnisse zur Durchführung von Ermittlungen und strafrechtlichen Verfolgungen dar und setzen nach Auffassung des Staatsrates eine sorgfältige Begründung ihrer Notwendigkeit voraus. Bei der Anwendung der vorgeschlagenen Ermittlungsbefugnisse besteht eine Verpflichtung, den Bürger zu informieren (Notifizierungspflicht), um ihm die Möglichkeit zu geben, Einspruchsmittel einzusetzen, wie sie in Paragraph 13 der europäischen Bestimmungen zum Schutz der Menschenrechte und Grundfreiheiten vorgesehen sind. In seiner Stellungnahme verweist der Staatsrat auf frühere Versäumnisse, die Notifizierungsverpflichtung im Rahmen des Gesetzes über Sonderermittlungsbefugnisse einzuhalten (Paragraph 126bb des Strafgesetzes). Die Regierung wird aufgefordert, darüber zu berichten, wie die Notifizierungsverpflichtung eingehalten werden soll.

Am 22. Dezember 2004 legte die niederländische Datenschutzbehörde *(College bescherming persoonsgegevens)* ihre Stellungnahme über den Vorabentwurf eines Geseztes vor, der die Ermittlungsbefugnisse in terroristischen Angelegenheiten ausweiten soll. Die Behörde äußerte sich, vom Datenschutzstandpunkt aus betrachtet, kritisch über die Erweiterung der Handlungsbefugnisse, die Erhebung und Verarbeitung weicher Fakten und die Nichterfüllung der Notifizierungverpflichtung.

Die Maßnahmen zur Bekämpfung des Terrorismus umfassen unter anderem eine Intensivierung des Datenaustauschs zwischen der Staatsanwaltschaft, der Polizei, den Einwanderungs- und Einbürgerungsdiensten (IND) und den allgemeinen Nachrichten- und Sicherheitsdiensten *(Algemene inlichtingen- en veiligheidsdienst, AIVD)* über die so genannte *Contraterrorism infobox* (CT Infobox). Die niederländische Datenschutzbehörde ist sich

der Bedeutung, die der Datenaustausch für die Terrorismusbekämpfung hat, bewusst und hebt die Bedeutung hervor, die einer klaren Beschreibung der juristischen Grundprinzipien sowie der Zuständigkeiten und Befugnisse der beteiligten Parteien und einer angemessenen Überwachung der Durchführung zukommt. Schließlich kann die Verarbeitung personenbezogener Daten im Rahmen der Maßnahmen zur Verhinderung terroristischer Straftaten das Risiko wesentlich erhöhen, dass unschuldige Personen, die aufgrund gewisser Kriterien oder Warnmeldungen in Datenbanken aufgenommen werden, von Regierungsstellen oder der Gesellschaft unfair behandelt werden.

Marktwirtschaftliche Mechanismen im Bereich der Gesundheitsversorgung

In den vergangenen Jahren wurden grundlegende Veränderungen im Bereich der Gesundheitsversorgung und des Systems zur Finanzierung der Krankenversicherungen eingeleitet, um die im Gesundheitssektor anfallenden Kosten besser kontrollieren zu können. Das neue System beruht auf dem Prinzip, dass ein Wettbewerb zwischen Versicherungsunternehmen den Preis und die Qualität der Versorgungsleistungen günstig beeinflussen wird. Der Entwurf des Krankenversicherung sgesetzes wurde am 17. September 2004 vorgelegt. Die parlamentarische Debatte über den Entwurf konnte im Jahr 2005 abgeschlossen werden und das Gesetz trat am 1. Januar 2006 in Kraft. Obwohl im Rahmen des neuen Systems ausführliche medizinische Daten über den Patienten und die Behandlung an die Versicherungsgesellschaften weitergeleitet werden, enthält das Gesetz keine Garantien zum Schutz der Privatsphäre. Tatsächlich werden diese Garantien in einem Ministerbeschluss und einem Verhaltenskodex für Krankenversicherer festgelegt.

In einer Reihe von Stellungnahmen kritisierte die niederländische Datenschutzbehörde die Auswirkungen des neuen Systems auf den Schutz personenbezogener Daten. Die Haupteinwände der Datenschutzbehörde lauteten:

- Der umfassende Anwendungsbereich der Verpflichtung, dass Anbieter von Gesundheitsdiensten personenbezogene Daten von Patienten an Krankenversicherer weiterleiten müssen, beinhaltet die ernste Verpflichtung zur Einhaltung des medizinischen Berufsgeheimnisses und der Vertraulichkeit der Patientendaten. Die so genannten Diagnose-Behandlungs-Kombinationen *(Diagnose Behandel Combinaties)*, die die Grundlage für den Datenaustausch zwischen Anbietern von Pflegeleistungen und Krankenversicherern darstellen, liefern mehr ausführliche Daten über Patienten als die diagnosegestützten Gruppensysteme, die in anderen europäischen Ländern verwendet werden.

- Fehlende Vorkehrungen zum Schutz medizinischer Daten bei der Entwicklung und Einrichtung des neuen Systems. Die Grundlagen für die Bereitstellung und Verarbeitung von medizinischen Daten und entsprechende Garantien werden nicht in dem Gesetz selbst geregelt, sondern im Rahmen einer untergeordneten Gesetzgebung sowie durch sektorale Vereinbarungen. Die Vermeidung einer Wiederverwendung medizinischer Daten, um zusätzliche Versicherungsleistungen zu erhalten, oder anderer Produkte und Dienstleistungen, die von den Versicherungsunternehmen angeboten werden, beruht ausschließlich auf Selbstregulierungsmodellen und der Aufmerksamkeit der Versicherten und derjenigen, die eine Versicherung abschließen möchten.

Persönliche Nummer für öffentliche Dienstleistungen

Am 22. September 2005 wurde der Entwurf für ein Gesetz allgemeiner Regelungen bezüglich der persönlichen Nummer für öffentliche Dienstleistungen vorgelegt *(Wet algemene bepalingen burgerservicenummer)*. Die persönliche Nummer für öffentliche Dienstleistungen *(burgerservicenummer, BSN)* wird die gegenwärtige Steuernummer und Sozialversicherungsnummer *(sofi-nummer)* ablösen, die von den Steuerbehörden ausgegeben und als

Registrierungsnummer in den Bereichen Steuern und Sozialversicherung verwendet wird. Diese BSN-Nummer ist eine allgemeingültige und spezifische Registrierungsnummer für jeden Bürger, die in allen öffentlichen Verwaltungen verwendet werden kann. Alle Regierungsstellen können die BSN-Nummer verwenden, um personenbezogene Daten im Rahmen ihrer Aufgaben zu verarbeiten, ohne dass hierfür die Annahme separater gesetzlicher Regelungen erforderlich wird. Die BSN-Nummer wird darüber hinaus hunderttausenden von nicht ansässigen Bürgern zugewiesen (EU-Bürgern und Niederländern, die sich im Ausland aufhalten), die regelmäßig mit öffentlichen Verwaltungen in Kontakt kommen; bisher wurden diesbezüglich aber noch keine spezifischen Vorkehrungen getroffen, und entsprechende Möglichkeiten werden zum Zeitpunkt der Einführung der BSN-Nummer noch nicht eröffnet. Handel und Industrie haben darum gebeten, die BSN-Nummer verwenden zu dürfen. Bisher wurde diesbezüglich noch keine endgültige Entscheidung getroffen.

Am 10. Februar 2005 veröffentlichte die niederländische Datenschutzbehörde eine Stellungnahme über den Vorentwurf des Gesetzes und kam darin zu dem Ergebnis, dass er keine ausreichenden Garantien enthielte, um zu gewährleisten, dass personenbezogene Informationen mit ausreichender Sorgfalt verarbeitet werden. In Ermangelung entsprechender Garantien wurde davon ausgegangen, dass die Bestimmungen gegen Artikel 8, Punkt 7, der Richtlinie 95/46/EG verstoßen, wozu auf Folgendes hingewiesen wird: *Mitgliedstaaten bestimmen, unter welchen Bedingungen eine nationale Kennziffer oder sonstige allgemein Identifizierungsmöglichkeiten in eine Verarbeitung einfließen dürfen*. Diese Bestimmung wird in dem Entwurf vom 22. September 2005 nicht beachtet. In seiner Stellungnahme vom 1. Juli 2005 kommt der Staatsrat außerdem zu dem Ergebnis, dass die Einführung der BSN-Nummer ohne die Annahme von Regeln und Mechanismen zum Schutz personenbezogener Daten unverantwortlich sei.

Die niederländische Datenschutzbehörde vertritt die Auffassung, dass der am 22. September 2005 vorgelegte Gesetzentwurf schwerwiegende Mängel im Hinblick auf die Reduzierung der Risiken beinhaltet, die mit der Verwendung und Nutzung einer persönlichen Nummer für öffentliche Dienstleistungen verbunden sind. Die Einführung der BSN-Nummer sollte erst erfolgen, nachdem Garantien für ihre sorgfältige Verwendung definiert und in der Gesetzgebung verankert worden sind. In einem Schreiben vom 25. Oktober 2005 forderte die niederländische Datenschutzbehörde die Mitglieder des ständigen Ausschusses des Parlaments für Innere Angelegenheiten und Angelegenheiten des Königreichs auf, die Interessen der einzelnen Bürger zu berücksichtigen, und gab folgende Erklärung ab:

Das Argument, dass ein Bürger immer von einer effizienten Regierung und deshalb auch von einer allgemein verwendbaren Registrierungsnummer profitiert, wird nicht den weitreichenden Auswirkungen der Einführung einer persönlichen Nummer für öffentliche Dienstleistungen gerecht. Die BSN-Nummer ist in erster Linie für die Regierung hilfreich, während die Risiken für den Bürger bisher nur ungenügend berücksichtigt oder in Frage gestellt werden:

- *„Computerfehler" können sich viel schneller über die BSN-Nummer verbreiten.*
- *Es wurden keine Regeln festgelegt, um Bürger über schwerwiegende Fehler zu informieren, die bei der Verarbeitung ihrer Daten auftreten könnten.*
- *Es würde einen einzelnen Bürger große Anstrengungen kosten, mögliche Fehler korrigieren zu lassen, und es gibt keine spezifische „Anlaufstelle", die bei auftretenden Problemen weiterhelfen könnte.*
- *Für Verwaltungsbehörden ist es einfacher, Daten ohne Einwilligung zu erheben.*
- *Der Identitätsmissbrauch wird zunehmen.*

Die niederländische Datenschutzbehörde ist sich durchaus bewusst, dass eine allgemeine Registrierungsnummer für Bürger Vorteile mit sich bringt, weil sie die Reaktionsschnelligkeit von

Verwaltungsbehörden erhöht und Verwaltungskosten senkt. Eine eindeutige Identifikation von Bürgern und die Wiederverwendung von Basisdaten können außerdem dazu beitragen, personenbezogene Daten zu schützen. Für den Bürger und aus Gründen des Schutzes seiner personenbezogenen Daten sowie der sozialen Akzeptanz der Einführung der persönlichen Nummer für öffentliche Dienstleistungen legt die niederländische Datenschutzbehörde deshalb großen Wert auf klare gesetzliche Regelungen in folgenden Punkten:

- *die Bedingungen, unter denen die BSN-Nummer verwendet werden darf*
- *die Verwaltungsbehörden (und gegebenenfalls Unternehmen), die die BSN-Nummer verwenden dürfen*
- *die Bürger müssen über Irrtümer und festgestellte Fehler informiert werden*
- *die Einrichtung eines Bürgerbeauftragten, der bei Schwierigkeiten weiterhilft*
- *die Festlegung von Anforderungen an die ICT-Sicherheit von Dateien, die die BSN-Nummer verwenden.*

B. Bedeutende Rechtssprechung

Anwendungsbereich des Zugriffsrechts

Im Jahr 2004 löste ein Streit zwischen einer Bank und tausenden von Bürgern über das Zuggriffsrecht eine Reihe von Gerichtsklagen und -urteilen aus. Angesichts des Zusammenbruchs der Börsen in den Jahren 2000 und 2001 verloren tausende Inhaber von Verträgen über Anteil-Leasing mit Dexia Bank Nederland N.V. (Dexia) beachtliche Geldsummen. Betrogene Kunden baten um Einsicht in ihre Daten. Dexia kooperierte nicht. Den Anfragen der Kunden stattzugeben, könnte ihrer Position in Rechtsverfahren schaden und zu unverhältnismäßigen Verwaltungskosten führen.

Die niederländische Datenschutzbehörde folgte den Schlichtungsgesuchen und traf eine Entscheidung, wie das Zugriffsrecht in dieser Situation ausgelegt werden könnte. Sie entschied, Dexia solle die gewünschten Daten zur Verfügung stellen, doch Dexia ignorierte diese Entscheidung. Entscheidungen durch die *Geschillencommissie Bankzaken* (Schlichtungskommission für Bankangelegenheiten) und Gerichtsurteile in der Folge haben die Anwendung dieses Rechts verändert.

Einige Fälle sind noch immer beim Berufungsgericht anhängig. Es ist nicht ganz klar, ob ein Antrag auf Zugriff einer Begründung bedarf, welche Daten zur Verfügung gestellt werden sollten, und in welchen Fällen die prozessierende Partei Gründe für Ausnahmen gemäß Artikel 13 der Richtlinie 95/46/EG und § 43 WBP geltend machen kann. Die Meinungen der Datenschutzbehörde, der Wirtschaft und der Industrie gehen in dieser Frage auseinander.

C. Wichtige spezifische Themen

Integrierte Vision über Menschenrechte: Gründung eines neuen Instituts

Vier Organisationen, der Gleichstellungsausschuss *(Commissie Gelijke Behandeling)*, der nationale Bürgerbeauftragte *(Nationale ombudsman)*, das niederländische Institut für Menschenrechte *(Studie- en Informatiecentrum voor de mensenrechten)* sowie die niederländische Datenschutzbehörde unterbreiteten der Regierung im September 2005 einen Vorschlag über die Bildung eines nationalen Menschenrechtsinstituts. Nach den Verfassern des Vorschlags sollten dem vorgeschlagenen Institut eine Reihe von Aufgaben und Funktionen – etwa Anlaufstelle, Beratung sowie Bildungs- und Forschungsmandat – übertragen werden.

Die Organisationen waren der Auffassung, die Auseinandersetzung mit sozialen Entwicklungen könnte von einem integrierten Standpunkt der Menschenrechte aus erforderlich sein. Zum Beispiel kann die Sammlung, Nutzung und Weitergabe oder Veröffentlichung von personenbezogenen Daten nicht dadurch bewertet

werden, sie allein auf praktische Garantien des Schutzes personenbezogener Daten zu testen. Andere Grundfreiheiten sind gleichermaßen davon betroffen, etwa die massive Verbreitung persönlicher Daten durch Veröffentlichungen im Internet, und diese betreffen die Freiheit der Meinungsäußerung und Kommunikation und das Verbot von Diskriminierung. Die Erfassung von Daten über Minderheitengruppen kann einerseits dem Grundsatz der Gleichheit dienen und andererseits zu Diskriminierung führen. Die Vorschläge der Politik zur Terrorismusbekämpfung berühren verschiedene Grundfreiheiten. Die Nutzung der Biotechnologie und die automatische Identifizierung über Funk (Radiofrequenzidentifi kation, RFID) sind weitere Beispiele gesellschaftlicher Entwicklungen, bei denen die Speicherung von personenbezogenen Daten eine große Rolle spielen und sie die verschiedenen Grundrechte und Grundfreiheiten wie die Würde der Bürger, das Recht auf Freiheit und den Grundsatz der Gleichheit antasten kann.

Umfrage „Die Bürger und ihre Privatsphäre"

Die niederländische Datenschutzbehörde gab eine Umfrage in Auftrag, um herauszufinden, wie vertraut die Bürger mit der Datenschutzgesetzgebung sind und welche Bedeutung sie dem Schutz personenbezogener Daten beimessen. Ähnliche Umfragen wurden bereits in einer Reihe von europäischen Ländern durchgeführt.

Aus der Umfrage ging hervor, dass die Bürger einerseits der Vertraulichkeit ihrer Daten in Bezug auf Steuerwesen, Finanzinstitutionen, Sozialversicherungsleistungen, Versicherungsgesellschaften, Schulden, Polizei usw. große Bedeutung beimessen, dass sie aber andererseits kein volles Vertrauen darin haben, dass ihre Daten mit der erforderlichen Sorgfalt behandelt werden.

Die Umfrage machte außerdem deutlich, dass die Bürger sehr ausgewogene Vorstellungen über den Schutz personenbezogener Daten im Vergleich mit anderen Interessen haben. Die Mehrheit der Bürger erklärte, sie erlaube andere (konkurrierende) Interessen, aber mit Einschränkungen. So wurden zum Beispiel das Führen „schwarzer Listen", die Überprüfung von E-Mails und der Internet-Nutzung am Arbeitsplatz unter der Voraussetzung akzeptiert, dass konkrete Hinweise vorliegen, die einen Alarm oder eine Überprüfung rechtfertigen.

Aus der Studie geht außerdem hervor, dass gerade mal die Hälfte der Bürger das Datenschutzgesetz kennt. Im Hinblick auf die Unterstützung des Schutzes personenbezogener Daten durch die Bürger ist in der niederländischen Gesellschaft eine offensichtliche Befürwortung der Datenschutzgesetzgebung zu verzeichnen. In der Befragung geben erstaunliche 92 Prozent aller Bürger an, dass sie die Existenz einer entsprechenden Gesetzgebung in diesem Bereich als wichtig bis sehr wichtig erachten.

Trotz der intensiven Werbung für Sicherheit und Terrorismusbekämpfung zu Zeiten der Umfrage machten die Bürger deutlich, dass der Schutz personenbezogener Daten durch Regierung, Wirtschaft und Industrie in geeigneter Weise geregelt werden muss.

Polen

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und weitere Entwicklungen in der Gesetzgebung

Am 12. Juli 2005 ratifizierte Polen das Zusatzprotokoll zur Konvention für den Schutz von Einzelpersonen in Bezug auf die automatische Verarbeitung personenbezogener Daten bezüglich Überwachungsbehörden und grenzüberschreitendem Datenverkehr (veröffentlicht im Gesetzesblatt von 2006 Nr. 3, Punkt 15). Das Zusatzprotokoll trat am 1. November 2005 in Kraft.

Soweit die Umsetzung der Richtlinie 2002/58/EG betroffen ist, erfolgte die gesetzgeberische Arbeit 2005 in Verbindung mit der Änderung des Gesetzes vom 16. Juli 2004 – dem Telekommunikationsgesetz. Die Änderung (das Gesetz vom 29. Dezember 2005 zur Änderung des Telekommunikationsgesetzes und die Zivilprozessordnung) sieht unter anderem vor, dass der Betreiber eines öffentlichen Telekommunikationsnetzwerks oder der Betreiber öffentlich verfügbarer Telekommunikationsdienstleistungen, die Daten aus dem Datenverkehr in Bezug auf Abonnenten und Endbenutzer bearbeiten, aufgrund der Leistung der bevollmächtigten Behörden für Landesverteidigung, nationale Sicherheit sowie für in Zusammenhang mit der öffentlichen Sicherheit und Ordnung stehende Aufgaben verpflichtet ist, diese Daten für zwei Jahre (neuer Wortlaut von Artikel 165 des Telekommunikationsgesetzes) zu speichern. Ein anderer während der Änderungsphase unterbreiteter Vorschlag sah die Verpflichtung zur Speicherung von Daten aus dem Datenverkehr für einen Zeitraum von 15 Jahren vor. Dieser Vorschlag wurde von den betroffenen Parteien indes strikt abgelehnt. Die Bestimmungen sehen die Verpflichtung zur Datenlöschung oder -anonymisierung nach Ablauf der vorgeschriebenen Frist sowie die Bereitstellung und Vertraulichkeit dieser Daten und der betroffenen Personen mit größter Sorgfalt vor.

Ein Entwurf des Gesetzes zur Offenlegung von Informationen und Dokumenten des Staatssicherheitsdienstes des kommunistischen Regimes im Zeitraum 1944–1990 und die Inhalte dieser Dokumente wurden von den Abgeordneten der Regierungspartei vorbereitet. Der Entwurf sieht Änderungen in den bisher gültigen Prüfungsbestimmungen vor und bezieht sich auf einen größeren Kreis von zu prüfenden Personen, einschließlich Träger öffentlicher Funktionen, Journalisten und Universitätsprofessoren. Der neue Entwurf legt das Recht der Bürger fest, Informationen über Träger öffentlicher Funktionen oder Berufe öffentlichen Vertrauens, das durch den Zugriff der Bürger auf Informationen über dieser Überprüfung unterworfenen Personen zur Anwendung käme, zu überwachen. Darüber hinaus wird das *Institute of National Remembrance (IPN)* Zertifikate für überprüfte Personen ausstellen, die den Inhalt von Geheimdienstaufzeichnungen beschreiben, die dann in dem im Internet verfügbaren IPN-Register veröffentlicht werden.

Der neue Artikel 105a wurde dem Bankengesetz im Rahmen des Gesetzes vom 15. April 2005 zur Änderung des Gesetzes über den Schutz klassifizierter Information und einiger anderer Gesetze hinzugefügt. Gemäß diesen Bestimmungen können Banken und andere, per Gesetz zur Kreditvergabe befugte Institute oder Kreditinformationsagenturen Informationen über Einzelpersonen (Verbraucher) zum Zweck der Kreditwürdigkeit und Kreditrisikoanalyse verarbeiten. Diese Institutionen sind zur Verarbeitung von Informationen nach Ende der Verpflichtung aus dem Vertrag, der mit einer Bank oder einer anderen, per Gesetz zur Kreditvergabe befugten Institution geschlossen wurde, unter der Voraussetzung berechtigt, dass die betroffene Person für die vorliegenden Daten

schriftlich ihre vorherige schriftliche Einwilligung erteilt. Die betreffende Einwilligung kann jederzeit widerrufen werden.

Diese Institutionen können Informationen in dieser gegebenen Situation bearbeiten, wenn alle folgenden Anforderungen erfüllt sind: 1) Eine betroffene Einzelperson kam der Verpflichtung nicht nach, oder sie ist seit mehr als 60 Tagen mit den Leistungen gemäß dem mit der Bank oder per Gesetz zur Kreditvergabe befugten Institution geschlossenen Vertrag in Verzug; 2) Wenn Umstände gemäß Punkt 1 vorliegen, ist die Verarbeitung von Informationen nur 30 Tage nach dem Zeitpunkt der Mitteilung über die Absicht der Verarbeitung personenbezogener, durch das Bankengeheimnis geschützter Daten ohne die Einwilligung der Person, auf die sich diese Informationen beziehen, möglich. Die Verarbeitung der Daten kann ohne Einwilligung der betroffenen Person nicht länger als fünf Jahre ab dem Zeitpunkt des Endes einer Verpflichtung erfolgen.

