10e Jahresbericht

der Art. 29

Datenschutzgruppe

EUROPÄISCHE
KOMMISSION

1830-6462

10. 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 2006

Angenommen am Juni 2007

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

Für die demokratische Gestaltung der Informationsgesellschaft ist der Schutz personenbezogener Daten von essentieller Bedeutung. Datenschutz gehört deshalb zu den wichtigsten Bürgerrechten des 21. Jahrhunderts. In den mehr als zehn Jahren ihres Bestehens hat sich die Arbeitsgruppe nach Art. 29 der europäischen Datenschutzrichtlinie 95/46/EG zu einem der wichtigsten Kooperationsgremien auf dem Gebiet des Datenschutzes in Europa etabliert und sich mit einer Vielzahl rechtlicher und technologischer Fragen beschäftigt.

Die folgenden Themenschwerpunkte prägten die Arbeit der Gruppe im Berichtsjahr 2006:

- Erstmals wurde eine europaweite Initiative mit dem Ziel gestartet, gemeinsam mit allen europäischen Mitgliedstaaten die Anwendung und Umsetzung von datenschutzrechtlichen Bestimmungen zu überprüfen.
- Die effektive Gewährleistung des Datenschutzes steht nach wie vor auf der Probe, wenn staatliche Stellen von Wirtschaftsunternehmen im Rahmen ihrer Kundenbeziehungen erhobene personenbezogene Daten im Bereich der Strafverfolgung nutzen wollen. Dies betrifft etwa Daten, die beim Buchen eines Fluges oder bei grenzüberschreitenden Banküberweisungen anfallen. Als besonders problematisch erweist sich dabei, dass es bis heute kein gemeinschaftsrechtliches Instrument gibt, das den Datenschutz in der Dritten Säule, also im Bereich Justiz und Strafverfolgung, regelt.
- Bei der Weiterentwicklung elektronischer Dienste und der Erschließung neuer Anwendungsbereiche der Telematik müssen Datenschutzaspekte möglichst frühzeitig berücksichtigt werden. Die Beobachtung und Begleitung von entsprechenden Vorhaben bildete einen weiteren Schwerpunkt der Tätigkeit der Arbeitsgruppe.

Mit dem Ziel einer einheitlichen Anwendung der EG-Datenschutzrichtlinie in den Mitgliedstaaten der EU unterstreicht die erste europaweite Überprüfung bei Krankenversicherungen die Wichtigkeit eines gemeinsamen Vorgehens der nationalen Aufsichtsbehörden. Unter Einbeziehung des Europäischen Verbandes der Versicherungsunternehmer war der Sektor ausgewählt worden, da er einen sehr großen Teil der Bevölkerung betrifft und dort bei den Versicherungsnehmern im besonderen Maße sensible Daten erhoben werden. Für die Art. 29-Gruppe ist eine solche Überprüfung für alle Beteiligten von großer Bedeutung. Sie zeigt, dass die Aufsichtsbehörden der EU-Mitgliedstaaten in einem derart sensible Bereich nicht nur eng zusammenarbeiten, sondern auch gemeinsam entwickelte Positionen zum Datenschutz durchsetzen können. Für die betroffenen Unternehmen hat dieses gemeinsame Vorgehen unterstrichen, dass die datenschutzrechtlichen Vorgaben im europäischen Raum einheitlich umgesetzt werden. Schließlich hat diese Aktion bei den Versicherungsnehmern das Bewusstsein für den Datenschutz gestärkt und sie über ihre Rechte aufgeklärt.

Nachdem der Europäische Gerichtshof mit Urteil vom 30. Mai 2006 entschieden hatte, dass das im Mai 2004 zwischen der EU und den USA von Amerika geschlossene Abkommen zur Übermittlung von Flugpassagierdaten wegen fehlender Rechtsgrundlage bis spätestens Ende September 2006 zu kündigen sei, wurde im Oktober 2006 ein Folgeabkommen mit einer Laufzeit bis zum 30. Juli 2007 ausgehandelt. Der Abschluss dieses Folgeabkommens ist grundsätzlich zu begrüßen, da es ansonsten keine Rechtsgrundlage für die Übermittlung von Passagierdaten an das US Heimatschutzministerium gegeben hätte und die Rechte und Freiheiten der Fluggäste fortan nicht gewährleistet gewesen wären. Die Art. 29 Gruppe hatte

sich zuvor entschieden gegen den Abschluss von bilateralen Abkommen ausgesprochen, da ansonsten eine uneinheitliche Anwendung der europäischen Datenschutzrichtlinie und eine damit einhergehende Schwächung der Rechte der betroffenen Passagiere zu befürchten gewesen wäre. Bei den Verhandlungen zu dem neuen Abkommen konnte erreicht werden, dass die im Jahre 2004 bei Vertragsabschluß von den USA gegebenen Zusicherungen weiterhin Bestand haben. Allerdings bleiben die von der Art. 29 Gruppe bei Abschluss des ersten PNR Abkommens geäußerten Vorbehalte zu wesentlichen Punkten der Vereinbarung weiterhin bestehen, was insbesondere die Zweckbindung, aber auch den Umfang der zu übermittelnden Daten betrifft. Nach wie vor erhalten die US-Behörden die Daten im sog. pull Verfahren, d.h. durch Zugriff auf die Reservierungssysteme der Fluggesellschaften und greifen damit auf den kompletten Datensatz zu, der zu jedem einzelnen Passagier vorliegt. Schon im ersten PNR Abkommen von 2004 war vorgesehen, dieses „pull Verfahren" auf ein aktives sog.„push Verfahren" umzustellen, bei dem erreicht wird, dass neben einer Reduzierung des Datensatzes auf höchstens 34 Elemente auch sensible Daten durch Einsatz einer Filtersoftware herausgefiltert werden. Nachdem die europäischen Fluglinien mehrfach mitgeteilt hatten, dass die Voraussetzungen für eine Übermittlung der Daten im „push Verfahren" erfüllt sind, sind nunmehr keine plausiblen Gründe mehr ersichtlich, die Umstellung weiter zu verzögern. Die Art. 29 Gruppe hat deshalb die Vertragsparteien im zurückliegenden Jahr wiederholt aufgefordert, die vereinbarte Lösung unverzüglich zu realisieren.

Ein wichtiges Thema der Arbeitsgruppe war der Zugriff von US–Behörden auf die von SWIFT (Society for Worldwide Interbank Financial Telecommunication) verarbeiteten Zahlungsverkehrsdaten für Zwecke der Terrorismusbekämpfung. Bei SWIFT handelt es sich um eine 1973 von der internationalen Kreditwirtschaft gegründete Genossenschaft belgischen Rechts. Die Zahlungsanweisungen, die durch den SWIFTNet FIN Service transportiert werden, enthalten personenbezogene Daten wie z.B. den Namen des Absenders und des Empfängers. SWIFT speichert alle Überweisungsdaten für 124 Tage in zwei Rechenzentren, von denen sich eines in Europa, das andere in den USA befindet. Amerikanische Behörden haben seit 2001 auf Grundlage behördlicher Beschlagnahmeanordnungen mehrfach die Herausgabe von Transaktionsdaten gegenüber SWIFT durchgesetzt, wobei der technische Anknüpfungspunkt für diese Anordnungen das in den USA befindliche SWIFT–Rechenzentrum war. SWIFT hat Daten herausgegeben, ohne dass es zu einer richterlichen Überprüfung gekommen ist. SWIFT und die US–Behörden haben 2003 eine Vereinbarung geschlossen, in der das Verfahren der Datenübermittlung festgelegt wurde. Die SWIFT–Nutzer wurden generell nicht über die Tatsache, den Umfang und den Zweck der Übermittlung informiert. Die Art. 29 –Gruppe hat im vergangenen Jahr festgestellt, dass das Gesamtverfahren wegen fehlender Rechtsgrundlage nach europäischem Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Art. 25 Abs. 1 und Abs. 2 der Richtlinie 95/46/EG. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl SWIFT als auch die Banken, die sich der Dienstleistungen von SWIFT bedienen. Die Banken wurden von der Art. 29-Gruppe aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT–Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gegen unangemessene Datenzugriffe gesichert werden. Alle Finanzinstitute in der EU, einschließlich der Zentralbanken, die die Dienstleistungen des SWIFTNet Fin Dienstes nutzen, haben gemäß Art. 10 und 11 der EG-Datenschutzrichtlinie sicherzustellen, dass sie ihre Kunden angemessen über deren Datenverarbeitung und ihre diesbezüglichen Rechte unterrichten. In diesem Rahmen müssen die Kunden auch darüber informiert werden, dass die US-Behörden Zugriff auf ihre Daten nehmen können.

Mit Blick auf die Intensivierung der Zusammenarbeit der europäischen Sicherheitsbehörden ist ein gemeinsamer europaweiter Datenschutzstandard auch für diesen Bereich unerlässlich. Aus datenschutzrechtlicher Sicht von größter Bedeutung ist das im Jahre 2004 durch die Staats und Regierungschefs der EU Mitgliedstaaten verabschiedete Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der EU, das Leitlinien im Bereich der Innen und Justizpolitik für den Zeitraum 2005 bis 2010 festlegt. So soll sich mit Wirkung vom 1. Januar 2008 der Austausch strafverfolgungsrelevanter Informationen nach dem Grundsatz der Verfügbarkeit richten, allerdings nur, wenn ein gemeinsamer Datenschutzstandard in den Mitgliedstaaten der EU gilt, der die Integrität und Vertraulichkeit der auf diese Weise ausgetauschten Daten sowie eine wirkungsvolle Datenschutzkontrolle gewährleistet. Die Kommission hat daraufhin im Oktober 2005 Vorschläge vorgelegt für Rahmenbeschlüsse über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit und für den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Bei dem vorgeschlagenen neuen Rechtsinstrument über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, hat sich die Kommission eng an die EG Datenschutzrichtlinie angelehnt und damit der Forderung der Europäischen Datenschutzkonferenz Rechnung getragen, die Datenschutzregelungen für die 3. Säule soweit möglich in Übereinstimmung mit dem geltenden Datenschutzniveau in der 1. Säule zu entwickeln. Ein Rahmenbeschluss zum Datenschutz würde zur Vereinheitlichung des Verfahrens beitragen und das beim grenzüberschreitenden Informationsaustausch erforderliche gegenseitige Vertrauen fördern, indem er einheitliche Standards vorgibt, wie die personenbezogenen Daten durch die Polizei und Strafverfolgungsbehörden der EU Mitgliedstaaten erhoben und verarbeitet werden und wie das informationelle Selbstbestimmungsrecht der von der Verarbeitung Betroffenen gewahrt wird. Der grenzüberschreitende Datenaustausch würde durch einen Rahmenbeschluss zum Datenschutz damit erleichtert. Der Rahmenbeschluss sollte die gesamte Informationsverarbeitung der Polizei und Strafverfolgungsbehörden auf nationaler Ebene und beim Informationsaustausch mit anderen Mitgliedstaaten und Drittstaaten umfassen. Ziel ist ein weitgehend einheitlicher Datenschutzstandard für die polizeiliche und justizielle Informationsverarbeitung in der gesamten EU, damit eine Divergenz der anzuwendenden Datenschutzregelungen vermieden wird. Insbesondere die tragenden Grundsätze der Zweckbindung, der Datenqualität und der Erforderlichkeit sind dabei zu wahren. Die Rechte der Betroffenen bei der Informationsverarbeitung müssen auf möglichst einheitlicher Grundlage gewährleistet sein. Neben einer unabhängigen Datenschutzkontrolle in jedem Mitgliedstaat muss zudem eine unabhängige Beratung des Rates durch die Vertreter der nationalen Datenschutzkontrollstellen sichergestellt werden.

Ein besonderes Augenmerk hat die Gruppe im zurückliegenden Jahr auch auf einen stetigen Meinungsaustausch mit Vertretern der Wirtschaft und mit anderen Interessengruppen gelegt, etwa bei der öffentlichen Konsultation vor Verabschiedung des Arbeitspapiers zu RFID (Radio Frequency Identification - WP 105). Mit Wirtschaftsvertretern wurde auch über die Verfahrensweise beim Einsatz von verbindlichen unternehmensinternen Verhaltensregeln (sog. Binding Corporate Rules, BCR) diskutiert, die die Übermittlung von personenbezogenen Daten in Länder ohne angemessenes Datenschutzniveau erheblich erleichtern soll. Bei der Erarbeitung von europaweit einheitlichen BCR Antragsformularen ist mit dem Abschluss des Abstimmungsverfahrens im Frühjahr 2007 zu rechnen. Weitere wichtige Themen waren die Verpflichtung von Unternehmen, ihre Kunden angemessen über deren Datenschutzrechte zu unterrichten (sog. Short Privacy Notices), der Schutz geistigen Eigentums und die datenschutzrechtlichen Aspekte bei Hinweisen in Unternehmen im Kampf gegen Korruption und Buchfälschung, das sog. Whistleblowing.

Auch im Jahr 2006 machte es die immer schnellere Entwicklung der Informationstechnologien erforderlich, die Instrumente des Datenschutzes auf den Prüfstand zu stellen und, soweit erforderlich, anzupassen. Für die Zukunft gilt, dass im Interesse aller Betroffenen weitere rechtliche und praktische Schritte zur Harmonisierung des Datenschutzes auf hohem Niveau unternommen werden müssen, wobei insbesondere die staatlichen Erwiderungen auf die Bedrohungen der Sicherheit nicht zu unzumutbaren Beeinträchtigungen der bürgerlichen Freiheitsrechte und insbesondere des Schutzes der personenbezogenen Daten führen dürfen.

Peter Schaar

Kapitel 1

Die Aufgaben der Artikel 29 Datenschutzgruppe[1]

[1] 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

1.1. FLUGGASTDATEN/PNR

Stellungnahme 4/2006[2] zu der Mitteilung eines Regelungsvorschlags des US Department of Health and Human Services (Gesundheitsministerium der Vereinigten Staaten) zur Kontrolle übertragbarer Krankheiten und zur Erhebung von Daten über Passagiere vom 20. November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)

Diese Stellungnahme der Artikel-29-Datenschutzgruppe enthält Überlegungen zur neuen amerikanischen Gesetzesvorlage über die Erhebung von Passagierdaten durch Fluggesellschaften und Schifffahrtslinien zur Kontrolle übertragbarer Krankheiten (Control of Communicable Diseases Proposed 42 CFR Parts 70 and 71). Die vorgesehenen Regelungen werden einer sorgfältigen Untersuchung und Analyse unterzogen, die sich auf die EU-Datenschutzrichtlinie 95/46/EG und auf die Internationalen Gesundheitsvorschriften (IGV 2005) der Weltgesundheitsorganisation WHO stützt. Letztere sind zwar nicht bindend, dienen aber dem wichtigen Ziel, die Staaten der Welt bei der Bekämpfung übertragbarer Krankheiten zu unterstützen.

Stellungnahme 5/2006[3] zum Urteil des Europäischen Gerichtshofs vom 30. Mai 2006 in den verbundenen Rechtssachen C-317/04 und C-318/04 zur Übermittlung von Fluggastdaten an die Vereinigten Staaten

Die vorliegende Stellungnahme ergeht nach dem Urteil des Europäischen Gerichtshofs vom 30. Mai 2006, durch welches der Kommissionsbeschluss zur Angemessenheitsfeststellung sowie der Kommissionsbeschluss zum Abschluss des Abkommens über die Weitergabe und Verarbeitung von Fluggastdatensätzen („PNR-Abkommen, *passenger name records*) aufgehoben und die Gemeinschaftsorgane verpflichtet werden, das genannte Abkommen mit den USA zu kündigen. Mit der vorliegenden Stellungnahme drängt die Datenschutzgruppe auf den rechtzeitigen Abschluss eines neuen Abkommens zwischen den USA und der EU, um ein rechtliches Vakuum zu vermeiden und um zu gewährleisten, dass die Rechte und Freiheiten der Fluggäste auch in Zukunft auf dem derzeitigen Niveau gewahrt bleiben. Die Stellungnahme gelangt ferner zur Schlussfolgerung, dass das EuGH-Urteil einmal mehr aufzeigt, welche Schwierigkeiten sich aus der künstlichen Aufteilung zwischen den einzelnen Säulen ergeben, und dass Bedarf nach einem kohärenten Datenschutzrahmen besteht.

Stellungnahme 7/2006[4] zum Urteil des Europäischen Gerichtshofs vom 30. Mai 2006 in den verbundenen Rechtssachen C-317/04 und C-318/04 über die Übermittlung von Fluggastdaten an die Vereinigten Staaten und zur Dringlichkeit eines neuen Abkommens

Mit dieser Stellungnahme ist die Datenschutzgruppe erneut in Sorge, dass noch kein neues Abkommen mit den USA über die Übermittlung von Fluggastdaten abgeschlossen wurde (siehe Stellungnahme WP 122). Sie betont, dass das Urteil des Europäischen Gerichtshofs zwar die Kündigung des Abkommens mit den USA nach sich gezogen hat, dass aber die Verpflichtung zur Einhaltung innerstaatlicher Datenschutzerfordernisse davon in keiner Weise berührt wird. Somit gelangt die Datenschutzgruppe zu dem Schluss, dass die fortlaufende Einhaltung der genannten Verpflichtungen von höchster Bedeutung ist. Weiterhin hofft sie auf den Abschluss eines neuen zufriedenstellenden Abkommens, so dass sich Maßnahmen der nationalen Datenschutzbehörden erübrigen.

Stellungnahme 9/2006[5] zur Umsetzung der Richtlinie 2004/82/EG des Rates über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln

In dieser Stellungnahme befürwortet die Datenschutzgruppe uneingeschränkt das Ziel, die illegale Einwanderung durch verbesserte Kontrollen bei Flügen in die EU nach Maßgabe der Richtlinie 2004/82/EG des Rates einzudämmen. Allerdings muss nach

[2] WP 112
[3] WP 122
[4] WP 124
[5] WP 127

Ansicht der Datenschutzgruppe bei der Umsetzung der genannten Richtlinie in nationales Recht so harmonisiert und einheitlich wie möglich vorgegangen werden, unter Berücksichtigung der in der Richtlinie 95/46/EG niedergelegten Datenschutzgrundsätze. Aus diesem Grund formuliert die Datenschutzgruppe in dieser Stellungnahme eine Reihe von Leitlinien für die Umsetzung und Auslegung, um zu verhindern, dass die Mitgliedstaaten in Ermangelung deutlicher Vorgaben einige Bestimmungen der betreffenden Richtlinie voneinander abweichend anwenden. Die Datenschutzgruppe ruft die Gesetzgeber der Mitgliedstaaten und alle zuständigen Behörden der Mitgliedstaaten auf, diese Leitlinien bei der Entwicklung und Anwendung ihrer nationalen Gesetze zur Umsetzung der Richtlinie zu berücksichtigen.

1.2. ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

Stellungnahme 2/2006[6] der Artikel-29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post

Vor dem Hintergrund der zunehmenden Verbreitung verschiedener onlinebasierter Kommunikationsdienste, wie etwa kostenlosen webbasierten E-Mail-Diensten und zugehörigen Diensten, ist die Datenschutzgruppe besorgt über den Datenschutz für auf solchem Wege getätigte Mitteilungen, insbesondere angesichts der bestehenden Praxis, die Mitteilungen einer „automatischen Durchleuchtung" *(Screening)* zu unterziehen, um Werbemüll (Spam) und Viren auszusondern und festgelegte Inhalte zu erkennen. Die Datenschutzgruppe ist sich bewusst, dass die meisten Anbieter von Internet- und E-Mail-Diensten Filterwerkzeuge einsetzen, um ihre Netze und Geräte zu schützen, in selteneren Fällen auch, um Nachrichten aus geschäftlichen Gründen zu prüfen. Sie ist jedoch der Ansicht, dass der Einsatz derartiger Filterwerkzeuge in bestimmten Fällen möglicherweise nicht mit den geltenden Datenschutzbestimmungen im Einklang steht, deren Anwendung auf diese neue Art von Dienstleistungen nicht immer klar ist. Mit dem vorliegenden Dokument sollen vor allem Leitlinien zur Frage der Vertraulichkeit von elektronischen Nachrichten und speziell zum Filtern von Online-Nachrichten gegeben werden. Zu diesem Zweck analysiert das Dokument unter anderem die Bestimmungen zur Vertraulichkeit elektronischer Nachrichten gemäß der Definition in Artikel 5 Absatz 1 der Richtlinie 2002/58 über den Schutz der Privatsphäre in der elektronischen Kommunikation sowie weitere einschlägige Bestimmungen, die Teil des gemeinschaftlichen Besitzstands und der zu seiner Umsetzung erlassenen innerstaatlichen Rechtsvorschriften sind. Die E-Mail-Dienstanbieter werden darin aufgefordert, die in dieser Stellungnahme enthaltenen Leitlinien und Empfehlungen bei ihrer Leistungserbringung zu berücksichtigen.

Stellungnahme 3/2006[7] zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG

Am 15. März 2006 verabschiedete der Rat die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Die Datenschutzgruppe stellt fest, dass in der Richtlinie bestimmte angemessene und besondere Sicherheitsvorkehrungen fehlen, die bei der Verarbeitung von Verbindungsdaten angezeigt sind, und es so zu einer unterschiedlichen Auslegung und Umsetzung in den Mitgliedstaaten kommen kann. Um eine einheitliche Umsetzung der Bestimmungen der Richtlinie zu erreichen und die Einhaltung der Anforderungen von Artikel 8 der Europäischen Menschenrechtskonvention zu gewährleisten, sollten die Mitgliedstaaten Sicherheitsvorkehrungen ein-

[6] WP 118

[7] WP 119

führen. In diesem Dokument wird dargelegt, welche Sicherheitsvorkehrungen in Erwägung gezogen werden sollten.

Arbeitsdokument:[8] Eingriffe in den Datenschutz im Rahmen der Initiative eCall

In diesem Arbeitsdokument werden die Bedenken der Datenschutzgruppe hinsichtlich der Eingriffe in den Datenschutz und den Schutz der Privatsphäre dargelegt, die sich im Zusammenhang mit der geplanten Einführung eines europaweiten bordeigenen Notrufdienstes („eCall") ergeben, der auf die einheitliche europäische Notrufnummer 112 aufbaut. Die Datenschutzgruppe erkennt zwar die sozioökonomischen Vorteile an, die die breite Einführung des eCall-Dienstes für die Bürger mit sich bringen könnte, weist jedoch darauf hin, dass die Einführung dieses Dienstes Auswirkungen auf den Datenschutz und den Schutz der Privatsphäre hat, die herausgearbeitet und angemessen berücksichtigt werden müssen.

Angesichts der dargelegten möglichen Beeinträchtigungen der Privatsphäre durch den eCall-Dienst empfiehlt die Datenschutzgruppe für den Fall der Einführung des Dienstes einen freiwilligen Ansatz. Aus datenschutzrechtlicher Perspektive ist ein Notruf, der automatisch durch ein Gerät oder manuell ausgelöst und dann über Mobilfunknetze übertragen wird, so dass der geografische Standort des Notfalls bestimmt werden kann, im Prinzip durchaus zulässig, sofern die entsprechende spezifische Rechtsgrundlage besteht und ausreichende Sicherheitsvorkehrungen für den Datenschutz getroffen werden.

Stellungnahme 8/2006[9] zur Überprüfung des Rechtsrahmens für elektronische Kommunikationsnetze und -dienste mit Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation

In dieser Stellungnahme legt die Datenschutzgruppe im Anschluss an die Überprüfung des Reformpakets für elektronische Kommunikation *(eCommunications)* ihre entsprechenden Besorgnisse und Anmerkungen dar, insbesondere hinsichtlich der Datenschutzrichtlinie für elektronische Kommunikation *(ePrivacy)*. Des Weiteren nimmt sie Bezug auf die Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation. Seinerzeit wurden eine Reihe von Anregungen gemacht, die jedoch keine Berücksichtigung fanden. In der vorliegenden Stellungnahme wiederholt die Datenschutzgruppe diese Vorschläge daher. Ferner empfiehlt sie eine Verstärkung der Sicherheitsvorkehrungen und betont, dass neben der Verbesserung der Sicherheit der Infrastruktur auch der Schutz der Nutzer und die Steigerung ihres Vertrauens in die elektronische Kommunikation umfassend berücksichtigt werden müssen. Die Datenschutzgruppe empfiehlt auch, dass auf Fragen im Zusammenhang mit Online-Anwendungen (Sicherheitsfragen, Verantwortlichkeit der Betreiber sowie Klärung des Rechtsstatus und Definition des für die Datenverarbeitung Verantwortlichen) eingegangen wird.

1.3. SWIFT

Stellungnahme 10/2006[10] zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Diese Stellungnahme 29/2006 der Artikel-29-Datenschutzgruppe enthält die Ergebnisse ihrer Untersuchung zur Verarbeitung von personenbezogenen Daten durch die *Society for Worldwide Interbank Financial Telecommunication (SWIFT)*. In diesem Zusammenhang betont die Artikel-29-Datenschutzgruppe, dass die Grundrechte auch beim Kampf gegen Terrorismus und Kriminalität gewahrt bleiben müssen. Daher beharrt sie auf der Einhaltung von weltweiten Datenschutzgrundsätzen. In der Stellungnahme werden einige Schlussfolgerungen

[8] WP 125
[9] WP 126
[10] WP 128

veröffentlicht, die die Datenschutzgruppe in Zukunft einer regelmäßigen Überwachung unterziehen möchte.

1.4. RECHNUNGSWESEN, WIRTSCHAFTSPRÜFUNG UND FINANZFRAGEN

Stellungnahme 1/2006[11] 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

Diese Stellungnahme enthält Leitlinien zur Umsetzung interner Verfahren zur Meldung von Missständen nach den EU-Datenschutzvorschriften, die in der Richtlinie 95/46/EG niedergelegt sind. Die Stellungnahme kommt zur Erkenntnis, dass die Einhaltung dieser Grundsätze den Unternehmen und Systemen zur Meldung von Missständen dabei hilft, die richtige Funktionsweise solcher Verfahren zu gewährleisten. Ferner wird betont, dass bei der Umsetzung eines Verfahrens zur Meldung von Missständen das grundlegende Recht auf den Schutz personenbezogener Daten sowohl des Hinweisgebers als auch der beschuldigten Person während des gesamten Meldeverfahrens gewährleistet werden muss. Die Datenschutzgruppe unterstreicht, dass die in der Richtlinie 95/46/EG niedergelegten Datenschutzgrundsätze umfassend auf Verfahren zur Meldung von Missständen angewandt werden müssen, insbesondere hinsichtlich der Rechte der beschuldigten Person auf Auskunft, Zugriff, Berichtigung und Löschung von Daten. Angesichts der unterschiedlichen Interessen erkennt die Datenschutzgruppe in ihrem Dokument allerdings an, dass die Ausübung dieser Rechte in bestimmten eng umgrenzten Fällen eingeschränkt werden kann, um das erforderliche Gleichgewicht zwischen dem Recht auf Schutz der Privatsphäre und den durch das Programm verfolgten Zielen zu erreichen. Derartige Beschränkungen sollten jedoch restriktiv gehandhabt und nur in dem Maße angewandt werden, das erforderlich ist, um die Ziele des Systems zu erreichen.

1.5. UNTERHALTSPFLICHTEN

Stellungnahme 6/2006[12] zu dem Vorschlag für eine Verordnung des Rates über die Zuständigkeit und das anwendbare Recht in Unterhaltssachen, die Anerkennung und Vollstreckung von Unterhaltsentscheidungen und die Zusammenarbeit im Bereich der Unterhaltspflichten

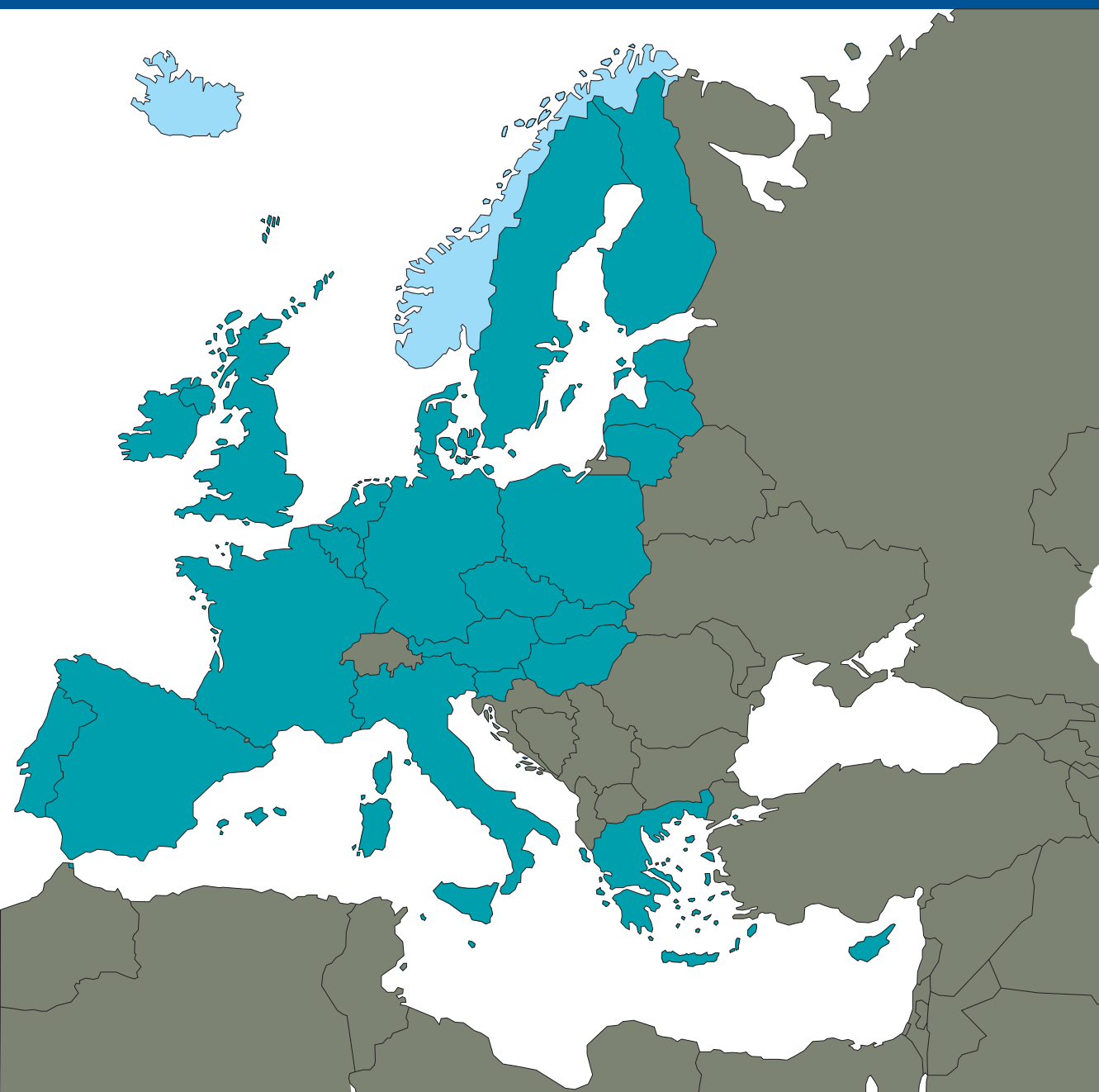
In diesem Dokument erörtert die Datenschutzgruppe eine Reihe von Datenschutzfragen im Zusammenhang mit dem Vorschlag der Kommission für eine Verordnung des Rates über die Zuständigkeit und das anwendbare Recht in Unterhaltssachen sowie die Anerkennung und Vollstreckung von Unterhaltsentscheidungen, und insbesondere zu Kapitel VIII: Zusammenarbeit im Bereich der Unterhaltspflichten. Dieses Kapitel VIII („Zusammenarbeit") enthält nämlich einen Mechanismus zur Sammlung von Daten über die wirtschaftliche Situation des Unterhaltspflichtigen und des Unterhaltsberechtigten sowie zum Austausch dieser Daten über ein Netz zentraler Behörden der Mitgliedstaaten. Die Stellungnahme ruft in Erinnerung, dass eine derartige Datenverarbeitung gemäß den in der Richtlinie niedergelegten Grundsätzen und Regeln erfolgen muss. Es wird darauf hingewiesen, dass der Vorschlag bereits eine Reihe von Elementen enthält, die darauf abzielen, die Einhaltung der genannten Prinzipien bei der Datenverarbeitung zu gewährleisten. Gleichzeitig werden jedoch weitere Punkte genannt, bei denen in das System für den Austausch personenbezogener Daten zusätzliche Datenschutzgarantien eingebaut werden sollten.

[11] WP 117

[12] WP 123

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

Die Richtlinie 2004/48/EG über die Durchsetzung von Urheberrechten wurde umgesetzt, so dass die Inhaber von Urheberrechten leichter an personenbezogene Daten von Urheberrechtsverletzern gelangen können. Von besonderer Relevanz ist dies für die Daten von Internetnutzern, die im Verdacht stehen, online Musikaufnahmen zu tauschen. Die Richtlinie wurde in das österreichische Urheberrechtsgesetz eingearbeitet und die abgeänderte Fassung am 21. Juni 2006 im Bundesgesetzblatt I Nr. 81/2006 veröffentlicht.

Das österreichische Sicherheitspolizeigesetz wurde ebenfalls geändert (vgl. Bundesgesetzblatt I Nr. 158/2005), so dass die Polizei nun über umfassendere Befugnisse für den Schutz von Staatsbesuchern und Sportveranstaltungen verfügt. Dazu zählen erweiterte Möglichkeiten für den Einsatz von Daten aus Videoüberwachung, auch wenn diese von Privatunternehmen durchgeführt wird.

Das Gesetz zur Durchsetzung von Rechtstiteln *(Exekutionsordnung)* wurde geändert, um die Privatsphäre von Menschen zu schützen, die unerwünschten Kontakten oder unerwünschter sonstiger Aufmerksamkeit seitens anderer Personen ausgesetzt sind (vgl. Bundesgesetzblatt I Nr. 56/2006). Der neue Paragraf 382g der Exekutionsordnung ermöglicht es den Gerichten, einer Person zu verbieten, die personenbezogenen Daten einer anderen Person in einer Weise zu verwenden, durch die es zu einer Verletzung von deren Privatsphäre oder zu einer Belästigung kommt (etwa durch die herabwürdigende Veröffentlichung personenbezogener Daten im Internet).

B. Bedeutende Rechtsprechung

1) Ein österreichischer Internetdienstanbieter (ISP – Internet Service Provider) führte eine Vorratsdatenspeicherung zur dynamischen IP-Adresse eines Kunden durch, um eine Fair Use Policy (FUP, ein Verbot der deutlich überdurchschnittlichen Bandbreitennutzung bei Pauschaltarifen) durchzusetzen. Der ISP wurde durch eine gerichtliche Anordnung gezwungen, diese Daten an eine Urheberrechtsverwertungsgesellschaft weiterzugeben. Zwei Kunden, denen in der Folge Urheberrechtspiraterie zur Last gelegt wurde, reichten Beschwerde gegen den ISP wegen illegaler Vorratsspeicherung der genannten Daten ein. Das österreichische Telekommunikationsgesetz 2003 (TKG 2003, Bundesgesetzblatt I Nr. 70/2003), durch welches geregelt wird, welche Daten ein ISP speichern darf, schreibt in Paragraf 99 Absatz 1 ausdrücklich vor, dass sämtliche Verkehrsdaten nach Beendigung der Verbindung unverzüglich zu löschen sind. Die Datenschutzkommission befand daher, dass der ISP kein Recht hatte, die dynamische IP-Adresse zu Rechnungszwecken länger als tatsächlich erforderlich zu speichern, denn bei dynamischen IP-Adressen handelt es sich um Verkehrsdaten.