Die Bestimmungen des Gesetzes über den Schutz personenbezogener Daten vom 29. August 1997 und die Durchsetzungsbestimmungen in Bezug auf dieses Gesetz wurden 2005 nicht geändert.

B. Bedeutende Rechtssprechung

Unter den Urteilen betreffend die Privatsphäre und den Datenschutz in Bezug auf den Berichtszeitraum sollte insbesondere das Urteil des Verfassungsgerichts vom 12. Dezember 2005 Erwähnung finden. Das Gericht urteilte, dass eine Diskrepanz bestünde zwischen der Verfassung der Republik Polen und einigen Bestimmungen des Polizeigesetzes vom 16. April 1990 über die Erfassung und Nutzung von Material, das während der Vornahme von Überprüfungen ohne gerichtliche Zustimmung oder schriftliche Einwilligung der Person, die Informationen erteilt oder erhält, zusammengetragen wurde. Darüber hinaus spezifiziert die fragliche Bestimmung weder den Umfang der auf diese Weise zusammengetragenen Informationen noch die Situation, in der eine solche Erfassung erfolgen sollte. Das Gericht betonte, dass die oben genannte Bestimmung nicht die Möglichkeit vorsieht, die betroffene Person von den Überprüfungstätigkeiten in Kenntnis zu setzen, sondern dies erst zu dem Zeitpunkt der Durchführung der Überprüfung erfolgt. Doch danach soll einer Person, über die Erkundigungen eingezogen wurden, Zugang zu ihren erfassten Daten gewährt werden. In demselben Urteil fordert das Gericht darüber hinaus, dass der Befehl des Chefkommandeurs der Polizei in Bezug auf die Erfassung, Verarbeitung und Nutzung von Daten durch die Polizei mit der Verfassung der Republik Polen konform sein muss, da die Bestimmungen und Vorschriften über die Erfassung und Offenlegung von Informationen über den Bürger nur per Gesetz geregelt werden können. Die oben genannten Bestimmungen finden innerhalb von zwölf Monaten ab dem Zeitpunkt der Urteilsveröffentlichung keine Anwendung mehr.

Am 26. Oktober urteilte das Verfassungsgericht über eine Abweichung zwischen der Verfassung der Republik Polen und den Bestimmungen des Gesetzes über das *National Remembrance Institute* – Kommission für die Verfolgung von Verbrechen gegen die polnische Nation –, welches das Recht auf Zugang zu Dokumenten und die angemessene Berichtigung nur unter der Voraussetzung vorsieht, dass der Status einer „benachteiligten Person" gegeben ist. Das Gericht betonte, dass das Verfassungsrecht zur Berichtigung oder Löschung unvollständiger oder rechtswidrig erfasster Daten nicht nur auf einen bestimmten Personenkreis, z. B. auf benachteiligte Personen, beschränkt werden könne. Aus der Sicht des Gerichts erlaubt das Gesetz über das IPN den betroffenen Personen Aktualisierungen, Dokumente oder Kopien beizufügen, die vom IPN akzeptiert und entsprechenden Dateien zugefügt werden sollen. Diese Lösung soll

die Echtheit, Vollständigkeit und Objektivität der zusammengetragenen Informationen, die auf den eingeholten Dokumente beruhen, garantieren.

In den Jahren 2004 und 2005 war der Generalinspektor mit zahlreichen Fällen betreffend die Offenlegung personenbezogener Daten von Schuldnern an Inkassounternehmen im Rahmen der Abtretung ausstehender Finanzschulden befasst. Das rücksichtslose Vorgehen mancher Inkassounternehmen führt häufig zur Einschüchterung der Verbraucher und zu willkürlich zustande gekommenen Gerichtskosten. Aus der Sicht des Datenschutzgesetzes kommt der Rechtmäßigkeit der Verarbeitung personenbezogener Daten des Schuldners durch Inkassounternehmen hier entscheidende Bedeutung zu. Der Generalinspektor vertrat die Ansicht, dass eine Offenlegung personenbezogener Daten des Verbrauchers in Verbindung mit der Abtretung ausstehender Finanzschulden nur mit Einwilligung der betroffenen Personen stattfinden kann. In einem solchen Fall sollte keine der Voraussetzungen in Bezug auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß Artikel 23 Absatz 1 des Gesetzes Anwendung finden. In den Fällen betreffend die Verarbeitung personenbezogener Daten in Verbindung mit der Abtretung ausstehender Schulden erging ein Urteil sowohl vom Verwaltungsgericht der Woiwodschaft in Warschau als auch vom Obersten Verwaltungsgericht. Es ist klar und deutlich hervorzuheben, dass diese Rechtsfrage gegenwärtig viele Zweifel in der Rechtssprechung der Verwaltungsgerichte aufkommen lässt. Am 6. Juni 2005 traf der Oberste Verwaltungsgerichtshof mit einem erweiterten Stab von sieben Richtern den Beschluss, der einen Präzedenzfall geschaffen hat. Der Oberste Verwaltungsgerichtshof urteilte, dass im Falle der Abtretung ausstehender Schulden die personenbezogenen Daten den Abtretungsempfängern gemäß Artikel 23 Absatz 1, Punkt 5 des Gesetzes zum Schutz der personenbezogenen Daten offengelegt werden können, das besagt, dass die Verarbeitung erlaubt ist, wenn sie für den Zweck der rechtmäßigen Interessen der für die Datenverarbeitung Verantwortlichen oder Datenempfänger erforderlich ist, soweit die Verarbeitung keine Verletzung der Rechte oder Freiheiten der betroffenen Person darstellt. Der Oberste Verwaltungsgerichtshof betonte jedoch, dass die Bewertung einer möglichen Verletzung der Verbraucherrechte und -freiheiten je nach Fall zu entscheiden sei.

C. Wichtige spezifische Themen

Anfang 2005 hat der Fall der Offenlegung personenbezogener Daten in Aufzeichnungen des *National Remembrance Institute* – der Kommission für die Verfolgung von Verbrechen gegen das polnische Volk (IPN) –, dessen Aufgabe unter anderem die Speicherung, Analyse und Offenlegung von Dateien des Staatssicherheitsdienstes (des kommunistischen Regimes) umfasst, die Öffentlichkeit bewegt. Ein bekannter Journalist hat im Internet den Beweis geliefert, dass die im Lesesaal des IPN zugänglichen Archiv-Quellen rund 200 000 Namen und Decknamen von Personen enthielten, die in den IPN-Archiven gespeichert sind. Diese Dateien umfassten personenbezogene Daten sowohl von Mitarbeitern des Sicherheitsdienstes als auch von Angestellten, von Einzelpersonen, die vom Geheimdienst ungerecht behandelt wurden, ohne Nennung besonderer Kategorien.

Im Anschluss an diesen Zwischenfall nahmen Inspektoren der Abteilung des Generalinspektors für Datenschutz eine Überprüfung der Verarbeitung personenbezogener Daten durch das IPN vor. Im Verlauf dieser Inspektion stellte sich heraus, dass die oben genannte Beweisliste für den Zweck geschaffen worden war, um im Archivmaterial zu stöbern, und gegen Beschädigung, Veränderungen oder Kopieren durch den Leser nicht

geschützt war. Diese Inspektion attestierte eine Verletzung des Datenschutzgesetzes unter anderem in der Form zahlreicher Verstöße gegen die Datenschutzbestimmungen, die bei der Verarbeitung personenbezogener Daten in Computersystemen beachtet werden müssen. Es wurde ebenfalls festgestellt, dass eine Liste von zur Verarbeitung personenbezogener Daten befugten Personen nicht vorhanden war. Darüber hinaus hatte das IPN seine Dateisysteme über die Daten nicht zur Registrierung an den Generalinspektor weitergegeben und machte die in den Archiven gespeicherten Daten Journalisten zugänglich, obwohl dies vom Gesetz her nicht vorgesehen ist. Der Generalinspektor erließ einen Beschluss, wonach die Versäumnisse bei der Verarbeitung personenbezogener Daten im IPN zu beheben sind.

Dagegen wurde jedoch Berufung eingelegt, und die Entscheidung des Obersten Verwaltungsgerichtshofs steht noch aus. Der Generalinspektor unterrichtete außerdem das Büro des Generalstaatsanwalts über den vorliegenden Verstoß, doch das Verfahren zur Klärung des Falls wurde von der Generalstaatsanwaltschaft eingestellt, die trotz der Verletzung der Bestimmungen des Datenschutzgesetzes erklärte, es habe keinen Verstoß gegeben.

Portugal

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und weitere Entwicklungen in der Gesetzgebung

Die Richtlinie 95/46/EG wurde in die nationale Gesetzgebung per Gesetz 67/98 vom 26. Oktober 1998 – Datenschutzgesetz – aufgenommen.

Die Richtlinie 2002/58/EG wurde per Gesetzesdekret 7/2004 (nur Artikel 13) und per Gesetz 41/2004 vom 18. August 2004 in die nationale Gesetzgebung aufgenommen.

Im Jahre 2005 traten wichtige Gesetze im Bereich des Datenschutzes in Kraft, insbesondere das Gesetz 1/2005 vom 10. Januar über den Einsatz der Videoüberwachung durch Strafverfolgungsbehörden und das Gesetz 12/2005 vom 26. Januar über persönliche genetische Informationen und Gesundheitsinformationen. Beide Gesetze erhielten die vorherige Zustimmung der portugiesischen Datenschutzbehörde, die außerdem zahlreiche Anregungen zur Verbesserung der Gesetzestexte unterbreitete.

2005 wurden ebenfalls zusätzliche Gesetze zum Einsatz der Videoüberwachung auf Autobahnen zum Zwecke der Verkehrsregelung, Erkennung von Verstößen oder Verhütung von Unfällen erlassen.

B. Bedeutende Rechtssprechung

Bezüglich der Möglichkeiten einer Berufung gegen eine Entscheidung der Datenschutzbehörde gemäß dem Datenschutzgesetz wurden gegen sie ca. zehn Berufungen wegen Sanktionsverfahren, aber keine einzige zu einem Verwaltungsbeschluss eingereicht.

Die meisten Klagen betrafen den Einsatz von Videoüberwachung oder biometrischen Systemen ohne das erforderliche Notifizierungsverfahren und das fehlende Recht auf Information. In der Mehrheit der Fälle hielt das Gericht an der von der Datenschutzbehörde verhängten Sanktion fest, in einigen wenigen Fällen wurde die Strafe gemildert.

C. Wichtige spezifische Themen

Das Jahr 2005 war allgemein gesehen für die portugiesische Datenschutzbehörde ein sehr aktives Jahr: Personalaufstockung, Neuorganisation der Arbeit, Entwicklung neuer interner Informationssysteme in Bezug auf die öffentliche Registrierung und das elektronische Notifizierungssystem sowie eine neue Website. Diese Umstrukturierung zielte darauf ab, bessere Bearbeitungsverfahren für die zunehmende Zahl von Notifizierungen, Stellungnahmen, Untersuchungen und Informationsanfragen einzuführen und betroffenen Personen und für die Datenverarbeitung Verantwortlichen eine bessere Unterstützung zu bieten.

Stellungnahmen zu Gesetzesentwürfen

Gemäß dem Datenschutzgesetz müssen Gesetzentwürfe, die Fragen zum Datenschutz enthalten, auf nationaler wie auch internationaler Ebene der Datenschutzbehörde zur Stellungnahme unterbreitet werden. Deswegen erarbeitete die Datenschutzbehörde im Jahr 2005 44 Stellungnahmen, wobei einige sich auf die bei EU-Institutionen in Vorbereitung befindlichen Gesetze bezogen, wie etwa die Rechtsgrundlage für SIS II, die Entwicklung von VIS und die Aufbewahrung von Verkehrsdaten. In Bezug auf nationale Gesetzesentwürfe erstellte die Datenschutzbehörde Stellungnahmen zur Umsetzung der Richtlinie über die Wiederverwendung öffentlicher Informationen, den Zugang von Wohlfahrtsdiensten zu Daten bei Steuerbehörden mit dem Ziel der Überprüfung der Einkommen von Personen, die Zuschüsse für die medizinische Versorgung beantragen, über den Einsatz einer Videoüberwachung auf Autobahnen und die Einrichtung einer schwarzen Liste mit Steuerschuldnern.

Notifizierungsgebühren

Die Datenschutzbehörde führte die Erhebung von Gebühren für das Notifizierungsverfahren ein. Für Rechtspersonen betragen die Gebühren 50 bzw. 100 Euro, abhängig davon, ob die Datenverarbeitung der vorherigen Genehmigung bedarf oder nicht. Für natürliche Personen belaufen sich die Kosten auf 30 bzw. 60 Euro. Die Gebühren sind vor oder bei Einreichung des Notifizierungsformulars zu zahlen.

Öffentliches Register und neue Website

Die Datenschutzbehörde veröffentlichte eine neue Website mit einer neuen Struktur und sehr viel mehr Informationen. Die Website bietet je eine Suchfunktionen für Entscheidungen und für thematische Informationen. Sie ist in englischer und französischer Sprache abgefasst und enthält Gesetze und Gerichtsurteile. Darüber hinaus bietet sie erstmals einen Online-Zugriff auf das öffentliche Register, das von betroffenen Personen und für die Datenverarbeitung Verantwortliche konsultiert werden kann. Diese können beispielsweise prüfen, ob ein bestimmtes Unternehmen, dem sie Daten übermitteln möchten, bei der Datenschutzbehörde auch ordnungsgemäß eingetragen ist. Die Datenschutzbehörde hat bereits ein positives Feedback von Personen erhalten, die das öffentliche Register eingesehen haben. Die Adresse der Website lautet: www.cnpd.pt

Grenzüberschreitende Datenflüsse

Darüber hinaus hat die Datenschutzbehörde auch das Verfahren für den grenzüberschreitenden Datenverkehr vereinfacht. Die Datenschutzbehörde beschloss, vorherige Genehmigungen nur noch für internationale Datentransfers gemäß Artikel 26 Absatz 2 der Richtlinie zu erteilen. Im Falle von Standardvertragsklauseln und einer angemessenen Entscheidung der EK bedarf es für die Datenverarbeitung keiner vorherigen Prüfung. Das Gleiche gilt für Situationen, die durch Artikel 26 Absatz 1 der Richtlinie geregelt sind.

E-Abstimmung

Im Jahr 2005 fand ein Pilotprojekt zur E-Abstimmung für die Parlamentswahlen statt, bei dem zwei verschiedene elektronische Verfahren getestet wurden: die E-Abstimmung in Wahllokalen und die Online-Abstimmung. Der Pilotversuch wurde von der Datenschutzbehörde, die den Zugriff auf die Wahldatenbank erlaubt hatte, streng überwacht. Auf der Grundlage dieser Ergebnisse des Pilotversuchs und verschiedener Diskussionen veröffentlichte die Datenschutzbehörde einige Leitlinien in Bezug auf den „Datenschutz der Wähler bei E-Abstimmungen". Die Datenschutzbehörde veranstaltete auch eine Konferenz im Parlament und lud die Universitätsteams, die das Pilotprojekt koordinierten, den Nationalen Wahlausschuss und alle Abgeordneten dazu ein. Es entwickelte sich eine sehr fruchtbare Diskussion und eine interessante Initiative.

Politikwerbung und elektronische Kommunikationsformen

Im Anschluss an die Umsetzung der Richtlinie über elektronische Kommunikation und der Rechtsvorschriften zur Regelung elektronischer Kommunikationsformen für Marketingzwecke in nationales Recht gab die Datenschutzbehörde einige Leitlinien für den Bereich der Politikwerbung heraus. Bei Wahlverfahren gehen bei der Datenschutzbehörde stets zahlreiche Beschwerden von betroffenen Personen wegen politischer Propaganda ein. Die Datenschutzbehörde beschloss daher die Aufstellung von Leitlinien, die die politischen Parteien beachten müssen. Diese Maßnahme ging durch die Presse, was zur Folge hatte, dass bei der darauf folgenden Wahl weniger Beschwerden eingingen.

Warnmeldungen

Die portugiesische Börsenaufsicht erteilte im vergangenen November Unternehmen die Empfehlung, eine Politik zur Kommunikation über interne Unregelmäßigkeiten einzuführen. Der Anwendungsbereich war nicht eindeutig definiert, und Datenschutzbestimmungen wurden auch nicht erwähnt. Um zu verhindern, dass Unternehmen möglicherweise solche Politiken ohne Berücksichtigung des Datenschutzes entwikkeln, und um herauszufinden, was genau das Ziel einer solchen Kommunikationspolitik ist, trafen die Datenschutzbehörde und Aufsichtsbehörde zu Beratungen zusammen. Auf diesem Treffen wurden Führung und Verantwortlichkeit als Anwendungsbereich der Kommunikation festgelegt. Darüber hinaus wurde beschlossen, dass die Aufsichtsbehörde Unternehmen auf die Beachtung von Datenschutzbestimmungen hinweisen sollte, und insbesondere, dass sie die Pflicht zur Mitteilung der Datenverarbeitung an die Datenschutzbehörde hat, damit diese die Genehmigung erteilen kann.

Slowakei

Am 1. Mai 2004 wurde die Slowakei Mitglied der Europäischen Union. Die Behörde erhielt einen neuen offiziellen Namen, der seit dem 1. Mai 2005 gilt: Amt für den Schutz personenbezogener Daten der Slowakei (nachstehend als „Datenschutzbehörde" bezeichnet) durch Gesetz Nr. 90/2005 Coll. zur Änderung des Gesetzes Nr. 428/2002 Coll. über den Schutz personenbezogener Daten (nachstehend als "Datenschutzgesetz" bezeichnet).

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und weitere Entwicklungen in der Gesetzgebung

Umsetzung der Richtlinie 95/46/EG

Die letzte Änderung des Datenschutzgesetzes wurde als angemessene Reaktion auf die Kommentare der Europäischen Kommission in den Jahren zuvor bewertet. Das Gesetz trat am 1. Mai 2005 in Kraft.

Trotzdem bat die Datenschutzbehörde der Slowakei die Europäische Kommission, Generaldirektion Justiz, Freiheit und Sicherheit, Referat Datenschutz, das geänderte Datenschutzgesetz im Detail zu prüfen. Ziel war, in Bezug auf die Qualität eine möglichst große Harmonisierung zwischen dem Datenschutzgesetzes und der Richtlinie 95/46/EC zu erreichen.

Ende 2005 übermittelte das Referat Datenschutz der Europäischen Kommission der Datenschutzbehörde seine Kommentare, die im Februar 2006 in Bratislava Gegenstand eingehender Beratungen mit einem Experten der Europäischen Kommission waren. Die Diskussion erwies sich als sehr fruchtbar und verfolgte den Zweck, geeignete Lösungen für einen effektiven Beitrag zum Schutz personenbezogener Daten in der Slowakei zu erarbeiten. Die Empfehlungen und neuen Ideen der Europäischen Kommission werden als Grundlage für die nächste Runde der Änderung des Datenschutzgesetzes dienen, die in Kürze stattfinden wird.

Umsetzung der Richtlinie 2002/58/EG

Die Richtlinie 2002/58/EG legt die Rechte und Pflichten im Rahmen des Anwendungsbereichs des Datenschutzes fest, insbesondere im Bereich der elektronischen Kommunikation. Die Richtlinie wurde per Gesetz Nr. 610/2003 Coll. über elektronische Kommunikation innerhalb des neuen Verordnungspakets für elektronische Kommunikation umgesetzt. Die Umsetzung dieser Richtlinie fällt in den Zuständigkeitsbereich des Ministeriums für Verkehr, Post und Telekommunikation der Slowakei.

Anfang 2005 übersandte die Europäische Kommission eine offizielle Mitteilung über die unvollständige Umsetzung der Richtlinie 2002/58/EG. Die Mitteilung betraf fehlende Bestimmungen über „Cookies" und mangelhafte Bestimmungen über unerbetene Mitteilungen. Die Slowakei antwortete innerhalb des vorgeschriebenen Zeitraums und unterbreitete einen Lösungsvorschlag. Der Änderungsprozess des Gesetzes Nr. 610/2003 Coll. über elektronische Kommunikation wurde mit der Entschließung Nr. 663 der slowakischen Regierung am 7. September 2005 eingeleitet und endete mit der Annahme des Gesetzes Nr. 117/2006 Coll. durch das slowakische Parlament am 2. Februar 2006. Die von der EK angemahnten Bestimmungen wurden in das Gesetz integriert. Die Änderung des Gesetzes Nr. 610/2003 Coll. trat am 1. April 2006 in Kraft.

Erläuterungen zu sonstigen Gesetzgebungsakten und Stellungnahmen

Im Jahr 2005 kommentierte die Datenschutzbehörde über 100 Gesetzgebungsakte aus der Sicht des Datenschutzes und erarbeitete mehr als 690 Stellungnahmen.

B. Bedeutende Rechtssprechung

Die Datenschutzbehörde war 2005 als Streitpartei in drei Fällen impliziert. Bei einem Fall ging es um eine Strafsumme, bei dem zweiten um die

Aufhebung einer Entscheidung, während der dritte Fall die gerichtliche Prüfung der von der Datenschutzbehörde durchgeführten Verfahren betraf. Zwei Fälle wurden nicht zugunsten der Datenschutzbehörde entschieden, obwohl Berufung bei einer höheren Instanz eingelegt wurde, und ein Fall ist noch immer anhängig.

C. Wichtige spezifische Themen

Privatsphäre und Transparenz

Das Gesetz Nr. 211/2000 Coll. des Nationalrates der Slowakei über den freien Zugang zu Informationen wurde per Gesetz Nr. 628/2005 Coll. geändert. Die Änderung trat am 2. Januar in Kraft und fand in den Medien weite Verbreitung. Die letzte Fassung des Gesetzes legt eine Verpflichtung zu einer erhöhten Transparenz in Bezug auf die wirtschaftliche und finanzielle Identität der Beamten und Angestellten des öffentlichen Dienstes (z. B. Leiter von staatlichen oder städtischen Behörden, Abgeordneten usw.) fest. Das Gesetz sieht die Offenlegung ihrer personenbezogenen Daten sowie Angaben zu Gehältern und Vergütungen vor. Darüber hinaus fordert es die Veröffentlichung personenbezogener Daten in Bezug auf Immobilieneigentum, das vom Staat auf andere Personen übertragen wurde. Außerdem lässt es die Offenlegung von Informationen über die Verwaltung von Eigentum im Besitz des Staates oder von Städten und Gemeinden, z. B. Verkäufe oder Mieten, zu. In diesem Zusammenhang müssen mehr personenbezogene Daten verfügbar oder offen gelegt werden als vorher. Angebliches Ziel der Änderung ist, den öffentlichen Sektor für die Bürger der Slowakei transparenter zu machen. Nach Ansicht der Datenschutzbehörde geht die entsprechende Änderung weit über den Rahmen der in den Richtlinien enthaltenen Standardbestimmungen über den Schutz personenbezogener Daten hinaus und löst in keiner Weise das Problem der mangelnden Transparenz in Bezug auf die Verteilung der Haushaltsmittel. All diese Bedenken wurden in schriftlichen Stellungnahmen und öffentlichen Erklärungen durch die Datenschutzbehörde dagelegt.

Betrügerischer Missbrauch personenbezogener und biometrischer Daten

Die Datenschutzbehörde hat Fälle des Missbrauchs personenbezogener Daten durch Vertreter von „Rentenversicherungsgesellschaften der zweiten Säule" registriert, die im Fernsehen und in der Presse weit verbreitet wurden. Private Altersvorsorgegesellschaften werden im Gesetz Nr. 43/2004 Coll. definiert. Die Vertreter schlossen Verträge im Namen der betroffenen Personen ohne deren ausdrückliches Einverständnis ab (Vertreter werden in der Regel für den Abschluss eines neuen Vertrags bezahlt). Die Rentenversicherungsgesellschaften der zweiten Säule erklärten, die Verträge seien gültig, die betroffenen Personen gehen vom Gegenteil aus. Die Pflichtbeiträge zur Sozialversicherung sind in zwei gleiche Teile jeweils für die Versorgungskasse der ersten Säule und der zweite Säule aufgeteilt. Bei der Datenschutzbehörde gingen über 60 Klagen von Opfern ein.

Die Datenschutzbehörde wird von betroffenen Personen häufig mit der Frage der Notwendigkeit der Nutzung biometrischer Daten für Authentifizierungs-/Prüfverfahren im Bank- oder Privatsektor befragt. Bei der Datenschutzbehörde gingen Mitteilungen über zahlreiche Fälle von Missbrauch personenbezogener Daten, von Betrug, gefälschten Verträgen, von über Kredit-/Debitkarten gestohlenem Geld usw. ein. Zur Vermeidung von Verlusten oder zur Schadensbegrenzung bei Kunden oder Geschäftspartnern gewinnt die Nutzung biometrischer Daten in zunehmendem Maße an Bedeutung. Die wichtige ausdrückliche Einwilligung der betroffenen Personen zur Nutzung biometrischer Daten ist gemäß dem Datenschutzgesetz nur dann erforderlich, wenn die biometrischen Daten in den Anwendungsbereich der Definition personenbezogener Daten fallen. In der Slowakei gibt es derzeit kein spezifisches Gesetz, das spezifische Bestimmungen über die Sammlung, Verarbeitung, Nutzung oder Herausgabe biometrischer Daten regeln würde.

Offenlegung früherer Akten der Staatssicherheit

Zurzeit drängen verschiedene Personen auf die Offenlegung von Geheimaufzeichnungen über die Tätigkeiten der Strafverfolgungsbehörden der ehemaligen Tschechoslowakei zwischen 1939–1989. Das Nationale Gedenkinstitut der Slowakei hat vor kurzem die Informationen über die Liquidierung jüdischer Unternehmen (1941–1942) öffentlich gemacht. Diese Informationen umfassen 10 112 Akten, einschließlich der Namen der so genannten „Arisierer", die einen Anteil vom Enteignungswert erhielten. Die so genannte Arisierung der jüdischen Unternehmen im zweiten Weltkrieg (1939–1945) war ein Ergebnis der von den Nazis aufgezwungenen Verfahren zur „Ausgrenzung der Juden aus Wirtschaft und Gesellschaft".

Internationale Zusammenarbeit

Zusätzlich zu regelmäßigen internationalen Aktivitäten auf dem Gebiet des Schutzes personenbezogener Daten und der Privatsphäre im Zuge der EU-Mitgliedschaft nimmt die Datenschutzbehörde an multilateralen MOE-Länderkonferenzen teil, die sich mit Themen von besonderem Interesse für die Gastgeberländer befassen. Auf dem 7. Treffen der Datenschutzbeauftragten der mittel- und osteuropäischen Länder am 24. Mai 2005 in Smolenitz, Slowakei, wurde eine Erklärung über die künftige Zusammenarbeit zwischen Bulgarien, Kroatien, der Tschechischen Republik, Estland, Ungarn, Lettland, Litauen, Polen und der Slowakei unterzeichnet. Im Bereich der bilateralen Zusammenarbeit zwischen der Slowakei und der Tschechischen Republik erfolgte am 21. März 2006 in Valtice, Südmähren, die Unterzeichnung des „Memorandums von Valtice über die Zusammenarbeit zwischen der Datenschutzbehörde der Slowakei und der Datenschutzbehörde der Tschechischen Republik".

Darüber hinaus nimmt die Datenschutzbehörde an Veranstaltungen mit ähnlicher Thematik teil, etwa an Konferenzen über Menschenrechte, die Informationsgesellschaft, internationale Strategien und Investitionen, Telekommunikation, Spams und Cyberkriminalität usw. und bemüht sich um die Schaffung oder Festigung der Verbindungen zu Privatinvestoren und Organisationen ohne Erwerbszweck.

Schengen-Bewertungsmission

Die Schengen-Bewertungsmission begab sich im Februar 2006 in die Slowakei, um die Bereitschaft des Landes zur Umsetzung des Schengen-Acquis im Bereich des Datenschutzes zu evaluieren. Die Experten der Mission konzentrierten ihre Kontrolltätigkeiten in der Slowakei auf folgende Themen: rechtlicher, institutioneller und organisatorischer Rahmen des personenbezogenen Datenschutzes, Prozess der Durchsetzung der Rechte der betroffenen Personen und Möglichkeiten über die Offenlegung dieser Klagen, Überwachungsaktivitäten der Datenschutzbehörde, aktueller Stand der technischen Sicherheit bei der Verarbeitung personenbezogener Daten, Schutz personenbezogener Daten in Zusammenhang mit dem Visaantrags- und genehmigungsverfahren, internationale Zusammenarbeit der Datenschutzbehörde mit ausländischen Datenschutzbehörden, Sensibilisierung der Bürger für den Schutz personenbezogener Daten.

Die Ergebnisse der Expertenmission wurden in einem Evaluierungsbericht zusammengefasst. Gemeinsam mit dem Innenminister erarbeitete die Datenschutzbehörde eine offizielle Stellungnahme über die Evaluierung der Ergebnisse. Im Anschluss wurden die im Evaluierungsbericht festgelegten Anforderungen in den Zeitplan des nationalen Schengener Aktionsplans aufgenommen. Die Datenschutzbehörde nimmt vorweg, dass die Arbeit, die aufgrund des Berichts zu tun ist, bis Ende 2006 abgeschlossen sein und die Slowakei die von der EK geforderten Auflagen erfüllen wird.

Öffentliches Bewusstsein

Um eine qualitativ gute Umsetzung der Richtlinie 95/46/EG sicherzustellen, unterrichtet die

Datenschutzbehörde die Minister und andere Vertreter der staatlichen Verwaltungsbehörden über die neuen Bestimmungen des Datenschutzgesetzes, insbesondere über die temporären Bestimmungen im Rahmen von Abschnitt 55 des Datenschutzgesetzes, das am 1. Mai 2005 in Kraft trat. Danach antwortete die Mehrheit der staatlichen Verwaltungsbehörden, dass sie gerade dabei seien, die Änderungen in die Gesetzesvorschriften ihres Ressorts zu integrieren, oder stellte fest, dass die Gesetze innerhalb ihres Zuständigkeitsbereichs eine solche Verpflichtung bereits garantierten. Einige Einrichtungen erklärten sich zur Umsetzung neuer Vorschriften im Rahmen einer direkten Konsultation der Datenschutzbehörde bereit.

2005 und 2006 organisierte die Datenschutzbehörde zahlreiche Seminare und Konsultationen über das kürzlich geänderte Datenschutzgesetz und die geänderten Datenschutzbestimmungen sowie die neuen Verpflichtungen der für die Datenverarbeitung Verantwortlichen, insbesondere für den Banken- und Leasingsektor, Wasserversorgungsunternehmen, das Katasteramt, Telekommunikationsgesellschaften und Mobilfunkbetreiber usw.

Die Datenschutzbehörde konzipierte ihre Website neu, und die Mitarbeiter der Datenschutzbehörde hielten unabhängige Fachvorträge über den Schutz personenbezogener Daten.

Um quantifizierbare Informationen über das öffentliche Bewusstsein in punkto Datenschutz zu erhalten, wurde eine öffentliche Umfrage durchgeführt. Das Bewusstsein der Bürger über den Schutz personenbezogener Daten war um 25 Prozent höher als im Jahr 1999. Die Umfrage machte deutlich, dass vom Standpunkt der Bürger aus die nationalen ID (so genannte Geburts-ID) die sensibelsten personenbezogenen Daten waren – 72 Prozent der Befragen teilten diese Meinung. Daten über persönliches Eigentum und Finanzen wurden von 40 Prozent als sensible Daten eingestuft, Gesundheitsdaten ebenfalls von 40 Prozent, biometrische Daten von 22 Prozent, mentale Identität (Geisteszustand) von 21 Prozent, Strafregister von 13 Prozent, Mitgliedschaft in einer politischen Partei bzw. politische Meinungen von 12 Prozent, Informationen über sexuelle Ausrichtung von 12 Prozent, Glaube/Konfession von 10 Prozent, Rasse und ethnische Daten von 5 Prozent und Nationalität ebenfalls von 5 Prozent.

Mitteilungen über die von den für die Datenverarbeitung Verantwortlichen benannten Datenschutzbeauftragten/Registrierungen der Ablagesysteme

Als Folge der jüngsten Änderung des Datenschutzgesetzes 2005 und 2006 registrierte die Datenschutzbehörde bis zum 12. April 2006 rund 37 500 Mitteilungen über die Ernennung von Datenschutzbeamten mit Zuständigkeit für die interne Überwachung des Schutzes personenbezogener Daten gemäß Abschnitt 19 des Datenschutzgesetzes. Diese Mitteilungen ersetzen die Registrierung von Ablagesystemen in den allermeisten Fällen.

Im Jahr 2005 veröffentlichte die Datenschutzbehörde 31 Standardregistriernummern auf der Grundlage der Bestimmungen von Abschnitt 26 und 25 Sonderregistriernummern gemäß Abschnitt 27 des Datenschutzgesetzes. Im Jahr 2006 gingen bei der Datenschutzbehörde bis zum 12. April insgesamt 4 639 Anträge auf Registrierung von Ablagesystemen für die Datenverarbeitung ein.

Die Datenschutzbehörde gab in 28 Fällen von grenzüberschreitendem Datentransfer in Drittländer gemäß Abschnitt 23 (7) des Datenschutzgesetzes ihr Einverständnis.

Beschwerden

2005 bearbeitete die Datenschutzbehörde 187 Beschwerden, wovon 134 einen Verstoß gegen das Datenschutzgesetz darstellten. Die anderen

53 gingen auf Ergebnisse und Entscheidungen des Chefinspekteurs zurück. Weitere 16 Beschwerden waren 2004 anhängig und wurden 2005 abgeschlossen.

Von den 150 Beschwerden, die 2005 eingingen, bewertete die Datenschutzbehörde 43 als begründete, 20 als teilweise begründete und 87 als unbegründete Beschwerden. Insgesamt betrafen 37 Beschwerden den öffentlichen Sektor und 112 den Privatsektor.

Im Jahre 2006 gingen bis zum 12. April bei der Datenschutzbehörde 38 Beschwerden ein.

Die Beschwerden hatten den folgenden Inhalt: Missbrauch personenbezogener Daten durch Vertreter von Rentenversicherungsgesellschaften der zweiten Säule. Diese wurden gemeinsam von der Datenschutzbehörde und der Kontrollbehörde für den Finanz- und Versicherungsmarkt untersucht; unerlaubte Herausgabe/Veröffentlichung personenbezogener Daten; Ausmaß und Zweck der Verarbeitung personenbezogener Daten; unerlaubte Videoüberwachung; unerlaubte Offenlegung personenbezogener Daten an Drittparteien und unerlaubte Bereitstellung personenbezogener Daten an Drittparteien.

Überprüfungen

Die Abteilung des Chefinspekteurs nahm 63 Überprüfungen von Dateinverarbeitungssystemen vor.

In Bezug auf die Videoüberwachung öffentlicher Plätze führte die Datenschutzbehörde 28 präventive Überprüfungen bei städtischen Polizeibehörden, Krankenhäusern, Tankstellen, Supermärkten und anderen Plätzen durch. Für alle Mängel wurden geeignete Maßnahmen getroffen, die eine angemessene Umsetzung fanden. In den Fällen, wo kein Gesetzesverstoß festgestellt wurde, erhielten die Datenschutzbeauftragten praktische Empfehlungen für ihre künftigen Tätigkeiten.

Prioritäten: Gesundheitsdaten

Die Hauptpriorität der Datenschutzbehörde für 2006 besteht darin, eine eingehende Untersuchung der Verarbeitung medizinischer Daten vorzunehmen. Das Datenschutzgesetz der Slowakei ist als allgemeine gesetzliche Regelung auf die Verarbeitung personenbezogener Gesundheitsdaten anwendbar. Das Gesetz zur Gesundheitsversorgung enthält – als als spezifische gesetzliche Regelung – detaillierte Beschreibungen der allgemeinen Regelungen.

Abschlussbemerkung

Der Schutz personenbezogener Daten und der Privatsphäre ist eine komplexe, disziplinenübergreifende Angelegenheit. Es ist nicht möglich, die Gesamtheit der Aktivitäten und die aktuellen „heißen" Themen erschöpfend auf einigen wenigen Seiten darzustellen. Die rasche Entwicklung neu aufkommender Technologien und elektronischer Dienste für die Datenverarbeitung führt dazu, dass ein adäquater gesetzlicher Schutz stets einige Schritte hinterherhinkt. Alle diese neuen Technologien, Anwendungen und Systeme müssen aus der Sicht des Datenschutzes kompromisslos bewertet werden.

Wir begrüßen insbesondere die internationale Zusammenarbeit innerhalb der Artikel 29 Arbeitsgruppe, die uns helfen will, den qualitativ besten Datenschutz in unserem Land zu erreichen.

Slowenien

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und weitere Entwicklungen in der Gesetzgebung

Das neue Gesetz zum Schutz personenbezogener Daten wurde am 15. Juli 2004[23] von der Nationalversammlung der Republik Slowenien angenommen. Es trat am 1. Januar 2005 in Kraft. Hauptzweck des neuen Datenschutzgesetzes der Republik Slowenien war die Angleichung an die Bestimmungen der Richtlinie 95/46/EG.

Gemäß dem neuen Gesetz nahm die Nationale Datenschutzbehörde am 1. Januar 2006 ihre Tätigkeit auf.

Am 30. November 2005 nahm die Nationalversammlung der Republik Slowenien das Gesetz über den Leiter der nationalen Datenschutzbehörde[24] an, das am 31. Dezember 2005 in Kraft trat. Das neue Gesetz schuf als neue staatliche Einrichtung den Leiter der nationalen Datenschutzbehörde und legte seine Pflichten und Befugnisse fest.

Die Datenschutzbehörde übernahm zwischen dem 1. Januar 2005 und dem 30. Dezember 2005 wie durch das neue Gesetz gefordert alle Aufgaben und Zuständigkeiten der Überwachungsbehörde unabhängig vom Justizministerium.

Der Leiter der nationalen Datenschutzbehörde ist ein autonomes und unabhängiges staatliches Organ mit den folgenden Zuständigkeiten:

- Entscheidung über die Berufung in Bezug auf die Entscheidung, aufgrund der eine Einrichtung die Beantragung des Zugriffs eines Antragstellers verweigert oder ablehnt oder das Zugriffsrecht oder die Wiederverwendung öffentlicher Informationen in einer anderen Weise verletzt und innerhalb des Rahmens von Berufungsverfahren auch gegen die Überwachung der Umsetzung des Gesetzes zur Regelung des Zugangs zu öffentlichen Informationen und die im Rahmen dieses Gesetzes angenommenen Bestimmungen verstößt;
- Inspektion und Überwachung der Umsetzung des Gesetzes und anderer Regelungen zum Schutz und der Verarbeitung personenbezogener Daten oder des Datentransfers von Slowenien aus sowie die Erfüllung anderer, in diesen Regelungen festgelegten Pflichten;
- Entscheidung über die Berufung einer Einzelperson, wenn der für die Datenverarbeitung Verantwortliche deren Antrag auf Daten, einen Auszug, eine Liste, Prüfung, Bestätigung, Informationen, eine Erklärung Übertragung und das Kopieren von Daten gemäß den Bestimmungen des Gesetzes über den Schutz personenbezogener Daten ablehnt;
- Einreichung eines Antrags an das Verfassungsgericht der Republik Slowenien zur Prüfung der Verfassungsmäßigkeit von Gesetzen, sonstige Verordnungen und allgemeinen Gesetzen, die zur Ausübung der öffentlichen Gewalt erlassen wurden, wenn die Frage der Verfassungsmäßigkeit und Rechtsmäßigkeit in Verbindung mit einem von ihm eingeleiteten Verfahren (in Fällen des Lesezugangs zu öffentlichen Informationen und des Schutzes von personenbezogenen Daten) auftaucht.

Der Leiter der nationalen Datenschutzbehörde ist außerdem Amtsträger, der Verletzungen ahnden muss, ihm obliegt die Überwachung des Gesetzes über den Leiter der Datenschutzbehörde und des Gesetzes über den Schutz personenbezogener Daten.

Der Leiter der nationalen Datenschutzbehörde nahm seine Tätigkeit am 31. Dezember 2006 auf und übernahm die Aufgaben, Zuständigkeiten und Mitarbeiter des früheren Leiters für den Zugang zu öffentlichen Informationen und der ehemaligen Behörde für den Schutz personenbezogener Daten.

Mit der Annahme des Gesetzes über den Leiter der Datenschutzbehörde und der Schaffung der Funktion des Leiters der Datenschutzbehörde wurde die Richtlinie 95/46/EG vollständig in slowenisches Recht umgesetzt.

[23] Staatliches Amtsblatt der Republik Slowenien, Nr. 86/2004

[24] Staatliches Amtsblatt der Republik Slowenien, Nr. 113/2005

Die Richtlinie 2002/58/EG wurde durch das Gesetz über elektronische Kommunikation[25] in slowenisches Recht umgesetzt, das am 9. April 2004 angenommen wurde und am 1. Mai 2004 in Kraft trat. Kapitel X des Gesetzes reguliert überwiegend den Schutz personenbezogener Daten, den Schutz der Privatsphäre und der Vertraulichkeit in elektronischen Kommunikationen.

B. Bedeutende Rechtssprechung

Im Jahr 2005 veröffentlichte die Behörde für den Schutz personenbezogener Daten (nachstehend als die „Behörde" bezeichnet) fünf Entscheidungen, mit denen sie Personen des privaten und öffentlichen Sektors in beschränktem Maße die Befugnis zur Ausführung biometrischer Maßnahmen im Hinblick auf ihre Mitarbeiter erteilte. Die Entscheidungen wurden an vier Banken weitergegeben. Ihnen wurde die Befugnis zur Durchführung biometrischer Maßnahmen an Mitarbeitern mit Zugang zu Finanzangelegenheiten und finanzbezogenen Bereichen sowie Bereichen mit Computerausrüstungen für die Verarbeitung personenbezogener Daten erteilt. Ein Unternehmen für mobile Telekommunikation erhielt ebenfalls die Befugnis, biometrische Maßnahmen in beschränktem Maße an Mitarbeitern durchzuführen, die Zugang zu den Systemumgebungen (Schaltzentralen, Serverräume, Computerzentren) haben.

Die Behörde traf außerdem eine Entscheidung, wonach die Durchführung biometrischer Maßnahmen an allen Mitarbeitern aus dem alleinigen Grund der Speicherung von Abwesenheit oder Anwesenheit am Arbeitsplatz rechtswidrig ist. Es wurde befunden, dass die Speicherung der Ab- oder Anwesenheit am Arbeitsplatz nicht von entscheidender Bedeutung für die Leistung der Tätigkeiten des Unternehmens sei. Die Durchführung biometrischer Maßnahmen würde deshalb einen unverhältnismäßigen und unnötigen Eingriff in die Privatsphäre des Mitarbeiters darstellen, da die Speicherung der Anwesenheit vom Arbeitsplatz auch durch weniger invasive Methoden erfolgen könne.

Im August 2005 beschloss die Behörde das Verbot der Offenlegung von Daten, in denen Wirtschaftsunternehmen aufgelistetet werden, in denen eine mit Namen und/oder Vornamen identifizierbare Person als Vertreter, Vorstandsmitglied, Gründer oder Mitglied des Aufsichtsrates benannt wird. Diese Entscheidung wurde einem Unternehmen mitgeteilt, das derartige Auskünfte an Kunden über das Internet als Bezahldienst anbot. Mit Eingabe des Namens und/oder Vornamens einer natürlichen Person in die Suchmaschine der Unternehmenssoftware würde der Benutzer einen Ausdruck aller Wirtschaftsunternehmen erhalten, in denen die fragliche Person als Vertreter, Vorstandsmitglied, Gründer oder Mitglied des Aufsichtsrates in Erscheinung getreten ist. Das Unternehmen holte diese Informationen vom slowenischen Handelsregister und anderen öffentlich zugänglichen Quellen ein. Die Behörde vertrat in dieser Angelegenheit den Standpunkt, das Unternehmen bediene sich eines neuen rechtwidrigen Speicherungssystems für personenbezogene Daten. Außerdem würde das Unternehmen rechtswidrig an seine Kunden Informationen herausgeben und übermitteln, die Wirtschaftsunternehmen benennen, in denen eine bestimmte Person als Vertreter, Vorstandsmitglied, Gründer oder Mitglied des Aufsichtsrats erscheint, und damit gleichzeitig eine Zweckentfremdung dieser ursprünglich in den öffentlichen Registern eingetragenen personenbezogenen Daten vornehmen. Das Unternehmen reichte eine Klage gegen die Entscheidung der Behörde ein, die vom Verwaltungsgericht mit der Begründung abgelehnt wurde, dass zuerst das Justizministerium mit der Entscheidung der Behörde befasst werden solle, da die Behörde in einer Übergangsphase (bis zur Bildung eines unabhängigen und autonomen Überwachungsorgans) nach wie vor als eine dem Justizministerium unterstehende Behörde anzusehen sei. Gegen die Entscheidung des Verwaltungsgerichts wurde vor dem Obersten Gerichtshof Berufung eingereicht, der entschied, dass das Justizministerium nicht länger die Zuständigkeit innehabe, über Einsprüche gegen die Entscheidungen der Schutzbehörde zu befinden, was wiederum bedeutet, dass ab dem

[25] Staatliches Amtsblatt der Republik Slowenien, Nr. 43/2004 und Nr. 86/2004

1. Januar 2005 die Entscheidungen ausschließlich vor dem Verwaltungsgerichtshof der Republik Slowenien angegangen werden können.