2) Ein Sanatorium hatte eine Bewilligung für einen Hubschrauberlandeplatz, allerdings unter der Auflage, dass die Anzahl an Flügen pro Wintersaison maximal zehn betragen dürfe. Eine Gruppe von Bürgern aus der Nachbarschaft war jedoch der Ansicht, dass die tatsächliche Anzahl an Flügen weit über dieser Zahl liege. Sie empfanden den Hubschrauberlärm als untragbar und beschlossen, die Landungen mit Videokameras zu dokumentieren. Ein Hubschrauberpilot reichte dagegen Beschwerde ein. Die Datenschutzkommission stellte fest, dass die Videobänder unter den Begriff der Datenverarbeitung fallen und dass daher im Prinzip ein Auskunftsrecht für die betroffene Person bestehen würde, allerdings unter der Bedingung, dass der Zweck dieser Aufnahme in der Überwachung von Einzelpersonen liegen würde. Die Aufnahmen verfolgten jedoch gerade nicht den Zweck, den Hubschrauberpiloten oder sonstige Personen persönlich zu überwachen, sondern vielmehr, die Anzahl

an Hubschrauberflügen zu dokumentieren. Daher entschied die Kommission, dass in diesem Fall kein Auskunftsrecht für die betroffene Person besteht, da diese (der Hubschrauberpilot) auf den Aufnahmen praktisch gar nicht zu identifizieren ist.

3) Eine Eisenbahngesellschaft betrieb mit Videokameras ausgerüstete Waggons. Diese waren jedoch nicht in Benutzung, da eine entsprechende Genehmigung seitens der Datenschutzkommission im Rahmen einer Vorabprüfung noch ausstand. Ein Bürger, der in einem dieser Waggons reiste, verlangte Recht auf Auskunft. Die Datenschutzkommission entschied, dass hier nicht von einer Datenerfassung auszugehen ist, da die Anlage sich nicht in Betrieb befand. Folglich brauchte die Eisenbahngesellschaft auch keine Auskunft zu gewähren.

4) In einem anderen Fall ging es um einen Bürger, dessen personenbezogene Daten in einem Dokument erschienen, das dem österreichischen Parlament vorgelegt und in der Folge auf der Website des Parlaments veröffentlicht wurde. Aufgrund einer Beschwerde des Bürgers an das Parlament wurde sein Name getilgt. Internet-Suchmaschinen fanden das nicht-anonymisierte vorherige Dokument jedoch weiterhin. Deshalb legte der Bürger Beschwerde bei der Datenschutzkommission ein. Diese entschied, dass das Parlament nicht für die Funktionsweise von Suchmaschinen hafte.

C. Wichtige spezifische Themen

Videoüberwachung

Die Anzahl an Meldungen von bzw. Beschwerden über Videoüberwachung ist im Lauf des vergangenen Jahres sehr stark angestiegen. Dies liegt sowohl am geschärften öffentlichen Bewusstsein als auch an einem systematischen Ansatz zur Durchsetzung der bestehenden Meldepflicht.

Grenzüberschreitende Datenflüsse

Die Österreichische Datenschutzkommission hat festgestellt, dass die meisten internationalen Konzerne, die Daten in Länder übertragen möchten, welche kein angemessenes Datenschutzniveau bieten, als bevorzugtes Rechtsinstrument auf die Standardvertragsklauseln zurückgreifen. Nur wenige Konzerne mit Hauptsitz in den USA nutzen die „Sichere Häfen" -Regelung, obwohl die Geschäftsstelle der Datenschutzkommission die Konzernvertreter und deren Rechtsanwälte regelmäßig über diese Möglichkeit informiert. Bitten um die Angabe von Gründen, aus denen die „Sichere Häfen"-Regelung nicht genutzt wird, bleiben unbeantwortet.

Auch bei der Einführung von verbindlichen unternehmensinternen Vorschriften (BCR - Binding Corporate Rules) legen die genannten Konzerne ein niedriges Tempo an den Tag. Allerdings konnte die Geschäftstelle der Datenschutzkommission mehrere Versuche verzeichnen, BCR-artige Systeme anhand abgeänderter Versionen der Standardvertragsklauseln aufzubauen.

Belgien

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

Richtlinie 95/46/EG und Richtlinie 2002/58/EG

Keine Entwicklung.

Weitere Entwicklungen in der Gesetzgebung

Koordinationsorgan für die Bedrohungsanalyse (OCAM/CODA)

Mit dem Gesetz vom 10. Juli 2006 über die Bedrohungsanalyse (Belgisches Staatsblatt *(Moniteur Belge/Belgisch Staatsblad)* wurde ein neues Sicherheitsorgan geschaffen: das Koordinierungsorgan für die Bedrohungsanalyse OCAM/CODA *(Organe de coordination pour l'analyse de la menace/Coördinatieorgaan voor de Dreigingsanalyse)*. Seine Aufgabe ist die Beurteilung der terroristischen und extremistischen Bedrohungen, welche die innere und äußere Sicherheit des Staates, die belgischen Interessen und die Sicherheit der belgischen Staatsangehörigen im Ausland gefährden könnten. Zur Durchführung seiner Aufgaben darf das OCAM/CODA eine oder mehrere Datenbanken anlegen, wobei der Zweck, die Art der verarbeiteten Daten und Informationen, die Speicherungsdauer der Daten, die Zugriffs- und Weitergabemodalitäten sowie die Löschungsmodalitäten durch einen Königlichen Erlass geregelt werden, der durch den Ministerrat nach Stellungnahme der belgischen Datenschutzkommission zu verabschieden ist.

Ein Entwurf für einen entsprechenden Königlichen Erlass wurde der Datenschutzkommission zur Stellungnahme vorgelegt. In ihrer Stellungnahme erhebt die Datenschutzkommission Einwände gegen die vorgesehene Speicherungsdauer von 30 Jahren. Ferner ist sie der Ansicht, dass die Notwendigkeit der weiteren Speicherung von Daten durch regelmäßig durchzuführende Beurteilungen ermittelt werden muss. Außerdem führt sie aus, dass die Relevanz der Daten bei jeder einzelnen Nutzung sowie für den gesamten Datenbestand im 5-Jahres-Turnus geprüft werden muss. Die Datenschutzkommission betont abschließend, dass angesichts des unzureichenden Rechtsrahmens der Einrichtung, deren Rechtsnachfolge das OCAM/CODA antritt, der faktische Zugriff seitens des neuen Organs auf bestimmte Informationssysteme nicht als Ausdruck der Rechtmäßigkeit eines solchen Zugriffs ausgelegt werden darf.

Der Königliche Erlass wurde am 28. November 2006 verabschiedet. Die Anmerkungen der Datenschutzkommission wurden nur zum Teil berücksichtigt (Königlicher Erlass zur Durchführung des Gesetzes vom 10. Juli 2006 über die Bedrohungsanalyse, Belgisches Staatsblatt *(Moniteur Belge/Belgisch Staatsblad)*, 1. Dezember 2006).

Elektronische Verwaltung – Informatisierung des Rechtssystems

Im Anschluss an das Gesetz vom 10. August 2005 zur Informatisierung des Rechtssystems (vgl. Bericht 2005) wurden zwei weitere Gesetze verabschiedet. Mit dem ersten wird das so genannte elektronische Gerichtsverfahren eingeführt (Erstellung elektronischer Schriftsätze in Zivil- und Strafsachen, Kennzeichnungskonventionen, elektronische Benachrichtigung und Einreichung). Das zweite Gesetz dient zur Abänderung einer Reihe von Bestimmungen des Gerichtsgesetzbuchs, um die Rechtsgrundlage für derartige papierlose Verfahren zu schaffen. Dabei ließ sich der Gesetzgeber von den Prinzipien der Notwendigkeit (nur solche Bestimmungen wurden geändert, bei denen dies tatsächlich erforderlich ist) und der technologischen Neutralität leiten. Ins Justizwesen halten damit neue Konzepte Einzug, wie etwa die elektronische Adresse, die an die Seite der klassischen Begriffe „Wohnort" und „Aufenthaltsort" tritt. Es kommt auch ein neuer Akteur ins Spiel, ein Mittelsmann zwischen den „klassischen" Akteuren des Justizwesens (Richter, Anwälte, Notare) und den Rechtssubjekten: Es handelt sich um den Kommunikationsdienstleister (Gesetz vom 10. Juli 2006 über das elektronische Verfahren, Belgisches

Staatsblatt *(Moniteur Belge/Belgisch Staatsblad)*, 7. September 2006; sowie Gesetz vom 5. August 2006 zur Änderung gewisser Bestimmungen im Hinblick auf das elektronische Verfahren, Belgisches Staatsblatt *(Moniteur Belge/Belgisch Staatsblad)*, 7. September 2006).

Elektronische Verwaltung – Informatisierung des Gesundheitswesens

In der Flämischen Gemeinschaft wird ein Gesundheitsinformationssystem *(Gezondheid Informatie Systeem – GIS)* eingerichtet. Dieses System verfolgt einen doppelten Zweck. Zum einen ist dies die Optimierung des Datenaustauschs zur Gewährleistung der Kontinuität und der Qualität der medizinischen Leistungen im Beziehungsgeflecht von Leistungserbringern, vor Ort tätigen Einrichtungen und Informationsknotenpunkten. In diesem Rahmen wird für jeden Empfänger medizinischer Leistungen eine individuelle elektronische Akte angelegt und unter der Verantwortung des Leistungserbringers geführt. Zum anderen wird die Optimierung des Datenaustauschs mit der Verwaltung angestrebt. Hierbei geht es um die erforderlichen Daten für die fundierte Beurteilung der Gesundheitspolitik, um ggf. Korrekturen vornehmen zu können. Mit dem Dekret wird auch eine Kontrollkommission auf Ebene der Flämischen Gemeinschaft eingerichtet (während die bestehende Datenschutzkommission auf föderaler Ebene tätig ist). Ihre Aufgabe ist insbesondere die Überwachung der Einhaltung des Dekrets, die Abgabe von Stellungnahmen und Empfehlungen sowie die Bearbeitung von Beschwerden und von Anträgen auf Weiterbehandlung (Dekret der Flämischen Gemeinschaft vom 16. Juni 2006 über das Gesundheitsinformationssystem, Belgisches Staatsblatt *(Moniteur Belge/Belgisch Staatsblad)*, 7. September 2006).

Auf der Ebene des föderalen Gesamtstaates wird voraussichtlich Anfang 2007 ein Gesetz zur Schaffung eines sektoriellen Ausschusses für soziale Sicherheit und Gesundheit verabschiedet (vgl. unten).

B. Rechtsprechung

Eine Entscheidung des Erstinstanzgerichts Dendermonde zum Thema Videoüberwachung zeigt auf, wie dringlich in diesem Bereich eine gesetzliche Regelung getroffen werden muss (vgl. unten). Eine Privatperson hatte im öffentlichen Raum mehrere Kameras zur Überwachung ihres Eigentums installiert. Obwohl diese Kameras zwangsläufig auch die Nachbargebäude und alles, was sich auf der Straße abspielte, filmten, befand das Gericht, dass das Gesetz über den Schutz der Privatsphäre auf diesen Fall nicht anwendbar ist (*Rechtbank van Eerste Aanleg te Dendermonde*, 25. Oktober 2006).

C. Wichtige spezifische Themen

Allgemeine Einführung

Die bereits in den Vorjahren festgestellte Tendenz zur Zentralisierung und Vernetzung von Daten setzte sich auch 2006 fort. In ihren Stellungnahmen und Positionen im Jahresverlauf hat die Datenschutzkommission, wie schon 2005, stets den Akzent auf die Einhaltung des Prinzips der Kompatibilität zwischen den Dateien (zur Vermeidung einer systematischen Datenvermehrung) sowie auf die Transparenz der Datenverarbeitung gegenüber dem Bürger gesetzt. Angesichts der wachsenden Anzahl von Projekten zur elektronischen Verwaltung (vgl. öffentlicher Sektor) verwies die Datenschutzkommission erneut mit Nachdruck auf diese Prinzipien.

Das allgemeine Ziel „Sicherheit" – im Einzelnen: „öffentliche Sicherheit", „Sicherheit im Finanzwesen" sowie „Sicherheit in der Wirtschaft" – schlug sich ebenfalls in zahlreichen belgischen (vgl. Schwarze Listen und Videoüberwachung) und ausländischen Initiativen nieder. Die Problemkreise *„Whistleblowing"* (innerbetriebliche Hinweisgeber) sowie „SWIFT", mit denen die Datenschutzkommission im Jahresverlauf 2006 intensiv beschäftigt war, sind symptomatisch für die Schwierigkeiten bei der Harmonisierung zwischen den europäischen Datenschutzsystemen – einschließlich der belgischen Regelungen – und den US-amerikanischen

Gesetzen und Verordnungen mit ihrem charakteristischen Extraterritorialitätsprinzip.

Polizei und Sicherheit

Geheimdienste – Am 18. Oktober 2006 veröffentlichte die Datenschutzkommission eine Stellungnahme zu einem Vorentwurf für ein Gesetz zur Regelung der Gesamtheit der seitens der Geheimdienste angewandten Datenerhebungsverfahren. Der Vorentwurf sieht neben den herkömmlichen Datenerhebungsverfahren auch spezifische Verfahren (beispielsweise Erfassung von Telefonverbindungsdaten, Ermittlung des Absenders einer Briefsendung, Ermittlung eines Abonnenten) sowie außerordentliche Verfahren (Ermittlung des Inhalts einer Briefsendung oder einer E-Mail, Erfassung von Daten zu Bankkonten usw.) vor. In ihrer Stellungnahme äußert sich die Datenschutzkommission in erster Linie zufrieden über die Absicht der Regierung, eine gesetzliche Grundlage für die Datenerhebung zu schaffen. Es folgt eine Prüfung der Einhaltung von Artikel 8 der Europäischen Menschenrechtskonvention sowie der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, aufgrund deren die Datenschutzkommission auf eine Reihe von Problemen hinweist, die bei der angestrebten Regelung hinsichtlich der erforderlichen Transparenz und Zugänglichkeit bestehen, eine Problematik, die ihre Ursache vor allem in der Vielzahl der Genehmigungs- und Kontrollmechanismen sowie Kontrollorgane hat. Insbesondere verweist die Datenschutzkommission auf folgende Punkte: (1) Unabhängigkeit und Zusammensetzung der Genehmigungs- und Kontrollorgane, (2) ordnungsgemäße Verteilung der Zuständigkeiten, (3) Sachkenntnis der für die Genehmigung zuständigen Person und (4) Gleichgewicht zwischen den verschiedenen durch die Regelung tangierten Interessen, Rechten und Freiheiten.

Videoüberwachung – Die Videoüberwachung stand 2006 im Zentrum des Interesses des Gesetzgebers und der Datenschutzkommission. Im Parlament wurden mehrere Gesetzentwürfe und zugehörige Änderungsanträge zur gesetzlichen Regelung der Videoüberwachung eingebracht. Mit einem dieser Gesetzentwürfe hat sich die Datenschutzkommission eingehend befasst. Zum Abschluss dieser Analyse bekräftigte die Datenschutzkommission ihre Ansicht, dass der Gesetzgeber angesichts des Legalitätsprinzips die wesentlichen Merkmale der Videoüberwachung genau definieren muss. Die Kommission fordert außerdem die Einrichtung eines speziellen, durch die Datenschutzkommission anzuwendenden Kontrollmechanismus, um die Einhaltung des Verbots der Speicherung sensibler Daten zu gewährleisten. Im Übrigen weist die Datenschutzkommission auf eine Reihe von schwerwiegenden Unstimmigkeiten gegenüber dem Gesetz über den Schutz der Privatsphäre und der Richtlinie 95/46/EG hin. Im Gefolge dieser Stellungnahme wurde die Datenschutzkommission über sämtliche Änderungen am Gesetzentwurf auf dem Laufenden gehalten. Die parlamentarische Erörterung des Gesetzentwurfs ist noch im Gange.

Eine weitere bei der Datenschutzkommission eingereichte Beschwerde betraf eine private Kinderkrippe, deren Leitung ein Videoüberwachungssystem (Webcams) im Betreuungsbereich installiert hatte. Der Beschwerdeführer betrachtete dies als Verstoß gegen das Gesetz über den Schutz der Privatsphäre. Diese Anlage sollte den Eltern die Möglichkeit geben, zu bestimmten Tageszeiten ihre Kinder per Internet zu beobachten. Die Datenschutzkommission befand diese Datenverarbeitung für gesetzwidrig, sowohl hinsichtlich des Schutzes der Privatsphäre der Kinder und der Betreuungskräfte als auch hinsichtlich der besonderen Datenschutzauflagen bei Kindern. Erschwerend hinzu kam die mangelnde Kontrolle über die Bilder, aufgrund deren das Risiko einer gesetzwidrigen sekundären Nutzung besteht.

Öffentlicher Sektor

Die bei der Datenschutzkommission eingegangenen Anträge zur Genehmigung von Datenübermittlungen belegen, dass immer mehr Einrichtungen der öffentlichen Verwaltung bestrebt sind, die verschiedenen Daten zu ein und demselben Bürger zusammenführen. In manchen Fällen ist der Beweggrund hierfür

eine Vereinfachung der Verwaltungsvorgänge, in anderen jedoch ein Kontrollstreben. Eine derartige Datenzusammenführung wünschen sich die entsprechenden Einrichtungen beispielsweise hinsichtlich der Finanzlage von Personen, die Leistungen oder Vorteile beantragen oder genießen, welche an bestimmte Einkommensgrenzen geknüpft sind. In diesen Fällen verweist die Datenschutzkommission besonders auf die erforderliche Einhaltung des Legalitätsprinzips und des Zweckbindungsprinzips sowie auf das Recht der betroffenen Person auf angemessene Auskunft.

Im Rahmen der Ausarbeitung des ehrgeizigen Projekts zur Informatisierung des Rechtssystems (vgl. oben) wurde die Datenschutzkommission um Stellungnahme zur Frage gebeten, ob man den verschiedenen Akteuren im Justizwesen (Rechtsanwälte, Gerichtsvollzieher, Notare…) auferlegen kann, ihren elektronischen Personalausweis sowohl für den Zugang zum System Phénix als auch zur elektronischen Signatur sämtlicher im Rahmen der Gerichtsverfahren elektronisch übermittelten und/oder eingereichten Dokumente zu verwenden. Im Einklang mit ihrer bisherigen Rechtsauffassung verlangt die Datenschutzkommission die Einführung von technischen Maßnahmen, um für die Rechtssubjekte im Verkehr mit den Justizbehörden eine spezifische, von der Nationalregisternummer abweichende Kennzahl verwenden zu können. Auf diese Weise sollen Suchen und Querverbindungen anhand der Nationalregisternummer unmöglich gemacht werden. Ferner empfiehlt die Datenschutzkommission auch ein Eingreifen des Gesetzgebers zur Klärung der Einsatzmodalitäten des elektronischen Ausweises der im Justizwesen tätigen Personen.

Privatsektor

Schwarze Listen – Im Bericht 2005 wurde mitgeteilt, dass die Datenschutzkommission auf Anfrage der Regierung die Grundlagen zusammengestellt hat, die bei einem gesetzlichen Rahmen für so genannte Schwarze Listen (Negativlisten) zu beachten wären. Die Datenschutzkommission hatte ein Eingreifen des Gesetzgebers bei den Schwarzen Listen in der Privatwirtschaft für notwendig erachtet, um hier für eine Stärkung des Datenschutzes zu sorgen. Ferner empfahl die Datenschutzkommission ein Vorabgenehmigungsverfahren für so genannte sensible Listen, zusätzliche allgemeine Garantien sowie interne Kontrollmechanismen. Im Jahr 2006 wurde die Datenschutzkommission nun um eine Stellungnahme zu einem Vorentwurf für ein Gesetz über Schwarze Listen gebeten. In ihrer Stellungnahme bekräftigt die Datenschutzkommission, dass das Gesetz klarstellen muss, dass Schwarze Listen grundsätzlich gesetzwidrig sind, außer in spezifischen, gesetzlich geregelten Ausnahmefällen. Der Gesetzgeber wird außerdem aufgefordert, zu definieren, welche Bedingungen erfüllt sein müssen, damit eine Person in eine derartige Schwarze Liste aufgenommen werden darf, welche Angaben die Liste enthalten darf, wie die Zweckbestimmung zu formulieren ist, wie lange die Daten gespeichert werden dürfen und wie die Verbreitung und der Zugriff auf die Daten geregelt werden. Dieses Gesetzesprojekt befindet sich noch in der Erörterungsphase.

SWIFT – Die Verarbeitung von personenbezogenen Daten durch die Firma SWIFT und insbesondere die Übermittlung dieser Daten in die Vereinigten Staaten sowie der Zugriff durch das US-Finanzministerium (*United States Treasury* - UST) mit dem erklärten Ziel der Terrorismusbekämpfung waren Gegenstand von zwei Stellungnahmen der Datenschutzkommission. Die erste geht auf die Vereinbarkeit dieser Datenverarbeitungen mit dem Gesetz über den Schutz der Privatsphäre ein. Die Datenschutzkommission gelangt zur Einschätzung, dass seitens der belgischen Firma, die in dieser Sache als der für die Datenverarbeitung Verantwortliche zu betrachten ist, gegen mehrere – strafrechtlich relevante – Bestimmungen verstoßen wurde. Insbesondere befand die Datenschutzkommission, dass die Firma SWIFT sich einer schwerwiegenden Fehleinschätzung schuldig gemacht hat, indem sie mehrere Jahre lang heimlich und systematisch sehr umfangreiche Mengen von personenbezogenen Daten für eine Überprüfung zur Verfügung gestellt hat, ohne dass

hierfür eine hinreichende und klare Rechtsgrundlage oder eine unabhängige Kontrolle bestanden hätte, wie sie durch belgisches und europäisches Recht vorgeschrieben ist. Bei der zweiten Stellungnahme handelt es sich um die Antwort auf ein Ersuchen der belgischen Regierung, detailliert darzulegen, welche Punkte aus Sicht des Datenschutzes in einem diesbezüglichen Übereinkommen mit den Vereinigten Staaten enthalten sein müssten und in welcher Form ein derartiges Übereinkommen geschlossen werden könnte. Vorrangig rief die Datenschutzkommission in Erinnerung, dass die Firma SWIFT sich unter allen Umständen an die belgischen und europäischen Regelungen halten muss. Was den Abschluss eines spezifischen Übereinkommens mit den Vereinigten Staaten anbelangt, so befand die Datenschutzkommission, dass es sich dabei nicht um den einzigen gangbaren Weg handelt, um Abhilfe gegen das unterschiedliche Schutzniveau des US-amerikanischen und des europäischen Rechtssystems zu schaffen. Die Datenschutzkommission empfiehlt, in einem ersten Schritt eine Anpassung der bestehenden Abkommen und Verfahren zur Terrorismusbekämpfung vorzunehmen, im Einklang mit den geltenden europäischen Datenschutzprinzipien, mit den Empfehlungen der Arbeitsgruppe „Finanzielle Maßnahmen gegen die Geldwäsche" *(Financial Action Task Force - FATF)* und mit den Verfahren für den Austausch personenbezogener Daten über die Zentralstellen für Geldwäsche-Verdachtsanzeigen *(Financial Intelligence Units - FIU)*. In die gleiche Richtung geht der Vorschlag der Datenschutzkommission, den Anwendungsbereich des Rahmenbeschlusses des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, dahingehend zu ändern, dass auch die Übermittlung von privaten Daten, wie den Daten der Firma SWIFT, an öffentliche Einrichtungen, wie das US-Finanzministerium, abgedeckt wird.

Die Datenschutzkommission verfolgt mit großer Aufmerksamkeit die weitere Entwicklung in dieser Frage sowie die seitens der Firma SWIFT ergriffenen Maßnahmen, um ihre Tätigkeit wieder mit den belgischen Regelungen für den Datenschutz in Einklang zu bringen. Diese Beobachtung erfolgt in enger Abstimmung mit den europäischen Partnerbehörden in der Artikel-29-Datenschutzgruppe.

Whistleblowing (innerbetriebliche Hinweisgeber) – Bereits im Bericht 2005 wurde mitgeteilt, dass bei der Datenschutzkommission häufig Anfragen hinsichtlich der Einführung von ethischen Arbeitsrichtlinien für innerbetriebliche Hinweisgeber *(„Whistleblowing")* eingehen.

Inzwischen hat die Datenschutzkommission eine *Empfehlung hinsichtlich der Vereinbarkeit von innerbetrieblichen Maßnahmen zur Unterstützung von Hinweisgebern („Whistleblowing") mit dem Gesetz über den Schutz der Privatsphäre* veröffentlicht (Originaltitel: *„Recommandation relative à la compatibilité des systèmes d'alerte professionnelle avec la loi sur la vie privée"*). In dieser Empfehlung wird vorrangig betont, dass bei der Einrichtung von innerbetrieblichen Maßnahmen zur Unterstützung von Hinweisgebern *(„Whistleblowing-System")* ein Gleichgewicht zwischen den legitimen Interessen sämtlicher Akteure (Unternehmen, Belegschaft, Hinweisgeber, Beschuldigter und etwaige Dritte) gefunden werden muss. Die Datenschutzkommission besteht zudem auf der Wahrung einer Reihe grundlegender Prinzipien: Loyalität, Zulässigkeit, Zweckgebundenheit und Angemessenheit sowie Transparenz, und zwar sowohl seitens der Gruppe als auch seitens des Einzelnen. Auch auf die Rechte der Person geht die Datenschutzgruppe ein, denn diese gelten gleichermaßen für den Hinweisgeber, für den Beschuldigten und für eventuelle Dritte.

Verpflichtung zur Sicherheit

Die Datenschutzkommission hat *Referenzmaßnahmen zur Gewährleistung der Sicherheit bei jedweder Verarbeitung von personenbezogenen Daten* veröffentlicht (Originaltitel: *„Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel"*). Es wurden zehn mit der Datensicherheit in Verbindung stehende Aktionsbereiche ermittelt, zu denen jede Einrichtung, die personenbezogene Daten speichert, verarbeitet oder übermittelt, entsprechende Maßnahmen ergreifen muss.

Zypern

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

Im Jahresverlauf 2006 gab es keine Änderungen am Gesetz zur Umsetzung der Richtlinie 95/46/EG, d. h. am Gesetz über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre aus dem Jahr 2001.

Im Jahr 2006 wurde im Zusammenwirken mit der Regulierungsbehörde für das Post- und Telekommunikationswesen OCTPR *(Office of the Commissioner of Telecommunications and Postal Regulation)* eine Gesetzesvorlage zur Änderung bestimmter Paragrafen des Gesetzes 114(I)/2004 erstellt (das unter anderem der Umsetzung der Richtlinie 2002/58/EG dient), um diese umfassend mit der Richtlinie in Einklang zu bringen. Die wichtigste Änderung betraf die Umsetzung von Artikel 16 der Richtlinie„Übergangsbestimmungen".

B. Bedeutende Rechtsprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Versicherungsgesellschaften, die private Krankenversicherungen anbieten

Bei unserer Behörde wurden zahlreiche Beschwerden von Personen eingereicht, die angaben, dass sie, um die von ihnen selbst verauslagten Kosten für medizinische Untersuchungen erstattet zu bekommen, von ihrer Versicherungsgesellschaft zur Mitteilung der Ergebnisse der Untersuchung gezwungen wurden. Die Versicherungsgesellschaften wandten diese Praxis offenbar an, um sich zu vergewissern, dass der Versicherte die Untersuchung tatsächlich hatte durchführen lassen und nicht versuchte, seine Versicherung zu betrügen.

Bei einem Treffen mit Vertretern der Versicherungsgesellschaften erläuterten wir unsere Position, dass diese Praxis, wenn sie generell und ohne jegliche Verdachtsmomente oder Betrugsanzeichen durchgeführt wird, offenkundig gesetzwidrig und daher abzustellen ist.

Montage und Betrieb von Kameras zur Aufzeichnung bestimmter Verkehrsverstöße im öffentlichen Raum

Durch ein 2001 in Kraft getretenes Gesetz wurde die Möglichkeit geschaffen, bestimmte Verkehrsverstöße mit Hilfe von Kameras aufzuzeichnen.

Das System ging 2006 in Betrieb, zunächst für einen Testzeitraum. Im betreffenden Parlamentsausschuss wurden Fragen hinsichtlich des Zugriffsrechts der Datensubjekte auf das System sowie hinsichtlich der Speicherungsdauer der betreffenden Daten – im Wesentlichen der mit den Kameras aufgezeichneten Bilder – laut.

Nach Rücksprache mit unserer Behörde traf der stellvertretende Polizeichef, bei dem die Zuständigkeit für das System liegt, die nötigen Vorkehrungen zu beiden Punkten, die wir für zufriedenstellend erachten.

Die einzige bisher bei uns eingegangene Beschwerde betraf die Ausübung des Zugriffsrechts. Es konnte eine Lösung gefunden werden, mit der sich der Beschwerdeführer zufrieden zeigte.

Wahl des griechisch-orthodoxen Erzbischofs

Nach Rücksprache mit unserer Behörde gab die Oberste Wahlbehörde der Republik Zypern, die das Wählerverzeichnis verwahrt, einen Auszug aus diesem Register, der nur die innerhalb der griechisch-orthodoxen Kirche wahlberechtigten Personen umfasst, an die Kirchenleitung weiter, um die Durchführung der Wahl des Erzbischofs zu ermöglichen. Zuvor erhielten diese Wähler jedoch die Möglichkeit, die Löschung ihres Namens aus dem Registerauszug vor dessen Weitergabe an die Kirche zu erwirken.

Im Wählerverzeichnis ist von Rechts wegen die Religion der Wähler vermerkt, da die zypriotische Verfassung den Begriff der Religionsgruppen kennt, denen jeweils das Recht zusteht, ihre Vertreter ins Parlament zu wählen.

Tschechische Republik

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

Die Rechtsgrundlage, die den Schutz personenbezogener Daten regelt, ist das Gesetz Nr. 101/2000 Coll. zum Schutz personenbezogener Daten und zur Änderung einiger damit zusammenhängender Gesetze, das am 1. Juni 2000 in Kraft getreten ist. Dieses Gesetz richtete die Datenschutzbehörde ÚOOÚ *(Úřad pro ochranu osobních údajů* - Amt für den Schutz personenbezogener Daten) ein und stattete es mit allen notwendigen Befugnissen aus, einschließlich des Rechts, unmittelbar Geldbußen zu verhängen. Das Gesetz leistet im Wesentlichen die Umsetzung der Richtlinie 95/46/EG in tschechisches Recht. Mit Wirkung vom 26. Juli 2004 wurde das Gesetz Nr. 101/2000 Coll. 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 beitrat, 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 Datenschutzbehörde ÚOOÚ 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 Nr. 127/2005 Coll. über elektronische Kommunikation 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 Coll., was von der Europäischen Kommission kritisiert wurde. Diese Unstimmigkeiten wurden mit einer rasch durchgeführten und zum 1. August 2006 in Kraft getretenen Gesetzesänderung abgestellt. Diese beinhaltet auch eine wichtige Änderung an der Bestimmung zur Verwendung von beim Verkauf von Waren oder Dienstleistungen erhobenen elektronischen Kontaktdaten für die Verbreitung von Werbenachrichten über eigene vergleichbare Waren oder Dienstleistungen. Die ursprüngliche strikte Bestimmung wurde durch eine flexiblere Regelung ersetzt, die auf dem Opt-out-Prinzip beruht, das heißt der Streichung aus der Verteilerliste nach Widerspruch.

B. Bedeutende Rechtsprechung

In Übereinstimmung mit den für die Regierung der Tschechischen Republik geltenden gesetzlichen Bestimmungen ist die Datenschutzbehörde ÚOOÚ die erste Stelle, der Entwürfe von in ihren Zuständigkeitsbereich fallenden Gesetzen und Verordnungen im Rahmen interministerieller Verfahren zur Stellungnahme vorgelegt werden müssen – also noch bevor die Entwürfe beim Parlament zur Vorlage kommen. Im Jahr 2006 gab die Datenschutzbehörde ÚOOÚ zu einer Reihe von Verordnungen Stellungnahmen ab, die in den meisten Fällen auch berücksichtigt wurden. Sehr positive Auswirkungen auf die Umsetzung der Datenschutzgrundsätze im Gesetzgebungsverfahren sind von der Tätigkeit eines neu geschaffenen parlamentarischen Kontrollgremiums zu erwarten: Dieser Ständige Ausschuss für den Schutz der Privatsphäre wurde im November 2006 im Senat eingerichtet.

Die Zuständigkeiten der Datenschutzbehörde ÚOOÚ wurden im Jahresverlauf 2006 durch neue bereichsspezifische Regelungen angepasst bzw. erweitert. Gemäß der Änderung zum Gesetz Nr. 329/1999 Coll. über Reisedokumente sowie gemäß der Änderung zum Gesetz Nr. 283/1991 Coll. über die Polizeikräfte der Tschechischen Republik, die beide zum 1. September 2006 in Kraft getreten sind, liegt bei der Datenschutzbehörde ÚOOÚ die erstinstanzliche Zuständigkeit für Vergehen und rechtswidrige Handlungen der Verwaltung durch die unrechtmäßige

Verarbeitung biometrischer Daten. Am 1. Januar 2007 treten die neuen gesetzlichen Beschränkungen hinsichtlich der Vereinbarkeit gewisser Tätigkeiten mit dem Beamtenstatus oder der Bekleidung öffentlicher Ämter in Kraft. Diese Bestimmungen sind Teil des Gesetzes Nr. 159/2006 Coll. über Interessenkonflikte. Dieses Gesetz berührt einen neuen Bereich der Verarbeitung personenbezogener Daten und legt unter anderem Strafen für von der Datenschutzbehörde ÚOOÚ festgestellte Vergehen fest. Dabei geht es um die nicht ordnungsgemäße Verarbeitung von Daten aus dem speziellen Melderegister, an das Beamte und öffentliche Amtsträger ihre Eigentums- und Einkommensverhältnisse, erhaltene Zuwendungen sowie Mitgliedschaften und Abhängigkeiten aller Art melden müssen.

Allerdings kann die Position der Datenschutzbehörde ÚOOÚ im Gesetzgebungsverfahren insbesondere bei bereichsspezifischen Gesetzen nicht immer berücksichtigt werden. Dies zieht die Gefahr einer lückenhaften Umsetzung der Grundsätze des Schutzes personenbezogener Daten nach sich, da das allgemeine Gesetz zum Schutz personenbezogener Daten (Datenschutzgesetz Nr. 101/2000 Coll.) in bestimmten Gesetzen möglicherweise nicht beachtet wird.