Das Verwaltungsgericht lehnte eine Klage gegen die Behörde in Zusammenhang mit einer Videoüberwachung in einem Mehrfamilienwohnhaus im November 2005 ab. Sie bestätigte die Entscheidung der Behörde, dass bei Zustimmung der Mehrheit der Miteigentümer zu einer Videoüberwachung des Betretens und Verlassens von Mehrfamilienwohnhäusern und der im Gemeinschaftseigentum stehenden Bereiche bei geeignetem Schutz des Filmmaterials in der Tat zulässig sei, dass jedoch eine Echtzeit-Übertragung oder Ausstrahlung des Filmmaterials von Videoüberwachungssystemen über das hauseigene Kabelfernsehen nicht erlaubt sei. Die Ausstrahlung von Videoüberwachungsmaterial über das hauseigene Kabelfernsehen ist ein unverhältnismäßiger und exzessiver Eingriff in die Privatsphäre des Einzelnen, bei der der Schutz personenbezogener Daten vor dem Zugriff durch unbefugte Personen nicht gewährleistet werden kann.

Im Jahre 2005 entschied das Verfassungsgericht, dass das Gesetz über das Referendum und die Öffentliche Initiative in einem Punkt gegen die Verfassung verstößt, da personenbezogene Daten einschließlich Signaturen, die gesammelt wurden, um die Initiative für das Referendum zu unterstützen, Teil des Materials in jedweden Referendumverfahren sind. Es sollte entweder vom Gesetzgeber entschieden werden, dass sie nicht Teil dieser Materialien sind oder dass ihr Schutz in einer anderen Weise garantiert werden sollte. Eine solche Regelung war nicht mit Artikel 38 der Verfassung konform.

In einem anderen Fall aus dem Jahr 2005 entschied das Verfassungsgericht, dass die Bestimmungen des Gesetzes über Wirtschaftsunternehmen nicht verfassungswidrig sind, da sie die obligatorische Veröffentlichung bestimmter personenbezogener Daten von Einzelkaufleuten (unabhängige Unternehmer) – die auch natürliche Personen sind – in ihren Jahresberichten, die der Öffentlichkeit uneingeschränkt zugänglich sind, vorsehen. Diese „Öffentlichkeits"-Bestimmung ist aus der Sicht des Verfassungsgerichts akzeptabel, da sie mit dem Abschließen von rechtsgültigen Verträgen mit Wirtschaftssubjekten in Verbindung steht. Das Verfassungsgericht prüfte die Verhältnismäßigkeit.

Im Jahr 2005 hob das Verfassungsgericht Paragraph 1 und 2 des Artikels 29 des Gesetzes über Zahlungstransaktionen auf, das zum Teil natürliche Personen betrifft, die keine Privatpersonen sind. Die abgeschafften Paragraphen sahen vor, dass das von der Bank von Slowenien kontrollierte Kontenregister Informationen über die Kontoinhaber der Transaktion (bei natürlichen Personen Name und Vorname, Adresse, Kontonummer, Titel und Bankleitzahl, das Transaktionskonto und Informationen über eine möglicherweise negative Kontobilanz) enthält und dass Informationen über die Transaktionskonten öffentlich und auf den Internet-Seiten der Bank von Slowenien zugänglich sind. Das Verfassungsgericht urteilte, dass das Gesetz verfassungswidrig ist, da es den Zweck der Nutzung der Information nicht spezifizierte und darüber hinaus die Möglichkeit zuließ, die erfassten Daten für nicht spezifizierte Zwecke zu benutzen, was per se einen Verstoß gegen Artikel 38 der Verfassung darstellt. In Zusammenhang mit der Entscheidung des Verfassungsgerichts muss an dieser Stelle auch erwähnt werden, dass die Behörde der Bank von Slowenien die Veröffentlichung von Daten über die Inhaber von Transaktionskonten, die keine privaten Personen sind, unmittelbar nach dem Inkrafttreten der angefochtenen Bestimmungen untersagte.

C. Wichtige spezifische Themen

Das mit 1. Januar 2005 in Kraft getretene Datenschutzgesetz spezifiziert im Detail die Bedingungen, unter denen die Videoüberwachung von Eingängen zu Betriebsstätten, Mehrfamilienhäusern und Arbeitsbereichen erlaubt sein kann. Gemäß diesen Bestimmungen benötigen die die Videoüberwachung ausführenden Personen keine Erlaubnis von der Datenschutzbehörde zur Einrichtung einer Videoüberwachung. Personen, die eine Videoüberwachung ausführen, müssen allein dafür Sorge tragen, dass die Einrichtung

einer Videoüberwachung mit den gesetzlichen Bestimmungen konform ist, was bedeutet, über die Ausführung einer Videoüberwachung eine Entscheidung zu treffen, eine angemessene diesbezügliche Mitteilung zu veröffentlichen, die Mitarbeiter schriftlich davon in Kenntnis zu setzen, die Zustimmungen der Miteigentümer des Mehrfamilienhauses einzuholen, die Gewerkschaft zu konsultieren usw. Die Mehrheit der für die Videoüberwachung Verantwortlichen versäumt es indes, ihre Videopraxis an die gesetzlichen Bestimmungen anzupassen, was zu einer Reihe von Beschwerden bei der Behörde führt.

Das neue Datenschutzgesetz schrieb auch Bedingungen vor, unter denen biometrische Maßnahmen erlaubt sind. Diese Maßnahmen können, sofern sie nicht in einem spezifischen Gesetz festgelegt sind, nur in Fällen durchgeführt werden, in denen sie sich bei der Vornahme einer Wirtschaftstätigkeit aus Gründen der Personensicherheit oder des Schutzes von Eigentum oder vertraulicher Daten und Geschäftsgeheimnissen als unbedingt notwendig erweisen. In solchen Fällen müssen die für biometrische Maßnahmen Verantwortlichen der Schutzbehörde eine vorherige Beschreibung der geplanten biometrischen Maßnahmen und die Gründe für deren Einführung übermitteln. Der Gebrauch biometrischer Maßnahmen ist nur nach dem Eintreffen der Einwilligung seitens der Behörde zur Verwendung biometrischer Maßnahmen erlaubt. Hier kam es zu einem Problem, da das Gesetz das Handeln für die Verantwortlichen, die biometrische Maßnahmen bereits vor der Annahme des neuen Gesetzes eingesetzt hatten, nicht festlegte. Diesbezüglich erklärte der Leiter der Datenschutzbehörde, dass solche Aufsichtspersonen der Behörde eine Beschreibung der biometrischen Maßnahmen und die Gründe für ihre Einführung übermitteln müssen, und sie erst dann befugt sind, diese weiter zu gebrauchen, nachdem sie die Entscheidung der Behörde über die Verwendung derselben erhalten haben.

Es gab verschiedentlich Unregelmäßigkeiten bei der vertragsmäßigen Verarbeitung personenbezogener Daten. Die Erfahrung hat gezeigt, dass Verträge zwischen für die Datenverarbeitung Verantwortlichen und vertragsgebundenen Verarbeitern häufig unangemessen sind, da eine spezifische Definition der Kompetenzen des vertragsgebundenen Verarbeiters fehlt. Auch spezifizieren diese Verträge die Prozeduren und Maßnahmen zum Schutz personenbezogener Daten durch den vertragsgebundenen Verarbeiter nur in unzureichender Weise.

Eines der fortbestehenden Schlüsselprobleme im Bereich der personenbezogenen Daten ist auf die Tatsache zurückzuführen, dass die meisten der für die Datenverarbeitung Verantwortlichen der Datenschutzbehörde noch nicht eine Beschreibung ihres Ablagesystems für personenbezogene Daten übermittelt und diese noch nicht in dem von der Datenschutzbehörde verwalteten Register eingetragen haben. Das Register der Ablagesysteme für personenbezogene Daten ist auf der Website des Leiters der Datenschutzbehörde veröffentlicht und erlaubt es jedermann, Informationen der Dateiensysteme der für die Datenverarbeitung Verantwortlichen in der Republik Slowenien, Informationen über von einzelnen, für die Datenverarbeitung Verantwortlichen verwalteten Dateisystemen, Typen von in einzelnen Dateisystemen enthaltenen, personenbezogenen Daten, den Verarbeitungszweck usw. einzusehen.

Das neue Datenschutzgesetz hat der Aufsichtsbehörde für den Schutz personenbezogener Daten die ausdrückliche Befugnis zur Durchführung präventiver Maßnahmen übertragen. In Einklang mit diesen Befugnissen bereitet die Behörde Stellungnahmen, Erläuterungen und Anweisungen in Verbindung mit der Verarbeitung persönlicher Daten in einzelnen Bereichen vor und veröffentlicht diese. Aufgrund von Personalmangel war die Schutzbehörde indes nicht in der Lage, 2005 ihren Zuständigkeiten in vollem Umfang wahrzunehmen.

2006 plant der Leiter der Datenschutzbehörde die Einstellung von sieben zusätzlichen Mitarbeitern im Bereich des Schutzes personenbezogener Daten.

Spanien

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG und weitere Entwicklungen in der Gesetzgebung

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 wurde innerhalb des spanischen Rechts in das verfassungsausführende Gesetz („Ley Orgánica") 15/1999 über den Schutz personenbezogener Daten aufgenommen.

Link: https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf (spanisch)

Der Text des Gesetzes kann in Englisch unter dem folgenden Link abgerufen werden: https://www.agpd.es/upload/Ley Orgánica 15-99_ingles.pdf

Im Laufe des Jahres 2005 wurden weitere Fortschritte bei den Vorbereitungen der Allgemeinen Bestimmungen ausgehend vom Gesetz und den neuen Agenturstatuten, welche die Bestimmungen gemäß dem Königlichen Erlass 428/1993 ersetzen, als Folge der Anwendung des LOPD und der ihm durch das Allgemeine Telekommunikationsgesetz verliehenen Befugnisse erzielt. Es ist wichtig, auf die umfassende Transparenz hinzuweisen, mit der die AEPD diese Arbeit in Angriff genommen hat und die es allen interessierten Sektoren und Bürgern erlaubt, ihre Vorschläge und Stellungnahmen zu unterbreiten. Die Bestimmungen befinden sich zurzeit in der Phase der Überprüfung durch das Justizministerium.

Neben der Entwicklung der Bestimmungen aus dem verfassungsausführenden Gesetz zum Datenschutz wurde der Rechtsrahmen, den dieses Gesetz bietet, um verschiedene allgemeine und sektorale Bestimmungen auf verschiedenen Anwendungsebenen ergänzt, die das Regelwerk der auf den Datenschutz anwendbaren Rechtsnormen umfassen. Von diesen und insbesondere den in 2005 veröffentlichten Regeln müssen die folgenden hervorgehoben werden:

Königlicher Erlass 1553/2005 vom 23. Dezember zur Regelung der Ausgabe von Personalausweisen und Zertifikaten mit digitaler Signatur

Dieser Königliche Erlass wurde nach dem vorausgehenden obligatorischen Bericht von der spanischen Datenschutzagentur veröffentlicht; sein Text beinhaltet den ausdrücklichen Bezug auf das verfassungsausführende Gesetz 15/1999 vom 13. Dezember über den Schutz personenbezogener Daten. Darüber hinaus nahm die Agentur vor der Prüfung der Artikel, die diese Regelung beinhalten, aktiv an der Entwicklung des Projekts für die Umsetzung der DNI Electrónico (Elektronische Personalausweise) als Mitglied des per Entschließung des Ministerrats am 23. Dezember 2004 eigens zu diesem Zweck gebildeten Koordinierungsausschusses teil. Die Agentur war außerdem aktives Mitglied des Technischen Unterstützungsausschusses, der an dieser Frage arbeitete, sowie der Arbeitsgruppe zur Validierung und Orientierung in der Entwicklung der einschlägigen Bestimmungen.

Verfassungsausführendes Gesetz *1/2005 vom 20. Mai,* das die Ratifizierung des Vertrags für eine Europäische Verfassung durch Spanien erlaubt – unterzeichnet am 29. Oktober 2004 in Rom.

Königliche gesetzesvertretende Verordnung („decreto legislativo") 2/2004 vom 5. März, das den geänderten Text des Gesetzes zur Regelung der lokalen Finanzabteilungen billigt.

Regionale Regierungsregelungen:

Erlass 309/2005 vom 18. Oktober, der die Statuten der Baskischen Datenschutzbehörde anerkennt.

Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli über die Verarbeitung personenbezogener Daten und den den Schutz der Privatsphäre in der elektronischen Kommunikation, die das Telekommunikationsgesetz 32/2003 vom 3. November außer Kraft setzt. Dieses Gesetz wird im Königlichen Erlass 424/2005 vom 15. April weiterentwickelt und legt die Bedingungen fest, die für die Bereitstellung elektronischer Kommunikationsdienstleistungen, Universal Service und Benutzerschutz erforderlich sind.

B. Bedeutende Rechtssprechung

Im Jahre 2005 ergingen von der *Audiencia Nacional* (Spanischer Nationaler Oberster Gerichtshof) insgesamt 99 Urteile, wobei Berufungen bei erst- und letztinstanzlichen Gerichten eingereicht wurden. Zwölf Urteile wurden durch den Obersten Gerichtshof gefällt, wobei er über Aufhebungsklagen oder Aufhebungen wegen der Kohärenz der Lehre, und ein Fall einer Aufhebungsklage wurde als nicht statthaft abgelehnt. Dieser Bericht wird sich ausschließlich auf solche Urteile beziehen, in denen bei kontroversen Fragen Präzedenzfälle geschaffen wurden und Aspekte des Datenschutzes zum Tragen kommen, die eine komplexe Auslegung erfordern.

Übermittlung von Daten an das Gericht bei Entlassungsklagen

In dem Urteil vom 19. Oktober 2005 wurde die Berufungsklage gegen die Entscheidung der Agentur abgewiesen, die Schritte, die in einer Klage gegen die Verwendung der Daten des Klägers ohne dessen Zustimmung und die Übermittlung solcher Daten an die Gerichte unternommen wurden, auszusetzen. Die Verwendung von Daten des Klägers durch das beklagte Unternehmen verstößt nicht gegen die Bestimmungen der Datenschutzregelungen, da durch das Unternehmen getroffene Untersuchungsmaßnahmen den Erhalt und die Erfüllung des Arbeitsverhältnisses und die erfolgten Kommunikationen betrafen (Artikel 11.2 des LOPD).

Bearbeitung von medizinischen Unterlagen über Dritte, die im Rahmen der Haftpflichtversicherung zu entschädigen sind

Das Urteil vom 21. September 2005 bestätigte die Entscheidung der Agentur, die eine Versicherungsgesellschaft und ein Diagnosezentrum von der Haftung befreite und befand, dass ihr Handeln nicht gegen Artikel 7.3 des LOPD verstoßen hat. Gemäß den Bestimmungen des Sektors müssen Versicherungsgesellschaften wesentliche formale Verpflichtungen, welche die Verarbeitung personenbezogener Daten des Patienten voraussetzen oder erfordern, erfüllen, und deshalb waren die mitbeklagten Unternehmen von der Aufgabe der Verarbeitung der personenbezogenen Daten des Klägers ohne Einwilligung der betroffenen Person befreit.

Übermittlung der personenbezogenen Daten des Patienten durch die Rückversicherungsgesellschaft

Das Urteil vom 20. Mai 2005 bestätigte die Entscheidung der Agentur, die disziplinarische Maßnahmen gegen eine Rückversicherungsgesellschaft wegen Verstoßes gegen Artikel 11 des LOPD und gegen ein zweites Unternehmen, das den Gesundheitszustand bewertet, gemäß Artikel 6 desselben Gesetzes ergriffen hat. Die Rückversicherungsgesellschaft reichte eine Klage ein, in der behauptet wird, dass sie auf der einen Seite mit der Datenverarbeitung für die Versicherungsgesellschaft beauftragt ist und dass auf der anderen Seite indes keine gesetzeswidrige Übermittlung von Daten an das Unternehmen, das den Gesundheitszustand des Versicherten beurteilte, vorgekommen sind, da dies als Dienstleistung für die Rückversicherungsgesellschaft angesehen wird – beides gemäß Artikel 12 des LOPD. Das Gericht prüfte die Behauptungen und befand, dass die

vorgelegten Dokumente das behauptete Rechtsverhältnis formal nicht belegten. Dementsprechend erging das Urteil, dass eine solche Handlungsweise, die eine Datenübermittlung umfasst, vom Gesetz als nicht erlaubt erachtet wird.

Nichterfüllung der Informationspflicht und Registrierung von Daten in Dateien, welche die erforderlichen Sicherheitsstandards nicht erfüllen

Das Urteil vom 27. April 2005 verwarf die Berufungsklage gegen die Entscheidung der Agentur über die Verletzung von Artikel 5 und 9 des LOPD. Die Informationsanforderung ist ein inhärenter Teil des von der Verfassung anerkannten Grundrechts auf Datenschutz, und aus diesem Grunde wird eine mündliche Information als unzureichend erachtet. Das Gericht fordert deshalb eine schriftliche Unterlage mit einer solchen Information, die der Kläger nicht beibringen konnte. Im Hinblick auf Sicherheitsmaßnahmen waren die in den Bestimmungen über Sicherheitsmaßnahmen (Königlicher Erlass 994/1999 vom 11. Juni) festgelegten Verpflichtungen nicht erfüllt, da weder der „incident log" gemäß Artikel 10 solcher Bestimmungen noch der „carrier log" gemäß Artikel 20 derselben Bestimmungen Anwendung fanden.

Übermittlung und Verarbeitung von Daten in Verträgen für den Transfer von Bankgeschäften

Das Urteil vom 16. Februar 2005 bestätigte die Entscheidung der Agentur und lehnte die Berufung wegen Verstoßes gegen Artikel 11.1 und 6.1 des LOPD ab. Das Gericht teilt, obwohl es die kommerzielle Legitimität des Transfers von Bankgeschäften nicht in Frage stellt, die von der Agentur vertretene Ansicht im Hinblick auf den genannten spezifischen Transfer und vertritt die Auffassung, dass dieser Sachverhalt gemäß dem LOPD eine Übermittlung personenbezogener Daten ist, die in dem vorliegenden Fall den individuellen Bankkontotransfer von einer Kreditinstitut auf ein anderes mittels einer solchen Transaktion umfasst. Und weiter, wenn der Datenempfänger die unwiderrufliche Zustimmung der betroffenen Person nicht geprüft hat, begründet dies einen Verstoß gegen Artikel 6.1 des Gesetzes, und zwar aus dem Grunde, dass der Empfänger einer solchen Mitteilung die Verpflichtung hat, die Bestimmungen gemäß 11.5 dieses Gesetzes zu erfüllen, sobald die Übermittlung erfolgt ist.

Verarbeitung durch Drittparteien und vorgeschriebene Garantien

Das Urteil vom 9. Februar 2005 bestätigte die Entscheidung der Agentur, die disziplinarische Maßnahmen wegen Verstoßes gegen Artikel 6.1 des LOPD auferlegte. Das Bestehen eines Vertrags zwischen dem Kläger und, in diesem Fall, einer staatlichen Universität, in dem es um die Bereitstellung einer bestimmten Dienstleistung geht, fällt unter Artikel 12 des LOPD, vorausgesetzt, dieser Vertrag enthält die in diesem Gesetz verankerten Garantien. Aufgrund der Tatsache, dass der Vertrag nicht explizit die durch den für die Datenverarbeitung Verantwortlichen durchgeführten Sicherheitsmaßnahmen festlegt, dass er nicht den Hinweis enthält, dass die Daten nur gemäß den Anweisungen des für die Datenverarbeitung Verantwortlichen verarbeitet werden dürfen, noch eine Verpflichtung vorgibt, die übermittelten Daten nicht für andere als die in dem benannten Vertrag festgelegten Zwecke zu benutzen und sie nicht an Drittparteien zu übermitteln, entschied das Gericht, dass der Beklagte den Verstoß begangen hat, aufgrund dessen die Disziplinarmaßnahme ergriffen wurde.

Verkauf einer CD-ROM mit Rückwärtssuche

Das Urteil vom 26. Januar 2005 bestätigte die von der Agentur getroffene Disziplinarmaßnahme wegen Verstoßes gegen Artikel 11 des LOPD.

Das Gericht entschied, dass in Anwendung der Bestimmungen über Telekommunikation der Zweck von Telefonbüchern, zu deren eigener Namenseintragung sich die Teilnehmer einverstanden erklären, darin besteht, anhand der Namen und Vornamen die Telefonnummern der Teilnehmer leichter zu finden. Die Nutzung dieser personenbezogenen Daten ist auf diesen spezifischen Zweck beschränkt, was der beabsichtigte Zweck ist, wenn Teilnehmer ihre Zustimmung zur Eintragung ihres Namens in Telefonbücher erteilen. Doch dies ist nicht Zweck, der hinter dem Produkt steht, das unter anderen Funktionen es dem Benutzer ermöglicht, eine Adresse durch Eingabe einer Telefonnummer zu erhalten. Da die betroffene Person ihre Einwilligung für diese Zweckbestimmung nicht erteilt hatte, urteilte das Gericht, dass ein solches Verhalten einen Fall unerlaubter Übermittlung von personenbezogenen Daten darstelle.

C. Wichtige spezifische Themen

Transparenz: Aktivitäten zur Verbreitung von Informationen zum Datenschutz

Eine der Hauptprioritäten der gegenwärtigen AEPD-Verwaltung besteht darin, das Grundrecht auf Datenschutz so weit wie möglich zu verbreiten. Dementsprechend konzentrierte die Agentur 2005 ihre Bemühungen auf dieses Ziel und band ihren Direktor und andere Mitglieder der Agentur in eine breite Palette von Aktivitäten ein. Diese Aktivitäten richteten sich an öffentliche und private Einrichtungen und befassten sich sowohl mit allgemeinen Aspekten des Themas als auch mit spezifischen Fragen für bestimmte Sektoren. Die Agentur beteiligte sich an Kursen, Lesungen, Konferenzen und Kongressen in Zusammenarbeit mit einer Vielzahl von Institutionen, zu denen Berufsverbände, Universitäten, offizielle Handelskammern und öffentliche Verwaltungen zählten.

In Bezug auf diese Aktivitäten verdienen verschiedene Veranstaltungen und Kurse zur Verbreitung der Informationen über die während des Jahres geleistete Arbeit in Zusammenhang mit dem Gesetzgebungsprozess des Datenschutzgesetzes besondere Erwähnung. Neben den zuvor genannten Aktivitäten fanden zahlreiche Treffen mit verschiedenen einschlägigen Akteuren statt, wobei über 150 Interviews in verschiedenen neuen Medien gegeben wurden.

Es wurden Informationen auch im Rahmen anderer Aktivitäten durch das Bürgerunterstützungsbüro verbreitet, das 2005 über 35 500 telefonische Anfragen persönlich, schriftlich oder über die Agentur-Website beantwortete.

Das gleiche Ziel vor Augen, nämlich möglichst viel Wissen über das Thema zu verbreiten, traf die Agentur zehn Kooperationsvereinbarungen zusätzlich zu den vielen anderen aus den Jahren davor mit Universitäten, Verbänden, Stiftungen und einer Vielzahl von Institutionen.

Strafverfolgung: Spam-Bekämpfung

Im Rahmen ihrer Befugnisse zur Bekämpfung von Spam errichtete die Agentur ein neues Verfahren, um dem massiven Versand von E-Mails Herr zu werden. Dieses Verfahren bietet Ratschläge für sicheres Internet-Surfen und Ideen, wie dieses internationale Problem bekämpft werden kann.
Link: https://www.agpd.es/upload/Canal_Documentacion/Lucha_contra_el_Spam/INFORMACIÓN SPAM (V. 30. Mai).pdf

Verfügbar in Englisch:
https://212.170.242.148/upload/English_Resources/INFORMACI%D3N%20SPAM.INGL%C9S%20%28V.%2030%20mayo%29.pdf

Förderung der Selbstregulierung: Verhaltensregeln

Der Verhaltenskodex gemäß Artikel 32 des verfassungsausführenden Gesetzes 15/1999 vom 13. Dezember zielt auf die Anpassung der Bestimmungen des Datenschutzgesetzes an die spezifische Verarbeitung durch die Personen, die diesen Kodex unterstehen.

2005 wurde mit der Agentur eine Änderung des Verhaltenskodex von AUTOCONTROL mit dem Titel „Verhaltenskodex im E-Commerce und bei der interaktiven Werbung" vorgenommen, um den ursprünglichen Wortlaut an die Änderungen wegen des Auftretens neuer technologischer Phänomene wie Spam anzupassen. Alle Mitgliedsorganisationen verpflichteten sich uneingeschränkt, ein umfassendes Selbstregulierungssystem für Werbung und kommerzielle Transaktionen mit Verbrauchern durch sog. Long-distance-Medien innerhalb des Rahmens der Verteidigung der Berufsethik zu schaffen und zu unterstützen.

Aktivitäten in Zusammenhang mit dem „Red Iberoamericana de Protección de Datos" (Iberoamerikanisches Datenschutznetzwerk)

2005 war ein entscheidendes Jahr, da es die Konsolidierung des *Red Iberoamericana de Protección de Datos* (Iberoamerikanisches Datenschutznetzwerk), das 2003 auf eine AEPD-Initiative hin gegründet worden war, brachte. In diesem Jahr basierte das Netzwerk seine Arbeit auf die von den Sonderarbeitsgruppen ausgeführten Aktivitäten und hat nun dank des Netzwerkstrategie-Dokuments ein Instrument für eine optimale Organisation und Vorgehensweise zur Verfügung.

Die 3. lateinamerikanische Datenschutzkonferenz setzte vier Arbeitsgruppen ein: „Netzwerkstrategie", „Die Machbarkeit der Errichtung von Datenschutzbehörden in lateinamerikanischen Ländern", „Zugang zu Personalinformation und Arten des Datenschutzes" und „E-Government und Telekommunikation". Die Gruppen trafen vom 6. bis 9. Juni 2005 in Cartagena de Indias (Kolumbien) zusammen und entwarfen Dokumente zu jedem dieser Themen.

Das Netzwerk zählt derzeit Vertreter aus 17 der 22 Staaten der Gemeinschaft der lateinamerikanischen Länder und wächst durch die stetige Aufnahme neuer Mitglieder weiter.

Schweden

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie weitere Entwicklungen in den Gesetzgebungen

In Schweden wurde die EU-Richtlinie 95/46/EG durch das Datenschutzgesetz (1998:204) (PDA), das am 24. Oktober 1998 in Kraft trat, umgesetzt. Das PDA wird durch den Datenschutzbeschluss vervollständigt, der am gleichen Tag in Kraft trat. Das Gesetz und auch die Richtlinie finden auf die automatisierte und manuelle Datenverarbeitung Anwendung. Jedoch kommen die grundsätzlichen Regelungen zur Datenverarbeitung und zum erlaubten Zeitraum einer solchen Verarbeitung nicht vor dem 1. Oktober 2007 zur Anwendung, insbesondere was die manuelle Datenverarbeitung betrifft, die vor dem Inkrafttreten des Datenschutzgesetzes begonnen wurde. Das Gesetz gilt zwar grundsätzlich für die Verarbeitung privater Daten in allen Bereichen der Gesellschaft, jedoch gibt es in bestimmten Bereichen mehrere spezielle Gesetze und Beschlüsse für die Datenverarbeitung, entweder anstelle des Datenschutzgesetzes oder ergänzend zu diesem. Auch beim Entwurf dieser Sondergesetze und -beschlüsse wurde der Richtlinie Rechnung getragen.

Im Achten Jahresbericht wurde der Vorschlag des mit der Überprüfung des Datenschutzgesetzes befassten Untersuchungsausschusses vorgelegt, der klären sollte, ob ein „Missbrauchsmodell" auf das Datenschutzgesetz angewandt werden könnte. In dem Vorschlag ging es vor allem darum, die Verarbeitung personenbezogener Daten in unstrukturiertem Material, wie z. B. fortlaufendem Text, Ton und Bild, von der großen Mehrheit der Datenhandhabungsregeln des Datenschutzgesetzes auszunehmen. Diese Regeln würden demnach keine Anwendung auf alltägliche Verarbeitungen, wie etwa das Schreiben durchgehender Texte mit einem Textverarbeitungsprogramm finden. Es würde stattdessen eine einfache Regel gelten: Die Datenverarbeitung ist nicht erlaubt, wenn sie einen unangemessenen Eingriff in die Privatsphäre darstellt. Der Vorschlag wird zurzeit weiter beim Justizministerium bearbeitet, und es wird erwartet, dass die Regierung in der ersten Hälfte 2006 einen Gesetzentwurf vorlegen wird, der solche Abänderungen enthält.

Die EU-Richtlinie 2002/58/EG wurde mit Inkrafttreten des Gesetzes über die elektronische Kommunikation (2003:389) (ECA) am 1. Juli 2003 in schwedisches Recht übertragen. In Kapitel 6 dieses Gesetzes stehen Datenschutzregeln für den elektronischen Kommunikationssektor. Die Einhaltung der Datenschutzbestimmungen des Gesetzes wird vom Staatlichen Post- und Fernmeldeamt überwacht. Artikel 13 der EU-Richtlinie über unerwünschte E-Mails wurde durch die Abänderung des Gesetzes zu Marketingpraktiken (1995:450) umgesetzt. Diese Änderungen traten am 1. April 2004 in Kraft. Das Gesetz zu Marketingpraktiken untersteht der Aufsicht der Verbraucheragentur.

In den vergangenen Jahren haben verschiedene Untersuchungsausschüsse zahlreiche Vorschläge unterbreitet, die darauf abzielen, die Bekämpfung von Verbrechen zu erleichtern (mehrere verschiedene Vorschläge 2005). Diese Vorschläge befassen sich mit verschärften Zwangsmaßnahmen und besseren Möglichkeiten zur Erhebung und Aufzeichnung personenbezogener Daten. Folgende Vorschläge mögen als Beispiele dienen: Vorschlag zum verstärkten Gebrauch von Zwangsmaßnahmen im Zusammenhang mit der Informationstechnologie (Ds 2005:6), Vorschlag zum verstärkten Gebrauch von Zwangsmaßnahmen zur Verhinderung von Schwerverbrechen (Ds 2005:21), Vorschlag zu geheimen Abhörmaßnahmen (Memorandum des Justizministeriums) und Vorschlag zum Zugang zu elektronischer Kommunikation bei der Aufklärung von Verbrechen (SOU 2005:38). Die Vorschläge wurden verschiedenen Behörden und Organisationen zur Beratung vorgelegt. In einer Stellungnahme vom Dezember 2005 erklärte die Datenschutzbehörde,

dass eine umfassende Bewertung, die sämtliche Auswirkungen der Vorschläge in Betracht ziehe, für den Gesetzgeber unerlässlich sei, bevor zu überlegen sei, welche Vorschläge angenommen werden sollten.

Im Juni 2004 wurden Vorschläge zu einem umfassenderen Gebrauch der DNA bei der Strafverfolgung unterbreitet. Ab 1. Januar 2006 können die DNA-Daten aller in Schweden Verurteilten – ausgenommen jener, die nur zu einer Geldstrafe verurteilt wurden – in eine DNA-Datei aufgenommen werden. Bis dahin war es nur erlaubt, die „genetischen Fingerabdrücke" von Personen zu speichern, die zu Gefängnisstrafen von mehr als zwei Jahren verurteilt wurden. Nach der neuen Gesetzgebung können auch die DNA-Analysedaten von jenen Personen, die zwar nicht rechtskräftig verurteilt wurden, aber eines Verbrechens verdächtigt werden, das eine Gefängnisstrafe nach sich ziehen würde, in einer sogenannten Ermittlungsdatei gespeichert werden. Falls diese Person wegen eines Verbrechens verurteilt wird, müssen die Daten aus der Ermittlungsdatei gelöscht werden und stattdessen in der DNA-Datei gespeichert werden. Wenn die Ermittlungen nicht zu einer Anklage führen, sollten die Daten aus der Datei gelöscht werden. Dasselbe gilt, wenn etwa die Anklage fallen gelassen wird.

B. Bedeutende Rechtsprechung

Über die Veröffentlichung personenbezogener Daten im Internet wurde erneut vor schwedischen Gerichten verhandelt. In diesem Fall hatte der Direktor eines Internats ohne Zustimmung Informationen über einen Angestellten auf der Internetseite des Internats veröffentlicht. Die Informationen enthielten personenbezogene Daten über den Angestellten, etwa dass er Schwierigkeiten bei der Zusammenarbeit mit Kollegen habe und dass er krankgeschrieben sei. Wie im vorhergehenden Fall befanden die Gerichte, dass hier personenbezogene Daten veröffentlicht wurden, deren Verarbeitung unter die Richtlinie fällt. Der Fall wurde vor den Obersten Gerichtshof gebracht, der in seiner richterlichen Entscheidung vom 26. Mai 2005 feststellte, dass die vorliegenden Umstände denen des Falles Lindqvist (C-101/01) entsprachen und daher die Auslegung des Europäischen Gerichtshofs beinhaltete, dass die Anklage in Bezug auf die verbotene Übermittlung personenbezogener Daten in Drittländer zurückgewiesen werden sollte. Der Direktor wurde jedoch wegen Zuwiderhandlung gegen das Datenschutzgesetz aufgrund der Weitergabe sensitiver Daten verurteilt.

Im Juni 2004 entschied das Komitee der Datenschutzbehörde, dass die Sammlung und Verarbeitung von Fingerabdrücken von Schülern für die Zugangsprüfung zur Schulkantine nicht angemessen und sachdienlich sei, und zwar ungeachtet der Tatsache, dass die Einverständniserklärung der Schüler eingeholt werde. Es wurde dargelegt, dass die Prüfung auf eine Art und Weise durchgeführt werden könnte, ohne derart in die Privatsphäre einzudringen. Gegen die Entscheidung der Datenschutzbehörde wurde beim zuständigen Verwaltungsgericht Berufung eingelegt, das im März 2005 die Entscheidung bestätigte. Der Fall wurde dann vor den Verwaltungsgerichtshof gebracht, der die Entscheidung der Vorinstanz aufhob und erklärte, dass das Bedürfnis der Gemeinde nach einem einfachen Prüfsystem höher zu bewerten sei als der Schutz der Privatsphäre der Schüler. Im November 2005 wurde die Rechtssache von der Datenschutzbehörde vor den Obersten Verwaltungsgerichtshof gebracht, wo sie noch anhängig ist.

Im Frühjahr 2005 erreichten die Datenschutzbehörde zahlreiche Beschwerden, die das Schwedische Amt für Produktpiraterie („das Amt") beschuldigten, in großem Umfang Daten gesammelt und benutzt zu haben, insbesondere IP-Adressen in Verbindung mit gemeinsamem Datenzugriff (Filesharing) von urheberrechtlich geschütztem Material im Internet. Die Datenschutzbehörde untersuchte die verarbeiteten personenbezogenen Daten des Amtes

und fand heraus, dass ein Teil der von dem Amt verarbeiteten Daten sich auf strafbare Handlungen im Sinne von Abschnitt 21 Datenschutzgesetz bezieht und daher die Bestimmungen dieses Abschnitts verletzt. Gemäß Abschnitt 21 ist es allen Parteien, außer Behörden, unter anderem untersagt, personenbezogene Daten zu verarbeiten, die Rechtsverletzungen und strafbare Handlungen einschließen. Das Amt beantragte dann für sich eine Ausnahmeregelung zu den Bestimmungen aus Abschnitt 21 Datenschutzgesetz, um die IP-Adressen zu verarbeiten, bei der Polizei Anzeige zu erstatten und Verfahren wegen besonders schwerer Urheberrechtsverletzungen einzuleiten, Internetdienstanbieter über die Verletzungen ihrer Teilnehmer zu informieren und zivilrechtliche Klagen gegen sie anzustrengen. Im Oktober 2005 entschied die Datenschutzbehörde zugunsten des Amtes eine Aufhebung des Verbots der Datenverarbeitung von IP-Adressen von Personen zuzulassen, die urheberrechtlich geschütztes Material Dritten gegenüber zugänglich machen. Die Behörde entschied zudem, dass diese Regelung bis auf Weiteres gilt, jedoch nicht länger als bis zum 31. Dezember 2006.

C. Wichtige spezifische Themen

Die Datenschutzbehörde hat bestimmte Aufsichtstätigkeiten in Form spezifischer oder thematischer Projekte fortgesetzt. 2005 wurden drei Überwachungsberichte veröffentlicht: *Verbesserter Zugang zu Patientendaten* (2005:1), *Bonus Cards und das Datenschutzgesetz* (2005:2) und *Überwachung der Nutzung von Internet und E-Mail durch Arbeitnehmer* (2005:3).

Die Behörde hat auch andere Druckschriften veröffentlicht, wie etwa die Broschüre *Personenbezogene Daten – welche Regeln gelten?* (zusammen mit dem Schwedischen Zentralamt für Gesundheitswesen und Sozialfürsorge und dem Schwedischen Statistischen Amt) und ein Informationsblatt zu *Rechtsverletzungen im Internet*.

Darüber hinaus standen 2005 die biometrischen Daten im Mittelpunkt der öffentlichen Diskussion. Ab 1. Oktober 2005 enthalten alle neuen schwedischen Pässe einen Mikrochip, auf dem ein digitales Passfoto und die Unterschrift gespeichert sind. Es wurden zudem Personalausweise eingeführt, die die gleichen digitalisierten Informationen enthalten. In Zukunft ist auch die Speicherung von Fingerabdrücken in Pässen und Personalausweisen vorgesehen.

Ein weiteres Thema, das im Jahr 2005 bezüglich der Privatsphäre Anlass zu lebhaften Diskussionen gab, war eine Maut oder Steuer für Autos, die Stockholms Innenstadt durchqueren. Sie wurde versuchsweise für ein halbes Jahr eingeführt. Wegen der Überwachungskameras, die die Nummernschilder der Autos registrieren, gab es Datenschutzbedenken.

Was die Selbstregulierung betrifft, gab die Datenschutzbehörde Stellungnahmen zu zwei Vorschlägen über Verhaltensregeln ab. Eine bezog sich auf die Verarbeitung personenbezogener Daten bei Schulfotos und die andere auf personenbezogene Daten im Zusammenhang mit Inkassoaufträgen.

Nach der Annahme der *Richtlinie über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden*, kündigte der schwedische Justizminister für das Frühjahr 2006 einen Untersuchungsausschuss zur Überprüfung der innerstaatlichen Rechtsvorschriften auf diesem Gebiet an, um gemeinsam mit den Diensteanbietern die erforderlichen Änderungen vorzuschlagen.

Vereinigtes Königreich

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie weitere Entwicklungen in den Gesetzgebungen

Die *Richtlinie 95/46/EG* wurde als Datenschutzgesetz 1998, das am 1. März 2000 in Kraft trat, in das Recht des Vereinigten Königreichs umgesetzt.

Die *Richtlinie 2002/58/EG* wurde als Gesetz über den Datenschutz und elektronische Kommunikation, das am 11. Dezember 2003 in Kraft trat, in das Recht des Vereinigten Königreichs umgesetzt.

B. Bedeutende Rechtsprechung

2005 gab es keine bedeutende Rechtsprechung bei den Gerichten des Vereinigten Königreichs, die sich auf 95/46/EG und 2002/58/EG bezogen hätte.

Im Oktober 2005 entschied das Amt für Datenschutz (Information Tribunal) in einem vom Datenschutzbeauftragten angestrengten Fall gegen die Polizei von West Yorkshire, South Yorkshire und North Wales. Der Beauftragte vertrat die Meinung, dass die Aufbewahrung von alten Schuldsprüchen bei Bagatelldelikten den dritten und fünften Grundsatz des Datenschutzgesetzes verletzte, da die Frist zur Speicherung für diesen Zweck als zu lange angesehen werden müsse. Das Amt für Datenschutz entschied, dass aus polizeilichen Erwägungen Informationen aufbewahrt werden können, und zwar für eine Dauer von sechs Monaten, ein Zugriff hierauf jedoch nur für leitende Polizeibeamte bestehen dürfe.

C. Wichtige spezifische Themen

Der Datenschutzbeauftragte setzt eine neue Strategie ein in Bezug auf gesetzgeberische Maßnahmen und konzentrierte sich auf jene für die Datenverarbeitung Verantwortliche, deren mangelnde Umsetzung des Datenschutzes einerseits schwere Folgen für Einzelpersonen oder andererseits weniger gravierende für weite Bevölkerungskreise hat. Gesetzgeberische Maßnahmen werden eingeleitet, wo personenbezogene Daten auf dem Spiel stehen, weil Verpflichtungen absichtlich oder fortdauernd missachtet werden, Beispiele gegeben oder Fragen geklärt werden müssen. Der Datenschutzbeauftragte setzte auch ein Prüfungsteam ein, welches bei Firmen die Einhaltung der Anforderungen für bewährte Verfahren überprüft und das mit seinen ersten Audits 2005 begann.

Das Büro des Datenschutzbeauftragten begann mit der Veröffentlichung einer Reihe von benutzerfreundlichen Leitfäden unter dem Namen „Good Practice Notes". Sie wurden konzipiert, um den Datenschutz zu vereinfachen, indem verbreitete Missverständnisse ausgeräumt und häufig gestellte Fragen beantwortet werden. Behandelte Themen in dieser fortlaufenden Serie sind z. B. E-Mail-Marketing, Kontoinformationen gegenüber Dritten, Videoüberwachung sowie Auskünfte über Mieter. Das Büro veröffentlichte auch eine überarbeitete Zusammenfassung seiner Regeln zur Einstellungspraxis (Employment Practices Code), die Arbeitgebern helfen soll, das Datenschutzgesetz zu verstehen und umzusetzen. In diesen Regeln werden die Arbeitgeber auf wichtige Themen hingewiesen und bekommen Tipps, was zu tun ist. Vier Hauptgebiete werden dabei behandelt: Personalauswahl und -einstellung, Personalunterlagen, Überwachung am Arbeitsplatz und gesundheitsbezogene Informationen. Eine Kurzfassung, die auf die Belange kleinerer Unternehmen eingeht, wurde ebenfalls erstellt.

Der Datenschutzbeauftragte gab erstmals durch die Verwendung von verbindlichen unterneh-

mensinternen Vorschriften (Binding Corporate Rules) seine Zustimmung zur Übermittlung von personenbezogenen Daten in ein Land, das nicht zum Europäischen Wirtschaftsraum gehört. Dem Unternehmen General Electric wurde gestattet, Arbeitnehmerdaten innerhalb der Unternehmensgruppe General Electric vom Vereinigten Königreich aus zu übermitteln.

Der Datenschutzbeauftragte nahm an Konferenzen mit den für das Projekt einer elektronischen Patientenakte („Connecting for Health") verantwortlichen Vertretern des Gesundheitsministeriums teil und beriet sie zu spezifischen Problemen. Er besuchte auch Arbeitsgruppen, die sich auf diesem Gebiet um einen Informationsaustausch mit der Politik bemühen und die den Sozialarbeitern das Wissen darüber vermitteln wollen, mit welcher Art von System sie nach Umsetzung des Projekts zu rechnen haben. „Connecting for Health" wird stufenweise umgesetzt und weitere Planungen werden mit dem Datenschutzbeauftragten abgestimmt.

Der Datenschutzbeauftragte diskutierte das Thema RFID (Radiofrequenzidentifikation) mit Ofcom, der Regulierungsbehörde für den Telekommunikationsmarkt, bereits vor Anhörung der Ofcom über die Frage, ob RFID von den Zulassungsbestimmungen für Funkfrequenzen befreit werden könne. Der Beauftragte bemerkte, dass bei der Verwendung von RFID in vielen Fällen keine personenbezogenen Daten beteiligt seien und daher das Datenschutzgesetz 1998 nicht anwendbar sei. Bei der Verarbeitung personenbezogener Daten sollte der Einhaltung des Gesetzes nichts im Wege stehen.