So trat im Jahr 2006 beispielsweise das Gesetz Nr. 348/2005 Coll. über Rundfunk- und Fernsehgebühren und zur Änderung einiger anderer Gesetze in Kraft. Im Rahmen dieses Gesetzes wurden neue Grundlagen für die Erhebung von Rundfunk- und Fernsehgebühren geschaffen, einschließlich der Führung von Aufzeichnungen über jene Personen, die ihre Gebühren bezahlt haben. Obwohl die Datenschutzbehörde ÚOOÚ anlässlich der Beratung des Gesetzentwurfs im Abgeordnetenhaus auf Mängel hinwies, die als grober Eingriff in das zivilrechtliche Verhältnis zwischen einem Bürger und seinem Eigentum zu betrachten sind, gestattet der schließlich verabschiedete Gesetzestext zum Zweck der Festsetzung und Eintreibung von Gebühren für den Rundfunk- und Fernsehempfang die Verarbeitung detaillierter Daten über Immobilien im Eigentum des Gebührenzahlers, seiner Familienangehörigen oder sonstiger Personen, die mit dem Gebührenzahler im selben Haushalt leben. Die Rundfunk- und Fernsehanstalt darf die genannten Daten von den Elektrizitätsversorgern anfordern.

Ein weiteres Beispiel für die Verabschiedung eines Gesetzes, durch welches das Recht auf den Schutz personenbezogener Daten und der Privatsphäre verletzt wird, sind die ohne ausreichende Debatte durchgeführten Änderungen am Gesetz über Strafverfahren und das Polizeiwesen hinsichtlich der Bedingungen für die Verarbeitung genetischer Daten bei der Prävention bzw. Untersuchung von Verbrechen. Auf Anregung des Innenministers berieten und verabschiedeten in diesem Jahr die Regierung und anschließend das Parlament eine Gesetzesänderung, durch welche die Befugnisse der Polizei zur Erhebung und anschließenden Verarbeitung von biologischem Material, wie etwa genetischer Daten, d. h. der DNS einer Person, erweitert werden. Der neue Wortlaut von Paragraf 42e (1) des Gesetzes Nr. 283/1991 Coll. über die Polizeikräfte der Tschechischen Republik sieht Folgendes vor: „Ein Polizeibeamter, der in Ausübung polizeilicher Aufgaben nicht in der Lage ist, auf anderem Wege personenbezogene Daten zu erlangen, die eine genauere Identifizierung ermöglichen, ist im Falle von Personen, gegen die aufgrund gesetzwidriger Handlungen Freiheitsstrafen verhängt worden sind oder denen eine Sicherungsverwahrung auferlegt worden ist, sowie ferner bei vermindert zurechnungsfähigen Personen, die aufgefunden worden sind oder nach denen gesucht wird, befugt, nicht nur Fingerabdrücke zu nehmen, körperliche Eigenschaften zu ermitteln, Vermessungen des Körpers durchzuführen sowie optische, akustische und sonstige Aufzeichnungen anzufertigen, sondern insbesondere auch biologische Proben zu nehmen, aufgrund deren genetische Daten gewonnen werden können."

Ein drittes Beispiel für ein problematisch abgelaufenes Gesetzgebungsverfahren ist die Änderung des Gesetzes Nr. 266/2994 Coll. über das Eisenbahnwesen. In der Schlussphase des parlamentarischen Verfahrens

wurde ohne Rücksprache mit der Datenschutzbehörde ÚOOÚ oder den zuständigen Ministerien die Bestimmung eingefügt, privaten Bahnbetreibern Zugriff auf das für die Staatsverwaltung bestimmte öffentliche Melderegister zu gestatten, um diesen Privatunternehmen die Ermittlung der Identität von Schwarzfahrern bzw. von Personen, die ihren Fahrschein verloren haben, zu ermöglichen.

C. Wichtige spezifische Themen

Die von der Datenschutzbehörde ÚOOÚ im Jahr 2006 ausgeführten Kontrollen umfassten in erster Linie Ad-hoc-Kontrollen, d. h. die Überprüfung von Beschwerden. Insgesamt wurden 154 derartige Kontrollverfahren eingeleitet und 90 zum Abschuss gebracht. Nicht eingeschlossen in diesen Zahlen sind Kontrollverfahren im Zusammenhang mit unerbetenen Werbenachrichten (Spam). Ferner wurden 14 Kontrollverfahren im Rahmen der regulären Jahresplanung durchgeführt. Diese konzentrierten sich auf 5 allgemeine Bereiche, die aufgrund schwerwiegender Probleme in den Vorjahren festgelegt wurden, nämlich:

- Informationssysteme der öffentlichen Verwaltung (insbesondere in den Bereichen Finanzen und Inneres)
- Ladenketten (insbesondere Supermärkte, aus dem Blickwinkel von Kunden und Mitarbeitern)
- Systeme zur Überwachung von Personen, insbesondere Kameraanlagen
- Verarbeitung der so genannten Geburtsnummer *(rodné číslo)*
- elektronische Kommunikation

Die massive ***Einführung von Kameraanlagen*** ist besonders alarmierend.

Unter bestimmten Umständen stellt der Betrieb einer Kameraanlage eine Verarbeitung personenbezogener Daten im Sinne des einschlägigen Gesetzes dar, so dass der für die Datenverarbeitung Verantwortliche unter anderem verpflichtet ist, eine entsprechende Meldung an die Datenschutzbehörde ÚOOÚ zu richten, damit der Sachverhalt registriert werden kann. Im Jahr 2006 beantragten circa 350 für die Datenverarbeitung Verantwortliche die Registrierung ihrer Kameraanlagen. Das ist eine deutliche Steigerung gegenüber den Vorjahren: 2005 wurden nur circa 5 Betreiber registriert. Trotzdem handelt es sich dabei nur um einen Bruchteil der tatsächlich in der Tschechischen Republik installierten Kameraanlagen, die in Schulen, Museen, Wohngebäuden, Banken, Ladenketten usw. immer mehr zunehmen. Es ging sogar eine Reihe von Meldungen bei der Datenschutzbehörde ÚOOÚ ein, bei denen der Betreiber der Kameraanlage beabsichtigte, die Überwachungsbilder aus einem bestimmten Bereich (öffentliche Bereiche, Ladengeschäfte, Internet-Cafés) online zu stellen. Auf dem Meldeformular teilen die für die Datenverarbeitung Verantwortlichen der Datenschutzbehörde ÚOOÚ in sehr vielen Fällen mit, dass sie beabsichtigen, die durch die Kameraüberwachung gewonnenen personenbezogenen Daten über ihre Mitarbeiter zur Kontrolle der Arbeitsleistung zu verwenden. In einer Reihe von Fällen verweigerte die Datenschutzbehörde ÚOOÚ die Registrierung der Verarbeitung personenbezogener Daten per Kameraanlage und stellte stattdessen einen Bescheid aus, mit dem sie die genannte Datenverarbeitung untersagte. Im Januar 2006 veröffentlichte die Datenschutzbehörde ÚOOÚ eine allgemeine schriftliche Stellungnahme zum Thema Kameraanlagen, in der u. a. die wesentlichen gesetzlichen Grundlagen für den Betrieb von Kameraanlagen erläutert werden.

Bei den Aktivitäten der Datenschutzbehörde ÚOOÚ hinsichtlich ***unerbetener Werbenachrichten*** (Spam) war ein deutlicher Anstieg zu verzeichnen. Im Jahr 2006 gingen bei der Datenschutzbehörde ÚOOÚ 1.296 entsprechende Anzeigen ein, 163 Kontrollverfahren wurden eingeleitet und 153 davon zum Abschluss gebracht. Die häufigsten Fälle von Gesetzesverstößen in diesem Bereich lassen sich in folgende Kategorien einteilen:

1. Viele der kontrollierten Unternehmen beriefen sich auf eine telefonisch erteilte Zustimmung der betroffenen Bürger, und praktisch keines der

Unternehmen wandte das *Opt-in*-Prinzip, d. h. die ausdrückliche vorherige Zustimmung vor Aufnahme in die Verteilerliste, in den gesetzlich vorgeschriebenen Fällen konsequent an.

2. Praktisch keine der Mitteilungen wurde ausdrücklich als Werbenachricht kenntlich gemacht. Die Mitteilungen tragen alle möglichen Arten von Bezeichnungen: Newsletter, Information, Nachrichten usw. Das Gesetz Nr. 480/2004 Coll. über gewisse Dienste der Informationsgesellschaft schreibt jedoch vor, dass eine Werbenachricht „klar und deutlich" als solche kenntlich gemacht werden muss.

3. Manche Anbieter von Internetdiensten erschweren die Auslegung des Gesetzes, indem sie Werbenachrichten nicht separat versenden, sondern als Fußnoten an von ihnen übermittelte E-Mails anhängen.

4. Manche Anbieter elektronischer Dienste gehen davon aus, dass das Anklicken eines Kontrollkästchens auf dem Registrierungsformular im betreffenden Bereich einer Webanwendung genügen würde, um seine Zustimmung zum Erhalt von Werbenachrichten zu erklären. Dabei übersehen sie jedoch, dass ein derartiges Formular von jeder beliebigen Person ausgefüllt werden kann, wenn der Zugriff nicht durch Benutzername und Kennwort geschützt ist.

5. Um den gesetzlichen Anforderungen umfassend zu genügen, muss in jeder Werbenachricht eine gültige Adresse angegeben sein, an welche sich der Empfänger der Werbenachricht gegebenenfalls wenden kann, damit der Absender ihm zukünftig keine Werbenachrichten mehr schickt. Wenn der Absender seine Kundendatenbank nach E-Mail-Adressen geordnet hat, ergibt sich allerdings eine Schwierigkeit, wenn die Absenderadresse des Kunden von der gespeicherten Adresse abweicht.

Umfangreiche Aktivitäten legte die Datenschutzbehörde ÚOOÚ im Bereich der internationalen Zusammenarbeit an den Tag, nämlich beim langfristigen ***Unterstützungsprojekt für Bosnien und Herzegowina***. Zusammen mit der spanischen Datenschutzbehörde AEPD (Agencia Española de Protección de Datos) begann die Datenschutzbehörde ÚOOÚ am 1. Februar 2006 mit der Umsetzung des Projekts „Unterstützung für die Datenschutzbehörde von Bosnien und Herzegowina" (BA04-IB-OT-01). Das Projekt wird durch die Europäische Union finanziert und findet im Rahmen des CARDS-Programms für die Staaten des westlichen Balkans statt. Allgemeines Ziel des Programms ist die Unterstützung für Bosnien und Herzegowina beim Aufbau von Institutionen, als eine der Vorbedingungen für das erfolgreiche Voranschreiten des Stabilisierungs- und Assoziierungsprozesses für diesen Staat. Im Einzelnen geht es um die Schaffung der gesetzlichen und verwaltungsmäßigen Grundlage für den Schutz personenbezogener Daten in Bosnien und Herzegowina. Dies soll auf drei Wegen erreicht werden:

- Änderung der einschlägigen Gesetze, um sie mit den in der EU üblichen Standards in Einklang zu bringen
- Vorschlag einer geeigneten Struktur und Arbeitsweise für eine unabhängige Behörde zur Überwachung des Datenschutzes
- eine schrittweise Sensibilisierung der Bürger, der Unternehmen und der staatlichen Institutionen für die Belange des Datenschutzes

Das 14-monatige Projekt wird nach dem Twinning-Konzept durchgeführt. Ein Experte der Datenschutzbehörde ÚOOÚ arbeitet während der gesamten Projektdauer als Twinning-Berater in Sarajewo. Weitere Fachleute der Datenschutzbehörde ÚOOÚ und der spanischen Datenschutzbehörde AEPD sowie zwei externe Berater aus Italien und dem Vereinigten Königreich bringen ihre Sachkenntnis bei kürzeren Arbeitstreffen ein, führen Workshops zu spezifischen Einzelthemen durch und erstellen Handbücher. Abgeschlossen wird das Projekt am 31. März 2007.

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

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

- die dänische Verfassung
- das Gesetz über Marketingpraktiken, Paragraf 6 (siehe Gesetz Nr. 1389 vom 21. Dezember 2005)
- das Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten
- das Gesetz über die Wettbewerbsbedingungen und den Verbraucherschutz auf dem Telekommunikationsmarkt (vgl. Durchführungsverordnung Nr. 784 vom 28. Juli 2005)
- die Durchführungsverordnung Nr. 638 vom 20. Juni 2005 über die Bereitstellung elektronischer Kommunikationsnetze und Dienstleistungen
- Kapitel 71 der Zivilprozessordnung *(Lov om rettens pleje)*, vgl. Durchführungsverordnung Nr. 777 vom 16. September 2002
- Paragraf 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 Datatilsynet hat zu verschiedenen Gesetzen und Regelungen, die Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz haben, Stellung bezogen.

1. Im Jahr 2006 legte das Justizministerium einen Gesetzentwurf zur Unterstützung der Strafverfolgungsbehörden im Rahmen der Terrorismusbekämpfung vor. Die Gesetzesvorlage sah unter anderem Möglichkeiten zur Datenübermittlung von Behörden an den Inlandsgeheimdienst PET *(Politiets Efterretningstjeneste)* vor. Ferner sollte die Polizei die Möglichkeit erhalten, private und öffentliche Einrichtungen zur Installation von Videoüberwachungssystemen sowie zur Aufbewahrung der Aufnahmen über einen gewissen Zeitraum zu verpflichten. Außerdem sollten Fluggesellschaften verpflichtet werden, auf Flügen von und nach Dänemark Daten über Passagiere und Besatzungsmitglieder zu erheben und an den Inlandsgeheimdienst PET weiterzugeben, sowie dem Inlandsgeheimdienst PET Zugriff auf ihre Buchungssysteme zu gewähren.

Hinsichtlich der Datenweitergabe von Behörden befand die Datenschutzbehörde Datatilsynet, dass eine derart umfassende Weitergabe nicht aufgrund der Regelung des Datenschutzgesetzes erfolgen könne, sondern einer separaten Gesetzesgrundlage bedürfen würde. Ferner brachte die Datenschutzbehörde Datatilsynet ihre Besorgnis darüber zum Ausdruck, dass die Weitergabe zu umfassend abgesteckt sei, und merkte an, dass eine Lockerung der im Gesetz über die Verarbeitung personenbezogener Daten enthaltenen Bestimmungen hinsichtlich der Weitergabe von Daten nur unter der Bedingung möglich sei, dass dadurch kein Widerspruch zur Datenschutzrichtlinie entstehen würde. Insbesondere verwies die Datenschutzbehörde Datatilsynet dabei auf Artikel 13 Absatz 1.

Im Hinblick auf die Vorschläge zur Videoüberwachung verwies die Datenschutzbehörde Datatilsynet auf ihre derzeitige Praxis, der zufolge weder öffentliche noch private Einrichtungen Videoüberwachungen in öffentlichen Bereichen installieren sollten und der für die Datenverarbeitung Verantwortliche nur solche Daten verarbeiten und speichern darf, für die er selbst eine angemessene und zulässige Verwendung hat. Daher wäre es nicht zulässig, dass öffentliche und private Einrichtungen Daten einzig und allein zu dem Zweck erheben, diese an die Strafverfolgungsbehörden weiterzugeben.

Im Hinblick auf die vorgeschlagene Verpflichtung der Fluggesellschaften, Daten über Passagiere und Besatzungsmitglieder zu erheben, befand die Datenschutzbehörde Datatilsynet, dass die oben angeführte Argumentation auch auf Fluggesellschaften zutrifft: Es wäre nicht zulässig, dass sie Daten einzig und allein zu dem Zweck erheben, diese an die Polizei weiterzugeben. Auch hinsichtlich der Datenweitergabe von Behörden führte die Datenschutzbehörde Datatilsynet das genannte Argument an.

Abschließend gab die Datenschutzbehörde Datatilsynet zu bedenken, dass im Falle einer seitens der Fluggesellschaften durchgeführten Erhebung von Daten über Passagiere und Besatzungsmitglieder die Regelungen hinsichtlich des Zugriffsrechts der Datensubjekte greifen würden.

2. Im Zuge der Reform der dänischen Territorialverwaltung wünschen Regierung und Steuerbehörde, dass die Gemeinden so genannte Bürgerservicezentren einrichten. Diese Zentren sollen von den Gemeinden betrieben werden, zugleich aber als Datenverarbeiter für die Steuerbehörde sowie als für die Datenverarbeitung Verantwortliche in anderen Bereichen fungieren.

Die Datenschutzbehörde Datatilsynet meldete Zweifel an, ob es wirklich nötig sei, diesen Zentren landesweiten Zugriff auf die Daten der Steuerbehörden zu gewähren, und regte an, diesen Zugriff auf Daten zu den Bürgern innerhalb der jeweiligen räumlichen Zuständigkeit der Zentren zu beschränken. Im Prinzip könnte anderen Zentren dann nur mit Zustimmung des Datensubjekts Zugriff auf personenbezogene Daten gewährt werden, und jeder derartige Zugriff sollte in der elektronischen Akte des jeweiligen Datensubjekts klar dokumentiert werden. Die Datenschutzbehörde Datatilsynet forderte ferner, die Protokolldateien Stichproben zu unterziehen, um zu gewährleisten, dass ausschließlich rechtmäßige Zugriffe auf personenbezogene Daten erfolgen.

Zudem forderte die Datenschutzbehörde Datatilsynet, auch die Systemprotokolle der in der Verantwortung der Zentren durchgeführten Datenverarbeitung Stichproben zu unterziehen. Damit ist die Datenschutzbehörde Datatilsynet erstmals über eine bloße Empfehlung von Stichproben der Protokolldateien hinausgegangen.

B. Bedeutende Rechtsprechung

1. Die Datenschutzbehörde Datatilsynet wurde aufgefordert, eine Stellungnahme zum Projekt „elektronische Patientenakte" abzugeben. Im Rahmen des Projekts sollen niedergelassene Allgemeinärzte mit Zustimmung der Patienten Zugriff auf deren seitens der Krankenhäuser angelegte elektronische Patientenakten erhalten. In der Praxis hätte das Projekt dazu geführt, dass im Prinzip sämtliche Ärzte eine technische Zugriffsmöglichkeit auf die Daten sämtlicher Patienten in Dänemark erhalten hätten, sofern ihnen die CPR-Nummer (Personenkennzahl) der betreffenden Person bekannt ist.

Die Datenschutzbehörde Datatilsynet befand, dass eine derartige technische Zugriffsmöglichkeit nur für den Arzt eröffnet werden sollte, der den betreffenden Patienten tatsächlich behandelt. Dabei verwies die Datenschutzbehörde Datatilsynet auf ihre in letzter Zeit verfolgte Grundlinie, der zufolge öffentliche Einrichtungen und deren Mitarbeiter nur Zugriff auf jene Daten erhalten sollten, die sie zur Durchführung ihrer Aufgaben unmittelbar benötigen.

Da das System zum gegenwärtigen Zeitpunkt jedoch keine technische Möglichkeit für eine derartige Zugriffseinschränkung bietet, erklärte sich die Datenschutzbehörde Datatilsynet damit einverstanden, dass das System fürs Erste mit einer anderen Lösung für den Zugriff auf Patientendaten in Betrieb geht.

Bei dieser alternativen Lösung überprüft das System, ob eine Person normalerweise bei dem Arzt in Behandlung ist, der auf ihre Daten zugreifen möchte. Wenn dies der Fall ist, kann der Arzt mit Zustimmung des Patienten auf die Daten zugreifen, ohne dass weitere Warnmeldungen angezeigt werden. Wenn die Person dagegen nicht zu den normalen Patienten des Arztes zählt, dann wird unter anderem ein Warnhinweis für den Arzt angezeigt, dass der Zugriff nur erfolgen darf, wenn es sich um einen Notfall handelt, und dass gesetzwidriger Zugriff strafrechtlich verfolgt wird.

Die Datenschutzbehörde Datatilsynet verlangte, dass zusätzlich zu den im System bereits vorhandenen

„üblichen" Sicherheitsvorkehrungen (Verschlüsselung, Systemprotokoll usw.) weitere Sicherheitsvorkehrungen geschaffen werden sollten. Die teilnehmenden Amtsbezirke *(amter)* sollten verpflichtet werden, das Systemprotokoll zu prüfen, um etwaiges ungewöhnliches Verhalten oder etwaige unbefugte Zugriffe feststellen zu können.

Die Patienten sollten per E-Mail oder auf dem gewöhnlichen Postweg informiert werden, wenn ein anderer Arzt als ihr Hausarzt auf ihre personenbezogenen Daten zugegriffen hat, und einen Online-Zugriff auf die im Systemprotokoll gespeicherten Angaben zur Identität des Zugreifers erhalten.

Ferner sollte der für die Datenverarbeitung Verantwortliche bei mindestens 1% der „normalen" Zugriffe und bei 10% der Notfallzugriffe eine Überprüfung durchführen, um sich zu vergewissern, dass es sich um rechtmäßige Zugriffe gehandelt hat.

Abschließend betonte die Datenschutzbehörde Datatilsynet, dass optimale Sicherheitsvorkehrungen eine Beschränkung des Zugriffs beinhalten würden, die gewährleistet, dass Ärzte ausschließlich auf Daten von Personen Zugriff erhalten würden, die tatsächlich zum Kreis ihrer Patienten zählen. Es wurde empfohlen, eine derartige Lösung umzusetzen, sobald sie technisch machbar ist. Die Datenschutzbehörde Datatilsynet regte an, dass jeder Patient eine elektronische Karte zur Authentifizierung gegenüber dem System erhalten sollte. Diese Karte würde der Patient seinem Arzt zur Anmeldung beim System jeweils kurzzeitig übergeben.

2. Das Museum der dänischen Widerstandsbewegung *(Frihedsmuseet)* bat die Datenschutzbehörde Datatilsynet um eine Stellungnahme zu einer Datenbank über die Mitglieder der dänischen Widerstandsbewegung während der Besatzungszeit 1940-45. Es bestand die Absicht, die Datenbank im Internet zu veröffentlichen. Die Datenschutzbehörde Datatilsynet befand, dass es sich bei Informationen über Verbindungen einer Person zur Widerstandsbewegung um rein private Daten im Sinne von Paragraf 8 des Gesetzes über den Schutz personenbezogener Daten handelt. Die Datenschutzbehörde Datatilsynet befand ferner, dass das Material möglicherweise sensible Daten enthalten könnte, etwa zu strafrechtlichen Verurteilungen oder zur politischen Gesinnung von Personen.

Die Datenschutzbehörde Datatilsynet stellte klar, dass die Veröffentlichung personenbezogener Daten über lebende Personen nur mit der ausdrücklichen Zustimmung des jeweiligen Datensubjekts stattfinden darf.

Hinsichtlich verstorbener Datensubjekte befand die Datenschutzbehörde Datatilsynet, dass die Veröffentlichung von Informationen über die politische Gesinnung einer Person nur unter der Bedingung gestattet ist, dass das betreffende Datensubjekt eine solche Veröffentlichung während seiner Lebenszeit selbst getätigt hat (Paragraf 7(2)(3) des Datenschutzgesetzes, in Umsetzung von Artikel 8 Absatz 2) Buchstabe e) der Richtlinie). Die Datenschutzbehörde Datatilsynet führte dazu aus, dass eine derartige Veröffentlichung beispielsweise über die Medien, durch Bücher oder auf sonstigem Wege erfolgt sein kann – sofern die Initiative dazu vom Datensubjekt selbst ausging.

Die Datenschutzbehörde Datatilsynet befand daher, dass sensible Daten im Sinne von Paragraf 8 des Datenschutzgesetzes nicht in der derzeit vorgesehenen Form veröffentlicht werden dürfen. Die Datenschutzbehörde Datatilsynet erklärte jedoch ihre Bereitschaft, den Fall einer erneuten Prüfung zu unterziehen, wenn das Museum der dänischen Widerstandsbewegung *(Frihedsmuseet)* im Rahmen einer Überarbeitung Vorschläge für eine klare Eingrenzung der in der Publikation berücksichtigten verstorbenen Datensubjekte vorlegen würde.

3. Die Datenschutzbehörde Datatilsynet erhielt eine Anfrage der Scandinavian Airlines Service (SAS) hinsichtlich der Absicht dieser Fluggesellschaft, biometrische Daten ihrer Fluggäste mittels Fingerabdruckmustern zu verarbeiten. Die Fluggesellschaft SAS plante, den Fingerabdruck eines jeden Fluggasts beim Check-In zu scannen, und dann erneut beim Boarding, um zu gewährleisten, dass die Person, die ein Gepäckstück aufgibt, tatsächlich mit der Person identisch ist, die an Bord des Flugzeugs geht.

Nach Einschätzung der Datenschutzbehörde Datatilsynet fallen biometrische Daten, wie etwa ein Fingerabdruckmuster oder ein aus einem Fingerabdruck errechneter Zahlenwert, unter Paragraf 6 des dänischen Datenschutzgesetzes, und nicht unter die Paragrafen zu sensiblen Daten.

Die Datenschutzbehörde Datatilsynet befand daher, dass mit der ausdrücklichen Zustimmung des jeweiligen Datensubjekts eine Verarbeitung durchaus stattfinden darf. In diesem Zusammenhang verwies die Datenschutzbehörde Datatilsynet darauf, dass Personen, die keine derartige Verarbeitung ihres Fingerabdrucks wünschen, als Alternative das manuelle Check-in-Verfahren nutzen können.

Die Datenschutzbehörde Datatilsynet fand nicht, dass die Verarbeitung gegen die Grundsätze der Verhältnismäßigkeit und der Zweckbestimmung verstoßen würde. Dabei stützte sie sich auf den Umstand, dass die Verarbeitung der Fingerabdruckmuster auf den engen zeitlichen Rahmen von circa 20-60 Minuten beschränkt sein wird.

C. Wichtige spezifische Themen

1. Durch Medienberichte wurde die Datenschutzbehörde Datatilsynet darauf aufmerksam, dass eine Reihe von Partnervermittlungen im Internet ihrer im dänischen Datenschutzgesetz niedergelegten Pflicht zur Vorabmeldung nicht nachkommen.

Die Datenschutzbehörde Datatilsynet beschloss, eine Kampagne zu starten, um diese für die Datenverarbeitung Verantwortlichen darüber zu informieren, dass sie verpflichtet sind, ihre Datenverarbeitung an die Datenschutzbehörde Datatilsynet zu melden und eine entsprechende Genehmigung einzuholen.

Die Datenschutzbehörde Datatilsynet setzte sich also mit den betreffenden Partnervermittlungen in Verbindung und informierte sie über ihre Verpflichtung, die Datenschutzbehörde Datatilsynet über die Datenverarbeitung zu informieren. Daraufhin reichten fast alle Agenturen die entsprechenden Meldungen ein. Einige beschlossen, die Datenverarbeitung zu beenden, nachdem sie über die Regelungen zur Verarbeitung personenbezogener Daten informiert wurden.

2. Der Berufsverband der Heilpraktiker (Akupunktur, Reflexzonentherapie usw.) wandte sich an die Datenschutzbehörde Datatilsynet und bat um Unterstützung bei der Information der Verbandsmitglieder über die Regelungen zur Verarbeitung personenbezogener Daten und über die Verpflichtung, die Verarbeitung an die Datenschutzbehörde Datatilsynet zu melden.

Daraufhin veröffentlichte die Datenschutzbehörde Datatilsynet auf ihrer Website einen Leitfaden für Meldungen durch Heilpraktiker, einschließlich einer Erläuterung der betreffenden Passagen des Datenschutzgesetzes sowie einer Schritt-für-Schritt-Anleitung zum Meldeformular.

Die Initiative hat bereits circa 300 Meldungen ergeben.

3. Im Jahr 2006 hat sich die Datenschutzbehörde Datatilsynet wie bereits in den Vorjahren sehr intensiv mit der Reform der Territorialverwaltung beschäftigt, die zum 1. Januar 2007 in Kraft tritt.

Im Jahr 2006 galt ein erheblicher Teil der Anstrengungen der Datenschutzbehörde Datatilsynet der Suche nach praktischen Lösungen für die vielen Änderungen bei den Meldungen und Genehmigungen für die verschiedenen öffentlichen Einrichtungen, Amtsbezirke *(amter)* und Gemeindeverwaltungen, bei denen aufgrund der Territorialverwaltungsreform der für die Datenverarbeitung Verantwortliche wechselt.

So treten beispielsweise an die Stelle der bisherigen Amtsbezirke (amter) fünf Regionen, und die Anzahl der Gemeinden wird von ungefähr 270 auf 98 verringert.

Daraus ergab sich für die Datenschutzbehörde Datatilsynet ein umfangreiches Projekt zur Beurteilung und Überarbeitung des Meldesystems, im Bestreben nach größerer Effizienz. Zudem mussten Vorkehrungen für die zahlreichen bisherigen für die Datenverarbeitung Verantwortlichen getroffen werden, die im Rahmen der Reform der Territorialverwaltung aufgelöst werden, einen neuen Namen erhalten oder Aufgaben übernehmen, die bisher von anderen Stellen getragen wurden.

Das neue Meldesystem der Datenschutzbehörde Datatilsynet wird die Meldung der Verarbeitung personenbezogener Daten an die Datenschutzbehörde Datatilsynet noch einfacher machen, und die Datenschutzbehörde Datatilsynet muss künftig weniger Ressourcen für die zahlreichen Meldungen aufwenden, die jeden Tag bei ihr eingehen.

Estland

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

Im Jahresverlauf 2006 erfolgten keine Änderungen am estnischen Gesetz zum Schutz personenbezogener Daten (*Isikuandmete kaitse seadusega* - IKS; Titel der offiziellen englischen Übersetzung: *Personal Data Protection* Act – PDPA; im Folgenden kurz: Datenschutzgesetzfn.Die Neufassung des Datenschutzgesetzes, die am 15. Februar verabschiedet wurde und am 1. Januar 2008 in Kraft tritt, enthält eine Reihe von Änderungen im Zusammenhang mit der Umsetzung der Richtlinie 95/46/EG.

Bereits die erste Fassung des Datenschutzgesetzes beruhte auf der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Diese Grundlage wurde auch bei der diesjährigen Neufassung des Gesetzes beibehalten, in der es im Wesentlichen um Präzisierungen und Vereinheitlichungen des Wortlauts geht.

Es gab während des abgelaufenen Jahres auch keine Entwicklungen in der Gesetzgebung hinsichtlich der Richtlinie 2002/58/EG.

B. Bedeutende Rechtsprechung

Während des Jahres 2006 schritt die estnische Datenschutzbehörde *(Andmekaitse Inspektsioon)* in mehreren Fällen ein, die auch Gegenstand umfangreicher Berichterstattung in den Medien waren.

Der erste ausgewählte Fall, auf den im vorliegenden Dokument eingegangen werden soll, betraf Rechnungen über medizinische Behandlungen, die auf der Straße gefunden wurden. Genauer gesagt handelte es sich bei den gefundenen Dokumenten um Durchschläge von Krankschreibungen für Patientinnen der Frauenklinik Narva Haigla.

Bis zum Jahr 2002 wurden in dieser Frauenklinik nicht mehr benötigte Dokumente mit sensiblen Daten durch Verbrennen zerstört. Darüber wurde laut vorliegenden Belegen ein Vertrag mit dem Betreiber der städtischen Müllverbrennungsanlage von Tallinn (Reval) abgeschlossen. Es konnte jedoch nicht festgestellt werden, ob zum Zeitpunkt der genannten Vorfälle noch immer ein Vertrag bestand.

Es konnte nicht ermittelt werden, wann und durch wen die Durchschläge zur Zerstörung aus dem Krankenhaus gebracht wurden, da keine Belege über den Vorgang auffindbar waren. Die Frauenklinik Narva Haigla verabsäumte es zudem, zu kontrollieren, ob die zur Zerstörung gegebenen Dokumente mit sensiblen Daten auch tatsächlich zerstört wurden. Dies führte letztlich dazu, dass Krankschreibungen mit sensiblen personenbezogenen Daten für jedermann zugänglich wurden.

Die Frauenklinik Narva Haigla bietet der Bevölkerung medizinische Betreuung durch Allgemeinärzte und Fachärzte an. In diesem Zusammenhang werden personenbezogene Daten zum Gesundheitszustand der Patientinnen verarbeitet. Gemäß Datenschutzgesetz § 4 (3) 3 sind Daten über den Gesundheitszustand einer Person als sensible Daten zu betrachten, so dass bei ihrer Verarbeitung § 6 (6) des Datenschutzgesetzes beachtet werden muss, dem zufolge der für die Datenverarbeitung Verantwortliche während der Verarbeitung derartiger personenbezogener Daten alle einschlägigen Sicherheitsgrundsätze einhalten muss. Diese Sicherheitsgrundsätze sehen vor, dass Sicherheitsvorkehrungen umgesetzt werden müssen, um personenbezogene Daten zu schützen und um unerwünschte bzw. unbefugte Änderungen an den Daten sowie eine Veröffentlichung oder Zerstörung zu verhindern. Während des Verfahrens über das Datenschutzvergehen wurde festgestellt, dass die Frauenklinik Narva Haigla es verabsäumt hatte, den Schutz personenbezogener Daten unter Verwendung der erforderlichen organisatorischen, physischen und IT-sicherheitstechnischen Verfahren gemäß § 6 und § 19 Datenschutzgesetz umzusetzen.

Daher verhängte die Datenschutzbehörde am 6. Juni 2006 im beschleunigten Verfahren gegen die Frauenklinik Narva Haigla eine Geldbuße in Höhe von 15.000 Estnischen Kronen.

Der zweite ausgewählte Fall betraf die Veröffentlichung von Daten aus dem Register der Wehrpflichtigen. Die Datenschutzbehörde leitete ein Verfahren über ein Datenschutzvergehen ein: Zwischen der Firma Mindworks Industries OÜ und der Militärverwaltung für den nördlichen Bereich war ein Vertrag über IT-Entwicklungsarbeiten hinsichtlich des Registers der Wehrpflichtigen abgeschlossen worden. Aufgrund dieses Vertrages handelte die genannte private GmbH als für die Datenverarbeitung Verantwortlicher im Sinne von § 8 des Datenschutzgesetzes. Im Juni 2005 nahm einer der Mitarbeiter dieses für die Datenverarbeitung Verantwortlichen nach Dienstschluss einen USB-Memorystick aus der Militärverwaltung für den nördlichen Bereich mit, auf dem sich in unverschlüsselter Form die Daten von 302.067 Männern befanden.

Diese Daten betrafen die zwischen 1950 und 1987 geborenen männlichen Bürger, oder mit anderen Worten: die Daten sämtlicher Wehrpflichtigen in der Republik Estland. Enthalten waren jeweils: Personenkennzahl, Vorname, Nachname, Vatername und Wohnort. Der Mitarbeiter verlor den Memorystick samt den darauf gespeicherten Daten in einem öffentlichen Park in Tallinn (Reval).

Zu diesem Verlust konnte es kommen, weil die Firma Mindworks Industries OÜ es verabsäumt hatte, die bei der Verarbeitung von personenbezogenen Daten erforderlichen organisatorischen, physischen und IT-sicherheitstechnischen Sicherheitsvorkehrungen gemäß Datenschutzgesetz umzusetzen.

Es handelte sich also um einen Verstoß gegen Datenschutzgesetz §19 (1) 3), dem zufolge der für die Datenverarbeitung Verantwortliche verpflichtet ist, die erforderlichen organisatorischen, physischen und IT-sicherheitstechnischen Sicherheitsvorkehrungen zu treffen, um die Vertraulichkeit personenbezogener Daten zu wahren und eine unbefugte Verarbeitung zu verhindern.

Gemäß Absatz 2, Satz 6 des genannten Paragrafen muss der für die Datenverarbeitung Verantwortliche gewährleisten, dass bei der Weitergabe von personenbezogenen Daten auf Datenkommunikationswegen oder über tragbare Speichermedien keinerlei unkontrollierte Datenzugriffe, wie etwa Lesen, Kopieren, Ändern oder Löschen, stattfinden. Gemäß Datenschutzgesetz § 19 (2) 7 muss der für die Datenverarbeitung Verantwortliche innerhalb seines Unternehmens bzw. innerhalb seiner Behörde die Arbeitsabläufe so organisieren, dass die Einhaltung der Datenschutzvorschriften gewährleistet ist.

Datenschutzgesetz § 20 (3) schreibt vor, dass der für die Datenverarbeitung Verantwortliche für eine ordnungsgemäße Schulung sämtlicher mit der Datenverarbeitung betrauten Mitarbeiter Sorge tragen muss.

Daher verhängte die Datenschutzbehörde im Mai 2006 zum Abschluss des Verfahrens gegen Mindworks Industries OÜ eine Geldbuße in Höhe von 15.000 Estnischen Kronen wegen Verstoßes gegen Datenschutzgesetz § 19 (1) 3), § 19 (2) 6) und 7) sowie § 20 (3).

C. Wichtige spezifische Themen

Das Datenschutzgesetz trat am 1. Oktober 2003 in Kraft. Ziel der im abgelaufenen Jahr durch das Justizministerium ausgearbeiteten Neufassung war die Klärung einiger Bereiche, deren Regelungen sich im Rahmen der Umsetzung des Gesetzes als unzureichend erwiesen hatten. Während des abgelaufenen Jahres wurde auch die estnische Datenschutzbehörde in die Erstellung der Neufassung des Gesetzes eingebunden.

Beamte der Datenschutzbehörde wirkten in mehreren nationalen Arbeitsgruppen mit, etwa zu den Themen elektronische Patientenakten und Beobachtung von Infektionskrankheiten, elektronische Akten,

biometrische Daten usw. Im Gesundheitswesen soll für das gesamte Staatsgebiet ein innovatives, intelligentes System mit elektronischen Patientenakten aufgebaut werden, das die patientenzentrierte Erfassung, Speicherung und Verarbeitung von Gesundheitsdaten ermöglicht. Auf diese Weise soll die Informations- und Kommunikationstechnologie zur Unterstützung und Verbesserung der Prävention, Diagnose, Behandlung, Überwachung und Verwaltung im Gesundheitswesen beitragen. Unsere Beamten haben an dieser Arbeitsgruppe als Fachleute für Datenschutz und technische Sicherheitsvorkehrungen mitgewirkt.

Finnland

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG

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 der Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union gemäß 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 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 Direktmarketings, Regulierung der Katalogisierungsdienste und Regulierung des Informationsrechts 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

Eine Person bat den Datenschutzbeauftragten um eine Stellungnahme zum folgenden Fall. Bei einem Bewerbungsgespräch hatte der Bewerber festgestellt, dass der potenzielle Arbeitgeber mit Hilfe der Internet-Suchmaschine Google Informationen über ihn gesammelt hatte. Dabei handelte es sich um die Zusammenfassung einer Podiumsdiskussion, an welcher der Bewerber fünf Jahre zuvor teilgenommen hatte. Aufgrund dieser Informationen zog der potenzielle Arbeitgeber bestimmte Schlüsse.

In Finnland gibt es ein spezielles Gesetz zum Schutz der Privatsphäre, das sich speziell auf das Verhältnis zwischen Arbeitgeber und Arbeitnehmer bezieht. Das Gesetz gilt für Beschäftigungsverhältnisse aller Art.

Das Gesetz erstreckt sich auch auf sämtliche Arten von Beschäftigungsverhältnissen im öffentlichen Dienst, das heißt auf Beamte und Angestellte im Staats-, Gemeinde- und Kirchendienst sowie bei sämtlichen sonstigen öffentlichen und öffentlich-rechtlichen Einrichtungen. Im Gesetz über den Schutz der Privatsphäre im Arbeitsleben (759/2004) sind die allgemeinen Anforderungen für die Erhebung von Daten über Arbeitnehmer sowie hinsichtlich der diesbezüglichen Auskunftspflicht des Arbeitgebers niedergelegt. Die Überwachung dieses Gesetzes ist auf die Arbeitsschutzbehörden und den Datenschutzbeauftragten verteilt.

Diesem Gesetz zufolge ist der Arbeitgeber verpflichtet, personenbezogene Daten über den Arbeitnehmer vorrangig direkt von dieser Person zu beziehen. Um personenbezogene Daten aus anderen Quellen zu beziehen, muss der Arbeitgeber die Zustimmung des Arbeitnehmers einholen. Diese Zustimmung ist allerdings nicht erforderlich, wenn eine Behörde dem Arbeitgeber im Rahmen einer gesetzlichen Verpflichtung des Arbeitgebers Informationen übermittelt oder wenn der Arbeitgeber Daten zur Kreditwürdigkeit bzw. ein

Führungszeugnis anfordert, um die Zuverlässigkeit des Arbeitnehmers zu ermitteln.

Gemäß dem Gesetz über den Schutz der Privatsphäre im Arbeitsleben muss der Arbeitgeber den Arbeitnehmer vorab informieren, dass er Daten anfordern wird, um die Glaubwürdigkeit des Arbeitnehmers zu ermitteln. Wenn Informationen über den Arbeitnehmer auf anderem Wege als direkt von diesem selbst beschafft worden sind, dann muss der Arbeitgeber den Arbeitnehmer über diese Daten in Kenntnis setzen, bevor diese verwendet werden, um Entscheidungen hinsichtlich des Arbeitnehmers zu treffen. Die Mitteilungspflicht des Arbeitgebers und das Recht des Arbeitnehmers zur Überprüfung von Daten zu seiner Person unterliegen auch den übrigen einschlägigen gesetzlichen Bestimmungen.

Mit Google und anderen vergleichbaren Diensten gesuchte Informationen stehen seit Längerem in der Kritik, weil derartige Daten unzuverlässig sein können. Das oben genannte Gesetz verpflichtet den Arbeitgeber jedoch, personenbezogene Daten über den Arbeitnehmer vorrangig direkt von dieser Person beziehen. Daher befand der Datenschutzbeauftragte, dass das von diesem Arbeitgeber in diesem Fall angewandte Verfahren einen Verstoß gegen das Gesetz über den Schutz der Privatsphäre im Arbeitsleben darstellt.

C. Wichtige spezifische Themen

Drittes Nationales Strategiepapier zur Informationssicherheit

Dieses Strategiepapier ist Teil des von der finnischen Regierung vorangetriebenen Programms für die Informationsgesellschaft und wurde (neben weiteren Papieren über strategische Prozesse) im Zusammenwirken mit Entscheidungsträgern und Akteuren aus zahlreichen Gesellschaftsbereichen erstellt. An dem Prozess beteiligten sich insgesamt circa 400 Fachleute aus Regierung und Staatsverwaltung, Regional- und Lokalverwaltungen, Universitäten und Forschungseinrichtungen, Unternehmen und verschiedenen Organisationen. Das Dritte Nationale Strategiepapier zur Informationssicherheit wurde am 26. September anlässlich der Fachmesse für Informations- und Kommunikationstechnologie Helsinki ICT Week veröffentlicht.

Ziel der neuen Strategie für die Informationsgesellschaft ist die Unterstützung der Herausbildung eines neuen „Finnland-Phänomens": Finnland soll zu einer international attraktiven, sachkundigen und serviceorientierten Informationsgesellschaft nach menschlichem Maß werden. Die Vision dieser Strategie lautet, für optimale Lebensqualität in der Informationsgesellschaft zu sorgen.

Leitlinien und Maßnahmen zur Unterstützung der Reform des Dienstleistungssektors, das Wohlergehen der Bürger sowie die Wettbewerbsfähigkeit der Volkswirtschaft und der einzelnen Betriebe – diesen Punkten kommt eine vorrangige Rolle in der neuen nationalen Strategie für die Informationsgesellschaft zu. Auf die genannten Themen wird dabei aus unterschiedlichsten Blickwinkeln eingegangen: Entwicklung von Fertigkeiten, Anwendung von vorhandenen und neuen Daten, Kreativität und Innovationskraft, Struktur- und Funktionsreformen, Netzwerkbildung sowie die Entwicklung und Nutzung von Informations- und Kommunikationstechnologien. Für den Zeitraum 2007-2011 wurden unter anderem folgende Hauptprojekte vorgeschlagen:

- Erarbeitung und Umsetzung eines Maßnahmenprogramms zur Erneuerung der Dienstleistungsstrukturen in der öffentlichen Verwaltung
- Anstrengungen zum Ausbau der Verbindungsgeschwindigkeiten in den Datennetzen sowie zur Gewährleistung der Interoperabilität zwischen den verschiedenen Strukturen in der Informationsgesellschaft
- Maßnahmen zur Förderung des lebenslangen Lernens
- Reformen an den Regelungen für das Arbeitsleben, sowie Entwicklung von Kompetenzen in Personal- und Unternehmensführung
- Reform des Innovationssystems
- Weiterentwicklung des Urheberrechtssystems
- Förderung der Digitalisierung von Geschäfts-

abläufen in Klein- und mittelständischen Unternehmen
- ein Beitrag zu internationalen Anstrengungen, besonders auf EU-Ebene, sowie enge Zusammenarbeit mit Nachbarregionen und mit Asien

Nationaler Datensicherheitstag

Das Büro des Datenschutzbeauftragten wirkte an der Vorbereitung und Durchführung der Dritten nationalen Datensicherheitskampagne sowie des Nationalen Datensicherheitstags im Februar 2006 mit. Ziel des Datensicherheitstages ist es, die Fertigkeiten der Bürger beim Umgang mit der Informationsgesellschaft zu steigern. Beim Nationalen Datensicherheitstag handelt es sich um ein Gemeinschaftsprojekt mit der öffentlichen Verwaltung sowie mit Privatunternehmen und verschiedenen Organisationen. Dieses Mal lag der Schwerpunkt bei Schulkindern sowie deren Lehrern und Eltern. Die Durchführung erfolgte in der Form von Internet-Lernspielen.

Computereinsatz an beliebigen Orten

Neue Technologien und Geräte ermöglichen es den Menschen, an den unterschiedlichsten Orten und praktisch jederzeit auf Informationen zuzugreifen bzw. Informationen weiterzuleiten. Verschlüsselungsvorrichtungen und anwendungsbezogene Sicherheitsmodelle können einen wichtigen unterstützenden Beitrag zum Schutz der Privatsphäre leisten. Wichtiger und schwieriger ist jedoch das von den Anwendern selbst zu leistende *Privacy Management*, d. h. das Erlernen und Anwenden von Verhaltensmustern zum bewussten Schutz seiner eigenen Privatsphäre. Dieses *Privacy Management* steht in einem engen Bezug zum bewussten Umgang eines jeden Einzelnen mit seinen privaten Daten. Die Benutzer müssen dafür sensibilisiert werden, welche Auswirkungen auf den Schutz ihrer Privatsphäre sich aus ihren jeweiligen Handlungen ergeben und wie sie Datenschutzfunktionen als unaufdringliche aber selbstverständliche Bestandteile der von ihnen genutzten Anwendungen und Dienste aktivieren und nutzen können.

Das finnische Verkehrs- und Kommunikationsministerium beauftragte ein universitäres Forschungsinstitut, das Helsinki Institute for Information Technology HIIT, mit der Erstellung einer Prognose bis zum Jahr 2015. Die Prognose wurde von 15 Wissenschaftlern des Instituts erstellt, von denen jeder einen bestimmten akademischen Fachbereich vertrat. Der Bericht sieht zahlreiche gute Möglichkeiten zur Beschleunigung der Wirtschaftsentwicklung und zur Steigerung des allgemeinen Wohlstands in Finnland, verweist aber zugleich auch auf eine Vielzahl von teilweise erheblichen Herausforderungen und Bedrohungen.

Die Technologieforschung spielt für Finnland eine sehr große Rolle. In den nächsten drei Jahren werden circa 25% der Erwerbsbevölkerung in Rente gehen. Daher besteht die Gefahr, dass ein erheblicher Teil der in der Volkswirtschaft vorhandenen Finanzmittel auf Sozialleistungen und Rentenzahlungen verwendet werden muss, anstatt das Geld in Forschung und Entwicklung investieren zu können. Das könnte in der Folge zu einer Schwächung der derzeit ausgezeichneten internationalen Wettbewerbsfähigkeit Finnlands führen. Die Antwort auf diese Herausforderung liegt in der Steigerung der Effizienz von Dienstleistungen für die Verwaltung von Industriebetrieben und sonstigen Unternehmen durch den forcierten Einsatz von Informations- und Kommunikationstechnologie.

Finnland befindet sich dafür in einer verhältnismäßig günstigen Ausgangsposition. Trotzdem äußert sich rund die Hälfte der Bevölkerung besorgt über Datensicherheit und Datenschutz. Daher müssen zum Wohle aller Systeme geschaffen werden, denen Bürger, Industriebetriebe und sonstige Unternehmen vertrauen können, und die zudem benutzerfreundlich und kostengünstig sind. Glücklicherweise setzt sich diese Einsicht in der finnischen Gesellschaft mehr und mehr durch. Datenschutz ist zum Erfolgsfaktor für Menschen aller Gesellschaftsschichten geworden. Er fristet nicht länger eine Randexistenz in der Rechtswissenschaft, sondern spielt inzwischen eine zentrale Rolle in der Gesellschaft.

Frankreich

A. Gesetzgebung

Von den im Jahr 2006 angenommenen und veröffentlichten Gesetzen und Verordnungen wirkten sich viele unmittelbar auf die Tätigkeit der nationalen Datenschutzbehörde (*Commission nationale de l'informatique et des libertés* - CNIL) im Jahr 2006 aus.

Die französische Nationalversammlung verabschiedete am 23. Januar 2006 ein wichtiges **Gesetz zur Terrorismusbekämpfung**. In der Folge wurde der Datenschutzbehörde CNIL eine immer größere Zahl von Gesetzestexten zur Stellungnahme vorgelegt. Diese Texte spiegeln eine Häufung computergestützter Überwachungsanlagen wider und erweitern die Möglichkeiten für den Zugriff und die Nutzung von Daten, die ursprünglich für einen anderen Zweck erhoben wurden, durch die Polizeikräfte. Zur Erläuterung sei darauf hingewiesen, dass im Gesetz selbst zahlreiche Bedingungen für die Durchführung dieser Verarbeitungsmethoden festgelegt sind und der Ermessensspielraum der Datenschutzbehörde CNIL daher begrenzt ist.

So sieht etwa das Gesetz vom 23. Januar 2006 die Einführung der automatisierten Verarbeitung der von Flug-, Eisenbahn- und Schifffahrtsgesellschaften erhobenen Daten vor. Die Datensätze von Passagieren, die in und aus Staaten außerhalb der Europäischen Union reisen, können zu Zwecken der Grenzkontrolle, Bekämpfung der illegalen Einwanderung und Terrorismusbekämpfung verarbeitet werden. Die Datenschutzbehörde CNIL hat zu den verschiedenen Durchführungstexten dieser Bestimmungen Stellung genommen.

Ferner musste sich die Datenschutzbehörde CNIL über andere Durchführungsbestimmungen desselben Gesetzes äußern, das zu Zwecken der Prävention und Ahndung von terroristischen Straftaten vorsieht, dass die befugten Bediensteten der speziell mit diesen Aufgaben betrauten Stellen der französischen Gemeinde- und Stadtpolizei *(Police municipale)* und Nationalpolizei *(Gendarmerie nationale)* unter den im Gesetz vom 6. Januar 1978 vorgesehenen Bedingungen auf folgende Datensätze zugreifen können:

- das KFZ-Register (*fichier national des immatriculations* – FNI)
- das Führerscheinregister (*système national de gestion des permis de conduire* – SNPC)
- das Personalausweisregister (*système de gestion des cartes nationales d'identité* – CNI)
- das Passregister (*système de gestion des passeports* – DELPHINE)
- das Ausländerregister (*système informatisé de gestion des dossiers des ressortissants étrangers en France* – AGDREF)
- das Visaregister (*système de délivrance des visas des ressortissants étrangers* – BIODEV).

Schließlich prüfte die Datenschutzbehörde CNIL den Verordnungsentwurf, der die Möglichkeiten zur Nutzung von Daten in Verbindung mit elektronischen Kommunikationsdiensten durch Polizeidienste ausdehnt, indem vor allem der Kreis der zur Aufbewahrung dieser Daten verpflichteten Personen erweitert wird.

Die Datenschutzbehörde CNIL befasste sich weiterhin mit der Durchführungsverordnung, in der im Einzeln die Bedingungen dargelegt sind, die für telematische oder computergestützte richterliche Beschlagnahmen im Hinblick auf die Datenverarbeitungsvorgänge bei den meisten öffentlichen Einrichtungen oder privatrechtlichen juristischen Personen gelten. Am 30. Mai 2006 gab die Datenschutzbehörde CNIL zu diesem Text eine sehr ausführliche Stellungnahme ab, in der sie die Ansicht vertrat, dass er nicht die notwendigen Garantien beinhalte, insbesondere in Bezug auf die Liste der öffentlichen und privaten Einrichtungen, bei denen telematische und computergestützte Beschlagnahmen erfolgen könnten.

Jedenfalls weist die Datenschutzbehörde CNIL darauf hin, dass Artikel 60 Absatz 2 des Strafgesetzbuchs,

wie die diesbezüglichen Parlamentsarbeiten zeigen, insbesondere auf Telekommunikationsbetreiber abzielt und elektronische Beschlagnahmen von unter dem Berufsgeheimnis stehende Daten aus dem Anwendungsbereich ausklammert, was nicht unproblematisch ist angesichts der Tatsache, dass der Verordnungsentwurf unter anderem Verwaltungen und Sozialversicherungsträger betrifft, die durch das Berufsgeheimnis geschützte Dateien verwalten.

Darüber hinaus wurde von der CNIL im Juni 2006 ein wichtiger **Gesetzentwurf zur Verbrechensverhütung** geprüft, der Anlass für zahlreiche Bemerkungen war, insbesondere zu den Bedingungen für eine Intervention der gesellschaftlichen Akteure und des Bürgermeisters bei Personen in Schwierigkeiten.

B. Rechtsprechung

Im Jahr 2006 wurde keine wichtige Entscheidung getroffen, die sich auf die Auslegung des französischen Datenschutzgesetzes auswirken würde.

Es könnte jedoch erwähnt werden, dass der Kassationsgerichtshof in einem Urteil seiner Strafkammer vom 14. März 2006 die Verurteilung eines Geschäftsführers bestätigte, der zahlreiche Werbenachrichten an Internetteilnehmer verschickt hatte, deren Adressen er in öffentlichen Internetforen einholte. Dieses Urteil beendet einen Rechtsstreit, der durch die Operation „Spambox" entstand, die von der Datenschutzbehörde CNIL im Jahr 2002 eingeleitet worden war.

Im Oktober 2002 hatte die Datenschutzbehörde nach ihrer Operation „Spambox" fünf Unternehmen vor Gericht verklagt, die diese illegale Geschäftswerbung praktizierten. Nur eine dieser Anzeigen führte zu strafrechtlichen Ermittlungen.

Der betroffene Unternehmensleiter wurde verklagt, weil er Namensdaten, in diesem Fall E-Mail-Adressen, erhoben hatte, um Dateien mit Werbekunden zu erzeugen, indem er Software einsetzte, die das „Absaugen" dieser Adresse im Internet (Websites, Jahrbücher, Foren) ermöglichte, ohne dass die betroffenen Personen ihre Einwilligung gegeben hätten oder informiert worden wären. Der Artikel 226 (18) des Strafgesetzbuchs verbietet die Erhebung personenbezogener Daten durch ein betrügerisches, unlauteres oder widerrechtliches Mittel.

Der Kassationsgerichtshof bestätigte damit die Auslegung der Datenschutzbehörde und des Berufungsgerichts, das die Ansicht vertrat, dass der Einsatz der beiden Softwareprogramme zum „Absaugen" von E-Mail-Adressen von natürlichen Personen eine gesetzwidrige und auf jeden Fall unlautere Erhebung von Namensdaten darstellt.

In einem weiteren Punkt schloss sich der Kassationsgerichtshof ebenfalls der Haltung des Berufungsgerichts und der CNIL an, indem er die Auffassung vertrat, dass *„die Identifikation elektronischer Adressen und ihre Nutzung eine Erhebung von Namensdaten darstellt, auch wenn diese nicht in einer Datei gespeichert werden, um an die Inhaber elektronische Nachrichten zu versenden"*.

Das Gesetz für das Vertrauen in die digitale Wirtschaft (*Loi pour la confiance dans l'économie numérique* - LCEN) unterwirft künftig die Nutzung von E-Mails bei geschäftlicher Werbung der vorherigen Einwilligung der betroffenen natürlichen Personen. Die Entscheidung des Kassationsgerichtshofs behält jedoch ihre ganze Tragweite für nichtkommerzielle Kommunikationsvorgänge per E-Mail. Sie legt eindeutig fest, dass E-Mail-Adressen und andere personenbezogene Angaben, die über öffentliche Interneträume zugänglich werden, deshalb noch nicht zur freien Verwendung zu Verfügung stehen.

C. Arbeitsweise und tätigkeiten der datenschutzbehörde cnil

1. Annahme von Beschlüssen

Im Jahr 2006 hat die CNIL 40 Mal getagt: 25 Plenarsitzungen, 9 reduzierte Sitzungen (Sanktionen)

und 6 beratende Sitzungen. Diese Sitzungen führten zur Annahme von 304 Beschlüssen, was eine ähnliche hohe Zahl von Entscheidungen wie im Vorjahr ergibt, nachdem sie zwischen 2004 und 2005 um 200% gestiegen war.

Diese Beschlüsse betreffen Stellungnahmen der CNIL im Rahmen ihrer Aufgabenfelder: Beratung oder Begutachtung (a), Sanktion (b), Vereinfachung vorhandener Formalitäten (c), Meldeformalitäten (Genehmigung oder Ablehnung einer Genehmigung, Stellungnahmen) (d).

a) Beratung und Begutachtung

Im Jahr 2006 gab die CNIL 9 Stellungnahmen zur Gesetz- oder Verordnungsentwürfen ab, darunter die Stellungnahme zum Gesetzentwurf über die Verbrechensverhütung, die Stellungnahme zu einem Entwurf für die Ratifizierung eines Vertrages über die grenzüberschreitende Zusammenarbeit bei der Bekämpfung von Terrorismus, Kriminalität und illegaler Einwanderung sowie die Stellungnahme zu einem Verordnungsentwurf zur Bekämpfung des Terrorismus.

Darüber hinaus gab sie 2 Empfehlungen ab, eine in Bezug auf die Dateien politischer Parteien und der gewählten Abgeordneten oder Bewerber für Wahlämter im Rahmen ihrer politischen Aktivitäten[1], die andere als Rahmen für die Vorkehrungen zur Geolokalisierung von Fahrzeugen von Arbeitnehmern[2].

b) Sanktionen

Seit dem Gesetz vom 6. August 2004 zur Änderung des Gesetzes über den Schutz personenbezogener Daten von 1978 verfügt die CNIL über Sanktionsbefugnisse, durch die sie Geldstrafen in einer Höhe von 150.000 Euro (300.000 Euro im Wiederholungsfall) innerhalb einer Grenze von 5% des Umsatzes verhängen kann. Während ihrer Sitzung vom 28. Juni machte die CNIL zum ersten Mal von ihren neuen Befugnissen Gebrauch, als sie eine Geldstrafe von 45.000 Euro gegen Crédit Lyonnais verhängte.

Im Jahresverlauf 2006 hat die CNIL insgesamt folgende Strafen verhängt:
- 13 Geldstrafen über einen Gesamtbetrag von 168.000 €, in Einzelbeträgen von 300 bis 45.000 €
- 7 Aufforderungen, eine Verarbeitung personenbezogener Daten zu beenden oder zu verändern, und 94 Mahnungen.
- 4 Verwarnungen gegen zwei Telekommunikationsbetreiber, eine Bank und eine Partei.

c) Vereinfachung vorhandener Formalitäten

Die CNIL setzte im Jahr 2006 die Arbeiten fort, die in diesem Sinne im Zeitraum 2004-2005 durchgeführt wurden, und verabschiedete dabei eine große Zahl von Maßnahmen zur Vereinfachung vorhandener Formalitäten, die bei ihren Diensten durchzuführen sind. Diese Vereinfachungen betreffen beispielsweise die Hilfe bei der Bewertung und Auswahl der Risiken bei der Kreditvergabe („credit scoring"), die Zugangskontrolle und Verwaltung der Arbeitsstunden und der Verpflegung am Arbeitsplatz durch Handflächenerkennung, die Kontrolle des Zugangs zum Arbeitsplatz durch die Erkennung des digitalen Fingerabdrucks, sofern dieser auf einem individuellen Datenträger gespeichert ist, sowie die Kontrolle des Zugangs zum Schulrestaurant per Handflächenerkennung. Diese Vereinfachungen finden jeweils in einem sehr konkreten Rahmen statt. Die genannten Vereinfachungen bleiben unerfüllt, wenn die für Datenverarbeitung Verantwortlichen nicht alle diesbezüglich von der CNIL gestellten Bedingungen erfüllen.

d) Meldeformalitäten

Die CNIL hat 2006 Folgendes verabschiedet:
- 17 Negativbescheide betreffend Genehmigungen

[1] http://www.cnil.fr/index.php?id=2133
[2] http://www.cnil.fr/index.php?id=1999&news[uid]=342&cHash=7845803996

insbesondere von digitalen Fingerabdruck-Kontrollen von Arbeitnehmern oder bestimmten Nutzungen der Sozialversicherungsnummer oder aber einer auf dem Klang der Namen beruhenden Datenverarbeitung.
- 17 Stellungnahmen zu sensiblen Datenverarbeitungsthemen oder Risiken, beispielsweise in Verbindung mit der mobilen elektronischen Überwachung, telematischen oder computergestützten Beschlagnahmen, mit Fluggastdatensätzen sowie mit der nationalen Personenfahndungsdatei (fichier national des personnes recherchées - FPR).

2. Gerichtliche Verfahren (Beschwerden und Anträge auf indirekten Zugang zu Polizeidateien)
Im Jahr 2006 sind bei der CNIL insgesamt 5167 Verfahren beantragt worden (3572 Beschwerden und 1595 Anträge auf indirekten Zugang zu Polizeidateien).

Es folgt - in absteigender Reihenfolge der Bedeutung - eine Auflistung der Tätigkeitsbereiche mit der größten Anzahl von Beschwerden. Werbeaktionen – Kreditinstitute - Arbeit – Telekommunikation. Häufigstes Beschwerdethema ist der Einwand gegen eine bestimmte Art der Datenverarbeitung.

Beschwerden stellen zwei Drittel der vom reduzierten Gremium der CNIL untersuchten Fälle dar, die für die Stellungnahme zu Sanktionen zuständig ist. Ferner gehen 25 % der Kontrollaufgaben, die von der CNIL wahrgenommen werden, auf über die Website der CNIL eingereichte Hinweise oder Beschwerden von Personen zurück. Schließlich sei darauf hingewiesen, dass die CNIL infolge einer Beschwerde des Rates der jüdischen Einrichtungen in Frankreich *(Conseil représentatif des institutions juives de France)* beschlossen hat, die Verantwortlichen einer Website zu verklagen, die eine Liste von Personen des öffentlichen Rechts verbreitete, die als zum jüdischen Glauben zugehörig dargestellt wurden.

3. Kontrollen
Im Jahr 2006:
- wurden 127 Organisationen kontrolliert (+34,73% gegenüber 2005)
- wurden 135 Reisen von Delegationen der CNIL durchgeführt (+ 40%)
- 25% der durchgeführten Kontrollen gingen auf Beschwerden von Privatpersonen zurück.

Die wichtigsten Tätigkeitsbereiche, die im Jahr 2006 kontrolliert wurden, sind Direktmarketing, private Ermittler (Dateiverwaltung, insbesondere von Schuldnern und Modalitäten für die Datenerhebung), die Anwendung des elektronischen Fahrscheinsystems (E-Ticketing) Navigo, das vom Pariser Verkehrsverbund RATP *(Régie autonome des transports Parisiens)* umgesetzt wurde, Personaleinstellung, lokale Gebietskörperschaften, Biometrie in Schulen, Hotels, Obdachlosenheimen, Sportvereinen usw. sowie Videoüberwachungssysteme.

Im Rahmen der internationalen Zusammenarbeit wurden zudem Aktenkontrollen anhand eines europaweit einheitlichen Musterfragebogens bei zehn Organisationen mit Niederlassung in Frankreich durchgeführt, die Zusatzversicherungen im Gesundheitsbereich anbieten. Unter den diesbezüglichen Antworten an die CNIL ist der Fall einer Mahnung zu erwähnen. Außerdem wurde für zwei weitere dieser Einrichtungen beschlossen, insbesondere unter technischen Gesichtspunkten zu überprüfen, dass die beschriebenen Maßnahmen tatsächlich umgesetzt werden.

Eine Reihe von Kontrollen wurde bei jedem der sechs für die Datenverarbeitung Verantwortlichen durchgeführt, die am Versuch zur Einführung der persönlichen elektronischen Patientenakte (*dossier médical personnel* – DMP) teilnahmen. Die Feststellungen, die anlässlich dieser Überprüfungen getroffen wurden, in die zum ersten Mal seit Inkrafttreten der neuen Bestimmungen des am 6. August 2004 geänderten Gesetzes vom 6. Januar 1978 sowie

seiner Durchführungsverordnung vom 20. Oktober 2005 Amtsärzte einbezogen wurden, ermöglichten der CNIL eine genauere Information über dieses System, bevor sie über seine allgemeine Einführung im Jahr 2007 Stellung nehmen konnte.

4. Meldeformalitäten

Im Jahresverlauf 2006 verzeichnete die CNIL 72.000 neue Verarbeitungen personenbezogener Daten und 1.800 Meldungen über die Veränderung bereits gemeldeter Verarbeitungen, so dass letztendlich im gesamten Jahresverlauf 73.800 Akten zu verwalten waren. Die jährliche Gesamtzahl der Meldungen von Dateien an die CNIL stabilisiert sich allmählich seit der Reform des Datenschutzgesetzes (*loi informatique et libertés*) von 2004, wodurch Dateien, die unter Datenschutzgesichtspunkten unproblematisch sind, von jeglichen Verwaltungsformalitäten befreit werden konnten und auf bestimmte Meldepflichten verzichtet werden kann, wenn ein externer Datenschutzbeauftragter (*correspondant informatique et libertés*) benannt wird. Diese Entwicklungen haben zwar eine Begrenzung der Anzahl an Dateimeldungen zur Folge, jedoch spiegeln sie zugleich eine Ausweitung der Tätigkeit der CNIL wider, etwa im Rahmen der Ausbildung der externen Datenschutzbeauftragten oder der Entwicklung der Freistellungsnormen.

Seit 1978 wurden der CNIL insgesamt 1.160.000 Dateien gemeldet.

5. Einige Schwerpunkte des Jahres 2006

a) Die Biometrie auf dem Vormarsch (Personalausweis, staatliches Bildungswesen, Casinos,…)

Die im Jahr 2005 beobachteten Technologietrends haben sich im Jahresverlauf 2006 bestätigt. Die wichtigste Tendenz betrifft den kontinuierlich steigenden Einsatz der Biometrie. Die CNIL verzeichnete eine deutliche Zunahme der Anzahl von Genehmigungsanträgen für biometrische Einrichtungen. Im Jahr 2005 genehmigte die Kommission die Umsetzung von 34 biometrischen Einrichtungen und lehnte 5 ab; im Jahr 2006 genehmigte sie 351 und lehnte 9 ab.

Diese spektakuläre Entwicklung der Anzahl der von der CNIL geprüften Akten beruht zum großen Teil auf der Annahme von drei vereinfachten Genehmigungsverfahren für die Einrichtungen:

- die Handflächenerkennung als Zugangskontrolle zum Schulrestaurant
- auf der Grundlage der Erkennung des digitalen Fingerabdrucks, der ausschließlich auf einem individuellen Datenträger gespeichert wird, welcher der betreffenden Person gehört und deren Zweck die Kontrolle des Zugangs zu den Räumlichkeiten am Arbeitsplatz ist
- auf der Grundlage der Handflächenerkennung zur Zugangskontrolle und zur Verwaltung der Arbeitsstunden und der Verpflegung am Arbeitsplatz.

Datenverarbeitungsvorgänge, deren Ablauf die strikten Vorgaben einer dieser drei Entscheidungsrahmen erfüllen (einheitliche Genehmigungen), können nach einer einfachen Konformitätserklärung umgesetzt werden. Sie erfüllen den Zweck, der biometrischen Einrichtungen am häufigsten zugeteilt wird, und stellen 299 der 351 von der CNL im Jahr 2006 ausgestellten Genehmigungen dar.

b) Empfehlung zur Geolokalisierung der von den Mitarbeitern genutzten Fahrzeuge

Die CNIL verabschiedete am 16. März 2006 eine Empfehlung über die Umsetzung von Einrichtungen zur Geolokalisierung von Fahrzeugen, die von Arbeitnehmern genutzt werden. Diese zielt darauf ab, für die Entwicklung bei diesen Vorrichtungen im Hinblick auf das Datenschutzgesetz und das Arbeitsgesetzbuch einen Rahmen zu geben.

Die Absicht der CNIL, eine solche Empfehlung zu verabschieden, ergab sich aus der Erkenntnis, dass die immer häufigere Nutzung von Systemen zur

Geolokalisierung von Fahrzeugen aufgrund der Verarbeitung von satellitengestützten Informationen (GPS) die von Unternehmen oder Verwaltungen angebotenen Dienstleistungen durchaus verbessern kann, dass es bei einer derartigen Nutzung jedoch auch zu Übertreibungen und Gesetzesverstößen kommen kann.

c) Empfehlung der CNIL zur Wahlwerbung

Im Hinblick auf die Wahltermine in den Jahren 2007 und 2008 hat die CNIL beschlossen, am 5. Oktober 2006 nach Konsultation der politischen Parteien eine Empfehlung über den Schutz personenbezogener Dateien bei Wahlkampfaktionen abzugeben.

Dabei erinnerte die Datenschutzbehörde daran, dass manche Dateien auf keinen Fall zu politischen Wahlkampfzwecken genutzt werden können (zum Beispiel die Dateien der Verwaltungen oder der lokalen Gebietskörperschaften, wie Standesamtregister, Steuer- und Abgabendateien oder Sozialhilfedateien). Die Wählerliste kann dagegen jeder Person oder Vereinigung zu Zwecken der Wahlwerbung mitgeteilt werden. Keine Bestimmung des Gesetzes untersagt einer Partei oder einem Kandidaten, die gleichen Wahlwerbemittel zu nutzen wie jene, die beispielsweise im Handel eingesetzt werden, nämlich das Anmieten von Dateien bei spezialisierten Unternehmen.