Der Datenschutzbeauftragte äußerte wiederholt Bedenken über die Vorschläge zur Einführung eines Personalausweises im Vereinigten Königreich, vor allem darüber, dass die Maßnahmen in Bezug auf die als Grundlage dienende nationale Personaldatenbank (National Identity Register) sowie auf die hinterlassene Datenspur bei Personenidentitätsprüfungen ein unnötiges und unverhältnismäßiges Eindringen in die persönliche Privatsphäre riskieren. Die Gespräche zwischen dem Datenschutzbeauftragten und dem Innenministerium über die Vorschläge zur Einführung eines Personalausweises wurden über das ganze Jahr 2005 fortgesetzt.

Im November veranstaltete der Datenschutzbeauftragte eine internationale Konferenz zur Feier des 21. Jahrestages des Datenschutzgesetzes im Vereinigten Königreich und nutzte die Gelegenheit zum Ausblick auf die nächsten 21 Jahre. Bei dieser Konferenz wurde auch Francis Aldhouse, Stellvertreter des Datenschutzbeauftragten seit der Eröffnung des Amtes im Jahre 1984, in den Ruhestand verabschiedet.

2005 unterrichtete der Datenschutzbeauftragte die nachstehenden parlamentarischen Ausschüsse:

- Untersuchung des Ausschusses Europäische Union über den Vorschlag für eine Verordnung zur Errichtung einer Agentur der Europäischen Union für Grundrechte
- Untersuchung des Ausschusses Bildung und Qualifikationen über „Every Child Matters" (Regierungsinitiative zur Verbesserung der Lebensgrundlagen für Kinder und Jugendliche bis zu 19 Jahren)
- Gemeinsame Untersuchung des Ausschusses für Verfassungsangelegenheiten und des Büros des Vizepremierministers: Ausschuss für Wohnungswesen, Planung, Kommunalverwaltungen und Regionen über die Eintragung ins Wählerverzeichnis

2005 beantwortete der Datenschutzbeauftragte die nachstehenden Anfragen:

- Gesetzesvorlage zu gemeinsamen Prüfungen von Einrichtungen für den Schutz und die Fürsorge von Kindern, „Joint Inspections of

Children's Services and Inspection of Social Work Services (Scotland) Bill", Oktober 2005
- Konsultationspapier des Nordirlandbüros über mehr Sicherheit bei Personaleinstellungen in Nordirland, „Safer Recruitment in Northern Ireland"
- Konsultationspapier zum Informationsprogramm zur Förderung der psychischen Gesundheit, „A Mental Health Information Strategy for Scotland"
- Beratung des Ministeriums für Bildung und Qualifikationen über Beratung quer durch alle Politikbereiche: Informationsaustausch über Kinder und junge Leute, „Cross-government Guidance: Sharing Information on Children and Young People"
- Beratung des gemeinsamen Lenkungsausschusses Geldwäsche zur Unterbindung der Geldwäsche/ Bekämpfung der Finanzierung von Terrorismus: Beratung des Finanzsektors des Vereinigten Königreichs

Kapitel 3

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. DIE EUROPÄISCHE KOMMISSION

Am 16. Februar 2005 entschied die Europäische Kommission, die Zuständigkeit für das Referat Datenschutz von der Generaldirektion Binnenmarkt und Dienstleistungen auf die Generaldirektion Freiheit, Sicherheit und Recht zu übertragen, damit die Aktivitäten der Kommission auf diesem Gebiet besser wahrgenommen und aufeinander abgestimmt werden. Mit dieser Übertragung wird das Referat Datenschutz die Zusammenarbeit und die Kohärenz der Tätigkeiten der Kommission in den Bereichen Freiheit, Sicherheit und Recht gewährleisten und die bürgerlichen Grundrechte, insbesondere das Recht auf den Schutz personenbezogener Daten, sichern. Diese Entscheidung trat am 15. März 2005 in Kraft.

3.1.1. Entscheidungen

Entscheidung Fluggastdatensätze Kanada

Entscheidung der Kommission vom 6. September 2005 über den angemessenen Schutz von personenbezogenen Daten in Fluggastdatensätzen, die an die kanadischen Grenzbehörden (Canada Border Services Agency) übermittelt werden.

Am 6. September 2005 erließ die Kommission eine Angemessenheitsentscheidung, in der sie feststellte, dass die kanadischen Grenzbehörden einen angemessenen Schutz auf der Basis der als Anhang beigefügten Verpflichtungserklärung für aus der Gemeinschaft übermittelte Fluggastdaten für Flüge nach Kanada bieten. Die Entscheidung wird nach Benachrichtigung der Mitgliedstaaten in Kraft treten.

Die Entscheidung ist Teil eines Pakets, das aus der Entscheidung des Rates über ein Abkommen mit Kanada bezüglich des Transfers von Fluggastdaten an die kanadischen Grenzbehörden und einer Verpflichtungserklärung der kanadischen Grenzbehörden zur Behandlung der Daten besteht. Diese Verpflichtungserklärung wurde in das kanadische Recht aufgenommen.

Gemeinsame Überprüfung der Fluggastdaten/USA

Die Verpflichtungen, wie im Anhang der Entscheidung der Kommission über den angemessenen Schutz personenbezogener Daten in den Fluggastdatensätzen niedergelegt, die an die US-Zoll- und Grenzschutzbehörden (CBP) weitergeleitet werden, gewährleisten eine gemeinsame Überprüfung der Durchführung der Verpflichtungen durch CBP und durch die Kommission im Hinblick auf ein beiderseitiges Bemühen um ein wirksames Funktionieren des in den Verpflichtungen beschriebenen Verfahrens.

Die erste Überprüfung fand am 20. und 21. September 2005 in Washington statt. Außer der Kommission waren Vertreter des Datenschutzes der Mitgliedstaaten und der Strafverfolgungsbehörden anwesend. Die Überprüfung bestand aus einem auf der Grundlage der Verpflichtungen basierenden Fragenkatalog, der detaillierte Fragen sowie die in Bezug auf die Verpflichtungen mit CBP zu besprechenden Themen enthielt, Ortsbesichtigungen bei CBP, um der gemeinsamen Überprüfungsgruppe der EU einen Echtzeitzugang zu Fluggastdaten zu verschaffen, ein ganztägiges Treffen zwischen CBP, der gemeinsamen EU-Überprüfungsgruppe und dem „Privacy Office" des Ministeriums für Heimatschutz, um über Einzelheiten der getroffenen Maßnahmen und beschlossenen Verfahren zu sprechen und um somit einen Überblick über die eingegangenen Verpflichtungen zu erhalten.

Das gesamte Überprüfungsteam der EU befand, dass die CBP die Verpflichtungsbedingungen an den Tagen der gemeinsamen Überprüfung (am 20. und 21. September 2005), in erheblichem Umfang erfüllt. Das EU-Team stellte auch fest, dass es bis zu deren vollständiger Befolgung noch einige Zeit dauerte und dass die CBP dafür umfangreiche Unterstützung vom „Privacy Office" des

Ministeriums für Heimatschutz erhielt. Einen zur Veröffentlichung bestimmten Bericht findet man auf der Internetseite der Generaldirektion Justiz, Freiheit und Sicherheit.

„Safe Harbor", Seminar „Safe Harbor" („Sicherer Hafen")

Am 7. Dezember 2005 wurde in Washington ein von der Artikel 29-Datenschutzgruppe und dem US-Handelsministerium gemeinsam veranstaltetes Seminar durchgeführt. Zweck dieses Seminars war es, der „Safe Harbor"-Regelung die Unterstützung durch die Artikel-29-Gruppe und das Handelsministerium zuzusichern, um US-Organisationen zu ermutigen, sich an die Vorschriften von „Safe Harbor" zu halten und die Probleme bei der Umsetzung von „Safe Harbor" anzugehen, die im Arbeitsdokument der Kommissionsdienststellen 2004 über die Durchführung von „Safe Harbor" angesprochen wurden (Bericht der Kommission 2004). Das Seminar erwies sich als eine hervorragende Gelegenheit, Datenschutzprobleme im Zusammenhang mit „Safe Harbor" und anderen internationalen Datenübermittlungen mit US-amerikanischen Organisationen und Behörden zu diskutieren. Es zeigte das Interesse von Unternehmen an Problemen bei internationalen Datentransfers und insbesondere das wachsende Interesse von US-Organisationen an „Safe Harbor" als Instrument der Übermittlung personenbezogener Daten von der EU in die Vereinigten Staaten, was durch die Anzahl der „Safe Harbor" beitretenden Organisationen belegt wird. Das Seminar gab der Kommission sowie der Artikel-29-Gruppe Gelegenheit zum Meinungsaustausch über Fragen wie die Umsetzung des „sicheren Hafens" bei den für die Durchführung von „Safe Harbor" zuständigen US-amerikanischen Organisationen, nämlich der Federal Trade Commission (Kartellbehörde) und dem Handelsministerium. Die meisten Teilnehmer sowie die US-Behörden hielten die Vorbereitung eines weiteren Seminars 2006 in Brüssel für nützlich, um Fragen zur internationalen Datenübermittlung zu diskutieren.

3.1.2. Legislativvorschläge

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt[26]

Dieser Vorschlag der Kommission vom 1. Dezember 2005 dient der Einführung eines vereinheitlichten Rechtsrahmens für einen integrierten Zahlungsverkehrsmarkt in der EU, der grenzüberschreitende Zahlungen innerhalb der Gemeinschaft erleichtern wird. Der Vorschlag sieht vor, dass eine Genehmigung der Mitgliedstaaten zur Verarbeitung von personenbezogenen Daten durch Zahlungssysteme und Zahlungsdienstleister erforderlich ist, wenn dies der Vorbeugung, Ermittlung, Aufdeckung und Verfolgung von Betrug im Zahlungsverkehr dient. Gemäß diesem Vorschlag wird die Verarbeitung der personenbezogenen Daten in Übereinstimmung mit der Richtlinie 95/46/EG durchgeführt.[27]

Schengener Informationssystem der zweiten Generation – SIS II

Am 31. Mai 2005 legte die Kommission ein Paket gesetzgeberischer Maßnahmen zum Aufbau der zweiten Generation des Schengener Informationssystems (SIS II) vor. Das Gesetzgebungspaket wird die derzeitigen Bestimmungen zu SIS im Schengener Durchführungsübereinkommen ersetzen (Artikel 92-119).

SIS ist ein gemeinsames Informationssystem zur Zusammenarbeit zwischen den zuständigen Behörden der Mitgliedstaaten durch Austausch von Informationen zur Umsetzung verschiedener Maßnahmen zwecks Schaffung einer Zone ohne Kontrollen an den Binnengrenzen. Diese Behörden erhalten durch ein automatisiertes Abfragesystem Informationen über Personen und Gegenstände, das vor allem für die polizeiliche und justizielle Zusammenarbeit in Strafsachen sowie für die Personenkontrolle an den Außengrenzen oder den

[26] KOM(2005) 603 endgültig, 1.12.2005

[27] Art. 71 des Vorschlags

nationalen Grenzen und für die Erteilung von Visa und Aufenthaltsgenehmigungen genutzt wird.

Die drei Vorschläge sind eine Weiterentwicklung des Schengen-Besitzstands[28], der am 1. Mai 1999 durch ein Zusatzprotokoll zum Vertrag von Amsterdam in den rechtlichen Rahmen der EU aufgenommen wurde. Obwohl die Vorschläge auf verschiedenen Bestimmungen und gesetzgebenden Verfahren (Mitentscheidung und Anhörung des Europäischen Parlaments) des Vertrags über die Europäische Union oder des EG-Vertrags beruhen, sind sie ein untrennbarer Teil des Pakets, da SIS II als ein eigenständiges Informationssystem anzusehen ist. Die Kommission hat betont, dass die Vorschläge bis Mitte 2006 angenommen sein müssen, damit der Start des Systems 2007 gewährleistet ist.

Zweck dieses Pakets ist die Aktualisierung des bestehenden Systems, um den neuen Mitgliedstaaten ab 2007 die volle Anwendung des Schengen-Besitzstands zu ermöglichen und die Kontrolle ihrer Binnengrenzen aufzuheben. Gleichzeitig wird der Funktionsumfang des Systems erweitert, z. B. Verarbeitung biometrischer Merkmale, Zugang für Europol und Eurojust, neue Bestimmungen in Bezug auf die Verknüpfung von Ausschreibungen zur Einreiseverweigerung.

Die Gesetzgebungsvorlagen enthalten Bestimmungen zum Datenschutz, die die bestehenden EU-Regelungen in dieser Hinsicht berücksichtigen. Dadurch unterliegen die Angelegenheiten der ersten Säule der Richtlinie 95/46/EG. Die unter Artikel 28 Absatz 1 der Richtlinie benannten Datenschutzbehörden sind für die Überwachung der Rechtmäßigkeit bei der Verarbeitung von SIS-II-Daten in ihrem Hoheitsgebiet zuständig. Verordnung 45/2001 gilt für die Tätigkeiten der Kommission, die für den Betrieb und die Funktionstüchtigkeit des Systems verantwortlich ist. Der Europäische Datenschutzbeauftragte überwacht diesen Prozess. Der Vorschlag sieht auch die aktive Zusammenarbeit der nationalen Datenschutzbehörden mit dem Europäischen Datenschutzbeauftragten vor.

Im Hinblick auf die Gesichtspunkte, die den Geltungsbereich von Titel VI des EU-Vertrags (dritte Säule) berühren, wird der Schutz personenbezogener Daten durch die Mitgliedstaaten gemäß Übereinkommen Nr. 108 des Europarats ausgeführt. Nationale unabhängige Behörden sollen die Rechtmäßigkeit des Verfahrens auf ihrem Hoheitsgebiet überwachen. Was die von Europol und Eurojust verarbeiteten Daten betrifft, so werden die gemeinsame Kontrollinstanz von Europol und die gemeinsame Kontrollinstanz von Eurojust die Rechtmäßigkeit der Tätigkeiten dieser Organe sicherstellen. Verordnung 45/2001 gilt für die Tätigkeiten der Kommission, die für den Betrieb und die Funktionsfähigkeit des Systems verantwortlich ist. Der Europäische Datenschutzbeauftragte soll diesen Prozess überwachen. Der Vorschlag bestimmt ebenfalls, dass die nationalen Datenschutzbehörden aktiv mit dem Europäischen Datenschutzbeauftragten zusammenarbeiten.

Visa-Informationssystem (VIS)

Um die Entscheidung 2004/512/EC zur Einrichtung des Visa-Informationssystems umzusetzen, hatte die Kommission am 28. Dezember 2004 einen Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) sowie den Austausch von Daten über Visa für einen kurzfristigen Aufenthalt zwischen Mitgliedstaaten vorgelegt. Der Vorschlag sieht eine Datenbank für kurzfristige Aufenthalte im Schengengebiet und Bestimmungen über den Informationsaustausch zwischen Mitgliedstaaten vor. Er enthält Bestimmungen über die zu verarbeitenden Daten (z. B. biometrische Daten), Bedingungen für den Informationsaustausch und Regeln zum Schutz personenbezogener Daten, die im VIS verarbeitet werden.

[28] Übereinkommen zur Durchführung des Übereinkommens von Schengen und weitere Bestimmungen, hauptsächlich Beschlüsse des Exekutivausschusses zur Durchführung dieses Übereinkommens (und folgende, nach der Eingliederung des Schengen-Besitzstands in den Rechtsrahmen der Europäischen Union angenommene Instrumente der EU).

Beschluss über den Zugang zum Visa-Informationssystem

Bei seiner Tagung am 7. März 2005 ersuchte der Rat die Kommission, den für die innere Sicherheit verantwortlichen Behörden der Mitgliedstaaten den Zugang zu VIS zu garantieren„um bei der Ausübung ihrer Befugnisse dem Ziel einer Verbesserung der inneren Sicherheit und der Bekämpfung des Terrorismus vollständig gerecht zu werden, und zwar im Bereich der Prävention, Aufdeckung und Ermittlung von Straftaten, einschließlich terroristischer Handlungen und Bedrohungen, unter strikter Einhaltung der Vorschriften zum Schutz personenbezogener Daten."

Daraufhin nahm die Kommission am 24. November 2005 einen Vorschlag an für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten.[29] Um den Bedenken der Artikel 29-Datenschutzgruppe[30] über den Zugang zu VIS von anderen Behörden als nur der Visabehörde Rechnung zu tragen, begrenzt der Vorschlag die Zugangsberechtigung zu VIS auf Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer Straftaten und schwerer Verbrechen, über zentrale nationale Kontaktstellen und nach Einzelfallprüfung, um dadurch ausdrücklich einen Routinezugang auszuschließen. Was die Vorschriften zum Schutz personenbezogener Daten betrifft, so gelten der künftige Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Zuge polizeilicher und justizieller Ermittlungen in Strafsachen verarbeitet werden (zum Vorschlag der Kommission siehe unten) sowie das Europol-Übereinkommen für die Verarbeitung personenbezogener Daten gemäß Beschluss. Eine wirkungsvolle Überwachung ist durch eine von der europäischen und den nationalen Datenschutzbehörden durchgeführte jährliche Überprüfung vorgesehen.

Vorratsdatenspeicherung

Am 21. September 2005 legte die Kommission einen Vorschlag vor für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG.[31] Dieser Vorschlag sieht die Umsetzung verschiedener Erklärungen des Rates über die Ergreifung geeigneter Maßnahmen zur Bekämpfung des Terrorismus vor und insbesondere die Schaffung einer Rechtsgrundlage für die erste Säule, im Gegensatz zu der Initiative, die von Frankreich, Irland, Schweden und dem Vereinigten Königreich 2004 eingebracht wurde.[32]

Zweck des Vorschlags der Kommission ist es, die Pflichten für Anbieter von öffentlich zugängigen elektronischen Kommunikationsdiensten oder Betreiber eines öffentlichen Kommunikationsnetzes im Zusammenhang mit der Vorratsspeicherung bestimmter Daten zur Weiterleitung an die zuständigen Behörden der Mitgliedstaaten mit dem Ziel der Verhütung, Untersuchung, Aufdeckung und Verfolgung von schweren Straftaten wie Terrorismus und organisierte Kriminalität in Einklang zu bringen. Der Vorschlag sieht eine Vorratsspeicherung vor von einem Jahr ab der Mitteilung und von sechs Monaten bei Daten in Bezug auf elektronische Kommunikation, die vollständig oder hauptsächlich unter Verwendung des Internetprotokolls stattgefunden hat. Die derzeitigen EU-Rechtsvorschriften über den Datenschutz, wie etwa die Richtlinie 95/46/EG und die Richtlinie 2002/58/EG, sind weiterhin bei der Verarbeitung von personenbezogenen Daten voll anwendbar. Die so erhaltenen Vorratsdaten werden auf Verlangen, ohne unangemessene Verzögerung an die zuständigen Behörden (Strafverfolgungs-

[29] KOM(2005) 600 endgültig, OJ 2006, C 49, S. 50
[30] WP 110
[31] KOM(2005) 438 endgültig, 21.9.2005; OJ 2006, C 49, S. 42
[32] 28.04.2004; Ratsdokument 8958/04; siehe Stellungnahme 9/2004 (WP 99)

behörden) weitergeleitet. Um die Kosten zu senken, die den Anbietern von Kommunikationsdiensten durch diese Verpflichtungen entstehen, setzt der Vorschlag der Kommission die Entschädigung durch die Mitgliedstaaten von ausgewiesenen, den Diensteanbietern entstandenen Zusatzkosten fest. Der Vorschlag ändert auch Artikel 15 Absatz 1 der Richtlinie 2005/58/EG.

Mitteilung der Kommission über die Interoperabilität europäischer Datenbanken im Bereich Justiz und Inneres

Am 24. November 2005 legte die Kommission eine Mitteilung über erhöhte Effektivität sowie Steigerung der Interoperabilität und der Synergien bei europäischen Datenbanken im Bereich Justiz und Inneres vor.[33] Das Dokument zeigt auf, wie bestehende Systeme über das derzeitige Entwicklungsstadium hinaus auf effektivere Art und Weise Maßnahmen, die mit der persönlichen Bewegungsfreiheit verbunden sind und der Bekämpfung des Terrorismus und der Schwerverbrechen dienen, unterstützen können. Darüber hinaus werden in der Mitteilung weitere mögliche Maßnahmen wie die Einrichtung eines Einreise/Ausreise-Erfassungssystems, die Einführung einer Regelung zur Erleichterung des Grenzübergangs für häufig die Grenze überschreitende Personen oder die Einrichtung eines automatisierten europäischen Fingerabdruck-Identifizierungssystems (AFIS) vorgeschlagen. In der Mitteilung werden ferner mögliche Szenarien herausgearbeitet, ohne einer notwendigen ausführlichen Debatte vorzugreifen. Sie weist darauf hin, dass ein ausgewogenes Gleichgewicht zwischen der Verfolgung dieser Ziele und dem Schutz der Grundrechte gefunden werden muss.

Schutz personenbezogener Daten, die bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden

Am 4. Oktober 2005 legte die Kommission einen Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten vor, die bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[34] Beabsichtigt ist die Gewährleistung des Schutzes personenbezogener Daten, die bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union verarbeitet werden. Der Vorschlag sollte zudem der Notwendigkeit, dass es die Effizienz der rechtmäßigen Maßnahmen der Polizei-, Zoll- und Justizbehörden sowie sonstigen zuständigen Behörden zu verbessern gilt, so weit wie möglich Rechnung tragen und daher die geltenden und bewährten Grundsätze und Begriffsbestimmungen übernehmen, die insbesondere in der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates festgelegt oder für den Informationsaustausch durch Europol bzw. Eurojust oder die Verarbeitung im Rahmen des Zollinformationssystems und vergleichbaren Instrumenten vorgesehen sind, wie etwa das Übereinkommen Nr. 108 des Europarates.

Rahmenbeschluss über den Grundsatz der Verfügbarkeit

Der Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit[35] wurde am 12. Oktober 2005 von der Kommission angenommen. Nach Maßgabe dieses Vorschlags müssen die zuständigen Behörden eines Mitgliedstaats ihnen zur Verfügung stehende Informationen auch den zuständigen Behörden anderer Mitgliedstaaten und Europol zugänglich machen. Deshalb muss gemeldet werden, ob Informationen online im Internet zugänglich sind und welche Behörden zu welchem Zweck Zugang haben. Außerdem müssen für solche Informationen Indexdaten zusammengestellt werden, die online nicht abgefragt werden können. Informationen, die online nicht zugänglich sind oder für die der Zugang nicht autorisiert ist, können mittels einer Informationsanfrage einer zuständigen Behörde beschafft werden, die die

[33] KOM(2005) 597 endgültig, 24.11.2005
[34] KOM(2005) 475 endgültig, OJ 2006, C 49, S. 44
[35] KOM(2005) 490 endgültig, OJ 2006, C 49, S. 45

gesuchte Information mit den Indexdaten abgeglichen hat, es sei denn, der Zugang wird aus einem der im Rahmenbeschluss aufgeführten Gründe verweigert. Dies betrifft DNA-Profile, Fingerabdrücke, ballistische Erkenntnisse, Fahrzeugzulassungsdaten, Telefonnummern und sonstige Verbindungsdaten sowie Namen aus Personenstandsregistern. Die Bestimmungen zum Datenschutz obliegen dem künftigen Rahmenbeschluss über den sich aus der dritten Säule ergebenden Datenschutz (siehe oben).

Normen für Sicherheitsmerkmale und biometrische Daten in Pässen der EU-Bürger

Auf der Grundlage von Artikel 2 der Verordnung des Rates (EG) Nr. 2252/2004 nahm die Europäische Kommission am 28. Februar 2005 einen Beschluss über die Festlegung technischer Spezifikationen zu den Normen für Sicherheitsmerkmale und biometrische Daten in von Mitgliedstaaten ausgestellten Pässen und Reisedokumenten an.[36] Der Beschluss richtet sich ausschließlich an die Schengen-Länder. Der Rat hatte am 13. Dezember 2004 die Verordnung (EG) Nr. 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Reisedokumenten angenommen. Diese Verordnung sieht das Digitalfoto als erstes biometrisches Pflichtmerkmal, Fingerabdrücke als zweites, ebenfalls zwingend vorgeschriebenes Merkmal vor. Die Verordnung trat am 18. Januar 2005 in Kraft.

3.2. DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Einleitung

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Behörde, die in erster Linie die Verarbeitung personenbezogener Daten durch die Institutionen und Behörden der Europäischen Gemeinschaft überwacht. Sie berät auch bei Legislativvorschlägen in Bezug auf die Verarbeitung personenbezogener Daten und arbeitet sowohl mit den Datenschutzbehörden der Mitgliedstaaten zusammen als auch, im Rahmen der dritten Säule der Europäischen Union, zusammen mit polizeilichen und justiziellen Behörden bei Strafsachen, um einen einheitlichen Datenschutz zu gewährleisten. Diese drei Aufgaben des Europäischen Datenschutzbeauftragten – Überwachung, Beratung und Zusammenarbeit – und seine Befugnisse sind in der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 festgelegt, unter Bezug auf Artikel 286 EG-Vertrag.

Während 2004, das erste Tätigkeitsjahr, die eigentliche Aufbauphase einer neuen Institution darstellte, lag 2005 der Schwerpunkt in der Verschmelzung des EDSB mit dem institutionellen Rahmen der EU.

Überwachung

Die Aufgabe besteht darin, die gemeinschaftlichen Institutionen und Behörden zu überwachen und dafür zu sorgen, dass sie die in 2001 festgeschriebenen Verpflichtungen für den Datenschutz einhalten. Die Entwicklung einer Datenschutzkultur ist eine dringende Notwendigkeit. Die Europäische Datenschutzbehörde hat eine Lernphase bis zum Frühjahr 2007 einkalkuliert, nach der gegebenenfalls Maßnahmen zur Durchsetzung dieser Verpflichtungen eingeleitet werden. Die wichtigsten Elemente im Jahr 2005 waren:

- Fortentwicklung eines Netzes von **Datenschutzbeauftragten** (DSB) in Institutionen und Behörden. Unabhängig in Bezug auf die interne Anwendung der Verordnung 45/2001 sind DSB strategische Partner bei der Überwachung. Der EDSB hat bereits ein Papier über deren Aufgaben vorgelegt. Alle Behörden müssen einen Datenschutzbeauftragten ernennen, der, so wird es in dem Papier betont, an seiner eigenen Dienststelle in angemessenerer Weise von der Verarbeitung personenbezogener Daten

[36] C(2005) 409 endgültig; online zugänglich: http://ec.europa.eu/justice_home/doc_centre/freetravel/documents/doc_freetravel_documents_de.htm

benachrichtigt werden muss. Der DSB leitet dann die Benachrichtigungen über risikobehaftete Datenverarbeitungen zur vorherigen Prüfung an den EDSB weiter.

- Etwa 34 **Stellungnahmen zu Vorabkontrollen** zu risikobehafteten Datenverarbeitungssystemen wurden veröffentlicht, von denen 30 Systeme in Betrieb waren, bevor der EDSB seine Tätigkeit aufnahm oder bevor die Verordnung in Kraft trat. Folgende Themenfelder kamen vor allem vor: Krankenakten, Personalbeurteilungen, Disziplinarverfahren, Sozialdienstleistungen und E-Monitoring.
- 27 **Beschwerden** gingen ein, von denen lediglich fünf zur weiteren Prüfung zugelassen wurden. Dies rührt daher, dass die überwiegende Zahl der Beschwerden nicht in den Zuständigkeitsbereich des EDSB fallen.
- Es wurde ein Papier vorgelegt darüber, wie zwei Grundrechte, nämlich der **öffentliche Zugang zu Dokumenten** und der **Datenschutz**, sich im Kontext der EU-Verwaltung miteinander vereinbaren lassen. Ein weiteres Papier über den Gebrauch **elektronischer Kommunikation** ist in Bearbeitung und wird bis Mitte 2006 veröffentlicht werden.
- Maßnahmen zur gemeinsamen Überwachung von **Eurodac** wurden eingeleitet, bei denen der Europäische Datenschutzbeauftragte die Aufsicht über die Zentraleinheit hat, während die nationalen Datenschutzbehörden für ihre jeweiligen Mitgliedstaaten verantwortlich zeichnen. Der EDSB war im Allgemeinen mit den Ergebnissen der ersten Überprüfungsphase der Zentraleinheit zufrieden.

Beratung

Die Tätigkeit des EDSB besteht darin, Institutionen und Behörden der Gemeinschaft in allen Angelegenheiten des Schutzes personenbezogener Daten zu beraten, vor allem zu Legislativvorschlägen, die einen Einfluss auf den Datenschutz beinhalten. Meilensteine des Jahres 2005 waren etwa:

- die Herausgabe und Umsetzung eines **Papiers zur beratenden Funktion** des EDSB, das dessen breites Betätigungsfeld betont und auch die dritte Säule der EU umfasst. Dieser Wirkungsbereich wurde anschließend vom Europäischen Gerichtshof bestätigt. Das Papier wurde gut aufgenommen und die Europäische Kommission bedient sich des EDSB, um informelle Kommentare zu einem Entwurf abzugeben, bevor dieser zur formalen Anhörung vorgelegt wird.
- die Abgabe von sechs formellen **Stellungnahmen,** die die einschlägigen Themen auf der politischen Agenda der Kommission, des Parlaments und des Rates widerspiegeln. Die wichtigsten davon sind:
  1. der Austausch von personenbezogenen Daten im Rahmen der dritten Säule der EU
  2. der Aufbau eines IT-Großsystems, wie etwa das Visa-Informationssystem (VIS) und das Schengener Informationssystems der zweiten Generation (SIS II), sowie
  3. das kontroverse Thema der vorgeschriebenen Vorratsdatenspeicherung elektronischer Kommunikationsdaten für den Zugriff durch Strafverfolgungsbehörden.
- Beratung zu **Verwaltungsmaßnahmen**, insbesondere zur Umsetzung behördlicher Vorschriften beim Datenschutz
- **Einspruchserhebung beim Gerichtshof** im Falle der Übermittlung von Fluggastdatensätzen an die Vereinigten Staaten, in Übereinstimmung mit den Schlussfolgerungen des Parlaments, das ersucht, die betreffenden Beschlüsse der Kommission und des Rates für nichtig erklären zu lassen.

Zusammenarbeit

Die Zusammenarbeit des EDSB berührt nicht nur den Datenschutz im Rahmen der ersten Säule (EG-Vertrag), sondern beinhaltet auch die Kooperation mit nationalen Aufsichtsbehörden der ersten EU-Säule mit dem Ziel einer besseren Kontinuität des

Schutzes personenbezogener Daten. 2005 waren folgende Entwicklungen wichtig:

- Zahlreiche wichtige Legislativvorschläge wurden in separaten Stellungnahmen vom EDSB und der **Artikel 29-Datenschutzgruppe** in Angriff genommen. In diesen Fällen war der Europäische Datenschutzbeauftragte für die Unterstützung von Kollegen aus anderen Mitgliedstaaten sowie zusätzlichen Anmerkungen zur Verbesserung des Datenschutzes dankbar.
- Die **Zusammenarbeit mit den Aufsichtsbehörden für Schengen, dem Zoll und Europol** konzentrierte sich auf das Erreichen gemeinsamer Standpunkte hinsichtlich des Aufbaus eines dringend erforderlichen allgemeinen Rahmens für den Datenschutz Europas im Bereich der dritten Säule. Im Hinblick auf SIS II fanden auch Diskussionen über ein neues Überwachungssystem statt, das sich auf eine enge Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten stützt.
- Der EDSB übernahm den Vorsitz bei einigen Sitzungen im Zusammenhang mit **europäischen und internationalen Konferenzen** der Datenschutzbeauftragten.

Zusammen mit dem Europarat und der OECD veranstaltete der EDSB einen Workshop zum Datenschutz in **internationalen Organisationen**. Obwohl internationale Organisationen oft nicht den einzelstaatlichen Rechtsvorschriften unterliegen, auch was das Datenschutzrecht betrifft, ist es doch unbedingt erforderlich, dass sie sich den allgemeinen Grundsätzen des Datenschutzes anschließen, umso mehr als sie oft sensitive Daten verarbeiten.

3.3. DIE EUROPÄISCHE DATENSCHUTZKONFERENZ

Vom 24. bis 26. April 2005 fand in Krakau, Polen, die von der Generalinspektorin für Datenschutz Dr. Ewa Kulesza organisierte Frühjahrskonferenz der europäischen Datenschutzbehörden statt. Die Konferenz fiel zeitlich mit dem zehnten Jahrestag der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zusammen. Die Konferenz hatte u. a. das Überdenken der Anwendung und Auslegung der Richtlinie sowie die Annahme einer Entschließung zum Datenschutz innerhalb der dritten Säule als Thema. Ein weiteres Thema war die Verlagerung des Referats Datenschutz von der Generaldirektion Binnenmarkt zur Generaldirektion Justiz, Freiheit und Sicherheit.

Kapitel 4

Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

Island

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie weitere Entwicklungen in den Gesetzgebungen

Im Jahre 2005 wurden eine Reihe von Gesetzen, Verwaltungsregeln und -verordnungen verabschiedet. Die wichtigsten davon waren die folgenden:

1. *Gesetz 15/2005 über den Staatsanzeiger und das Gesetzblatt*. Dieses Gesetz ersetzte Gesetz 64/1943. Laut neuem Gesetz können die erwähnten amtlichen Organe im Internet zugänglich gemacht werden. Das erste Amtsblatt enthält Gesetze, Verordnungen, andere Verwaltungsvorschriften sowie internationale Verträge und Übereinkommen, das letztere gerichtliche Vorladungen, Beschlüsse zu Zwangsversteigerungen, Insolvenzentscheidungen usw. Daher ist es in erster Linie das Gesetzblatt, das personenbezogene Daten enthält. Gemäß Artikel 7 des Gesetzes sollte die Veröffentlichung im Internet möglichst nicht zu einer Verknüpfung und weiterer Verarbeitung personenbezogener Daten führen. Die isländische Datenschutzbehörde, Persónuvernd, hat in ihren Stellungnahmen zu dieser Sache unterstrichen, dass der Aufbau einer im Internet zugänglichen Datenbank, z. B. über finanzielle Angelegenheiten, vermieden werden sollte. Die oben erwähnten Gesetzesbestimmungen entsprechen diesen Stellungnahmen.

2. *Verordnung 623/2005 über die Veröffentlichung des Gesetzblatts*. Diese vom Justizminister erlassene Verordnung enthält u. a. Bestimmungen, wie personenbezogene Daten bei der Veröffentlichung dieses Blattes im Internet geschützt werden sollten. Bekanntmachungen, z. B. von Beschlüssen über Zwangsversteigerungen, sollten für Abonnenten nicht länger als drei Jahre zugänglich sein.

3. *Gesetz 58/2005 zur Änderung des Arzneimittelgesetzes 93/1994 und des Gesetzes 97/1990 über Gesundheitsdienstleistungen*. Dieses Gesetz dient der Umsetzung der Richtlinie 2002/98/EG über Blut und Blutbestandteile. Die Datenschutzbehörde Persónuvernd bemängelte in ihrer Stellungnahme das Fehlen einer Bestimmung zum Schutz personenbezogener Daten in Blutbanken zur Umsetzung von Artikel 24 der Richtlinie. Eine nachträglich hinzugefügte Bestimmung besagt, dass die Datenschutzbehörde die Verarbeitung personenbezogener Daten in Biobanken, in Übereinstimmung mit Datenschutzgesetz 77/2000 und Gesetz 74/1997 über Patientenrechte, überwachen sollte.

4. *Gesetz 78/2005 zur Änderung des Telekommunikationsgesetzes 81/2003*. Die Bestimmungen enthalten u. a. die Abänderung von Artikel 47 Telekommunikationsgesetz. wonach Telekommunikationsunternehmen verpflichtet sind, Informationen über die Nutzer von IP-Adressen und Telefonnummern an die Polizei weiterzugeben, obwohl die Beschaffung der Informationen nicht durch richterlichen Beschluss angeordnet wurde. Die Datenschutzbehörde Persónuvernd kritisierte diese Bestimmung in ihrer Stellungnahme zur Sache.

5. *Vorschriften 36/2005 zur Registrierung von Personen mit dem Wunsch nach Werbefreiheit und zum Gebrauch einer solchen Datei*. Diese Vorschriften wurden vom isländischen Statistikbüro gemäß Artikel 28 Datenschutzgesetz 77/2000 verabschiedet. Die darin niedergelegten, über Artikel 28 hinausgehenden Bestimmungen enthalten das Recht, sich gegen Direktmarketing zur Wehr zu setzen und in eine entsprechende, vom Statistikbüro verwaltete Datei aufgenommen zu werden.

6. *Bekanntmachung 638/2005 über die Übermittlung personenbezogener Daten an Drittländer*. Diese von der Datenschutzbehörde verabschiedete rechtsverbindliche Bekanntmachung ersetzt Bekanntmachung 435/2003. Sie enthält Bestimmungen über den von Drittländern zu gewährenden angemessenen Schutz für personenbezogene Daten, vertragliche Standardklauseln zur Übertragung personenbezogener Daten an Drittländer usw.

B. Bedeutende Rechtsprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Eine der Hauptaufgaben der Datenschutzbehörde im Jahre 2004 waren Inspektionen. Es wurden formelle administrative Entscheidungen in Bezug auf Inspektionen gefällt, die 2002 und 2003 begannen: über die Rechtmäßigkeit und Sicherheit der Datenverarbeitung bei zwei Kreditkartengesellschaften und bei drei Versicherungsgesellschaften (Lebens- und Unfallversicherung, Versicherung von Berufskrankheiten). Bei der Sicherheit wurden nur geringfügige Mängel festgestellt. Die Datenschutzbehörde machte jedoch einige Bemerkungen hinsichtlich der Rechtmäßigkeit der Verarbeitung.

So führte eines der Kreditkartenunternehmen seit seiner Gründung 1980 eine Vorratsdatenspeicherung personenbezogener Daten über den Kreditkartengebrauch seiner Kunden durch. Die Datenschutzbehörde wies das Unternehmen an, übermittelte Daten, die älter als sieben Jahre sind, zu vernichten. Jüngere Daten sind jedoch zurückzubehalten, denn nach den Buchführungsvorschriften beträgt die Aufbewahrungsfrist für Buchungsunterlagen sieben Jahre.

Die Datenschutzbehörde machte auch einige Anmerkungen hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Versicherungsgesellschaften und vertrat die Ansicht, dass Angehörige von Versicherungsantragstellern um Zustimmung gebeten werden sollten, bevor Gesundheitsdaten über sie eingeholt werden. Angesichts des neuen Gesetzes über Versicherungsverträge 30/2004, das am 1. Januar 2006 in Kraft treten sollte, war die Behörde des weiteren der Meinung, dass es ab diesem Zeitpunkt illegal sei, Daten über Erbkrankheiten von Angehörigen zu erheben.

Liechtenstein

Die Datenschutzverordnung (DSV) wurde erneut revidiert:[37] Die Revision, welche in enger Zusammenarbeit mit dem Datenschutzbeauftragten (DSB) erfolgte, sieht vor, dass die Bekanntgabe von Identifikationsdaten (Vorname, Name, Adresse, Geburtsdatum) durch Behörden zu ideellen Zwecken möglich ist. Ergänzend wird bestimmt, dass der Gesuchsteller bei der Bekanntgabe der Daten ausdrücklich darauf hinzuweisen ist, dass die Daten nicht weitergegeben und ausschließlich für den im Gesuch angegebenen Zweck verwendet werden dürfen. Ist die Bekanntgabe für die Behörde mit einem erheblichen Aufwand verbunden, kann eine Gebühr zu einem Stundensatz von 100 Schweizer Franken erhoben werden. Der zweite Punkt betraf die Schaffung einer rechtlichen Grundlage für Behörden, welche in der Praxis verschiedene Personendaten über ihre Internetseite in einem offenen Abrufverfahren bekannt gegeben hatten. Konkret geht es um die Bekanntgabe von Namen und Kontaktdaten von Mitarbeitern von Behörden oder etwa um die Bekanntgabe von Verbandsmitgliedern. Dabei wurde vorgesehen, dass gewisse weitere Daten (wie Fotos der betroffenen Personen) bekannt gegeben werden können, wenn diese darüber informiert wurden und damit einverstanden sind.

Meinungen des DSB zu Gesetzestexten: Neben der erwähnten Revision der DSV wurde der DSB zu 15 weiteren Gesetzesvorhaben konsultiert. Erwähnt seien an dieser Stelle:

- Rechtsgrundlage zur Zentralen Personenverwaltung (ZPV) der Landesverwaltung: In diesem wichtigen Gesetzesentwurf wird insbesondere die Rechtsgrundlage für eine nationale Kennziffer im Sinne von Art. 8 Abs. 7 der Richtlinie 95/46/EG geschaffen. Daneben wird unter anderem auch festgehalten, unter welchen Bedingungen diese Nummer verwendet werden darf. Weitere Elemente bestehen darin, dass ein Antragsverfahren für Datenfelder vorgesehen ist. Eine rechtmäßige Datenbearbeitung (in Bezug auf einzelne Datenfelder, aber auch auf die Kennnummer) ist nur gegeben, wenn die Bearbeitung recht- und verhältnismäßig ist und den Anforderungen des Datenschutzes genügt.
- Revision des Heimatschriftengesetzes zur Einführung der biometrischen Pässe: In Abstimmung mit verschiedenen Dokumenten zum Thema aus dem internationalen Bereich[38] wurde eine Stellungnahme abgegeben und insbesondere angeregt, die Bestimmung zur Sicherheit der biometrischen Daten im Gesetz zu verstärken und dies auch in der Praxis zu berücksichtigen.

Spezifische Themen: Die Prüfung der Anträge auf Zugriffsberechtigungen von Feldern der Zentralen Personenverwaltung (ZPV), einer zentral geführten Datenbank der Liechtensteinischen Landesverwaltung, konnte Mitte 2005 abgeschlossen werden. Die Umsetzung der Bewilligungen musste danach überprüft werden. Diese aufwändige Arbeit konnte nicht bis Jahresende abgeschlossen werden.

Die ZPV wurde vor Inkrafttreten des DSG aufgebaut und enthält insbesondere Daten der gesamten ständigen Wohnbevölkerung. Wohl konnten die Zugriffsberechtigungen auf gewisse Felder beschränkt werden, nicht jedoch auf bestimmte Personengruppen. Amtsstellen, welche mit der ZPV arbeiten, benötigen Daten derjenigen Personen, mit denen ein amtlicher Kontakt besteht. Die Daten aller anderen Personen sind für die jeweilige Amtsstelle irrelevant. Eine Einschränkung auf gewisse Personengruppen ist bei der gegebenen Struktur der ZPV nur schwer möglich. Überlegungen, wie dies dennoch erreicht werden kann, waren am Ende des Berichtsjahres noch im Gange.

[37] LGBl. 2005 Nr. 206.

[38] Vgl. z.B. WP 112.

Auf der **Internetseite** der Stabsstelle für Datenschutz www.sds.llv.li wurden über aktuelle und/oder wichtige Themen informiert. Davon sind vor allem die folgenden stichwortartig zu nennen: datenschutzgerechter Umgang mit Personalakten; aktualisierte Liste der Drittländer mit gleichwertigem Datenschutz; biometrische Daten; RFID-Funkchips; Surfen am Arbeitsplatz – Datenschutzwegweiser; Präsentation zum Thema „Datenschutz – wirklich was Neues in Liechtenstein?" und zu „Grundsätze und Anwendung bei Forschung, Medien und Internet"; Entscheidung zu Spam-Mails der Eidgenössischen Datenschutzkommission. Die Internetseite wurde zudem um eine neue Rubrik „Presseartikel und Interviews" erweitert.

Schließlich wurden **Richtlinien** zum Thema „Internet- und E-Mail-Überwachung des Arbeitnehmers am Arbeitsplatz" und „Rechte nach dem Datenschutzgesetz" verabschiedet.

Register: Das **Register der Datensammlungen** wurde Ende des Berichtsjahres auf die Internetseite gestellt.

Norwegen

Bedeutende Änderungen in Datenschutzgesetzen bzw. Gesetzen zum Schutz der Privatsphäre

Keine nennenswerten Entwicklungen.

Bedeutende Änderungen in anderen Datenschutzgesetzen bzw. Gesetzen zum Schutz der Privatsphäre

Änderungen der Strafprozessordnung

2005 gab es eine Reihe von Änderungen bei der Strafprozessordnung. Dazu gehört die Möglichkeit elektronischer Überwachung von Räumen, wenn die Voraussetzungen gegeben sind. Die Möglichkeit einer breit angelegten Telefonüberwachung in einem bestimmten Bereich zur Lokalisierung der von einem Verdächtigten benutzten Telefone wurde ebenfalls ausgeweitet.