Dennoch vertritt die Datenschutzbehörde die Ansicht, dass angesichts der besonderen Sensibilität der Wahlkampfaktionen eine klare und transparente Aufklärung der Betroffenen über die Bedingungen für die Nutzung ihrer Daten angeraten ist.

Deutschland

A. Implementation of Directives 95/46/EC and 2002/58/EC and other legislative developments

In der Bundesrepublik Deutschland wurde mit dem Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz – BGBl. I, Nr. 66 vom 30.12.2006, S. 3409 ff) erstmals die Zusammenführung von Datenbeständen der Polizeien und der Nachrichtendienste in einer gemeinsamen Antiterrordatei zur Bekämpfung des internationalen Terrorismus ermöglicht. Das Gesetz begegnet verfassungs- und datenschutzrechtlichen Bedenken vor allem im Hinblick auf die Beachtung des Gebots der Trennung von Polizei und Nachrichtendiensten. Das Trennungsgebot begrenzt die Zusammenarbeit von Polizei und Geheimdiensten, um den jeweiligen unterschiedlichen Aufgaben und Befugnissen der verschiedenen Behörden Rechnung zu tragen.

Auch das am 11. Januar 2007 in Kraft getretene Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes aus dem Jahr 2002 (Terrorismusbekämpfungsergänzungsgesetz – BGBl. I, Nr. 1 vom 10. Januar 2007, S. 2 ff) erscheint datenschutzrechtlich problematisch. Durch dieses Gesetz sind die bereits 2002 ausgeweiteten Befugnisse der Nachrichtendienste erneut erweitert worden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mehrere Entschließungen zur Gewährleistung des Datenschutzes bei der Terrorismusbekämpfung beschlossen.

Mittelstandsentlastungsgesetz

Am 26. August 2006 trat das Erste Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft in Kraft, das auch Einschränkungen bei der Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter enthält (BGBl. I S. 1970). Dabei wurde die Verpflichtung für Unternehmen, einen betrieblichen Datenschutzbeauftragten zu ernennen, gelockert. In diesen Fällen entfällt die Meldepflicht. Bei der Bestellung eines externen Datenschutzbeauftragten wurde die rechtlichen Möglichkeiten in Bereichen, in denen besondere Berufsgeheimnisse gelten, erweitert.

B. Major case law

Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung 2001 gesetzgeberische Konsequenzen?

Mit Beschluss vom April 2006 hat das Bundesverfassungsgericht die Durchführung der Rasterfahndung nach dem nordrhein westfälischen Polizeigesetz aus Anlass der Terroranschläge vom 11. September 2001 beanstandet. Der Gesetzgeber dürfe den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person vorsehen. Eine Rasterfahndung im Vorfeld einer konkreten Gefahr sei verfassungsrechtlich nicht zulässig.

Der Beschluss hat Auswirkung auf die Ausgestaltung der präventiv polizeilichen Rasterfahndung in den Ländern und beim Bund. Auch andere präventiv polizeiliche Maßnahmen mit ähnlicher Eingriffstiefe und Streubreite an den vom Bundesverfassungsgericht aufgestellten Grundsätzen zu messen und auszurichten.

Entscheidung LG Darmstadt zu Verkehrsdatenspeicherung

Nach einem inzwischen rechtskräftigen Urteil des Landgerichts Darmstadt vom 25. Januar 2006 dürfen Internet-Zugangsprovider die IP-Adressen ihrer Flatrate-Kunden grundsätzlich nicht mehr speichern.

Das Gericht hat seine Entscheidung auf § 96 Abs. 2 Telekommunikationsgesetz gestützt, wonach Internet-Zugangsprovider Verkehrsdaten grundsätzlich unverzüglich nach dem Ende der Verbindung löschen müssen. Eine Verwendung dieser Daten

über das Ende der Verbindung hinaus ist nur für bestimmte im Telekommunikationsgesetz im Einzelnen genannten Zwecke zulässig, so etwa für die Entgeltberechnung und die Abrechnung.

Der Entscheidung ist zuzustimmen, weil das Prinzip einer Flatrate gerade darin besteht, dass die Internetverbindungskosten pauschal abgerechnet werden. Vor dem Hintergrund dieses Geschäftsmodells ist eine Speicherung der jeweiligen IP-Adresse des Flatrate-Kunden zu Abrechnungszwecken völlig unnötig

Mit dieser Entscheidung stärkt das Gericht das Recht auf informationelle Selbstbestimmung der Internetnutzer.

BVG-Entscheidung zu Versichertenrechten (Formularmäßige Einwilligungserklärungen)

„Das Bundesverfassungsgericht hat in einer Entscheidung vom 23.Oktober 2006

(1 BvR 2027/02) zur Verletzung des Rechts auf informationelle Selbstbestimmung durch eine allgemeine Schweigepflichtentbindungserklärung

in Versicherungsverträgen festgestellt, dass eine formularmäßige und zum Teil sehr allgemein umschriebene Erklärung das Interesse des Betroffenen an einem wirksamen informationellen Selbstschutz erheblich beeinträchtigt.

Weil wegen der weiten Fassung der Erklärung nicht absehbar sei, welche Auskünfte von wem eingeholt werden können, werde dem Betroffenen die Möglichkeit genommen, die Wahrung seiner Geheimhaltungsinteressen selbst zu kontrollieren. Dieser Beschluss hat große Bedeutung weit über den entschiedenen Fall hinaus, weil sehr allgemein gehaltene Einwilligungserklärungen in vielen Bereichen die Grundlage für Erhebung und Verarbeitung personenbezogener Daten bilden und die Betroffenen keine Alternative zur Abgabe solcher Erklärungen haben."

Beschluss des Bundesverfassungsgerichts vom 22. August 2006 zum Einsatz des IMSI-Catchers im Strafverfahren (Az.: 2 BvR 1345/03)

Mit Hilfe des sog. IMSI-Catchers ist es möglich, Karten- und Gerätenummer sowie den Standort eines empfangsbereiten Mobiltelefons zu ermitteln. Das Bundesverfassungsgericht hat festgestellt, dass die Datenerhebung durch den IMSI-Catcher nicht in das Fernmeldegeheimnis, aber in das Recht auf informationelle Selbstbestimmung auch unbeteiligter Dritter eingreift. Dieser Eingriff beruhe jedoch im Strafverfahren auf einer wirksam zustande gekommenen gesetzlichen Grundlage (§ 100i StPO) und sei nicht unverhältnismäßig. Das Bundesverfassungsgericht hat allerdings ausdrücklich darauf hingewiesen, dass bei der Durchführung von Maßnahmen nach § 100i StPO die Ermittlungsbehörden darauf zu achten haben, dass die Grundrechtspositionen der unbeteiligten Dritten nicht über das unbedingt notwendige Maß hinaus berührt werden. Außerdem hat es den Gesetzgeber aufgerufen, im Rahmen der anstehenden Neuregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen die technischen Entwicklungen aufmerksam zu beobachten und im Hinblick auf den erforderlichen Grundrechtsschutz ggf. korrigierend einzugreifen.

C. Major specific issues

Die 72. Konferenz der Datenschutzbeauftragten des Bundes und er Länder hat am 26./27. Oktober 2006 hat gefordert, dass sich die Wirtschaft verbindlichen Regelungen beim Einsatz von RFID unterwerfen möge. Wenn die Hersteller und der Handel nicht zu einer Selbstverpflichtung kommen, muss der Gesetzgeber die Rechte der Verbraucher bei der Anwendung der RFID-Technologie schützen. Dabei ist kritisch zu prüfen, ob auf eine eindeutige Kennzeichnung von Verbrauchsgütern nicht verzichtet werden kann. Die Einhaltung bestimmter Rahmenbedingungen wie Transparenz, Kennzeichnungspflicht, Möglichkeit der Deaktivierung sowie wirksame Blockierungsmöglichkeiten beim Einsatz von RFIDs müssen gewährleistet sein. Eine

heimliche Profilbildung darf es nicht geben. Auch der Düsseldorfer Kreis, ein Zusammenschluss der obersten nationalen Aufsichtsbehörden für den nichtöffentlichen Bereich, hat eine ähnliche Entschließung beschlossen. Außerdem hat der Arbeitskreis-Technik der Landes- und des Bundesbeauftragten eine Orientierungshilfe erarbeitet, welche sich mit datenschutzrechtlichen Fragestellungen zum Thema RFID anhand von Use-Cases auseinandersetzt.

Nutzung von Signaturverfahren

Elektronische Signaturen sichern elektronische Dokumente, insbesondere ihre Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist in Deutschland durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zwischen Computersystemen werden Authentisierungsverfahren eingesetzt, um die Identität der Systeme - gegebenenfalls auch eines Nutzers dieser Systeme - nachzuweisen.

Beide Verfahren nutzen in der Regel die asymmetrische Verschlüsselung. Gleichwohl unterscheiden sie sich im Inhalt ihrer Aussagen. Dies muss bei der Planung und beim Einsatz in Verwaltungsverfahren (eGovernment) berücksichtigt werden. Die eingesetzten Signaturverfahren werden ständig durch das BSI auf ihre Sicherheit, Robustheit und Gültigkeit geprüft und überwacht. Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Diese Verfahren werden beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System benutzt.

Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur. Die Trennung dieser beiden Bereiche ist für die technische Entwicklung eines Verfahrens und seine Anwendung wichtig und sollte gerade aus datenschutzrechtlicher Sicht beachtet werden.

Schülerstatistik

In den für die Schul- und Bildungspolitik in Deutschland zuständigen Bundesländern wird seit einigen Jahren ein einheitliches System der Schulstatistik angestrebt. Hierzu soll auf Landesebene über alle SchülerInnen und LehrerInnen ein umfangreicher Datensatz angelegt werden, der das gesamte Schulleben dokumentiert. Darüber hinaus ist an eine spätere Ergänzung des Schülerdatensatzes durch sozioökonomische Daten über das Elternhaus gedacht und an eine Einbeziehung von Kindergarten- und Hochschulzeit. Die Daten sollen über eine Identifikationsnummer pseudonymisiert und in dieser Form in einer bundesweiten Datenbank zusammengeführt werden. Der Zweck dieser Datensammlung wird von der politischen Seite eher unbestimmt mit der Erforderlichkeit für bildungsplanerische Maßnehmen angegeben.

Die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 hat in einer Entschließung ausdrücklich vor dem Aufbau eines derart umfassenden Registers in personenbeziehbarer Form gewarnt und auf die verfassungsrechtlichen Vorgaben hingewiesen. Eine derartige Totalerhebung ist nach deutschem Verfassungsrecht nur zulässig, wenn das angestrebte Ziel nicht mit weniger einschneidenden Maßnahmen erreicht werden kann. Nach Auffassung der Konferenz der Datenschutzbeauftragten können die notwendigen Planungsunterlagen auch durch stichprobenbasierte wissenschaftliche Studien auf freiwilliger Basis erreicht werden. Zur Zeit wird durch Gespräche und Workshops mit den Vertretern der Kultusministerien der Länder versucht, die Ausführung dieses datenschutzrechtlich bedenklichen Konzepts zu verhindern

Forschungsprojekt „Fotofahndung"

Das Bundeskriminalamt testete im Mainzer Hauptbahnhof mittels des Forschungsprojekts „Foto Fahndung",

inwieweit moderne Gesichtserkennungssysteme die Polizei bei der Suche nach bestimmten Personen unterstützen können.

Bei diesem Projekt wurden Gesichtsbilder (biometrische Merkmale) von freiwilligen Testteilnehmern aufgenommen und zum späteren Abgleich in einer Datenbank gespeichert. Die biometrischen Systeme verglichen die Gesichter aus der Menge der vorbeigehenden Passanten mit diesen gespeicherten Bilddaten. Für die Bewertung der Messdaten wurden die Gesichtsbilder erkannter Personen fotografiert, gespeichert und anschließend ausgewertet.

Vorausgesetzt die Fehlerrate ist gering, wird der kombinierten Anwendung von Videotechnik und Biometrie voraussichtlich eine wachsende Bedeutung zukommen. Da die Technik grundsätzlich für eine breit angelegte individuelle Überwachung geeignet ist, kommt es ganz entscheidend darauf an, wie und zu welchen Zwecken ein eventueller späterer Echtbetrieb erfolgen wird. Dabei muss immer die Balance zwischen den Bürgerrechten und den Belangen der öffentlichen Sicherheit gewahrt bleiben. Sie darf nicht zur Totalüberwachung führen. Zudem muss noch nachgewiesen werden, ob und inwieweit diese Technologie überhaupt für Fahndungsmaßnahmen geeignet ist. Das Bundeskriminalamt hat bisher noch keinen Erfahrungsbericht vorgelegt.

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 in nationales Recht umgesetzt. Der laufende technologische Fortschritt sowie die Erfahrungen seit dem Inkrafttreten des Datenschutzgesetzes vor acht Jahren haben nun eine Überarbeitung einer Reihe von Bestimmungen des Gesetzes 2472/97 erforderlich gemacht. Die vorliegende Gesetzesänderung (Gesetz 3471/2006) ergänzt die vorherigen Änderungen (Gesetz 2819/2000, Gesetz 2915/2001 und Gesetz 3156/2003). Geist und Bestimmungen des Gesetzes bleiben durch die Änderungen unberührt. Zentrales Anliegen ist und bleibt die Gewährleistung eines möglichst hohen Schutzniveaus für personenbezogene Daten durch entsprechende Vorschriften und Garantien. Das durch den gesetzlichen Rahmen in der Republik Griechenland gewährleistete hohe Schutzniveau für personenbezogene Daten entspricht auch den Anforderungen der jüngsten Verfassungsreform (2001) und insbesondere des neuen Artikels 9A der Verfassung.

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

Richtlinie 2000/58/EG

Die Richtlinie 2000/58/EG wurde durch das genannte Gesetz 3471/2006 (über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sowie zur Änderung von Gesetz 2472/97) in nationales Recht umgesetzt. Das neue Gesetz wurde in der Form eines neuen Gesamttexts verabschiedet, und nicht als Änderung zu Gesetz 2774/1999 (über den Schutz von personenbezogenen Daten im Bereich der Telekommunikation), das im Interesse der Klarheit und zur Vermeidung von Missverständnissen durch den neuen Text außer Kraft gesetzt und vollständig ersetzt wird.

Eine englische Fassung des Gesetzes 3471/2006 wird in Kürze unter www.dpa.gr verfügbar sein.

Die wichtigsten Entwicklungen

Die griechische Datenschutzbehörde *(Αρχη Προστασιασ Δεδομενων Προσωπικου Χαρακτηρα)* erhielt durch Paragraf 29 des Gesetzes 3471/2006 die Befugnis zur Durchführung unabhängiger Prüfungen der nationalen Bereiche des Schengener Informationssystem (SIS) gemäß Artikel 114, Absatz 1 des Schengener Durchführungsübereinkommens (Gesetz 2514/1997), ferner zur Ausübung der Aufgaben der nationalen Kontrollinstanz gemäß Artikel 23 des Europol-Übereinkommens (Gesetz 2605/1998) sowie zur Ausübung der Aufgaben der nationalen Kontrollinstanz gemäß Artikel 17 des Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich (Gesetz 2706/1999).

B. Bedeutende Rechtsprechung

Entscheidung 52/2006

In ihrer Entscheidung 52/2006 befand die griechische Datenschutzbehörde die seitens der griechischen Schutzgemeinschaft für allgemeine Kreditsicherung TIRESIAS Bank Information Systems SA (Τειρεσίας AE) praktizierte Erfassung und Verarbeitung von Daten über Vertreter von juristischen Personen, die selbst keine Kreditnehmer sind, für gesetzwidrig. Die Datenschutzbehörde wies die TIRESIAS SA an, sämtliche derartigen Daten binnen sechs Monaten zu löschen.

Entscheidung 68/2006

In ihrer Entscheidung 68/2006 erteilte die Datenschutzbehörde einer Bank und einer

Kreditkartengesellschaft eine Verwarnung wegen Verstoßes gegen das Datenschutzgesetz durch Gewährung eines Kredits und Ausstellung einer Kreditkarte ohne vorherige Zustimmung, Antrag und Information des Datensubjekts. In diesem Fall hatte der Geschäftsführer eines Ladengeschäfts für Elektrogeräte die personenbezogenen Daten eines Kunden erhoben, um damit bei einer bestimmten vereinbarten Bank einen Kreditantrag einzureichen. Die Daten dieser Person wurden durch den genannten Geschäftsführer jedoch an eine andere Bank weitergeleitet, um damit einen Kredit sowie die Ausstellung einer Kreditkarte zu beantragen, und zwar ohne einen entsprechenden Auftrag und ohne die Einwilligung dieses Kunden. Gemäß Gesetz 2472/97 ist die Verarbeitung personenbezogener Daten im Prinzip gestattet, soweit das betroffene Datensubjekt seine Einwilligung erteilt hat. Eine der in Paragraf 5 Absatz 2 Buchstaben a bis e des Gesetzes 2472/97 niedergelegten Ausnahmen gestattet die Verarbeitung ohne Einwilligung des Datensubjekts, sofern diese Verarbeitung erforderlich ist, um einen Vertrag zu erfüllen, bei dem das Datensubjekt Vertragspartei ist, oder um im Auftrag des Datensubjekts vor dem Abschluss eines Vertrags erforderliche Schritte zu absolvieren. Das Anbieten einer Bankdienstleistung sowie die Ausstellung einer Kreditkarte ohne die vorherige Verständigung des Datensubjekts bzw. ohne seinen diesbezüglichen Antrag sind jedoch gesetzwidrig. Das Erheben von personenbezogenen Daten durch Unternehmen, die mit Banken zusammenarbeiten, und die Übermittlung dieser Daten an ein Unternehmen, das Kreditkarten ausstellt, ist gesetzeskonform, soweit diese Datenverarbeitung für die Ausstellung einer Kreditkarte nach einem entsprechenden Antrag des Datensubjekts erforderlich ist (Paragraf 5 Absatz 1 und 2 Buchstabe a) und sofern das Datensubjekt zuvor ordnungsgemäß informiert worden ist (Paragraf 11 des Gesetzes 2472/97).

Entscheidung 39/2006

Die Datenschutzbehörde erhielt vom Ministerium für öffentliche Ordnung einen Antrag zur Verlängerung der Betriebserlaubnis seines Videoüberwachungssystems für das Straßennetz in der Verwaltungsregion Attika. Dieses Videoüberwachungssystem war zur Gewährleistung der Sicherheit bei den Olympischen Spielen eingerichtet worden. Der weitere Betrieb, so argumentierte das Ministerium, sei im Interesse der Allgemeinheit und insbesondere für die Zwecke der Verkehrsüberwachung erforderlich.

Das Ministerium beantragte ferner die Verlängerung der Verarbeitungserlaubnis für die durch das System gelieferten personenbezogenen Daten. Als nachrangiger Zweck für die Datenverarbeitung wurde der Schutz von Personen und Eigentum unter anderem in folgenden Bereichen angeführt:

a) zielgerichtete Prävention und Untersuchung schwerer Straftaten durch die Möglichkeit zur Nutzung des Systems bei Kundgebungen oder Versammlungen
b) Bewältigung von schwerwiegenden Sicherheitsproblemen und Krisensituationen
c) Schutz wichtiger Persönlichkeiten („VIPs“) bei Autofahrten
d) Schutz besonders gefährdeter Objekte (öffentliche Gebäude, Botschaften usw.), ohne diese jedoch im Einzelnen zu nennen
e) Koordination und Steuerung der griechischen Polizeikräfte bei der Ausübung ihrer Dienstpflichten
f) Aufzeichnung und Übermittlung von Daten an die zuständigen Polizeidienststellen, die Staatsanwaltschaft und die Justizbehörden bei tödlichen Verkehrsunfällen und bei Verkehrsunfällen, bei denen das Unfallopfer den Unfallort vor Erfassung der Personalien verlässt, sowie ferner bei schweren Straftaten.

In ihrer Entscheidung 39/2006 verlängerte die Datenschutzbehörde die Betriebserlaubnis des Videoüberwachungssystems für das Straßennetz in der Verwaltungsregion Attika ausschließlich für Zwecke der Verkehrsüberwachung bis zum 24. Mai 2007, gemäß den in der Entscheidung Nr. 63/2004 der Datenschutzbehörde niedergelegten Bedingungen.

Entscheidung 33/2006

Das Generalsekretariat für Information - Generalsekretariat für Kommunikation der Republik Griechenland fragte bei der Datenschutzbehörde an, ob es gemäß Gesetz 2472/97 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gesetzlich befugt sei, im Falle von unbefristet beim Generalsekretariat beschäftigten Journalisten bei den zuständigen Sozialversicherungsbehörden Daten zu den Versicherungszeiten dieser Journalisten anzufordern.

Das Generalsekretariat für Information - Generalsekretariat für Kommunikation beabsichtigte, die genannten wichtigen Daten anzufordern, um jene Journalisten, die sämtliche Anforderungen für den Erhalt voller Pensionsbezüge erfüllen, gemäß Paragraf 8 des Gesetzes 3198/1955 über ihr Pensionierungsrecht sowie über das Recht der Sekretariate (als Arbeitgeber) zur Beendigung der Arbeitsverträge gemäß dem genannten Artikel zu informieren.

Die Datenschutzbehörde erließ daraufhin ihre Entscheidung 33/2006, in der sie befand, dass eine Mitteilung von Daten über den Gesamtversicherungszeitraum seitens der zuständigen Sozialversicherungsbehörden an das Generalsekretariat für Information - Generalsekretariat für Kommunikation angesichts von dessen Absicht zur Beendigung von Vertragsverhältnissen mit seinen Beschäftigten einen Verstoß gegen Paragraf 4 des Gesetzes 2472/1997 darstellen würde. Die Datenschutzbehörde befand ferner, dass bereits das Anlegen einer derartigen Datei einen Verstoß gegen Paragraf 4 des Gesetzes 2472/97 darstellen würde. Die Entscheidung beruht auf dem Umstand, dass die Erstellung und Pflege einer derartigen Datei auf die Entlassung von Beschäftigten einzig und allein aus Altersgründen abzielen würde. Damit würde der beabsichtigte Zweck der Verarbeitung einen Verstoß gegen die Bestimmungen der Richtlinie 2000/78/EG „zur Bekämpfung der Diskriminierung wegen der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung in Beschäftigung und Beruf" darstellen, denn diese Richtlinie untersagt im Arbeitsleben direkte oder indirekte Diskriminierungen aus Altersgründen. Die Richtlinie 2000/78/EG wurde mit dem Gesetz 3304/2005 in griechisches Recht umgesetzt. d. h. höherrangige internationale und gemeinschaftliche Rechtsprinzipien wurden in den griechischen Rechtsrahmen überführt. Daher untersagt die Datenschutzbehörde die Erstellung und Pflege jedweder Datei zur Erhebung und Verarbeitung von personenbezogenen Daten im Hinblick auf die Ermittlung der Versicherungsdauer und die Beendigung von Arbeitsverhältnissen von Beschäftigten, ungeachtet der Art der jeweiligen Arbeitsverträge. Derartige Fälle sind allerdings deutlich zu unterscheiden von Fällen, in denen eine Vertragsbestimmung ausdrücklich die Beendigung des Arbeitsvertrags und die Pensionierung eines Mitarbeiters bei Erreichen einer bestimmten Altersgrenze vorsieht.

Entscheidung 49/2006

Der private Sicherheitsdienst HERMES SA fragte bei der Datenschutzbehörde an, ob das Allgemeine Krankenhaus Athen im Rahmen einer internationalen öffentlichen Ausschreibung „zur Beschaffung von Sicherheitsdienstleistungen mit Auftragsvergabe an das kostengünstigste Angebot" gesetzlich befugt sei, von den Ausschreibungsteilnehmern Einzelangaben zu den vorgeschlagenen Wachleuten zu verlangen.

Aufgrund von Paragraf 4 des Gesetzes 2472/1997 prüfte die Datenschutzbehörde, ob es angesichts des seitens des Allgemeinen Krankenhauses Athen angeführten Zwecks der Datenverarbeitung gesetzmäßig ist, die Vorlage derartiger Daten zu verlangen. Besonders berücksichtigt wurden dabei die Bestimmungen des Gesetzes 2518/1997 „über die Bedingungen für den Betrieb privater Sicherheitsdienste, die Pflichten ihrer Mitarbeiter sowie weitere Bestimmungen" sowie ferner die Bestimmungen der Richtlinie

2000/78/EG „zur Bekämpfung der Diskriminierung wegen der Religion oder der Weltanschauung, einer Behinderung, des Alters oder der sexuellen Ausrichtung in Beschäftigung und Beruf", die durch das Gesetz 3304/2005 in griechisches Recht umgesetzt worden ist (vgl. oben, Entscheidung 33/2006). Mit ihrer Entscheidung 49/2006 befand die Datenschutzbehörde, dass das Allgemeine Krankenhaus Athen gemäß Gesetz 2472/1997 befugt ist, personenbezogene Daten zu den vorgeschlagenen Wachleuten zu erheben und zu verarbeiten. Allerdings entschied die Datenschutzbehörde, dass es gegen die Bestimmungen von Gesetz 2472/1997 verstößt, zu jedem einzelnen der vorgeschlagenen Wachleute personenbezogene Daten über das Alter zu erheben (da die Ausschreibung ohnehin eine allgemeine Altersbeschränkung auf 23 bis 40 Jahre enthält) sowie eine Angabe zum Schulabschluss und für jeden der vorgeschlagenen männlichen Wachleute ein Zertifikat hinsichtlich der Ableistung bzw. Entbindung vom Militärdienst zu verlangen. Diese Entscheidung beruht auf dem Umstand, dass die Erfassung und Verarbeitung derartiger Daten zu Diskriminierungen in Beschäftigung und Beruf führen.

Entscheidung 40/2006

In ihrer Entscheidung 40/2006 befand die Datenschutzbehörde, dass eine ordnungsgemäße Erfüllung des Zugriffsrechts von Bewerbern auf ihre Prüfungsunterlagen im Rahmen einer seitens des Obersten Rats für die Personalauswahl für den griechischen öffentlichen Dienst ASEP *(ΑΝΩΤΑΤΟ ΣΥΜΒΟΥΛΙΟ ΕΠΙΛΟΓΗΣ ΠΡΟΣΩΠΙΚΟΥ)* durchgeführten Prüfungsverfahrens sowie im Rahmen sonstiger Prüfungsverfahren für den öffentlichen Dienst bedeutet, dass dem Datensubjekt Fotokopien seiner Prüfungsunterlagen ausgehändigt werden müssen, damit es sich vergewissern kann, dass die gesetzlichen Bestimmungen für die ordnungsgemäße Verarbeitung seiner personenbezogenen Daten seitens des für die Datenverarbeitung Verantwortlichen eingehalten worden sind. Grundsätzlich liegt es auf der Hand, dass die Bestimmungen von Artikel 12 und 13 der Richtlinie 95/46/EG, die durch das Gesetz 2472/1997 in griechisches Recht umgesetzt worden sind, dem Datensubjekt ein umfassendes Zugriffsrecht auf Daten zu seiner Person gewähren. Allerdings ist per Gesetz eine Einschränkung des Zugriffsrechts auf die genannten Daten möglich, sofern die in Artikel 13 der genannten Richtlinie niedergelegten Bedingungen gewahrt sind. Im vorliegenden Fall bestanden jedoch keine derartigen Gründe. Daher wurden sämtliche gegenteiligen Ausführungen des ASEP als unbegründet zurückgewiesen. Die Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors wurde durch das Gesetz 3448/2006 in griechisches Recht umgesetzt. Im Gegensatz zu den Ausführungen des ASEP stehen die Bestimmungen des genannten Gesetzes weder im Widerspruch zu den Bestimmungen des Gesetzes 2472/97 noch schränken sie die Aufgaben der Datenschutzbehörde ein. Daher ist die Datenschutzbehörde umfassend zuständig für die Umsetzung des genannten Gesetzes 3448/2006. Ferner kann ein Bewerber sein Zugriffsrecht innerhalb des Zeitraums, während dessen das Datensubjekt Anspruch auf Entschädigung bei einer gesetzwidrigen Behandlung seitens öffentlicher Einrichtungen hätte, jederzeit ausüben.

Entscheidung 66/2006

Mit seiner Entscheidung 66/2006 befand die Datenschutzbehörde, dass die Bestimmungen von Paragraf 22, Absatz 1 des Gesetzes 3475/2006, aufgrund deren den Bewerbern bei landesweiten Zulassungsprüfungen für Universitäten und sonstige tertiäre Bildungseinrichtungen der Zugriff auf ihre Prüfungsunterlagen verwehrt wird, im Widerspruch zu den Bestimmungen der Artikel 12 und 13 der Richtlinie 95/46/EG, die durch das Gesetz 2472/1997 in griechisches Recht umgesetzt worden ist, sowie im Widerspruch zu den einschlägigen Bestimmungen des oben genannten Gesetzes stehen. Ferner besteht auch ein Widerspruch zu den Artikeln 2 Absatz 1, 5 Absatz 1, 9A, 10, 25, 26, 28, 101A, 120, 4 und 20

der Verfassung. Daher muss das Ministerium für Unterricht und Kultus den Bewerbern Zugriff auf ihre Prüfungsunterlagen gewähren und ihnen Fotokopien dieser Unterlagen aushändigen, damit die Datensubjekte überprüfen können, ob die gesetzlichen Bestimmungen für die ordnungsgemäße Verarbeitung ihrer personenbezogenen Daten eingehalten worden sind. Die Bewerber können ihr Zugriffsrecht zu jedem beliebigen Zeitpunkt innerhalb des für die Aufbewahrung dieser Prüfungsunterlagen vorgeschriebenen Zeitraums ausüben.

C. Wichtige spezifische Themen

Die Datenschutzbehörde entwickelt derzeit ihr neues Informationssystem, das nicht nur die Back-Office-Funktionen für interne Benutzer verbessern, sondern zugleich ein neues Portal mit E-Government-Funktionen für die Bürger bieten wird. Zu den E-Government-Funktionen werden unter anderem die Online-Einreichung von Beschwerden und Fragen sowie von Meldungen über Datenverarbeitungen, ein elektronisches Verzeichnis aller für die Datenverarbeitung Verantwortlichen sowie erweiterte Suchfunktionen zu Datenschutzfragen zählen. Bürger und für die Datenverarbeitung Verantwortliche können den Fortschritt ihrer Fälle online nachverfolgen. Das neue Informationssystem wird voraussichtlich Mitte 2007 in Betrieb gehen. Ferner hat die Datenschutzbehörde eine neue Telefonzentrale eingerichtet, um ihren Helpdesk-Aufgaben besser nachkommen zu können. Abschließend ist festzuhalten, dass das Informationssystem der Datenschutzbehörde an das allgemeine Netz der griechischen Regierungsstellen und Behörden SIZEFXIS angeschlossen worden ist.

Ungarn

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

Richtlinie 95/46/EG

Keine nennenswerten Entwicklungen.

Richtlinie 2002/58/EG

Die am 15. März 2006 im Rahmen der europäischen Initiativen zur Bekämpfung des Terrorismus und der organisierten Kriminalität verabschiedete Richtlinie bezweckt die Harmonisierung der Verpflichtungen von Dienstanbietern hinsichtlich der Speicherung bestimmter Verkehrsdaten, um zu gewährleisten, dass diese Daten für die Untersuchung, Ermittlung und Verfolgung von schweren Straftaten im Sinne der Gesetze der einzelnen Mitgliedstaaten zur Verfügung stehen. Die Richtlinie bezieht sich allerdings nur auf Verkehrsdaten und Ortungsdaten, die bei der Kommunikation bzw. durch den Kommunikationsdienst erzeugt oder verarbeitet werden, nicht jedoch auf die eigentlichen Inhalte der übermittelten Informationen. Der vorgeschriebene Zeitraum für diese Vorratsdatenspeicherung kann sich auf sechs Monate bis zwei Jahre erstrecken. Anschließend müssen die Daten gelöscht werden.

Was die weiteren Bestimmungen der Richtlinie anbelangt, wurde ein Ministerialerlass zur einheitlichen europäischen Notrufnummer 112 entworfen, um die gesetzlichen Grundlagen zur Erfüllung der erforderlichen technischen Anforderungen zu schaffen. Die Änderung des Gesetzes über elektronische Kommunikation im Sinne der durch die Richtlinie angestrebten Harmonisierung wurde in diesem Jahr in Angriff genommen. Damit sollen die geeigneten Gesetzes- und Zulassungsgrundlagen für den oben genannten Ministerialerlass geschaffen werden.

B. Bedeutende Rechtsprechung

Seit der 2004 erfolgten Änderung des Gesetzes LXIII von 1992 über den Schutz von personenbezogenen Daten und den öffentlichen Zugang zu Daten von öffentlichem Interesse ist der Datenschutzbeauftragte befugt, bindende Entscheidungen zu treffen, gegen welche der für die Datenverarbeitung Verantwortliche klagen kann. Im Jahr 2004 wurde eine Untersuchung zur Zulässigkeit der Datenverarbeitung in einer Sendereihe des ungarischen TV-Senders RTL Klub eingeleitet, in der jeweils zwei Familien die Mütter tauschten. Im Rahmen des zwischen den Datensubjekten und dem TV-Sender geschlossenen Vertrags erklärten die Datensubjekte ihr Einverständnis mit der Datenverarbeitung einschließlich der Datenübermittlung an namentlich nicht genannte Untervertragsnehmer und ohne jede zeitliche oder räumliche Einschränkung. Die untersuchte Frage lautete, ob eine derartige unbeschränkte Einwilligung rechtskonform ist. Im Rahmen der Vertragserfüllung wurden auch personenbezogene Daten von Minderjährigen verarbeitet. Die Einwilligung der Eltern in ihrer Funktion als Erziehungsberechtigte ist in dieser Hinsicht jedoch nicht als ausreichende rechtliche Grundlage anzusehen. Daher wurde der TV-Sender aufgefordert, seine gesetzwidrige Datenverarbeitung zu unterlassen. Der TV-Sender klagte gegen diese Stellungnahme des Datenschutzbeauftragten und forderte ihre Änderung. Das Datenschutzgesetz bietet nämlich die Möglichkeit, gegen Entscheidungen des Datenschutzbeauftragten, mit denen dieser die Unterlassung von Datenverarbeitungen vorschreibt, zu klagen. Es lag jedoch gar keine derartige Entscheidung vor. Das Amtsgericht schloss sich diesem Argument an und wies die Klage ab.

Auch die ungarische Scientology-Kirche klagte gegen den Datenschutzbeauftragten. Grund war die Veröffentlichung einer Empfehlung an die Scientology-Kirche, in der diese aufgefordert wurde, auf die Einhaltung der Datenschutzanforderungen

zu achten, insbesondere durch eine angemessene Information der Datensubjekte im Rahmen von deren religiösen Aktivitäten. Die Empfehlung bezog sich auch auf das Sachverständigengutachten der Abteilung Strafsachen bei der Nationalen Ermittlungsbehörde (*Nemzeti Nyomozó Iroda* - NNI), das im Zusammenhang mit der Anwendung/Zulässigkeit eines so genannten „E-Meters" (eines Geräts in der Art eines so genannten Lügendetektors) durch die Scientology-Kirche erstellt worden war. Die Scientology-Kirche forderte vom Datenschutzbeauftragten die Veröffentlichung dieses Gutachtens. Da der Datenschutzbeauftragte seine eigene Untersuchung jedoch noch nicht abgeschlossen hatte, veröffentlichte er das Dokument nicht. Die Scientology-Kirche erhob daher Klage und verwies dabei auf die gesetzlichen Bestimmungen zur Informationsfreiheit, insbesondere auf das Zugangsrecht zu Daten von öffentlichem Interesse. Die Klage wurde später abgewiesen, weil der Scientology-Kirche im Laufe des Verfahrens das gewünschte Gutachten zugeleitet wurde, so dass der Klagegrund entfiel.

C. Wichtige spezifische Themen

Die Unruhen infolge der politischen Krise in Ungarn und die daraus entstandenen Datenverarbeitungsfragen warfen im Oktober 2006 eine Reihe von Problemen auf, von denen drei im Folgenden erörtert werden sollen.

Es wurde eine Untersuchung im Zusammenhang mit an die Krankenhäuser gerichteten brieflichen Aufforderungen der Polizei zur Mitteilung von personenbezogenen Daten von „Menschen, die im Verlauf der Unruhen verletzt wurden", eingeleitet. Der Datenschutzbeauftragte befand, dass dieser Brief der Polizei weder die vorgeschriebenen formalen noch gesetzlichen Voraussetzungen erfüllte, so dass eine Datenweitergabe seitens der Krankenhäuser einen Verstoß gegen das verfassungsmäßig garantierte Recht der Patienten auf den Schutz ihrer personenbezogenen und spezifischen Daten darstellen würde. In ihrer Antwort nannte die Polizei die Straftat, zu deren Untersuchung das Verfahren eingeleitet worden war, sowie die gesetzlichen Grundlagen für die allgemeine und die spezifisch verlangte Weitergabe von Daten. In diesem Zusammenhang muss betont werden, dass spezifische Daten im Rahmen einer Strafermittlung nur für spezifische Zwecke verarbeitet werden dürfen. Im zweiten Brief wurde als Zweck „Datenverarbeitung im Rahmen einer Strafermittlung" genannt, was jedoch eine zu weit gefasste Zweckbestimmung darstellt. Die Anforderung erfüllte auch das Prinzip der Erhebung möglichst weniger Daten nicht. Die angegebene Zeitspanne war zu weit gefasst und der Patiententyp wurde nicht angegeben, so dass auch Daten von Patienten ohne Verbindungen zu Straftaten an die Polizei weitergegeben worden wären. Der Datenschutzbeauftragte informierte die Krankenhausleiter, dass die dritte und letzte Fassung des Briefs der Polizei als angemessen zu betrachten war.

Eine weitere Untersuchung betraf ebenfalls die Datenverarbeitung seitens der Polizei: Bei der Datenschutzbehörde gingen Beschwerden ein, dass Datensubjekte trotz entsprechender Anträge keinen Zugriff auf die Aufzeichnungen von Überwachungskameras erhalten, die von der Polizei und anderen Strafverfolgungsbehörden betrieben werden. Auch als die Datensubjekte argumentierten, dass die Überwachungskameras gar nicht innerhalb der betreffenden Einrichtungen betrieben werden, blieb ihnen der Zugriff verwehrt. Die Datensubjekte hatten beabsichtigt, die Aufzeichnungen für Verfahren gegen die Polizei zu nutzen, in denen sie sich auf das Recht auf informationelle Selbstbestimmung berufen wollten. Im Rahmen der Untersuchung gelang keiner der beiden Seiten eine stichhaltige Argumentation, weil die gesetzlichen Regelungen zu Videoüberwachungssystemen zu viele Lücken aufweisen. Daher wird 2007 eine Untersuchung von Amts wegen eingeleitet werden, um die Zulässigkeit und den Rechtsrahmen für Videoüberwachungssysteme in Ungarn zu klären.

Der Fall zur Veröffentlichung von Daten auf der rechtsextremen Website www.kuruc.info stieß auf

reges Medieninteresse. Auf dieser Website wurden die Namen, Adressen, Festnetz- und Mobiltelefonnummern von Richtern und Staatsanwälten veröffentlicht. Die Namen, Positionen und Arbeitsorte von Richtern und Staatsanwälten sind allgemein bekannt, die übrigen Daten sind dagegen als personenbezogen zu betrachten. Somit fehlt die gesetzliche Grundlage für eine Veröffentlichung, so dass eine Veröffentlichung nur unter der Bedingung zulässig gewesen wäre, dass die Datensubjekte vorab eingewilligt hätten. An der Gesetzwidrigkeit der Veröffentlichung ändert auch der Umstand nichts, dass ein Teil dieser Daten möglicherweise bereits öffentlich zugänglich war – etwa in einem Telefonbuch oder auf der Website einer Tierschutzvereinigung. Im zuletzt genannten Fall – der öffentlichen Zugänglichkeit auf der Website einer Tierschutzvereinigung – besteht kein Zusammenhang mit der Tätigkeit der betreffenden Person als Richter oder Staatsanwalt. Eine erneute Veröffentlichung derartiger Daten ist jedoch nur zu Zwecken zulässig, die mit der ursprünglichen Absicht identisch oder zumindest vereinbar sind. Der Zweck der Datenveröffentlichung auf der Website www.kuruc.info ist jedoch eindeutig abweichend. Daher ist diese Datenveröffentlichung als gesetzwidrig zu betrachten. Das Problem wurde noch komplexer, als sich herausstellte, dass die Website gar nicht auf einem ungarischen Server betrieben wurde, sondern dass das Impressum diesbezüglich falsche Angaben enthielt.

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 2006 gab es in der Gesetzgebung keine Entwicklungen mit nennenswerten Auswirkungen auf den Datenschutz.

B. Bedeutende Rechtsprechung

Die Datenschutzbehörde erließ einen Zwangsbescheid gegen eine medizinische Einrichtung, die einem Zugriffsantrag auf die Patientenakte eines Kindes nicht nachgekommen war. Die medizinische Einrichtung klagte gegen den Zwangsbescheid. Die gerichtliche Anhörung wurde auf Dezember 2006 festgesetzt. Bei der gerichtlichen Anhörung zog die medizinische Einrichtung ihre Klage zurück und erklärte sich zur Herausgabe der gewünschten personenbezogenen Daten bereit.

Der Datenschutzbeauftragte traf eine Reihe von weiteren Einzelentscheidungen zu Beschwerden, die aufgrund der Datenschutzgesetze eingereicht wurden. Gegen keine dieser Entscheidungen wurde geklagt. Die wesentlichsten darunter waren:

- Eine bekannte irische Unterhaltungskünstlerin legte beim Datenschutzbeauftragten Beschwerde gegen eine Zeitung ein, die ein Foto von ihr und ihrem Kind samt einem Kommentar zur Beziehung zwischen den beiden veröffentlicht hatte. Nach Ansicht des Datensubjekts wurden die Daten weder rechtmäßig erhoben noch verarbeitet. Die vorrangige Frage, die es in diesem Fall zu entscheiden galt, war, ob die Presse- und Meinungsfreiheit, die in Artikel 9 der Richtlinie 95/46/EG (bzw. in Paragraf 22A der beiden in Umsetzung der Richtlinie erlassenen irischen Datenschutzgesetze) ausdrücklich als Ausnahme angeführt ist, auf die Veröffentlichung des Fotos und des Texts über das Datensubjekt und dessen Tochter anwendbar ist. Bei seiner Entscheidung stützte sich der Datenschutzbeauftragte auf die Artikel 8 und 10 der Europäischen Menschenrechtskonvention (EMRK) (Recht auf Achtung des Privat- und Familienlebens bzw. Freiheit der Meinungsäußerung), auf Leitlinien des Europäischen Gerichtshofs für Menschenrechte zur relativen Gewichtung dieser beiden Rechte, auf einschlägige Verhaltenskodizes sowie auf frühere Entscheidungen des Datenschutzbeauftragten, in denen die Bedeutung der elterlichen Einwilligung sowie des Schutzes von Minderjährigen bei der Veröffentlichung von Fotos von Kindern und Jugendlichen betont wird. In seiner Entscheidung befand der Datenschutzbeauftragte, dass die Veröffentlichung des Fotos und des Textes über das Datensubjekt und dessen Tochter sowie über deren Beziehung nicht durch öffentliches Interesse gerechtfertigt werden kann und dass diese personenbezogenen Daten über das Datensubjekt und dessen Tochter weder rechtmäßig erhoben noch verarbeitet wurden.

- Ein Datensubjekt, das eine unerbetene Direktmarketing-Nachricht von einem Telekommunikationsunternehmen erhalten hatte, legte beim Datenschutzbeauftragten Beschwerde hinsichtlich des Weges ein, auf dem sich der Absender seine Mobilfunknummer verschafft hatte: Es wurden nämlich die Besucher eines Konzerts eingeladen, Texte zur Unterstützung der Armutsbekämpfung zu verfassen. Ihre Mobilfunknummern wurden in einer Datenbank gespeichert, um sie später zu Direktmarketing-Zwecken einzusetzen. Der Datenschutzbeauftragte befand, dass ein Verstoß gegen die Datenschutzgesetze vorlag, da die Daten für einen spezifischen Zweck gesammelt und dann für einen anderen Zweck verwendet wurden. Im Anschluss an die Entscheidung weigerte sich das Telekommunikationsunternehmen zunächst, die Datenbank zu löschen. Daraufhin erließ der Datenschutzbeauftragte einen entsprechenden Zwangsbescheid.

C. Wichtige spezifische Themen

Hypothekenmakler

Durch einen Bericht in den Medien wurde der Datenschutzbeauftragte auf eine Reihe schwerwiegender Anschuldigungen aufmerksam, dass in der Interaktion zwischen Hypothekenmaklern und Immobilienmaklern gegen die Datenschutzgesetze verstoßen worden sei. Kern der Anschuldigungen war, dass Hypothekenmakler an Immobilienversteigerer sensible personenbezogene Daten weitergegeben hätten, wie etwa Jahreseinkommen, finanzielle Unterstützung seitens der Eltern, Geldanlagen usw. Der Datenschutzbeauftragte lud Vertreter der Berufsverbände der Hypothekenmakler sowie die Finanzaufsichtsbehörde ein, um den Problemkreis gemeinsam zu erörtern und Abhilfe zu suchen. Der Datenschutzbeauftragte veranlasste ferner eine Reihe von stichprobenartigen Vor-Ort-Inspektionen bei Hypothekenmaklern und Immobilienmaklern. Im Laufe dieser Inspektionen stellte der Datenschutzbeauftragte fest, dass sich viele Hypothekenmakler nicht über das Ausmaß ihrer Verantwortung im Rahmen der irischen Datenschutzgesetze im Klaren sind. Im Anschluss an die Inspektionen übersandte der Datenschutzbeauftragte sämtlichen 1.633 bei der Finanzaufsichtsbehörde registrierten Hypothekenmaklern Leitlinien und ein Informationsheft zum Datenschutz. In den Leitlinien wurde besonders betont, dass personenbezogene Daten von Kunden nur in einer Weise verwendet und weitergegeben werden dürfen, die mit dem Zweck vereinbar ist, zu dem sie der Kunde mitgeteilt hat. Dieser laufende Einsatz und das enge Zusammenwirken mit dem Hypothekenbereich haben zu zahlreichen positiven Überarbeitungen von Verfahren und Verhaltenskodizes im Sinne einer verbesserten Wahrung der Vertraulichkeit von Kundendaten geführt. Die stichprobenartigen Inspektionen bei Hypothekenmaklern werden dessen ungeachtet während des gesamten Jahres 2007 fortgeführt.

Italien

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

- Durch das Gesetz Nr. 38/2006 wurde das Nationale Zentrum zur Bekämpfung von Kinderpornografie im Internet (*Centro Nazionale per il Contrasto alla Pedopornografia Online* - CNPO) eingerichtet. Seine Aufgabe besteht in der zentralen Sammlung der seitens der Polizeikräfte erstellten Berichte über Websites, die Materialien im Zusammenhang mit der sexuellen Ausbeutung von Kindern verbreiten. Ferner soll das Zentrum ein Register derartiger Websites sowie ihrer Betreiber und Zahlungsempfänger führen. Außerdem sammelt das Zentrum Meldungen von Dienstanbietern für elektronische Kommunikation über Verträge mit Unternehmen und/oder sonstigen juristischen oder natürlichen Personen, die derartige Materialien verbreiten oder damit handeln. Kürzlich veröffentlichte der Kommunikationsminister in Abstimmung mit dem Minister für Reformen und Innovationen in der öffentlichen Verwaltung und nach Rücksprache mit dem Datenschutzbeauftragten *(Garante)* einen Erlass zur Festlegung der technischen Maßnahmen, die Anbieter von Internetverbindungen treffen müssen, um den Zugriff auf kinderpornografische Websites zu unterbinden.

- Gesetz Nr. 281/2006 legt Maßnahmen zur Zerstörung von Materialien fest, die durch gesetzwidrige Abhöraktivitäten sowie Rasterfahndungen gewonnen wurden. Derartige Materialien dürfen in Gerichtsverfahren nicht verwendet werden und müssen unter der Verantwortung des zuständigen Staatsanwalts als vertrauliche Informationen an einem sicheren Ort aufbewahrt werden, bis der betreffende Richter nach einer entsprechenden Prüfung ihre Zerstörung anordnet. Damit soll verhindert werden, dass unbefugte Personen in den Besitz der Materialien gelangen. Das Gesetz schmälert in keiner Weise die Befugnisse des Datenschutzbeauftragten, eine gesetzwidrige Verbreitung von Daten und/oder Dokumenten festzustellen und zu unterbinden sowie ggf. entsprechende Sanktionen anzuordnen, auch im Hinblick auf das Recht der Datensubjekte auf Zugriff und/oder Berichtigung von Daten.

- Mit dem Haushaltsgesetz 2007 (Gesetz Nr. 296/2006, Paragraf 542) wurde eine Aufstockung des permanenten Mitarbeiterstabs des Datenschutzbeauftragten *(Garante)* genehmigt, damit die Datenschutzbehörde *(Ufficio del Garante per la protezione dei dati personali)* ihre Aufgaben, insbesondere ihre Überwachungs- und Kontrollfunktionen, besser wahrnehmen kann. Der Datenschutzbeauftragte wurde bevollmächtigt, seinen Mitarbeiterstab um maximal 25% der im Datenschutzgesetz niedergelegten Gesamtbelegschaftsstärke aufzustocken, wobei dies schrittweise über die nächsten drei Jahre zu erfolgen hat (Budgeterhöhung um € 21.846.000 für 2007, um € 21.591.000 für 2008 und um € 21.986.000 für 2009).

- **Parlamentarische Anhörungen:** Der Datenschutzbeauftragte trat im Jahresverlauf 2006 mehrmals bei Anhörungen zu wichtigen Fragen auf, die durch die zuständigen Parlamentsausschüsse erörtert wurden. Hier sind insbesondere zu nennen: technologische Innovationen in der öffentlichen Verwaltung und die Auswirkung dieser Innovationen auf den Schutz der Privatsphäre, im Hinblick auf die Gewährleistung des Zutrauens der Bevölkerung zu den Behörden und öffentlichen Einrichtungen. Außerdem leistete der Datenschutzbeauftragte seinen Beitrag zur parlamentarischen Untersuchung von Fragen der Telefonüberwachung, d. h. hinsichtlich der Einhaltung von Sicherheitsvorkehrungen durch die Justizbehörden und die Telefongesellschaften sowie hinsichtlich der Veröffentlichung des Inhalts von gesetzeskonformen (d. h. zulässigen) Telefonabhörmaßnahmen. Ferner ist zu verweisen auf die Anhörung über die Sicherheitsvorkehrungen für den Datenschutz, welche der Datenschutzbeauftragte im Zusammenhang mit den neuen gesetzlichen Bestimmungen zur Bekämpfung der

Steuerhinterziehung gefordert hatte – insbesondere was die Verknüpfung unterschiedlicher Datenbanken anbelangt.

- **Stellungnahmen:** Gemäß Paragraf 154(4) des Datenschutzgesetzes müssen der Premierminister und jeder Minister beim Entwerfen von Verordnungen und Verwaltungsvorschriften, die Auswirkungen auf den Datenschutz haben könnten, Rücksprache mit dem Datenschutzbeauftragten halten. In diesem Rahmen gab der Datenschutzbeauftragte im Jahresverlauf 2006 eine ganze Reihe von Stellungnahmen zu wichtigen Themen ab. Hier sind insbesondere zu nennen: medizinische Zwangsuntersuchungen bei Nicht-Drogensüchtigen, elektronische Verknüpfung von Informationssystemen und automatisierten Archiven der Ausländerbehörden, Zugriff auf Verwaltungsdokumente, Erfassung und Speicherung von Daten im nationalen Register der zugelassenen Einrichtungen für Reproduktivmedizin, Verwaltung der Daten von Telefonkunden im Zusammenhang mit Aktivitäten, die unter die Zuständigkeit des Innenministeriums fallen, sowie Verhinderung von Bank- und Scheckkartenbetrug.

B. Bedeutende Rechtsprechung

Verwendung von Verkehrsüberwachungsdaten für abweichende Zwecke: Der Verfassungsgerichtshof entschied mit seinem Urteil Nr. 372 vom 6. November 2006, dass das in Paragraf 132 des Datenschutzgesetzes niedergelegte Verbot, nach Ablauf des für die Speicherung festgelegten Zeitraums (von beispielsweise 24 Monaten) Verkehrsüberwachungsdaten für andere abweichende Zwecke als die Bekämpfung des organisierten Verbrechens und des Terrorismus zu verwenden, nicht gegen die Verfassung verstößt.

Mobiltelefone mit Kamera: Der Kassationsgerichtshof entschied mit seinem Urteil Nr. 10444 vom 5. Dezember 2005, dass es einen gesetzwidrigen Eingriff in die Privatsphäre einer Person darstellt, wenn eine andere Person ohne die Einwilligung des genannten Datensubjekts und/oder ohne Kenntnisnahme durch das genannte Datensubjekt Bilder mit einem Mobiltelefon mit Kamera aufnimmt, wobei dies auch für ein derartiges Verhalten am Arbeitsplatz gilt. Nach Ansicht des Gerichts bezieht sich Paragraf 615 bis des Strafgesetzbuchs auf gesetzwidrige Eingriffe in die Privatsphäre einer anderen Person durch technische Vorrichtungen, welche diese Verletzung der Privatsphäre auch noch reproduzieren können, indem Dritten dadurch Aufnahmen zugänglich gemacht werden können, die nicht für sie bestimmt sind.

Rechtsprechung in Datenschutzfällen: Der Kassationsgerichtshof entschied mit seinem Urteil Nr. 12980 vom 10. April 2006, dass der Gerichtsstand am Sitz des für die Datenverarbeitung Verantwortlichen liegt. Dies bedeutet, dass hier andere Regeln gelten als beim Gerichtsstand in Verbraucherschutzfällen (niedergelegt in den Paragrafen 1469 bis, Absatz 3, Satz 19 des Bürgerlichen Gesetzbuchs), was insbesondere für Klagen auf Schadenersatz relevant ist. Das Gericht betonte, dass der durch das Datenschutzgesetz gewährte Schutz für die Datensubjekte auf einer anderen rechtlichen Konstellation beruht als der Verbraucherschutz, denn Verbraucher stehen zum Verkäufer bzw. Leistungserbringer in einer Vertragsbeziehung. Daraus lässt sich nach Ansicht des Gerichts ableiten, dass in Datenschutzfällen der Gerichtsstand möglichst nahe bei jenem Ort liegen muss, an dem die tatsächliche Verarbeitung und Verbreitung der Daten erfolgt.

Arbeitsrecht: In einem Urteil vom 13. September 2006 entschied die Abteilung Arbeitsrecht beim Kassationsgerichtshof, dass die Entlassung eines Beschäftigten rechtmäßig ist, wenn Dritte mit Hilfe des persönlichen Kennworts dieses Beschäftigten ins Firmennetzwerk eindringen konnten.

Zugriff auf öffentliche Unterlagen der öffentlichen Verwaltung vs. Datenschutz: In einem Urteil vom 21. Februar 2006 entschied der Staatsrat – bei dem die höchstrichterliche Gewalt in Verwaltungssachen liegt –, dass eine öffentliche Verwaltungsbehörde gesetzwidrig handelte, als sie einem Teilnehmer an einer öffentlichen Ausschreibung zwar Einblick in Unterlagen zur genannten Ausschreibung gewährte,

es ihm jedoch unter Verweis auf den Datenschutz verwehrte, Fotokopien anzufertigen.

Zum gleichen Thema äußerte sich der Staatsrat in einer Entscheidung vom 7. Juni 2006 über die Wahrung des Gleichgewichts zwischen dem Zugriff auf Unterlagen der öffentlichen Verwaltung und dem Datenschutz im Rahmen von Ausschreibungsverfahren. Insbesondere befand der Staatsrat, dass dem Ausschreibungsteilnehmer auf jeden Fall ein Zugriffsrecht auf die entsprechenden öffentlichen Unterlagen zusteht, ungeachtet der Frage, ob sonstige Rechte des Ausschreibungsteilnehmers verletzt worden sind und/oder ob er ein begründetes Interesse für den Zugriff nachweisen kann, denn Sinn und Zweck des Zugriffsrechts ist die Gewährleistung der Transparenz bei den Ausschreibungen der öffentlichen Hand.

C. Wichtige spezifische Themen

Datenbanken für die Strafverfolgung

Zu den wichtigsten Tätigkeitsbereichen für den italienischen Datenschutzbeauftragten zählten Datenbanken, die von Polizeibehörden zu Präventions- und Sicherheitszwecken eingerichtet wurden. Insbesondere galt das Augenmerk dem so genannten „Gemeinsamen Polizeidatensystem", das bei der Abteilung für öffentliche Sicherheit im Innenministerium eingerichtet wurde. Diese Datenbank wurde aufgrund eines entsprechenden Gesetzes eingerichtet und wird von den verschiedenen italienischen Polizeibehörden gemeinsam betrieben.

Der Umfang dieser Datenbank, die Art der darin enthaltenen Daten sowie die große Anzahl der Beschäftigten, die gesetzlich befugt sind, zu Präventions- und/oder Ermittlungszwecken auf die Daten zuzugreifen, verleihen dieser Datenbank eine große landesweite Bedeutung.

Die Datenschutzbehörde wies die Abteilung für öffentliche Sicherheit im Innenministerium an, geeignete organisatorische und technische Maßnahmen und Sicherheitsvorkehrungen zu ergreifen, um die Sicherheitsstufen zu erhöhen, auch im Hinblick auf die Verknüpfung mit Datenbanken, die unter der Kontrolle anderer öffentlicher oder privater Einrichtungen stehen. Die wichtigsten derartigen Maßnahmen sind:

- Verschlüsselung bei bestimmten Dateisystemen
- Authentifizierungs- und Autorisierungsverfahren, für welche starke Authentifizierungsinstrumente umgesetzt werden müssen, einschließlich der möglichen Verwendung biometrischer Daten
- Sicherheitsaudits
- Zugriffs- und Betriebsprotokollierung mit höchster Integrität und Zuverlässigkeit (zertifizierte Protokollierungssysteme)
- digitale Zertifizierung der Workstations im Hinblick auf Bestandsverwaltung und Sicherheit
- Ernennung eines internen Datenschutzbeauftragten, der für die IT-Sicherheitsfunktionen der Datenbank sowie für die Beziehungen zur italienischen Datenschutzbehörde zuständig ist.

Es handelt sich um die erste Stufe einer von der Datenschutzbehörde in Angriff genommenen Untersuchung. Folgen sollen detaillierte Analysen der einzuführenden Maßnahmen, auch im Hinblick auf Verhältnismäßigkeit, Zweckbindung usw.

Ferner forderte der Datenschutzbeauftragte eine umfassende Auflistung aller durch die Strafverfolgungsbehörden durchgeführten Datenverarbeitungsoperationen, so wie es das Datenschutzgesetz vorschreibt, um effektive Inspektionen und Kontrollen durchführen zu können. Derzeit erfolgt eine solche Meldung nur für das genannte „Gemeinsame Polizeidatensystem".

Zu verweisen ist ferner auf die im Jahresverlauf 2006 eingeleiteten – und teilweise noch andauernden – Untersuchungen hinsichtlich der in die nationalen Bereiche des Schengener Informationssystems (SIS) eingetragenen Meldungen von verdeckten Überwachungen. Mit diesen Untersuchungen sollte insbesondere die Einhaltung der im Schengener Durchführungsübereinkommen niedergelegten Datenschutzanforderungen hinsichtlich Datenqualität

und Richtigkeit der Angaben überprüft werden. Der Datenschutzbeauftragte leitete auch eine Untersuchung zu den für die EURODAC-Datenbank eingerichteten Mechanismen ein, unter besonderer Berücksichtigung der Rechtmäßigkeit der Verarbeitung und der Angemessenheit der umgesetzten Sicherheitsmaßnahmen.

Als Reaktion auf einen bei der Datenschutzbehörde eingegangenen Bericht entschied der Datenschutzbeauftragte, Vorinformationen zu sammeln, zur Vorbereitung einer unter anderem durch Vor-Ort-Inspektionen durchzuführenden Beurteilung der seitens einer Sondereinheit der Carabinieri durchgeführten Datenverarbeitung. Diese Sondereinheit hatte dem Bericht zufolge eine Datenbank mit an Tatorten erhobenen genetischen Daten eingerichtet, um diese für Strafermittlungen zu verwenden.

Ferner widmete sich der Datenschutzbeauftragte im Jahresverlauf 2006 den Sicherheitsvorkehrungen bei der Verarbeitung personenbezogener Daten durch Justizbehörden und deren Geschäftsstellen. Dies erfolgte im Zusammenwirken mit den betreffenden Justizbehörden. Um die Einhaltung der einschlägigen Sicherheitsanforderungen zu überprüfen, ordnete der Datenschutzbeauftragte Vor-Ort-Untersuchungen in einigen Geschäftsstellen der Justizbehörden an.

Sicherheit bei Telefongesprächen und in der elektronischen Kommunikation

Im abgelaufenen Jahr führte der Datenschutzbeauftragte detaillierte Kontrollen der Verarbeitung von Verkehrsdaten sowie bestimmter Sicherheitsvorkehrungen im Zusammenhang mit Telefongesprächen und mit der elektronischen Kommunikation durch.

Die Verarbeitung von Verkehrsdaten fand in der Öffentlichkeit ein zunehmend prominentes Interesse, besonders da Medienberichte über mehrere gerichtliche Untersuchungen zur gesetzwidrigen Verarbeitung von Telefonverbindungsdaten für Unruhe gesorgt hatten.

Als Reaktion auf die eingegangene Beschwerde eines Bürgers über die mutmaßlich gesetzwidrige Offenlegung seiner Telefonverbindungsdaten wies der Datenschutzbeauftragte die größte italienische Telefongesellschaft an, spezifische Maßnahmen und Sicherheitsvorkehrungen zur Steigerung des Sicherheitsniveaus zu ergreifen. Der Schwerpunkt dieser Maßnahmen lag auf den Autorisierungsverfahren und auf der Auditfähigkeit der IT-Systeme, die sich im Hinblick auf technische Mitarbeiter mit hochrangigen Zugriffsrechten – wie etwa Systemadministratoren und Datenbankadministratoren – als besonders unzureichend erwiesen hatten.

Der Datenschutzbeauftragte leitete auch eine detaillierte Untersuchung der seitens der maßgeblichen Telefongesellschaften eingerichteten Systeme ein, um sich ein umfassendes Bild verschaffen und wirksame Maßnahmen festlegen zu können, die – gemäß Paragraf 132 des Datenschutzgesetzes – bei der Vorratsspeicherung von Telefonverbindungsdaten und elektronischen Verkehrsdaten eingehalten werden müssen, da derartige Daten einzig und allein für Strafermittlungszwecke verwendet werden dürfen.

Ferner ergriff der Datenschutzbeauftragte Schritte zur Stärkung von Sicherheitsvorkehrungen in Telefonsystemen, um die seitens der Telefongesellschaften im Rahmen von rechtmäßigen Telefonabhörmaßnahmen gesammelten Daten sowie sonstige bei der Zusammenarbeit mit den Strafverfolgungsbehörden erhobene Daten wirksam zu schützen. Insbesondere zielte die Datenschutzbehörde damit darauf ab, dass der Datenaustausch zwischen Telefongesellschaften und Justizbehörden über gesicherte Kommunikationswege erfolgt (bzw. über Kanäle, die durch den Einsatz von IT-Technologien spezifisch gesichert werden). Daher untersagte die Datenschutzbehörde auch jedwede Übermittlung von Klartext über nicht-gesicherte Kanäle und verpflichtete die Telefongesellschaften, ausschließlich E-Mails mit qualifizierten digitalen Signaturen und/oder gesicherte webbasierte Dienste mit SSL-Verschlüsselungsprotokollen und starken Authentifizierungsverfahren zu verwenden.

Was die umfassendere Frage der Sicherheit in der elektronischen Kommunikation anbelangt, so leitete der Datenschutzbeauftragte einen Meinungsaustausch und in Kooperation durchgeführte Aktivitäten mit anderen Behörden und öffentlichen Einrichtungen ein, die für spezifische Aufgaben in diesem Bereich zuständig sind.

Datenschutz und Internet-Suchmaschinen

Der Datenschutzbeauftragte ergriff Schritte, die es Datensubjekten ermöglichen sollen, ihr Recht auf die Richtigstellung von sie betreffenden Daten auf Webseiten durchzusetzen, einschließlich der Aktualisierung von Daten, die durch Internet-Suchmaschinen gefunden werden, ausgehend vom Grundsatz, dass jede Person das Recht auf eine zutreffende Darstellung im Internet hat, ungeachtet des Speicherorts der betreffenden Daten. Zu diesem Zweck richtete der Datenschutzbeauftragte ein Schreiben an die im US-Bundesstaat Kalifornien befindliche Konzernzentrale von Google, denn dort ist auch der Standort der Server für die Suchmaschine. Das Unternehmen wurde aufgefordert, Lösungen zu entwickeln, die das hartnäckige Verbleiben veralteter und/oder unzutreffender personenbezogener Daten im Internet unterbinden, nachdem die betreffenden Informationen auf den Quell-Websites, von denen die Extraktion erfolgt ist, längst berichtigt worden sind. Diese Initiative erfolgte als Reaktion auf die eingegangene Beschwerde einer Bürgerin, die festgestellt hatte, dass Informationen zu einem gegen sie eingeleiteten Ermittlungsverfahren nach wie vor über die Suchmaschine von Google auffindbar waren, obwohl sie inzwischen in sämtlichen Punkten für unschuldig befunden worden war. Die technische Ursache dafür sind die zahlreichen Cache-Kopien und die verschiedenen durch die Suchmaschine erzeugten Kurzfassungen. Dies führte zu einer verzerrten Darstellung der Situation der genannten Bürgerin, während auf den Quell-Websites längst zutreffende Angaben zu lesen waren. Obwohl Google einen Mechanismus aufweist, der es einer Website ermöglicht, veraltete Verknüpfungen und/oder nicht-existerende URLs zu löschen, ist dies nicht ausreichend, um das so genannte „Recht auf Vergessen" angemessen zu gewährleisten. Google Inc. wurde auch aufgefordert, auf der Website www.google.it einen deutlicheren Hinweis zu platzieren, der den Benutzern erläutert, dass der für die Datenverarbeitung durch die Suchmaschine Verantwortliche ein Unternehmen mit Sitz in den USA ist, und der den Benutzern detailliert darlegt, welche Schritte sie ergreifen müssen, um eine rasche Löschung oder Aktualisierung von Webseiten zu erreichen, sobald die betreffenden Seiten auf den Quell-Websites geändert worden sind. In der Folge fand am Sitz des Datenschutzbeauftragten ein Treffen mit Vertretern von Google Inc. statt, das den Beginn eines fruchtbaren Dialogs markierte.

Förmliche Beschwerden

Im Jahr 2006 wurde über 435 förmliche Beschwerden entschieden. Die meisten Beschwerden betrafen Verarbeitungsoperationen durch Banken, Finanzunternehmen und private Kreditsicherungsgesellschaften. Einige der Fälle erstreckten sich jedoch auf neue Bereiche und zogen besondere Aufmerksamkeit auf sich. Dies gilt insbesondere für folgende Fälle:

- In zwei Fällen ging es um die Überwachung von Beschäftigten in der Privatwirtschaft, nämlich um auf einem Firmencomputer gespeicherte personenbezogene Daten sowie um die detaillierte Überwachung der Internetnutzung. In beiden Fällen befand der Datenschutzbeauftragte die seitens der Arbeitgeber durchgeführte Verarbeitung für gesetzwidrig, da die Beschäftigten nicht im Voraus informiert worden waren, dass eine derartige Überwachung stattfinden würde, und auch weil die betreffende Datenverarbeitung im Hinblick auf den angestrebten Zweck (nämlich die Gewährleistung der ordnungsgemäßen Erledigung der Arbeitspflichten) unverhältnismäßig war. Der Datenschutzbeauftragte betonte insbesondere, dass sich eine Überwachung darauf beschränken kann, das Vorhandensein von „personenbezogenen Dateien" auf dem Firmencomputer festzustellen, anstatt auf die Inhalte zuzugreifen, und dass man

sich bei der Überwachung der Internetnutzung ggf. auf die Erfassung der Gesamtzeit beschränken kann, anstatt die einzelnen Seiten zu erfassen.

Eine weitere interessante Beschwerde stammte von einer Bürgerin, welche die mutmaßlich gesetzwidrige Verwendung ihres Bildes seitens einer politischen Partei beklagte. Diese Partei hatte anlässlich einer Einschreibungskampagne Plakate mit dem Bild der genannten Bürgerin geklebt. Die Bürgerin erkannte sich auf dem betreffenden Bild und wandte sich an den Datenschutzbeauftragten. Dieser gab ihrer Beschwerde statt und befand, dass diese Art der Datenverarbeitung eine Verletzung ihrer Privatsphäre darstellt. Das betreffende Bild war 20 Jahre zuvor anlässlich einer Demonstration aufgenommen worden. Es bestand die Gefahr, dass mit diesem Bild die Persönlichkeit der Bürgerin in einem Licht dargestellt wurde, das von ihrer heutigen Situation abweicht. Der Datenschutzbeauftragte wies die betreffende politische Partei an, die Plakate unverzüglich zu entfernen, und untersagte die zukünftige Verwendung des Bildes auf Websites, in Druckerzeugnissen und/oder auf Werbematerial aller Art.

Eine Beschwerde über die Zusendung von Werbe-E-Mails gab dem Datenschutzbeauftragten Anlass, erneut auf das Verbot der Versendung derartiger E-Mails ohne die vorherige Einwilligung des Empfängers hinzuweisen, wobei sich dieses Verbot auch auf E-Mails zur ersten Kontaktaufnahme erstreckt. Der Datenschutzbeauftragte wies das betreffende Unternehmen an, die personenbezogenen Daten des Beschwerdeführers aus seiner Datenbank zu löschen, und betonte, dass eine Veröffentlichung im Internet keineswegs als Freibrief für eine schrankenlose Nutzung einer E-Mail-Adresse ausgelegt werden darf.