B. Wichtige spezifische Themen

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Inspektionen

Biometrische Pässe

Am 3. Oktober 2005 wurde in Norwegen mit der Herstellung biometrischer Pässe begonnen, für die die Datenschutzbehörde im Laufe des Jahres viele Ressourcen eingesetzt hat. Hintergrund sind die Sicherheitsprobleme bei den Pässen, vor allem im Hinblick auf das Speichern und Lesen von Passdaten. Das Justizministerium hat darauf hingewiesen, dass die internationalen Standards der Maßstab für die Sicherheitsanforderungen sein sollen. Leider gibt es bis heute auf internationaler Ebene keine Einigung auf gemeinsame Normen. Daher bedauert es die Datenschutzbehörde, dass der Pass bereits vor der Abklärung der Sicherheitsfragen eingeführt wurde. Im Gegensatz zu Norwegen haben die Vereinigten Staaten und das Vereinigte Königreich seine Einführung verschoben.

Dopingtests im Sport

Im Jahre 2005 führte die Datenschutzbehörde ein Projekt durch, bei dem die Verarbeitung personenbezogener Daten im Sport bewertet wurde, und zwar sowohl im Spitzensport als auch beim Freizeit- und Fitnesssport. Dabei konzentrierte man sich auf Dopingtests bei Berufs- und Amateursportlern innerhalb und außerhalb des organisierten Sports. Das Projekt wird 2006 fortgesetzt werden.

Das Pilotprojekt offenbarte die Notwendigkeit einer Überprüfung der rechtlichen Grundlagen für Dopingtests und deren Verhältnis zum Datenschutz. Es muss bewertet werden, ob die Zustimmung zu Dopingtests grundsätzlich angemessen ist, oder ob solche Tests eine klare gesetzliche Grundlage bekommen sollten. Ferner müssen jene Bereiche, in denen Dopingtests akzeptiert werden können, von solchen abgegrenzt werden, bei denen ein Test als eine unverhältnismäßige Beeinträchtigung betrachtet wird. Die Leistungsstufe und das Alter des Sportlers sind hierbei besonders zu berücksichtigen.

Berufsleben

2005 beschäftigte sich die Datenschutzbehörde mit einer großen Anzahl von Fällen, bei denen Arbeitgeber bei der Überwachung ihrer Angestellten zu weit gegangen waren. Nach einer Überprüfung entschloss sich die Behörde, einige dieser Fälle der Polizei zu melden. Zwei dieser Fälle betreffen Arbeitgeber, die alle E-Mails, auch die pri-

vaten, speicherten, die ihre Angestellten an ihrem Arbeitsplatz versandten oder erhielten, ohne die Angestellten zu informieren. In einem anderen Fall installierte ein Arbeitgeber eine versteckte Kamera im Umkleideraum, um stehlende Angestellte zu entlarven. Im vierten Fall benutzte eine Bank die Bilder einer Überwachungskamera, um herauszufinden, ob die Reinigungskraft ihre Arbeit korrekt erledigte, was natürlich nicht die Aufgabe der Kamera war.

Beratungen

Amt für Arbeit und Sozialfürsorge

Um Sozialhilfeempfängern bessere Anreize zur Aufnahme einer regulären Beschäftigung anbieten zu können und die Anzahl jener Hilfsbedürftigen zu verringern, die aus verschiedenen Gründen durch das Raster der Sozialleistungen fallen, regten Regierung und Storting (Norwegische Nationalversammlung) eine Zusammenarbeit der Behördendienste in den Bereichen Beschäftigung, Sozialversicherung und Sozialhilfe an. Die Datenschutzbehörde kritisierte den über das Amt für Arbeit und Sozialfürsorge vorgelegten Gesetzentwurf aufgrund mangelnden Datenschutzes. Zudem wiesen die Datenschutzbehörde und das Amt für Gesundheitswesen (Norwegian Board of Health) darauf hin, dass die Bestimmungen zur Vertraulichkeit nicht eindeutig und schwer verständlich seien.

Die Datenschutzbehörde befürchtet, dass das neue Amt den Sachbearbeitern einen umfassenden Zugang zu Personendaten ermöglicht, ohne dass der Einzelne weiß, was mit seinen persönlichen Daten geschieht.

Einige grundsätzliche Dinge sind zu beachten, um zu einer annehmbaren Lösung zu gelangen:

Niemand sollte Zugang zu einer größeren Menge personenbezogener Daten bekommen, als für die ordnungsgemäße Durchführung seiner Aufgaben benötigt wird. Jede Anfrage eines Angestellten muss protokolliert werden, die Protokolle müssen geprüft werden. Die Datenschutzbehörde hat den Eindruck gewonnen, dass keine Vorkehrungen getroffen wurden, um den Sachbearbeitern nur einen begrenzten Zugriff auf Datenbankinformationen zu gestatten. Dies bedeutet, dass Vertraulichkeit und Integrität der Bearbeiter in Wahrheit die einzigen Garanten für den Datenschutz sind, während auf System- und Beamtenebene die meisten unangemessenen Anfragen als „menschliches Versagen" entschuldigt werden können.

Vorschlag für ein neues Einwanderungsgesetz

Der Vorschlag für ein neues Einwanderungsgesetz wirft viele Fragen auf im Zusammenhang mit dem Datenschutz. Eine wichtige ist, welche Informationen den Einwanderungsbehörden bei ihrer Beurteilung zugänglich sein sollten, ob und wenn ja, welche Kategorie von Aufenthaltsgenehmigung einer Person erteilt werden soll. Eine andere zentrale Frage ist, welche Daten von einer in Norwegen ansässigen Person, einer sogenannten „Referenzperson", gesammelt werden dürfen, die für einen ausländischen Staatsangehörigen ein Besuchervisum beantragt. Die Datenschutzbehörde vertritt die Meinung, dass der Einwanderungsausschuss mit seinem Vorschlag, Referenzpersonen zu überprüfen, eindeutig zu weit gegangen ist. Die Datenschutzbehörde glaubt, dass dieser Vorschlag zu viele Möglichkeiten zur Erhebung von Daten eröffnet, etwa solche über den persönlichen Leumund oder unbestätigte Informationen. Es ist schwierig, an unbestätigte Informationen, etwa an vertrauliche Mitteilungen in einem Krisenzentrum, zu kommen und noch schwieriger, solche Informationen zu widerlegen.

Führungszeugnisse

Die Datenschutzbehörde gab mehrfach ihre beratende Stimme zu dem Thema ab, bei dem es um die Anforderung von Führungszeugnissen geht. Es handelt sich sowohl um ein Problem von Berufsgruppen als auch um eines im Bereich gesellschaftlicher Selbstorganisation (gemeinnütziger Bereich). Die Behörde stellt die Frage, ob der Erwerb eines solchen Zeugnisses wirklich einen angemessenen Schutz garantiert, oder ob damit nur ein falsches Sicherheitsgefühl erweckt wird. Die Datenschutzbehörde hat bei diesen Fällen die Bedeutung unterstrichen, keine umfassenden Maßnahmen zu ergreifen, die zu einem solchen unechten Gefühl der Sicherheit beitragen könnten. Bei der Mehrzahl der erhaltenen Konsultationspapiere war die Darstellung dieses Problems ungenügend.

Die Datenschutzbehörde beobachtet, dass Führungszeugnisse bei einer wachsenden Zahl von Arbeitsstellen erforderlich sind, und könnte sich vorstellen, dass diese Entwicklung auch auf den Bereich gesellschaftlicher Selbstorganisation übergreift und schwer umzukehren sein könnte. Hauptsächlich Grund dafür, in einigen Branchen und bei verschiedenen Berufsgruppen Führungszeugnisse zu verlangen, ist, dass auch in anderen Bereichen Zeugnisse erforderlich sind und dass die Bereiche, in denen keine Zeugnisse erforderlich sind, ungeeignete Personen anziehen, die an anderer Stelle nicht untergekommen sind. Die Datenschutzbehörde warnt daher vor einer Entwicklung, bei der ein Auftritt auf der gesellschaftlichen Bühne von einer polizeilichen Unbedenklichkeitsbescheinigung abhängig gemacht wird.

Beschlüsse und Klarstellungen

Untersuchung auf Rauschmittel

Anfang 2006 schloss der Beschwerdeausschuss der Datenschutzbehörde (Privacy Appeals Board) einen Fall ab, bei dem es um die Untersuchung von Mitarbeitern einer Sicherheitsfirma auf Rauschmittel ging. Gemäß norwegischem Recht darf ein Arbeitgeber eine solche Untersuchung nur dann verlangen, wenn sie auf Gesetze oder Verordnungen gestützt ist, bei besonderem tätigkeitsbedingtem Risiko oder wenn es der Arbeitgeber für den Schutz von Leben und Gesundheit für notwendig erachtet. Einige Berufsgruppen, wie etwa Seeleute, sind zu solchen Tests gesetzlich verpflichtet. Dies trifft jedoch nicht für Mitarbeiter eines Sicherheitsunternehmens zu. Der Beschwerdeausschuss kam zu dem Schluss, dass das Sicherheitsunternehmen nicht das Recht hatte, alle Angestellten, ungeachtet ihrer Tätigkeit, untersuchen zu lassen.

Freiheit der Meinungsäußerung im Internet

Eine Gruppe von Personen, die vorgab, von Behörden des Missbrauchs im Zusammenhang mit Kinderfürsorgefällen beschuldigt worden zu sein, veröffentlichte im Internet Bemerkungen zu den persönlichen Eigenschaften der mit den Fällen betrauten Mitarbeitern. Das Datenschutzgesetz sieht wichtige Ausnahmen beim Gebrauch personenbezogener Daten für „meinungsbildende" Aktivitäten vor. Die betroffenen Personen betrachteten die Informationen über sie als falsch und diffamierend. Die Datenschutzbehörde wies den Fall ab, mit der Begründung, dass eine Beeinträchtigung der Freiheit der Meinungsäußerung so schwerwie-

gend sei und daher in diesem Fall eine eindeutige Rechtsgrundlage erforderlich sei, die jedoch beim Datenschutzgesetz nicht in ausreichendem Maß gegeben sei. Die betroffenen Personen legten gegen die Entscheidung des Beschwerdeausschusses Einspruch ein. Der Ausschuss bejahte, dass die Internetseiten meinungsbildend seien, lehnte den Einspruch jedoch ab.

Löschung von Tonaufnahmen

Einer Person wurde der Zugriff auf personenbezogene Daten verwehrt, die auf den Tonaufzeichnungen von Telefonaten gespeichert waren, an denen die Person beteiligt war. Der Beschwerdeausschuss kam zu dem Schluss, dass der Fall außerhalb der Kompetenz des Datenschutzgesetzes liege. In diesem Zusammenhang entschied der Ausschuss darüber, ob die Tonaufnahme mit elektronischen Hilfsmitteln durchgeführt wurde oder nicht. Wenn Start und Stopp der Aufnahme manuell waren, konnte nicht von einer Aufnahme mit elektronischen Hilfsmitteln ausgegangen werden, selbst wenn das Aufnahmegerät aus technischer Sicht als elektronisch zu bezeichnen ist und unbeschadet dessen, ob die Aufnahme digital oder analog war.

Erfassung persönlicher Einstellungen

Studien zu Gesetzgebung und Schutz der Privatsphäre

2005 führten die Datenschutzbehörde und das Ministerium für Regierungsverwaltung und Reform (Ministry of Government Administration and Reform) in der Bevölkerung und auf Wirtschaftsebene eine Umfrage zum Thema „Schutz der Privatsphäre" durch. Die Umfrage ergab insgesamt, dass die Bevölkerung im Allgemeinen über den Missbrauch personenbezogener Daten nicht sehr besorgt ist und dass die meisten Leute meinen, die Unternehmen handelten vernünftig. Wenn jedoch die Unternehmen befragt wurden, stellte sich heraus, dass dieses Vertrauen doch etwas unangebracht sein könnte. Unternehmen sehen den Schutz der Privatsphäre durchaus positiv, aber nur sehr wenige befassen sich systematisch mit solchen Fragen. Zudem besitzen die meisten Unternehmen nur sehr wenig Wissen über das Datenschutzgesetz.

Kapitel 5

Mitglieder der Art. 29 Datenschutzgruppe im Jahr 2005

MITGLIEDER DER ART. 29 DATENSCHUTZGRUPPE IM JAHR 2005

Österreich	**Belgien**
Frau Dr. Waltraut Kotschy Österreichische Datenschutzkommission Ballhausplatz 1 - AT - 1014 Wien Tel: +43 1 531 152679; +43 1 531 152525 Fax: +43 1 531 152690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Herr Michel Parisse Präsident Commission de la protection de la vie privée (Datenschutzbehörde) Rue Haute, 139 - B-1000 Brüssel Tel: +32 2 213.85.40 Fax: +32 2 213.85.65 E-Mail: commission@privacycommission.be Website: http://privacycommission.be
Zypern	**Tschechische Republik**
Frau Goulla Frangou Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Datenschutzbeauftragte) 40, Themistokli Dervi str. Natassa Court, 3rd floor - CY-1066 Nikosia oder P.O. Box 23378 - CY-1682 Nikosia Tel: +357 22 818 456 Fax: +357 22 304 565 E-Mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy	Herr Igor Nemec Präsident Úřad pro ochranu osobních údajů (Datenschutzbehörde) Pplk. Sochora 27 - CZ-170 00 Prag 7 Tel: +420 234 665 281 Fax: +420 234 665 501 E-Mail: info@uoou.cz Website: http://www.uoou.cz/
Dänemark	**Estland**
Frau Janni Christoffersen Direktorin Datatilsynet (Dänische Datenschutzagentur) Borgergade 28, 5th floor - DK-1300 Kopenhagen V Tel: +45 33 193236 Fax: +45 33 193218 E-Mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	Herr Urmas Kukk Generaldirektor Andmekaitse Inspektsioon (Estnische Datenschutzbehörde) Väike - Ameerika 19 - EE-10129 Tallinn Tel: +372 6274 135 Fax:+372 6274 135; +372 6274 137 E-Mail: urmas.kukk@dp.gov.ee; info@dp.gov.ee Website: http://www.dp.gov.ee
Finnland	**Frankreich**
Herr Reijo Aarnio Datenschutzombudsmann Tietosuojavaltuutetun toimisto (Büro des Datenschutzombudsmanns) P.O. Box 315 - FI-00181 Helsinki Tel: +358 10 36 66700 Fax: +358 10 36 66735 E-Mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi	Herr Georges de La Loyère Commissaire en charge du secteur international (Beauftragter für den internationalen Aufgabenbereich) Commission Nationale de l'Informatique et des Libertés (CNIL) (Nationale Datenschutzbehörde Frankreichs) Rue Vivienne, 8 - F-75002 Paris Tel: +33 1 53 73 22 31; +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-Mail: laloyere@cnil.fr Website: http://www.cnil.fr

Deutschland	**Griechenland**
Herr Peter Schaar **Vorsitzender** Bundesbeauftragter für den Datenschutz und die Informationsfreiheit Herr Peter Schaar Husarenstraße 30 - D-53117 Bonn Tel: +49 228 81995 0 (Zentrale) Tel: +49 228 81995 100 (Durchwahl) Fax: +49 228 81995 550 E-Mail: peter.schaar@bfdi.bund.de Website: http://www.bfdi.bund.de	Herr Nikolaos Frangakis Rechtsanwalt Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Griechische Datenschutzbehörde) Kifisias Av. 1-3, PC 115 23 Ampelokipi - GR-Athen Tel: +30 210 64.75.601, +30 210 36.32.671 Tel: +30 210 64.75.629, +30 210 64.75.679 Fax: +30 210 33.52.617, +30 210 36.31.631 Fax: +30 210 64.75.728 E-Mail: info@sofralaw.gr Website: http.//www.dpa.gr
Ungarn	**Irland**
Herr Dr. Attila Peterfalvi Parlamentarischer Beauftragter Adatvédelmi Biztos Irodája (Büro der parlamentarischen Beauftragten) Nador u. 22 - H-1051 Budapest Tel: +36 1 475 7186; +36 1 475 7100 Fax: +36 1 269 3541 E-Mail: adatved@obh.hu Website: http://www.abiweb.obh.hu	Herr Billy Hawkes Datenschutzbeauftragter Irish Life Centre, Block 6 Lower Abbey Street - IRL-Dublin 1 Tel: +353 1 8748544 Fax: +353 1 8745405 E-Mail: info@dataprotection.ie Website: http://www.dataprotection.ie
Italien	**Lettland**
Herr Professor Francesco Pizzetti Präsident Garante per la protezione dei dati personali (Datenschutzbeauftragter /-gewährsmann) Piazza di Monte Citorio, 121 - I-00186 Rom Tel: +39 06 69677403 Fax: +39 06 69677405 E-Mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	Frau Signe Plumina Direktorin Datu valsts inspekcija (Datenschutzbehörde) Kr. Barona Street 5-4 - LV-1050 Riga Tel: +371 722 31 31 Fax. +371 722 35 56 E-Mail: info@dvi.gov.lv Website: http://www.dvi.gov.lv
Litauen	**Luxemburg**
Herr Algirdas Kunčinas Direktor Valstybinė duomenų apsaugos inspekcija (Staatliche Datenschutzbehörde) Gedimino Ave 27/2 - LT-01104 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-Mail: ada@ada.lt Website: http://www.ada.lt	Herr Gérard Lommel Präsident Commission nationale pour la Protection des Données (Staatliche Datenschutzbehörde) 41, avenue de la Gare - L-1611 Luxemburg Tel: +352 26 10 6020 Fax: +352 26 10 6029 E-Mail: info@cnpd.lu Website: http://www.cnpd.lu

Malta	**Niederlande**
Herr Paul Mifsud Cremona Data Protection Commissioner (Datenschutzbeauftragter) 2, Airways House High Street - MT-Sliema SLM 16 Tel: +356 2328 7100 Fax: +356 23287198 E-Mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	Herr Jacob Kohnstamm College Bescherming Persoonsgegevens (CBP) (Niederländische Datenschutzbehörde) Juliana van Stolberglaan 4-10 Postbus / P.O. Box 93374 NL-2509 AJ Den Haag Tel: +31 70 8888.500 Fax: +31 70 8888.501 E-Mail: info@cbpweb.nl Website: http://www.cbpweb.nl; www.DutchDPA.nl
Polen	**Portugal**
Frau Dr. Ewa Kulesza Generalinspektorin für Datenschutz Biuro Generalnego Inspektora Ochrony Danych Osobowych (Büro der Generalinspektorin für Datenschutz) ul. Stawki 2 - PL-00193 Warschau Tel: +48 22 860 70 81; +48 22 860 73 12 Fax: +48 22 860 70 90 E-Mail: sekretariat@giodo.gov.pl; dp@giodo.gov.pl Website: http://www.giodo.gov.pl	Herr Luís Da Silveira Präsident Comissão Nacional de Protecção de Dados (Nationale Datenschutzkommission) Rua de São Bento, 148, 3o PT-1 200-821 Lissabon Codex Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-Mail: geral@cnpd.pt Website: http://www.cnpd.pt
Slowakei	**Slowenien**
Herr Gyula Veszelei Präsident Úrad na ochranu osobných údajov Slovenskej republiky (Datenschutzbehörde) Odborarska namestie 3 - SK-81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-Mail: statny.dozor@pdp.gov.sk; gyula.veszelei@pdp.gov.sk Website: http://www.pdp.gov.sk	Frau Natasa Pirc Musar Informationsbeauftragte Vosnjakova 1, SI-1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78 E-Mail: gp.ip@ip-rs.si Website: http://www.ic-rs.si, http://www.ip-rs.si

Spanien	**Schweden**
Herr José Luis Piñar Mañas Vizevorsitzender Director Agencia de Protección de Datos (Spanische Datenschutzbehörde) C/ Jorge Juan, 6 E-28001 Madrid Tel: +34 91 399 6220 Fax: +34 91 447 1092 E-Mail: director@agpd.es Website: http://www.agpd.es	Herr Göran Gräslund Generaldirektor Datainspektionen (Datenschutzbehörde) Fleminggatan, 14 (9. Stock) Box 8114, S-104 20 Stockholm Tel: +46 8 657 61 00; +46 8 657 61 57 Fax: +46 8 650 86 13; +46 8 652 86 52 E-Mail: datainspektionen@datainspektionen.se; goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
Vereinigtes Königreich	**Europäischer Datenschutzbeauftragter Supervisor**
Herr Richard Thomas Datenschutzbeauftragter Information Commissioner's Office (Büro des Datenschutzbeauftragten) Wycliffe House Water Lane - GB - SK9 5AF Wilmslow Tel: +44 1625 545700 Fax: +44 1625 524510	Herr Peter Hustinx Europäischer Datenschutzbeauftragter Postanschrift: 60, rue Wiertz, B-1047 Brüssel Büro: rue Montoyer, 63, B-1047 Brüssel Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-Mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

BEOBACHTER DER ART. 29 DATENSCHUTZGRUPPE IM JAHR 2005

Island	**Norwegen**
Frau Sigrun Johannesdottir Direktorin Isländische Datenschutzbehörde Raudararstigur 10 - IS-105 Reykjavik Tel: +354 560 9010; +354 510 9600 Fax: +354 510 9606 E-Mail: postur@personuvernd.is Website: http://www.personuvernd.is	Herr Georg Apenes Generaldirektor Datatilsynet (Datenschutzbehörde) P.B. 8177 Dep - N-0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E-Mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Bulgarien**
Herr Dr. Philipp Mittelberger Stabsstelle für Datenschutz Aeulestrasse 51 - LI-9490 Vaduz Tel: +423 236 6090/91 Fax: +423 236 6099 E-Mail: info@sds.llv.li Website: http://www.liechtenstein.li; http://www.sds.llv.li	Herr Ivo Stefanov Datenschutzkommission 1 Bvld Dondukov - BG-1000 Sofia Tel: +359 2 940 2046 E-Mail: kzld@government.bg
Rumänien	
Frau Georgeta Basarabescu Präsidentin Nationale Datenschutzkontrollbehörde Olari Street 32, 2. Distrikt, RO-Bukarest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E-Mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro	

Sekretariat der Art. 29 Datenschutzgruppe
Frau Niovi Ringou Referatsleiterin Referat Datenschutz Generaldirektion Justiz, Freiheit und Sicherheit Europäische Kommission Büro: LX46 01/53 - B-1049 Brüssel Tel: +32 2 296 3037 Fax: +32 2 299 8094 E-Mail: Niovi.Ringou@ec.europa.eu Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

NE-AC-07-001-DE-N

EUROPÄISCHE
KOMMISSION

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 festgelegt.

- 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 Richtlinie 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 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 in der Europäischen Gemeinschaft betreffen.

ISBN 978-92-79-04788-6