Inspektionen

Die Inspektionsaktivitäten des Datenschutzbeauftragten wurden 2006 ausgeweitet, teilweise auf der Grundlage von der Behörde erstellter 6-Monatspläne. Insgesamt wurden 350 Inspektionsverfahren durchgeführt. Diese betrafen vorrangig private Unternehmen und Einrichtungen und zielten auf die Überprüfung der Einhaltung der wesentlichen im Datenschutzgesetz niedergelegten Anforderungen ab. Insbesondere konzentrierte sich die Inspektionsabteilung auf die Verarbeitung von personenbezogenen Daten durch Kreditsicherungsgesellschaften, auf die Verarbeitung medizinischer Daten durch Pharmaunternehmen und Einrichtungen des Gesundheitswesens, auf die Online-Verarbeitung von personenbezogenen Daten sowie auf die Verarbeitung für den Fernabsatz von Waren und Dienstleistungen. Bei der Durchführung derartiger Inspektionen kann sich der Datenschutzbeauftragte auch auf eine Sondereinheit innerhalb der Finanzpolizei *(Guardia di Finanza)* stützen. Aufgabe dieser Sondereinheit ist die Überwachung der Melde- und Informationspflichten, der Sicherheitsvorkehrungen sowie der Durchsetzung der Entscheidungen des Datenschutzbeauftragten.

Im Anschluss an die Inspektionen wurden 159 Verfahren zur Verhängung von Verwaltungsstrafen eingeleitet, und in 11 strafrechtlich relevanten Fällen wurden die Unterlagen zur weiteren Bearbeitung an die Staatsanwaltschaft weitergereicht. Zu den strafrechtlich relevanten Verstößen zählten die Nicht-Einhaltung von Entscheidungen des Datenschutzbeauftragten, die Unterlassung selbst minimaler Sicherheitsvorkehrungen sowie die Missachtung des Verbots der Fernüberwachung von Beschäftigten. Die verhängten Verwaltungsstrafen werden 2006 voraussichtlich Einnahmen von mindestens € 600.000 erbringen.

Öffentlicher Dienst:

Öffentliche Verwaltung

Seit dem Jahr 2006 ist die öffentliche Verwaltung verpflichtet, ihre Sicherheitsvorkehrungen für die Verarbeitung von sensiblen Daten und von Gerichtsdaten zu veröffentlichen, um nicht nur deren Angemessenheit zu gewährleisten, sondern dabei auch für Transparenz gegenüber der Allgemeinheit zu sorgen. Das Datenschutzgesetz verpflichtet Behörden und öffentliche Einrichtungen zur Festlegung von Ad-hoc-Verordnungen hinsichtlich der Erfassung, Nutzung und Speicherung derartiger sensibler Daten

und Gerichtsdaten, soweit diese für die vorgesehene Tätigkeit der jeweiligen Einrichtung unverzichtbar sind. In den betreffenden Verordnungen muss zur Information der Öffentlichkeit niedergelegt sein, welche Daten verarbeitet werden, und zu welchen Zwecken. Dies gilt insbesondere in den Bereichen, in denen die einschlägigen Gesetze es Behörden und öffentlichen Einrichtungen gestatten, bestimmte Aufgaben, die eine Verarbeitung sensibler personenbezogener Daten mit sich bringen, an externe Leistungserbringer zu delegieren, ohne dass in den betreffenden Gesetzen entsprechende Leitlinien enthalten wären. Die genannte Verpflichtung zur Festlegung transparenter Regelungen ergibt sich aus Artikel 8(4) der Richtlinie 95/46/EG, welche - wie ja allgemein bekannt ist – die Verarbeitung von personenbezogenen Daten nur aus spezifischen Gründen, aufgrund eines wesentlichen öffentlichen Interesses und unter geeigneten Sicherheitsvorkehrungen erlaubt. Die von den Behörden bzw. öffentlichen Einrichtungen erstellten Verordnungsentwürfe müssen dem Datenschutzbeauftragten zur Genehmigung vorgelegt werden.

Beim Entwurf der genannten Verordnungen für die internen Datenschutzregelungen handelt es sich aber nicht nur um eine Verpflichtung gemäß dem Datenschutzgesetz, sondern zugleich um eine Chance für die gesamte öffentliche Verwaltung in Italien zur weiteren Modernisierung ihrer Strukturen, auch im Hinblick auf die verfügbaren Sicherheitsvorkehrungen und auf die Transparenz der Abläufe. So bietet sich für die öffentliche Verwaltung die Möglichkeit zur Anpassung ihres Organisations- und Funktionsrahmens unter Berücksichtigung der grundlegenden Menschen- und Bürgerrechte und der Freiheiten des Einzelnen, denn diese Faktoren müssen die Richtschnur für alles Handeln der öffentlichen Verwaltung bilden.

Bei der Beurteilung der Einhaltung des Datenschutzgesetzes in den verschiedenen Bereichen des öffentlichen Diensts konnte sich der Datenschutzbeauftragte ein Bild machen über die zunehmende gesellschaftliche Sensibilisierung für die Notwendigkeit, das Grundrecht auf den Schutz personenbezogener Daten immer wirksamer und immer spezifischer umzusetzen - auch in Bereichen, in denen diesem Umstand bisher noch nicht ausdrücklich Rechnung getragen worden ist.

Zur Gewährleistung der ordnungsgemäßen Anwendung des Datenschutzgesetzes und angesichts der immer näher rückenden im Gesetz festgelegten Frist (28. Februar 2007) verstärkte der Datenschutzbeauftragte seine Zusammenarbeit mit Regionen, Stadtverwaltungen und Universitäten, um die entsprechenden Entwürfe für die Verordnungen über die internen Datenschutzregelungen niederzulegen. Zu diesem Zweck stellte der Datenschutzbeauftragte auch Modelle für die Entwürfe zur Verfügung, und die Zusammenarbeit erstreckte sich sogar auf die Kanzlei des Premierministers sowie auf weitere Ministerien, Behörden und öffentliche Einrichtungen, jeweils unter Beachtung ihrer Rolle im institutionellen Gefüge der Italienischen Republik. Auf diese Weise konnte gewährleistet werden, dass die Entwürfe, die dem Datenschutzbeauftragten zur Genehmigung vorgelegt wurden, ohne großen Aufwand auf den Gesetzesrahmen abgestimmt werden konnten, da sie diesem schon in ihrer Konzeption Rechnung trugen. Daraus ergab sich eine Steigerung der positiven Bescheide, ein Beleg für das reibungslose Funktionieren der Koordination zwischen den einzelnen Ministerien, Behörden und öffentlichen Einrichtungen einerseits und der Datenschutzbehörde andererseits.

Die vergleichende Beurteilung von 92 Verordnungsentwürfen gab dem Datenschutzbeauftragten einer breite Basis an die Hand, um eine systematische Beurteilung der Mechanismen durchführen zu können, die bei der Verarbeitung sensibler Daten in der öffentlichen Verwaltung eingesetzt werden.

Dabei zeichnete sich ab, dass einige kritische Punkte in vielen Entwürfen anzutreffen waren. In manchen Fällen führte dies zur Ablehnung des Verordnungsentwurfs. Häufiger allerdings wurde die Genehmigung unter gewissen Auflagen erteilt,

wodurch für die Datenschutzbehörde ein erheblicher fallspezifischer Arbeitsaufwand entstand. So gab es beispielsweise bei einigen Stellen der öffentlichen Verwaltung den Trend, eine „Legalisierung" von Datenverarbeitungsoperationen zu versuchen, die eindeutig außerhalb des Aufgabenbereichs der betreffenden Einrichtung lagen, oder die im Hinblick auf die angestrebten Zwecke eindeutig unverhältnismäßig waren.

Als besonders schwierig erwies sich die Beurteilung, ob die in den Verordnungsentwürfen für die Datenverarbeitung vorgesehenen sensiblen Daten und Gerichtsdaten tatsächlich für die Tätigkeit der jeweiligen Einrichtung unverzichtbar sind. In vielen Fällen mussten bestimmte Kategorien von sensiblen Daten und/oder Gerichtsdaten bzw. bestimmte Verarbeitungsoperationen aus den Verordnungsentwürfen gestrichen werden.

Der Datenschutzbeauftragte erließ unter anderem Bescheide zu den Verordnungsentwürfen des Innenministeriums, des Verteidigungsministeriums, des Erziehungsministeriums, des Nationalen Forschungsrats, des Rechnungshofs, des Staatsrats, der Verwaltungsgerichtshöfe der Regionen sowie von mehreren Lokalverwaltungen und Forschungseinrichtungen.

Gesundheitswesen
Der Datenschutzbeauftragte ergriff Schritte gegen ein Krankenhaus, um es zur Einstellung einer bestimmten Art der Datenverarbeitung zu bewegen: Das Krankenhaus hatte auf seiner Website Fotos von Kindern mit typischen Kinderkrankheiten veröffentlicht. Hier lag also eine Verarbeitung sensibler personenbezogener Daten von Kindern vor. Derartige Daten dürfen jedoch nicht verbreitet werden und erfordern besondere Sicherheitsvorkehrungen, um die Persönlichkeitsentwicklung nicht zu gefährden. Wie auch im Verhaltenskodex für Ärzte niedergelegt, ist es den Beschäftigten im Gesundheitswesen untersagt, über die Presse oder über sonstige Medien Informationen zu verbreiten, die Rückschlüsse auf die Datensubjekte zulassen. Zudem sind die Beschäftigten im Gesundheitswesen verpflichtet, bei Fachveröffentlichungen von klinischen Daten und/oder Beobachtungsdaten für eine umfassende Anonymisierung der Patienten Sorge zu tragen.

NS-Archiv Bad Arolsen (Holocaustarchiv)
Der Datenschutzbeauftragte beschäftige sich auch mit Fragen des Zugriffs auf das NS-Archiv in Bad Arolsen (Deutschland). Im Jahr 2006 erstellten Regierungsvertreter der Signatarstaaten der Bonner Verträge von 1955, durch welche die Einrichtung und der Betrieb des Archivs geregelt werden und zu denen auch Italien zählt, einen Regelungsentwurf für den Zugriff. Der Datenschutzbeauftragte erhob keine Einwände gegen Vor-Ort-Zugriffe auf die Akten, sofern dies zu Forschungszwecken und unter Wahrung der unten dargelegten Sicherheitsvorkehrungen geschieht. Dagegen würde eine Vervielfältigung des Archivs, wie von manchen Staaten verlangt, wesentlich komplexere Probleme aufwerfen: Nach Ansicht des Datenschutzbeauftragten müssten sämtliche beteiligten Staaten (darunter Nicht-EU-Mitglieder wie die USA und Israel) eine Verpflichtungserklärung abgeben, mindestens gleichwertige Sicherheitsvorkehrungen zu gewährleisten, wobei insbesondere die in der EU geltenden Richtlinien zur Übermittlung von Daten in Drittländer zu berücksichtigen wären. Auf jeden Fall müssen für das Archiv die in der EU-Datenschutzrichtlinie sowie im italienischen Verhaltenskodex zur Verarbeitung personenbezogener Daten für historische Forschungszwecke niedergelegten Sicherheitsvorkehrungen eingehalten werden.

Privatwirschaft:
Erstellung von Kundenprofilen: Hotels und Paybackkarten
Der Datenschutzbeauftragte verbot die seitens einer großen Hotelkette durchgeführte Datenverarbeitung: Dort wurden Daten über Vorlieben, Geschmack, Gewohnheiten, Aufenthaltsdauer und sonstige personenbezogene Daten der Kunden gesammelt, um die Kunden besser kennenzulernen und ihre Wünsche proaktiv erfüllen zu können. Dies erfolgte jedoch

ohne eine angemessene diesbezügliche Information der Kunden und ohne ihre Einwilligung in weitere Verarbeitungsoperationen (zur Marketingzwecken und/oder zur Weitergabe an andere Unternehmen). Der Datenschutzbeauftragte verbot daher jede Verwendung der auf die oben geschilderte Weise erhobenen Daten und verpflichtete die Hotelkette, ihre Informationstexte an die Kunden neu zu formulieren, die Einwilligung zur Datenverarbeitung einzuholen, auch im Hinblick auf die Erstellung von Kundenprofilen und auf Marketingaktivitäten, sowie einen bestimmten Zeitraum für die Speicherung festzulegen. Ferner wurden Verwaltungsstrafen verhängt, weil die Informationstexte unzureichend waren und weil die gesetzlich vorgeschriebene Meldung der Datenverarbeitung an den Datenschutzbeauftragten versäumt wurde.

Ein anderer Fall betraf eine große Einzelhandelskette. Hier untersagte der Datenschutzbeauftragte die Verarbeitung von personenbezogenen Daten, die zur Ausstellung so genannter Paybackkarten an die Kunden erhoben wurden, dann aber gesetzwidrig auch für Marketingzwecke eingesetzt wurden. Der Datenschutzbeauftragte ordnete eine Neuformulierung der Informationstexte an, um klar zu machen, dass auch die Erstellung von Kundenprofilen sowie die Weitergabe der Daten des Kunden an eine Bank zu den mit der Datenerhebung verfolgten Zielen zählen. Insbesondere untersagte der Datenschutzbeauftragte es dem Unternehmen, die Ausstellung von Paybackkarten von der Einwilligung der Kunden in die Verarbeitung ihrer Daten zur Erstellung von Kundenprofilen und zu Marketingzwecken abhängig zu machen.

Eigentumswohnanlagen

Seit es sein Amt gibt, erhält der Datenschutzbeauftragte regelmäßig Beschwerden und Bitten um Klarstellung hinsichtlich der Datenverarbeitung im Zusammenhang mit Eigentumswohnanlagen. In der Vergangenheit wurden so zahlreiche Einzelentscheidungen getroffen. Im Jahr 2006 wurden nun all diese Entscheidungen zusammengefasst, im Rahmen einer öffentlichen Anhörung überarbeitet und in Form eines regelrechten kleinen „Leitfadens" für Eigentumswohnanlagen veröffentlicht. Dieser Leitfaden legt detailliert dar, wie die Datenschutzbestimmungen auf die verschiedenen Situationen im Alltag von Eigentumswohnanlagen anzuwenden sind: dass es etwa verboten ist, Listen säumiger Mitglieder der Eigentümergemeinschaft öffentlich auszuhängen, oder dass bei der Verarbeitung sensibler Daten besondere Sicherheitsvorkehrungen getroffen werden müssen.

Leitlinien zur Erfassung und Verwendung von personenbezogenen Daten durch Beschäftigte in der Privatwirtschaft

Im Dezember 2006 veröffentlichte der Datenschutzbeauftragte vereinheitlichte Leitlinien hinsichtlich der Verarbeitung der personenbezogenen Daten von Beschäftigten. Dies erfolgte nicht zuletzt als Reaktion auf zahlreiche Informationsanfragen und Beschwerden von Beschäftigten, Gewerkschaften und Branchenverbänden.

Die wichtigsten Punkte in diesen Leitlinien sind: a) die Verpflichtung, die Verarbeitung auf unverzichtbare Daten zu beschränken (Prinzip der minimalen Datenmenge). Dies gilt auch für die Regelungen zum Tragen sichtbarer elektronischer Mitarbeiterausweise *(Badges)* usw. b) die Verpflichtung, die Beschäftigten über die Verwendung ihrer Daten, ihre Datenschutzrechte und deren Ausübung angemessen zu informieren. c) die Verpflichtung, vor der Weitergabe der personenbezogenen Daten eines Beschäftigten dessen Einwilligung einzuholen (Dies gilt auch für das Aushängen personenbezogener Daten an Schwarzen Brettern usw.); d) die Verpflichtung, von der pauschalen Nutzung biometrischer Daten Abstand zu nehmen. Diese muss auf spezifische, angemessen dokumentierte Fälle beschränkt bleiben (etwa auf den Zugang bestimmter Beschäftigten zu Hochsicherheits- oder Gefahrenbereichen) und erfordert eine Vorabüberprüfung durch den Datenschutzbeauftragten. e) die Verpflichtung zur Anwendung besonderer Sicherheitsvorkehrungen beim Umgang mit sensiblen Daten der Beschäftigten.

Diese müssen getrennt von anderen, nicht-sensiblen Daten aufbewahrt bzw. gespeichert werden.

Diese allgemeinen Leitlinien beziehen sich auf die Privatwirtschaft im Allgemeinen. Weitere, spezifischere Dokumente werden folgen, etwa zur E-Mail- und Internet-Nutzung am Arbeitsplatz.

Kreditsicherungsgesellschaften

Nach Inspektionen bei mehreren Kreditsicherungsgesellschaften veröffentlichte der Datenschutzbeauftragte sechs Punkte, in denen er die seitens dieser Gesellschaften praktizierte Datenverarbeitung für gesetzwidrig erachtet. Insbesondere wurde die Praxis mehrerer Telefongesellschaften beanstandet, die vor Vertragsabschluss die Kreditwürdigkeit und Zuverlässigkeit der potenziellen Kunden per Anfrage bei einer Kreditsicherungsgesellschaft abklären. Auf diese Weise werden die von den Kreditsicherungsgesellschaften zum Zweck der Absicherung von Kreditgebern und der Eingrenzung der mit der Kreditvergabe verbundenen Risiken erhobenen Daten an Unternehmen weitergegeben, die zum Zugriff auf derartige Daten nicht befugt sind. Außerdem wurden die Informationstexte für die Datensubjekte für unvollständig und die Sicherheitsvorkehrungen für unzureichend befunden. In manchen Fällen stand auch der Umfang der Datenverarbeitung in keinem angemessenen Verhältnis zum verfolgten Zweck, nämlich der Gewährleistung der rechtzeitigen Begleichung von Telefonrechnungen.

In einer weiteren Entscheidung ging der Datenschutzbeauftragte auf den Speicherungszeitraum für so genannte „positive" Daten ein, d. h. Daten über die regelmäßige Bezahlung der Grund- und Gesprächsgebühren bzw. Pauschalen und/oder die vollständige Begleichung von Rückständen. Der Datenschutzbeauftragte stellte fest, dass der maximal zulässige Zeitraum für die Speicherung in derartigen Fällen 36 Monate beträgt.

E-Tickets im ÖPNV

Eine Entscheidung im Oktober 2006 bot dem Datenschutzbeauftragten die Möglichkeit, eine Reihe allgemeiner Grundsätze zu E-Tickets im öffentlichen Personennahverkehr (ÖPNV) darzulegen. Die Entscheidung bezog sich spezifisch auf die E-Tickets in den Verkehrsverbünden von Rom und Mailand, in denen seit mehreren Jahren EDV-basierte automatische Ticketsysteme bestehen. Beide Systeme haben eine Reihe von Merkmalen gemeinsam (beispielsweise dass die Benutzer in beiden Fällen Smart-Cards verwenden und dass in beiden Fällen eine zentrale Datenbank für Verwaltungszwecke und zur Analyse der anfallenden Gesamtdaten eingerichtet worden ist). Eine weitere Gemeinsamkeit ist, dass bei beiden Systemen die Möglichkeit besteht, über die Smart-Cards weitere Daten zu erfassen (über die Angaben der Kunden beim Abschluss des Abonnements hinaus). Derartige zusätzliche Daten werden auf dem Chip der Smart-Card (Authentifizierungsdaten und Anzahl der erfolgreichen Authentifizierungen), in den Authentifizierungsgeräten an den Stationseingängen (Identifizierungsdaten wie Seriennummer, Abonnementnummer und Authentifizierungsnummer) sowie in der zentralen Datenbank (Daten zur Person des Abonnenten, Seriennummer der Chip-Karte und Authentifizierungsdaten von den einzelnen Zugangsgeräten) gespeichert. Es wurden folgende Leitlinien veröffentlicht, die in Zukunft möglicherweise einer Anpassung bedürfen werden, auch um weiteren technologischen Entwicklungen Rechnung zu tragen:

- Es ist gestattet, Authentifizierungsdaten (Zeit/Ort) auf dem E-Ticket (Smart-Card) zu speichern, aber nur in angemessenem Umfang. (Für die vorliegenden Zwecke sind vier bis fünf Datensätze ausreichend.)

- Es ist gestattet, Daten (wie etwa die Seriennummer des E-Tickets) in den Authentifizierungsgeräten an den Stationseingängen zu speichern, allerdings nur für einen begrenzten Zeitraum, etwa von 24 Stunden, um einen Abgleich mit schwarzen Listen (gestohlene Daten, abgelaufene Abonnements usw.) vornehmen zu können.

- Es sollte keinerlei zentralisierte Speicherung der personenbezogenen Daten in Kombination mit den Daten des betreffenden E-Tickets erfolgen. Für statistische Auswertungen und zur Verbesserung des Leistungsangebots sind keinerlei personenbezogene Daten erforderlich. Ein beschränkter Speicherungszeitraum (72 Stunden) ist hinnehmbar, um auf Funktionsstörungen und sonstige Probleme angemessen reagieren zu können. Anschließend müssen die Daten im Interesse des Datenschutzes und des freien Personenverkehrs unbedingt anonymisiert werden. Dessen ungeachtet dürfen einzelne Datensätze über längere Zeiträume in einem zuordenbaren Format gespeichert bleiben, sofern dies aus spezifischen Gründen erforderlich ist (etwa bei einer detaillierten Untersuchung in einem spezifischen Fall).

Unerbetene Telefondienstleistungen
Als Reaktion auf eine ganze Reihe von Beschwerden, Berichten und Untersuchungen zu wiederkehrenden Gesetzesverstößen durch die unerbetene Aktivierung von Telefonverträgen, Telefonkarten und/oder sonstigen Telefondienstleistungen erachtete es der Datenschutzbeauftragte für erforderlich, grundlegende Sicherheitsvorkehrungen zur Gewährleistung der Wahrung der Rechte und Freiheiten der Bürger zu veröffentlichen. Dabei ging es um verschiedene Fälle: um Mobilfunkkarten, die ohne Einwilligung der Datensubjekte aktiviert wurden, um die unerbetene Aktivierung der Vorauswahl eines bestimmten Netzbetreibers, um zusätzliche Telefondienstleistungen, die durch die eigene Telefongesellschaft oder durch einen anderen Anbieter aktiviert wurden… Der Datenschutzbeauftragte betonte, dass sämtliche an der Verarbeitung derartiger Daten beteiligten Unternehmen dafür Sorge tragen müssen, dass die Daten für spezifische, explizite und rechtmäßige Zwecke erfasst und gespeichert werden und dass die Verarbeitung sowie etwaige weitere Verarbeitungen ordnungsgemäß und rechtmäßig erfolgen. Dabei müssen die Bestimmungen des Datenschutzgesetzes sowie alle sonstigen für die Datenverarbeitung relevanten gesetzlichen Bestimmungen beachtet werden. Hierzu zählt auch die Verpflichtung, vor der Aktivierung die Identität des Abonnenten bei Mobilfunkverträgen bzw. des Käufers bei Prepaid-Mobilfunkkarten zu ermitteln, bevor die betreffenden Telefondienstleistungen aktiviert werden. Mit anderen Worten: Diese Identitätsprüfung muss im Rahmen der Übergabe der Mobilfunkkarten erfolgen. Es wurde empfohlen, zu diesem Zweck geeignete Verfahren festzulegen.

Verhaltenskodizes
Im gesamten Jahresverlauf 2006 wurden die Arbeiten am Entwurf für einen Verhaltenskodex zum Thema Internet fortgesetzt, wobei zahlreiche Vertreter von verschiedenen Branchenverbänden und speziell aus der Internet-Branche eingebunden wurden. Auch die Verhaltenskodizes zu anderen Branchen (Privatdetektive sowie Untersuchungen seitens des Anwalts der Verteidigung im Rahmen von Strafverfahren) sind in Arbeit.

Angesichts der Bedeutung eines derartigen Werkzeugs wurde im Amtsblatt der Italienischen Republik *(Gazzetta Ufficiale della Repubblica Italiana)* eine Ad-hoc-Verordnung veröffentlicht, um die Mechanismen darzulegen, mit denen der Datenschutzbeauftragte die Einführung von Verhaltenskodizes in bestimmten Branchen von erheblichem öffentlichem Interesse fördern kann, in denen ein spezifischer Regelungsbedarf besteht (beispielsweise Arbeitsbeziehungen und Marketing). In der Verordnung ist auch niedergelegt, welche Kriterien erfüllt sein müssen, damit eine bestimmte Branchenvereinigung als repräsentative Vertretung der betreffenden Branche betrachtet werden darf.

Medien
Der Datenschutzbeauftragte erließ eine einstweilige Anordnung zur Verhinderung der Verwendung von personenbezogenen Daten, die einer Fernsehsendung zugrunde lagen: 50 Mitglieder des italienischen Parlaments waren ohne ihr Wissen einem Drogentest unterzogen worden. Der Datenschutzbeauftragte befand, dass in diesem Fall eine gesetzwidrige Verarbeitung medizinischer Daten vorlag, verschärft durch die

Art ihrer Erhebung, was durch die beabsichtigte Verbreitung in einer Fernsehsendung keineswegs zu rechtfertigen sei. Die betroffenen Personen waren nicht über die beabsichtigten Zwecke der Datenverarbeitung informiert worden, und die biologischen Proben wurden auf irreführende und unrechtmäßige Weise gewonnen. Aus diesen Gründen untersagte der Datenschutzbeauftragte die Erfassung, Speicherung und Verwendung der genannten Daten.

Der Datenschutzbeauftragte nutzt einen Antrag auf Vorabüberprüfung zu einer allgemeinen Klärung der Sicherheitsvorkehrungen, die Unternehmen treffen müssen, wenn sie über digitales terrestrisches Fernsehen (DVB-T) interaktive Werbedienstleistungen anbieten. Der Datenschutzbeauftragte entschied, dass die Erfassung und Verwendung von Daten zu derartigen Zwecken rechtmäßig ist, sofern vor dem Anbieten der betreffenden Dienstleistungen bestimmte spezifische Vorkehrungen und Maßnahmen ergriffen werden. Es wurde insbesondere darauf hingewiesen, dass vor der Erfassung der Daten über einen Ad-hoc-Bildschirm ein detaillierter Informationstext eingeblendet werden muss, der umfassend über die beabsichtigte Verwendung der Daten und über die gesetzlichen Rechte der Datensubjekte aufklärt. Sofern eine Einwilligung erforderlich ist, muss diese frei und spezifisch erfolgen, d. h. durch Drücken einer Ad-hoc-Taste. Unter keinen Umständen darf ein Unternehmen eine zentrale Datenbank einrichten, die Daten dürfen nur für einen begrenzten Zeitraum (von sechs Monaten) gespeichert werden, und es müssen strikte Sicherheitsvorkehrungen eingehalten werden.

Die Medien und die Achtung der Menschenwürde

Nach einer Reihe von Fällen, in denen Zeitungen Transkripte von richterlich angeordneten Abhörmaßnahmen veröffentlicht hatten, veröffentlichte der Datenschutzbeauftragte im Juli 2006 von Amts wegen eine allgemeine Erklärung, in der die Punkte dargelegt sind, die in derartigen Fällen unbedingt beachtet werden müssen. Der Datenschutzbeauftragte betonte, dass genau abgewogen werden muss zwischen dem Informationsrecht aller Bürger und der Pressefreiheit auf der einen Seite und der Achtung der Grundrechte und Freiheiten einzelner Bürger auf der anderen Seite, insbesondere hinsichtlich des Rechts auf Schutz der Privatsphäre. Die ungekürzt veröffentlichten Transkripte der Abhörmaßnahmen enthielten Passagen über persönliche und/oder familiäre Beziehungen oder über die Opfer der betreffenden Straftaten (wobei in manchen Fällen auch von Dritten die Rede war, die in keinerlei Beziehung zu den spezifischen Strafverfahren standen). Der Datenschutzbeauftragte rief die geltenden Bestimmungen in Erinnerung und mahnte die Einhaltung des Grundsatzes an, dass ausschließlich für den jeweiligen Fall relevantes Material veröffentlicht werden darf und dass unter keinen Umständen Verwandte oder sonstige Personen ohne Bezug zum spezifischen Fall erwähnt werden dürfen. Oberste Priorität hat die Achtung der Menschenwürde, wobei hinsichtlich Informationen zum Intimleben einer Person spezielle Sicherheitsvorkehrungen getroffen werden müssen. Die Erklärung richtete sich an sämtliche für die Datenverarbeitung Verantwortlichen im Medienbereich und wurde im Amtsblatt der Italienischen Republik *(Gazzetta Ufficiale della Repubblica Italiana)* veröffentlicht. Sämtliche Medien wurden aufgefordert, von sich aus jeweils eine sorgfältige, detaillierte und verantwortungsbewusste Analyse durchzuführen, um zu ermitteln, inwiefern es sich bei Einzelheiten tatsächlich um zur Veröffentlichung geeignetes Material handelt. Nach Auffassung des Datenschutzbeauftragten muss eine Balance zwischen der in der Tat eingeschränkten Privatsphäre von Personen des öffentlichen Interesses und/oder von politischen Amtsträgern einerseits und der dringenden Pflicht der Journalisten zur Achtung der Menschenwürde und zur Wahrung der Rechte Dritter gefunden werden.

Lettland

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

Richtlinie 95/46/EG

- Änderungen des Gesetzes zum Schutz personenbezogener Daten

Zur Gewährleistung der Übereinstimmung der lettischen Gesetze mit den Anforderungen der Richtlinie 95/46/EG wurde im Dezember 2005 der Gesetzentwurf über „Änderungen des Gesetzes über den Schutz personenbezogener Daten" ausgearbeitet. Diese Änderungen sollen umreißen, welche Systeme zur Verarbeitung personenbezogener Daten gemeldet werden müssen, die Meldeverfahren erläutern, die zur Einrichtung von Datenschutzbeauftragten führen, die gesetzlichen Normen nennen, die bei der Auslegung des Gesetzes Schwierigkeiten bereitet haben, und die Anforderungen der Richtlinie 95/46/EG, die in dem Gesetz zum Schutz personenbezogener Daten umgesetzt werden, benennen. Folglich ist vorgesehen, dass sich die staatliche Datenschutzbehörde (DVI) künftig stärker auf die Kontrollen (einschließlich der vorbeugenden Kontrollen) als auf die Meldung von Systemen konzentrieren kann. Der Gesetzentwurf wurde im August 2006 von der Regierung angenommen.

- Gesetzentwurf zur staatlichen Datenschutzbehörde

Um die vollständige Einhaltung der Bestimmungen der Richtlinie 95/94/EG in Bezug auf den Status der lettischen Behörde für den Schutz personenbezogener Daten zu gewährleisten, wurden sowohl im Fach- und Führungskräftebereich als auch im akademischen Bereich Konferenzen abgehalten. Eine Einigung wurde dahingehend erzielt, dass es kein gemeinsames „Dachgesetz" für alle unabhängigen Behörden in Lettland geben wird, sondern dass für jede Behörde ein Einzelgesetz verabschiedet werden soll. Denn die Behörden sind sehr unterschiedlich, so dass sie nicht dem Kabinett unterstellt werden sollten. Vielmehr sollte durch separate, spezifische Gesetze der jeweiligen Situation Rechnung getragen werden.

Im Hinblick auf die Ermittlung der Rechtsstellung unabhängiger Einrichtungen im Rahmen der Verfassung *(Satversme)* räumte das Verfassungsgericht von Lettland durch sein Urteil Nr. 2006-05-01 vom 16. Oktober 2006 (Rechtssache Staatliche Rundfunk- und Fernsehanstalten) zudem ein, dass Körperschaften möglich sind, die nicht dem Ministerkabinett unterstellt werden. Bei seiner Auslegung von Artikel 58 der Verfassung der Republik Lettland (Satversme, zusammen mit anderen Artikeln der Verfassung) ist das Verfassungsgericht zu dem Schluss gekommen, dass das Parlament kraft seiner gesetzgeberischen Befugnis beschließen kann, eine Einrichtung aus der Zuständigkeit und der Überwachung durch das Ministerkabinett auszuklammern. Dieses Urteil wurde bei der Ausarbeitung des Gesetzentwurfs über die staatliche Datenschutzbehörde berücksichtigt.

In Erwägung aller oben genannten Ausführungen billigte das Ministerkabinett die Strategie des Justizministers für den Zeitraum 2007-2009, deren Ziel die Konformität der Rechtsakte in Lettland mit den Anforderungen der Richtlinie 95/46/EG ist. Einem der Schwerpunkte dieser Strategie zufolge ist dafür Sorge zu tragen, dass die staatliche Datenschutzbehörde (die derzeit dem Justizministerium unterstellt ist) eine völlig unabhängige Einrichtung wird. «Daher hat die lettische Datenschutzbehörde den Entwurf eines Gesetzes über die staatliche Datenschutzbehörde ausgearbeitet, der am 3. Januar 2007 dem Justizministerium vorgelegt wurde. Für das kommende Jahr (2007) wird ein besonderes Augenmerk auf Gesetzgebungsakte erwartet, die in Kraft gesetzt werden, um die Unabhängigkeit der lettischen Datenschutzbehörde nach Maßgabe der Richtlinie 95/46/EG zu gewährleisten.

- Änderungen des Strafrechts

Lettland hat die Haftung für Verstöße bei der Verarbeitung von personenbezogenen Daten einer

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

Weiterhin wurde beschlossen, die strafrechtliche Haftung für Übertretungen bei der Verarbeitung von personenbezogenen Daten festzulegen. Der Gesetzentwurf „Änderungen des Strafrechts" wurde am 29. Januar 2007 von der Regierung genehmigt. 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.

Derzeit prüft die staatliche Datenschutzbehörde die Notwendigkeit, die Bußgelder für Übertretungen bei der Verarbeitung von personenbezogenen Daten zu erhöhen, um die Änderung des Verwaltungsstrafgesetzes auszuarbeiten.

Richtlinie 2002/58/EG

Bezüglich der Richtlinie 2002/58/EG wurden am 1. Juli 2006 Änderungen des Verwaltungsstrafgesetzes angenommen, die die Überwachung von Spam-Aktivitäten vorsehen. Diese Bestimmungen werden am 1. Juli 2007 in Kraft treten.

B. Bedeutende Rechtsprechung

- Rechtsprechung zum Schengener Informationssystem

Der Gesetzentwurf zum Schengener Informationssystem wurde der Regierung im September 2006 vorgelegt. Er schreibt vor, wie das System und die diesbezüglichen Sicherheitsmaßnahmen genutzt werden, und benennt die Einrichtungen, die das Funktionieren des Systems und die Überwachung der Verarbeitung von personenbezogenen Daten gewährleisten werden.

- Gesetz über die Verarbeitung biometrischer Daten

Der Gesetzentwurf über die Verarbeitung biometrischer Daten wurde im April 2006 ausgearbeitet und von der Regierung am 2. Januar 2007 genehmigt. Dieses Gesetz soll die Einführung eines einheitlichen biometrischen Datenverarbeitungssystems gewährleisten.

C. Wichtige spezifische Themen

- Bewertung der Umsetzung des Schengen-Besitzstands im Datenschutzbereich

Die Schengen-Bewertung der neuen Mitgliedstaaten wurde 2006 durchgeführt. In Lettland erfolgte der Besuch der Schengen-Expertengruppe am 19.-20. September 2006. Während dieses Besuchs gaben die Experten Empfehlungen ab, damit Lettland die Anforderungen des Schengen-Besitzstands erfüllen kann. Dies ist eines der Schwerpunktthemen der lettischen Regierung und der staatlichen Datenschutzbehörde für die Jahre 2006 und 2007 (insbesondere in Bezug auf den unabhängigen Status der staatlichen Datenschutzbehörde DVI).

Am 1. November 2006 wurde innerhalb der staatlichen Datenschutzbehörde DVI eine neue Abteilung gegründet, die Abteilung für Datenschutzaufsicht in der dritten Säule, die die Umsetzung des Schengen-Besitzstands und die Datenschutzkontrolle bei den Strafverfolgungsbehörden gewährleisten soll.

- Allgemeine Hinweise

Im Jahr 2006 gingen bei der staatlichen Datenschutzbehörde 133 Beschwerden natürlicher und juristischer Personen ein. Von diesen Beschwerden betrafen 90 mutmaßliche Datenschutzverletzungen bei der Verarbeitung personenbezogener Daten, insbesondere die Datenverarbeitung ohne Rechtsgrundlage, die Verletzung des Verhältnismäßigkeitsgrundsatzes und die Verletzung der Rechte von Datensubjekten.

Die staatliche Datenschutzbehörde DVI führte zu den eingegangenen Beschwerden Untersuchungen durch. Für das Gesamtjahr 2006 ergibt sich, dass bei 21 von 90 durchgeführten Untersuchungen eine Verletzung des Gesetzes über den Schutz personenbezogener Daten vorlag.

Gegen die Entscheidungen der staatlichen Datenschutzbehörde DVI können Rechtsmittel eingelegt werden (Artikel 31 des Gesetzes über personenbezogene Daten). Im Jahresverlauf 2006 wurden zwei Entscheidungen angefochten, und gegen vier Entscheidungen in Verwaltungsrechtssachen wurde Berufung eingelegt.

Die staatliche Datenschutzbehörde DVI stattete mehrere unangemeldete Besuche ab, zum Teil aufgrund von Hinweisen in den Fernsehnachrichten. So fand zum Beispiel landesweit eine große Debatte über die auf Wochenendtage fallenden öffentlichen Feiertage statt. Ein Fernsehsender beschloss, eine Kampagne - *Unterschrift für Urlaub* - zu starten, bei der Teilnehmer die Möglichkeit erhielten, durch ihre Unterschrift auf einer Liste in einer der Supermarktketten ihre Unterstützung für diese Initiative zu erklären. Diese Unterschriftenliste war für die Öffentlichkeit zugänglich (da sie einfach an den Kassen auslag) und enthielt personenbezogene Daten, jedoch ohne Einwilligung der Datensubjekte, ihre Daten der Öffentlichkeit preiszugeben.

- Sonstige Themen

- Das Zusatzprotokoll zum Übereinkommen Nr. 108 betreffend Überwachungsbehörden und grenzüberschreitenden Datenverkehr wurde von der Regierung im Februar 2007 genehmigt.

- Aufgrund der Änderungen des Gesetzes über den Schutz personenbezogener Daten werden im Jahr 2007 Änderungen beim Meldeverfahren für die Datenverarbeitung vorgenommen. Die staatliche Datenschutzbehörde DVI begann jedoch bereits 2006 mit den notwendigen Vorkehrungen, um den Datenschutzbeauftragten als Alternative zur Meldung von Datenverarbeitungssystemen einzuführen. Diese Alternative wird eine Aufstockung der administrativen Kapazitäten im Bereich der Überwachungstätigkeiten der staatliche Datenschutzbehörde DVI ermöglichen, wodurch sie besser agieren statt nur reagieren kann, indem sie in verstärktem Umfang präventive Kontrollmaßnahmen durchführt.

Litauen

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

1. Die staatliche Datenschutzbehörde *(Valstybinė duomenų apsaugos inspekcija)* hat Vorschriften für die Vorabüberprüfung ausgearbeitet, die durch die Entscheidung des Direktors Nr. 1T-6 vom 2. Februar 2006 genehmigt wurden. Die Vorschriften betreffen den Inhalt der Meldung, ihre Einreichung und das Verfahren für die Vorabüberprüfung.

2. Infolge der Entschließung Nr. 1317 der Regierung der Republik Litauen vom 7. Dezember 2005 zur „Änderung der Entschließung Nr. 262 der Regierung der Republik Litauen vom 20. Februar 2002 über die Neuorganisation des staatlichen Verzeichnisses der für die Verarbeitung personenbezogener Daten Verantwortlichen, über die die Annahme dieses Verzeichnisses betreffenden Bestimmungen und über das Meldeverfahren, das die für die Datenverarbeitung Verantwortlichen bei der Verarbeitung von personenbezogenen Daten befolgen müssen", hat die staatliche Datenschutzbehörde ein neues Muster-Meldeverfahren für Datenverarbeitungen entwickelt.

3. Am 25. Mai 2006 wurde eine Änderung des Gesetzes über das Einwohnerverzeichnis angenommen, welche die Speicherung von Gesichtsbildern, Fingerabdrücken und Unterschriften im Einwohnerverzeichnis vorsieht. Die erfassten Daten dürfen nur an Strafverfolgungsbehörden und Einrichtungen, die Personaldokumente ausstellen, übermittelt werden.

B. Bedeutende Rechtsprechung

Direktmarketing

Die staatliche Datenschutzbehörde erhält immer mehr Beschwerden über Angebote von Waren und Dienstleistungen, die ohne Einwilligung der Empfänger per Telefon, Post oder auf direktem Weg unterbreitet werden.

Ein Antragsteller beschwerte sich über Werbung durch eine Telekommunikationsgesellschaft. Betroffene wurden durch nach dem Zufallsprinzip ausgewählte Rufnummern angerufen und gebeten, Informationen über das Dienstleistungsangebot verschiedener Anbieter anzuhören. Nach Einwilligung des Betroffenen wurden die Informationen dargelegt, und am Ende wurde er zum Vertragsabschluss mit der Telekommunikationsgesellschaft aufgefordert. Die beschriebenen Handlungen wurden während eines einzigen Telefongesprächs ausgeführt. Paragraf 68 Absatz 1 des Gesetzes über elektronische Kommunikation legt fest, dass die Nutzung elektronischer Kommunikationsdienste, einschließlich E-Mail, zu Zwecken des Direktmarketings nur zulässig ist, wenn die Teilnehmer ihre vorherige Einwilligung erteilt haben. Während der Untersuchung wurde festgestellt, dass der Telekommunikationsgesellschaft keine vorherige Einwilligung vorlag. Die staatliche Datenschutzbehörde erteilte der Telekommunikationsgesellschaft deshalb ein Strafmandat. Der Oberste Gerichtshof kam nach Verhandlung in dieser Verwaltungssache zu dem Schluss, dass das Gesetz über elektronische Kommunikation, das die Nutzung elektronischer Kommunikationsdienste zum Zwecke des Direktmarketings (kommerzielle Zwecke) mit vorheriger Einwilligung des Teilnehmers genehmigt, den Begriff der vorherigen Einwilligung, die Art ihrer Einholung sowie die Klausel, welche die Pflicht zur vorherigen Einholung der Einwilligung implizieren könnte, nicht definiert. Folglich ist die vorherige Einwilligung auch auf Anrufe von nach dem Zufallsprinzip ausgewählten Rufnummern anwendbar. Die Einwilligung ist vom Teilnehmer bei Beginn des Gesprächs einzuholen, bevor er Informationen über die angebotenen Dienste hört. «In der Berufungsverhandlung befand der Oberste Verwaltungsgerichtshof von Litauen, dass die Einwilligung des Teilnehmers, elektronische Kommunikationsdienste zum Zwecke des Direktmarketings zu nutzen, gemäß dem Wortlaut von Paragraf 68 Absatz 1 des Gesetzes über elektronische Kommunikation vor dem Einsatz der Mittel des Direktmarketings und nicht während des Einsatzes eingeholt werden muss.

Dreizehn Beschwerden gingen im Zusammenhang mit einem Verleger ein, der an Personen ohne ihre Einwilligung Angebote zur Teilnahme an einem Spiel versandte. Dieses Unternehmen beauftragte mittels Untervertrags ein Privatunternehmen mit der Erhebung personenbezogener Daten von potenziellen Kunden, mit ihrer Speicherung und mit der Verwaltung der Datenbank. Das letztgenannte Privatunternehmen kaufte personenbezogene Daten von anderen Privatunternehmen, die personenbezogene Daten aus öffentlichen Quellen gesammelt hatten. Im Rahmen der Überprüfung der Gesetzmäßigkeit der Verarbeitung personenbezogener Daten erteilte die staatliche Datenschutzbehörde dem Leiter des Verlags ein Strafmandat, da Daten zum Zwecke des Direktmarketings ohne Einwilligung der Betroffenen verarbeitet wurden und die Betroffenen über diese Vorgänge nicht informiert worden waren. Bei der Verhandlung in dieser Verwaltungssache ergab sich die Frage, wer hier eigentlich der für die Datenverarbeitung Verantwortliche war, d. h. wer für die Einhaltung der Bestimmung des Datenschutzgesetzes haftet: War es der Verleger, der das Privatunternehmen vertraglich mit der Erhebung personenbezogener Daten beauftragte, oder war es das Privatunternehmen, das diesen Auftrag übernahm? Das Gericht befand, dass der Verleger für den Datenschutz verantwortlich war, da der Vertrag den eindeutig festgelegten Zweck der Erhebung und Weiterverarbeitung von Daten (für den Verkauf von Gütern durch Direktmarketing) und die Einrichtung von Datenbanken beinhaltete.

Die Grundsätze der Datenverarbeitung

Immer mehr Probleme entstehen in Bezug auf die verwaltungsrechtliche Verfolgung von Personen (per Strafmandat) wegen Verletzung der allgemeinen Grundsätze der Datenverarbeitung. Absatz 1 Unterabsatz 4 von Paragraf 3 des Gesetzes über den Schutz personenbezogener Daten sieht vor, dass personenbezogene Daten identisch, im Verhältnis zu den Zwecken, zu denen sie erhoben und verarbeitet werden, angemessen und ihr Umfang nicht übermäßig hoch sein sollen. Die staatliche Datenschutzbehörde erteilte einem Privatunternehmen ein Strafmandat wegen Verstoßes gegen diesen Grundsatz der Datenverarbeitung auf, da es zu viele personenbezogene Daten erfasste – in diesem Fall die Personenkennzahl, die für die Zwecke des für die Datenverarbeitung Verantwortlichen (nämlich Buchhaltung) nicht notwendig gewesen wäre. Der Oberste Verwaltungsgerichtshof von Litauen stellte fest, dass die Auslegung allgemeiner Grundsätze, allein aufgrund der Natur der gesetzlichen Bestimmungen nicht klar, präzise und einheitlich erfolgen kann. Darüber hinaus werden die in dem Gesetz genannten Grundsätze, Zielsetzungen, Anwendungsbereiche und sonstigen allgemeinen Einführungsbestimmungen in vielen Fällen erst durch die systematische Anwendung zusammen mit anderen gesetzlichen Vorschriften verständlich. Die direkte Anwendung von Rechtsvorschriften von allgemeiner deklaratorischer Natur wird bei der Definition von strafbaren Handlungen besonders problematisch. Eine verwaltungsrechtliche Haftbarkeit kann nur bei Missachtung ausdrücklich und unmissverständlich formulierter Verbote entstehen, nicht aber bei der Verletzung allgemeiner Grundsätze. Deshalb ist die verwaltungsrechtliche Verfolgung wegen Verletzung allgemeiner Grundsätze ohne Angabe von Verstößen gegen spezifische Verbote nicht möglich.

C. Wichtige spezifische Themen

Mitschneiden von Gesprächen in Banken

Die staatliche Datenschutzbehörde führte im Zusammenhang mit der Aufzeichnung von Kundengesprächen Inspektionen in Banken durch. Dabei wurde festgestellt, dass die meisten Banken Telefongespräche aufzeichnen, und zwar sowohl Anrufe von Bankmitarbeitern bei Kunden als auch Anrufe von Personen (ob Kunde oder nicht), bei der Bank. Abgehende Telefongespräche werden in der Regel als Nachweis für eine kommerzielle Transaktion oder geschäftliche Kommunikation aufgezeichnet. In den meisten Fällen wurden die Bankkunden über die Aufzeichnungen von Telefongesprächen informiert und unterzeichneten hierzu eine Vereinbarung mit der Bank. Wie sich jedoch herausstellte, gibt es sehr wohl einige Bankkunden, deren Telefongespräche mit

der Bank aufgezeichnet wurden, obwohl sie weder eine Vereinbarung unterzeichnet hatten noch über diese Aufzeichnung oder deren Zweck informiert wurden. Mehrere Banken führten Aufzeichnungen von eingehenden Anrufen von Bankkunden oder anderen Personen unter speziell für die Öffentlichkeit zugänglichen Rufnummern durch, die zu dem Zweck eingerichtet wurden, dass Anrufer Informationen über Bankdienstleistungen erhalten oder Auskünfte über bestehende Vereinbarungen mit der Bank einholen konnten. Sofern sich diese Anrufe nicht auf bestehende Vereinbarungen bezogen, wurde die Identität des Anrufers nicht preisgegeben, es wurde jedoch die Rufnummer aufgezeichnet, von der aus der Anruf getätigt wurde. Während der Inspektionen wurde festgestellt, dass die Einwilligung der Anrufer nicht eingeholt wird und dass sich die Anrufer über die Aufzeichnung der Gespräche nicht bewusst sind. Es besteht kein Zusammenhang zwischen diesen Telefongesprächen und der Erbringung von Nachweisen für eine kommerzielle Transaktion oder für eine sonstige geschäftliche Kommunikation. Gemäß Paragraf 63 Absatz 1 des Gesetzes über elektronische Kommunikation kann die Bank ein Telefongespräch aufzeichnen, wenn der Anruf zum Erhalt von Informationen oder zur Beratung dient, jedoch nur mit Zustimmung des Kunden. Seit den Inspektionen haben die Banken Verbesserungen durchgeführt: So werden die Bankkunden über die Aufzeichnung von Telefongesprächen und den Zweck der Aufzeichnung informiert und erhalten Gelegenheit, den Anruf an dieser Stelle auf Wunsch zu beenden.

Inspektionen bei Konsularbehörden

Die staatliche Datenschutzbehörde führte Inspektionen beim litauischen Konsulat in Kaliningrad (Russische Föderation) und bei der litauischen Botschaft in Kiew (Ukraine) durch. Sie überprüfte, wie personenbezogene Daten von Personen, die litauische Visa beantragten, verarbeitet wurden, insbesondere solche, die die Ausstellung von vereinfachten Transitdokumenten betrafen. Während der Inspektion wurde festgestellt, dass die Verarbeitung personenbezogener Daten in Bezug auf das Voranmeldesystem, das System der Ausstellung von vereinfachten Transitdokumenten und das Verfahren für die Vernichtung personenbezogener Daten nicht geregelt war. Auch die Dauer der Datenspeicherung war für das System zur Verwaltung des Konsularverfahrens, das Voranmeldesystem und das System zur Ausstellung von vereinfachten Transitdokumenten nicht festgelegt. Ferner stellte sich heraus, dass Datensubjekte nicht angemessen über ihre Rechte aufgeklärt wurden.

Internationaler Datenverkehr

Die staatliche Datenschutzbehörde erteilte einem Unternehmen, das Ahnenforschung betreibt, die Genehmigung zur Übermittlung von personenbezogenen Daten in die Vereinigten Staaten von Amerika. Personenbezogene Daten werden im Rahmen des Vertrags über die gegenseitige Übermittlung personenbezogener Daten zwischen dem Unternehmen für Ahnenforschung und der betroffenen Person, die in den USA lebt und den Auftrag für eine Ahnenforschung erteilt hat, offengelegt. Der Vertrag sieht angemessene Garantien für das Recht des Einzelnen auf den Schutz seiner Privatsphäre sowie für den Schutz und die Ausübung der anderen Rechte des Datensubjekts sowie organisatorische Maßnahmen für den Schutz von personenbezogenen Daten gegen jede unbeabsichtigte oder gesetzwidrige Vernichtung, Abänderung, Offenlegung und jede andere gesetzwidrige Verarbeitung vor.

Öffentliches Bewusstsein

Ende September 2006 fand eine gemeinsame Pressekonferenz des Rechtsausschusses des Parlaments *(Seimas)* und der Datenschutzbehörde über „Die Datenschutzlage in Litauen" statt. Auf dieser Konferenz wurden wichtige Tendenzen bei den Aktivitäten der Datenschutzbehörde und ihre Ergebnisse vorgestellt, einschließlich einer Umfrage unter den Einwohnern Litauens zu Datenschutzthemen, ferner wurde anhand einer Evaluation die Bereitschaft Litauens zur Umsetzung des Schengen-Besitzstands auf dem Gebiet des Datenschutzes diskutiert, und es wurde eine Zusammenfassung zu den Inspektionen präsentiert,

die die Datenschutzbehörde im Zusammenhang mit der Aufzeichnung von Telefongesprächen bei Banken in Litauen durchgeführt hatte.

Im November 2006 wurde vom Seimas-Ausschuss für die Entwicklung der Informationsgesellschaft eine Konferenz zum Thema „Gesetzliche Regelung des Schutzes personenbezogener Daten: Probleme und Ausblick" abgehalten. Die Leitlinien des Gesetzentwurfs zur Änderung des Gesetzes zum Schutz personenbezogener Daten wurden dargestellt. Dieser Gesetzentwurf wurde von der staatlichen Datenschutzbehörde ausgearbeitet. Auf der Konferenz wurden auch Themen der Verarbeitung und des Schutzes personenbezogener Daten in Litauen behandelt.

Mit dem Ziel, das öffentliche Bewusstsein und die Information der für die Datenverarbeitung Verantwortlichen zu fördern, organisierte die staatliche Datenschutzbehörde Seminare zu aktuellen Datenschutzthemen für Strafvollzugsbehörden, Bildungs- und Entwicklungseinrichtungen und Meldestellen sowie Einrichtungen, die mit Jugendstraftätern arbeiten. Weiterhin wurden mit verschiedenen für die Datenverarbeitung Verantwortlichen Rundtischgespräche abgehalten, um die Suche nach Lösungen für Probleme auf dem Gebiet des Datenschutzes zu fördern.

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 (Umsetzung der Richtlinie 95/46/EG)

Die Gesetzesvorlage zur Änderung gewisser Bestimmungen des Rahmengesetzes für Datenschutz, zu der die Nationale Kommission für den Datenschutz (Commission nationale pour la protection des données – CNPD) die Regierung im Jahr 2005 beraten hatte, wurde am 23. März 2006 ins Parlament eingebracht. Mit Ausnahme von fünf Stellungnahmen durch die jeweiligen beratenden Gremien gab es keine weiteren Entwicklungen.

Das künftige Gesetz wird umfassendere Ausnahmen von Meldeverpflichtungen vorsehen, und einige Formen der Datenverarbeitung werden nicht länger einer Vorabüberprüfung (Genehmigung durch die CNPD) unterliegen.

- Gesetz vom 30. Mai 2005 über die besonderen Vorschriften zum Schutz der Privatsphäre im Bereich der elektronischen Kommunikationen (Umsetzung der Richtlinie 2002/58/EG)

Geringfügige Änderungen der Bestimmungen des Gesetzes vom 30. Mai 2005 werden nach Verabschiedung des oben genannten Gesetzes durch das Parlament vorgenommen.

- Erlasse und Verordnungen

Im Zusammenhang mit den oben erwähnten Gesetzen wurden im Jahr 2006 keine Verordnungen oder Erlasse verabschiedet.

- Weitere Entwicklungen in der Gesetzgebung

Das Gesetz vom 31. Juli 2006 zur Einführung eines einheitlichen Arbeitsgesetzbuchs setzt einige Bestimmungen des Datenschutzgesetzes vom 2. August 2002 in Bezug auf die Überwachung des Arbeitsplatzes außer Kraft, da diese im Bestreben um Einheitlichkeit und Kodifizierung direkt in das Arbeitsgesetzbuch einbezogen wurden.

Das Gesetz über die Verwendung genetischen Datenmaterials zur Identifizierung von Personen in den Bereichen der Strafverfolgung und des Strafrechts, zu dem die CNPD die Regierung im Jahr 2004 beraten hatte, trat am 25. August 2006 in Kraft.

B. Bedeutende Rechtsprechung

- Zivilrechtliche und strafrechtliche Rechtsprechung

Der Appellationsgerichtshof zu Luxemburg, 8. Arbeitskammer, über die Rechtsgültigkeit von Beweismaterial (Zugangskontrollsystem), das unter Verletzung des Datenschutzgesetzes von 2002 erhoben wurde

Die für Arbeitsrecht zuständige Kammer des Appellationsgerichtshofs von Luxemburg befand am 26. Januar 2006, dass eine Kündigung aufgrund der Nichterfüllung der Arbeitsstunden gerechtfertigt sei, auch wenn keine vorherige Genehmigung der CNPD für das Zugangskontrollsystem erteilt wurde. Der Antragsteller führte unter anderem an, dass der Arbeitgeber ein solches System missbrauchen würde, da die CNPD dazu keine vorherige Genehmigung erteilt hatte, und dass das Beweismaterial, das der Arbeitgeber verwendete, deshalb von den gerichtlichen Verfahren auszuschließen sei. Der Appellationsgerichtshof wies dieses Argument zurück, indem er feststellte, dass, selbst für den Fall, dass der Arbeitgeber gegen die Bestimmungen des Datenschutzgesetzes verstoßen haben sollte, ein solcher Verstoß weder sein Recht auf eine ordentliche Gerichtsverhandlung beeinträchtigen noch die Zuverlässigkeit des Beweismaterials berühren würde, das von den Parteien diskutiert wurde.

Es sei darauf hingewiesen, dass die vom Appellationsgerichtshof eingenommene Haltung

von der luxemburgischen Rechtsauffassung nicht akzeptiert wurde. In diesem Zusammenhang sei auf das Urteil der 9. Strafkammer des Bezirksgerichts von Luxemburg vom 13. Juli 2006 hingewiesen, das genau die gegenteilige Auffassung widerspiegelte.

Der Bezirksgerichtshof zu Luxemburg, 9. Strafkammer, über die Rechtsgültigkeit von Beweismaterial (Videoüberwachungsbilder), das unter Verletzung des Datenschutzgesetzes von 2002 erhoben wurde

Am 13. Juli 2006 urteilte die 9. Strafkammer des Bezirksgerichts von Luxemburg, dass in einer Strafsache Beweismaterial, das unter Verletzung des Datenschutzgesetzes von 2002 erhalten oder erhoben wird, unzulässig und deshalb in gerichtlichen Verhandlungen nicht verwertbar sei. Die Rechtssache bezog sich auf eine öffentliche Videoüberwachung, die von einem Unternehmen ohne vorherige Genehmigung der CNPD durchgeführt wurde. Die Richter kamen zu dem Urteil, dass das erhaltene Beweismaterial ohne eine solche vorherige Genehmigung als gesetzwidrig zu betrachten sei. Durch die Ablehnung des Beweismaterials wurde die gesamte gerichtliche Verfolgung gegenstandslos, da sie sich ausschließlich auf diese Videoüberwachungsbilder stützte. Die Rechtssache ist derzeit beim Appellationsgerichtshof anhängig.

Darüber hinaus sei darauf hingewiesen, dass der Appellationsgerichtshof in der 5. Strafkammer durch eine Entscheidung vom 11. Oktober 2005 in einer sehr ähnlichen Angelegenheit (Videoüberwachung am Arbeitsplatz ohne vorherige Genehmigung durch die CNPD) wiederum genau die gegenteilige Auffassung vertreten hatte - die Verwendung von Beweismaterial, das auf ordnungswidrige Weise und unter Missachtung der Bestimmungen des Datenschutzgesetzes von 2002 erhalten wurde, wurde von den Richtern bei der Verhandlung zugelassen.

- Verwaltungsrechtliche Entscheidungen

Für das Jahr 2006 liegen keine Gerichtsentscheidungen in Bezug auf die Anwendung des Datenschutzgesetzes auf verwaltungsrechtliche Angelegenheiten vor.

C. Wichtige spezifische Themen

Die CNPD erteilte ihre erste Genehmigung für die Einführung eines biometrischen Systems, das in einem größeren Wellness- und Fitness-Center für die Zugangskontrolle verwendet wird. Ein solches System wurde 2005 abgelehnt, da die Speicherung von biometrischen Daten in einer zentralen Datenbank im Hinblick auf den Zweck der Zugangskontrolle für unverhältnismäßig befunden wurde. Der Antragsteller rüstete sein System um, damit die Anforderungen der CNPD erfüllt werden können. Die zentrale Datenbank wurde durch ein System ersetzt, bei dem die biometrischen Daten ausschließlich auf einer gesicherten Karte gespeichert werden, die stets beim Datensubjekt verbleibt.

Während des Jahres 2006 führte die CNPD eine umfassende Prüfung der Sicherheitsmaßnahmen durch, die von den wichtigsten öffentlichen Gesundheitsversorgungs- und Pensionsversicherungsanstalten ergriffen wurden. Die CNPD verfolgte das Ziel, sich einen Überblick zu verschaffen, wie Gesundheitsdaten verarbeitet wurden und ob die Rechte der Datensubjekte von dem für die Datenverarbeitung Verantwortlichen sowie von der mit der Verarbeitung beauftragten Stelle beachtet werden. Die CNPD gab umfassende Empfehlungen und Leitlinien ab und stattete die geprüften Einrichtungen mit den notwendigen Befugnissen aus.

Der großherzogliche Erlass über biometrische Pässe trat am 31. Juli 2006 in Kraft. Die CNPD lieferte den zuständigen Behörden und öffentlichen Stellen umfassende Beratung über technische und praktische Aspekte biometrischer Dokumente.

Die CNPD setzte ihre Informations- und Sensibilisierungskampagne fort, indem sie Anfang Januar 2006 in Zusammenarbeit mit der luxemburgischen Verbraucherschutzvereinigung einen Datenschutzkalender herausgab.

Malta

(a) Umsetzung der Richtlinien 95/46/EG und 2002/58/EG

Die Richtlinie 95/46/EG wurde durch das Datenschutzgesetz, Kapitel 440 der Gesetze von Malta, in die maltesische Gesetzgebung umgesetzt. Das Gesetz, das im Juli 2003 endgültig in Kraft trat, sah eine Übergangsphase für die Meldung automatisch verarbeiteter Vorgänge bis Juli 2004 vor. Für manuelle Ablagesysteme traten bis Oktober 2007 einige Bestimmungen in Kraft.

Die Richtlinie 2002/58/EG wurde teils im Rahmen des Datenschutzgesetzes durch die gesetzliche Mitteilung 16 aus dem Jahr 2003, teils im Rahmen des Gesetzes über elektronische Kommunikationen durch die gesetzliche Mitteilung 19 aus dem Jahr 2003 in Kraft gesetzt; die ergänzende Gesetzgebung trat im Juli 2003 in Kraft.

Weitere Entwicklungen in der Gesetzgebung

Keine nennenswerten.

(b) Wichtige spezifische Themen

Ein Staatssekretär reichte bei der Datenschutzbehörde eine Beschwerde im Zusammenhang mit einer Rechtssache ein, bei der eine Journalistin, die sich selbst als normale Bürgerin ausgab, den Minister in seinem Privatbüro anrief und um einen Termin für Beratungsdienste bat. Die von der Journalistin durchgeführte Untersuchung war darauf angelegt, den Minister durch dieses Täuschungsmanöver dazu zu bewegen, eine vergütete Privatarbeit zu übernehmen, was gegen den Verhaltenskodex für Minister und parlamentarische Staatssekretäre verstoßen würde. Das aufgezeichnete Telefongespräch wurde im Fernsehsender der Oppositionspartei ausgestrahlt. Der Datenschutzbeauftragte wägte das Recht des Ministers auf Schutz seiner Privatsphäre gegen die von der Journalistin ausgeübte Meinungsfreiheit ab. Dabei wurde unter anderem die Tatsache berücksichtigt, dass der Minister eine Person von öffentlichem Interesse ist, die öffentliche Aufgaben wahrnimmt, und dass die Öffentlichkeit ein Recht darauf hat, über solche Fälle informiert zu werden. Bei der Prüfung dieses Falls wurden auch ähnlich gelagerte Urteile des Europäischen Gerichtshofs für Menschenrechte herangezogen. Der Datenschutzbeauftragte kam zu dem Schluss, dass die Meinungsfreiheit, die von der Journalistin zur Information der Allgemeinheit ausgeübt wurde, gegenüber dem Recht des Ministers auf Schutz seiner Privatsphäre überwog. Diese Entscheidung wurde nicht angefochten.

Die Datenschutzbehörde erhielt ferner von Mobilfunkbetreibern ein Ersuchen um eine Vorabüberprüfung und um Leitlinien des Datenschutzbeauftragten im Zusammenhang mit einer Aufforderung der Polizei zur Weitergabe von Verkehrs- und Standortdaten in einer laufenden Ermittlung. Diese erfolgte im Anschluss an eine Welle von Brandanschlägen auf Pressevertreter, nämlich auf einen Journalisten und einen Kolumnisten einer führenden Zeitung. In seiner Entscheidung führte der Datenschutzbeauftragte an, dass solche Angriffe eine Bedrohung der öffentlichen Sicherheit darstellten und die Mobilfunkbetreiber daher berechtigt seien, der Polizei unter genau vorgegebenen Bedingungen die erforderlichen Daten zur Verfügung zu stellen. Die Mobilfunkunternehmen legten gegen diese Entscheidung vor dem Berufsgericht für Datenschutz Rechtsmittel ein. Das Gericht entschied zugunsten des Datenschutzbeauftragten. Die Parteien fühlten sich durch eine solche Entscheidung in ihren Rechten eingeschränkt und gingen unter Anwendung der Bestimmungen des Datenschutzgesetzes, das Gegenstand der Berufungsklage war, vor dem Appellationsgerichtshof in Revision. Diese Rechtssache ist noch anhängig.

(c) Bedeutende Rechtsprechung

Im Jahr 2006 traf sich der Datenschutzbeauftragte regelmäßig mit Vertretern aus verschiedenen Sektoren, um Datenschutzthemen zu diskutieren und Leitlinien für die Regulierung der Datenverarbeitung in den

jeweiligen Sektoren auszuarbeiten. Dazu gehörten Finanzinstitute, Medien, Versicherungswesen, Sozialfürsorge, Bildungswesen und Polizei. Gespräche wurden auch mit Vertretern aus zwei anderen Bereichen aufgenommen, nämlich mit den Fotografen und den Sicherheitsdiensten, für die bei spezifischen Fragen eine Intervention des Datenschutzbeauftragten erforderlich war, um den Schutz der Privatsphäre zu gewährleisten. Für diese Sektoren sollen bis Ende nächsten Jahres Leitlinien veröffentlicht werden. Im Februar wurden in Zusammenarbeit mit der Vereinigung der maltesischen Versicherer *(Malta Insurance Association)*, der Vereinigung der Versicherungsmakler *(Association of Insurance Brokers)* und der Maltesischen Finanzdienstleistungsaufsichtsbehörde (*Malta Financial Services Association* - MFSA) Leitlinien zur Förderung vorbildlicher Praktiken in der Versicherungswirtschaft verabschiedet. Diese Leitlinien beziehen sich auf die Datenverarbeitung in Versicherungsunternehmen bei der Vorbereitung und Ausfertigung von Versicherungsverträgen, Prämien, zur Schadenregulierung und im Bereich Rückversicherung. Der Datenschutzbeauftragte arbeitet eng mit anderen Regulierungsbehörden, Vereinigungen und Verbänden zusammen.

Am 25. Januar wurde das neue Portal der Datenschutzbehörde vom Minister für Investitionen, Industrie und Informationstechnologie anlässlich einer Pressekonferenz in der Datenschutzbehörde offiziell eröffnet.

Das neue System wurde im Rahmen des E-Government-Programms entwickelt. Dieses System bietet der Allgemeinheit Online-Dienste an und stellt die notwendigen Back-Office-Einrichtungen zur Verfügung, um die Verwaltungslast zu reduzieren, damit die Personalressourcen besser auf die zentralen technischen Datenschutzaufgaben konzentriert werden können.

Während dieses Jahres setzte die Datenschutzbehörde das Twinning-Light-Projekt für kürzere Partnerschaften fort, das im Oktober 2005 mit dem deutschen Bundesdatenschutzbeauftragten begonnen wurde. Die umfassenden Ziele lagen darin, den Datenschutzbeauftragten bei der Wahrnehmung seiner Aufgaben und Pflichten zur Überwachung der Umsetzung des Datenschutzgesetzes mit geeignetem Fachwissen zu unterstützen und außerdem das Datenschutzreferat beim Büro des Premierministers im Hinblick auf die Verbesserung der Datenschutzkompetenzen im öffentlichen Dienst zu begleiten. Die Zusammenarbeit im Rahmen der Twinning-Vereinbarung wurde am 3. Juni zum Abschluss gebracht. Das Programm lieferte wichtige positive Ergebnisse in Bezug auf den Wissenstransfer und bei der Annahme konkreter Empfehlungen, die von den verschiedenen Experten in den jeweiligen Kompetenzbereichen abgegeben wurden. Während dieses Zeitraums wurden Experten in die Datenschutzbehörde entsandt, wo sie dem Mitarbeiterstab angehörten. In diesem Zusammenhang nahmen sie an Sitzungen teil, berieten den Datenschutzbeauftragten bei Beschwerdebehandlungen und nahmen auch an Inspektionsbesuchen teil. Abgesehen von der unmittelbaren Durchführung des Twinning-Projekts konnte die Datenschutzbehörde so auch ihre Beziehungen zu den Kollegen aus Deutschland vertiefen.

Im Rahmen der Vorbereitungen Maltas auf den Beitritt zum Schengen-Abkommen wurde vom Ausschuss für die Bewertung der Schengen-Daten, der sich aus 12 europäischen Evaluatoren zusammensetzt, ein Peer Review durchgeführt. Diese Experten besuchten die Datenschutzbehörde, um interne Abläufe und Verfahren, insbesondere die Ausübung der Aufsichtsfunktion durch den Datenschutzbeauftragten, zu bewerten. Der maltesische Datenschutzbeauftragte, technische Mitarbeiter und der interne Datenschutzbeauftragte im Außenministerium hielten Vorträge zu diesem Thema. Das Ergebnis der Bewertung wurde der Schengen-Arbeitsgruppe anlässlich einer Ratssitzung vorgelegt, bei der die Datenschutzbehörde eine sehr gute Beurteilung für ihre gute Vorbereitung zur Wahrnehmung der Aufsichtsaufgaben durch alle für Datenverarbeitung Verantwortlichen, einschließlich

der Polizei, erhielt. Die Datenschutzbehörde führt nun regelmäßige Inspektionen bei Polizeisystemen durch. Die erste Prüfung erfolgte mit Hilfe deutscher IT-Spezialisten. Ziel dieser Systemprüfungen war es, ein möglichst hohes Sicherheitsniveau zu gewährleisten und den unberechtigten Zugriff auf personenbezogene Daten zu verhindern. Darüber hinaus sollte die Einhaltung europäischer Auflagen sichergestellt werden. In einigen Fällen wurden Empfehlungen abgegeben. Im Rahmen seiner Aufsichtsfunktionen wird vom Datenschutzbeauftragten zudem erwartet, dass er Inspektionen bei für Datenverarbeitung Verantwortlichen durchführt. Insgesamt wurden 14 Inspektionen durchgeführt, unter anderem bei den maltesischen Botschaften und Konsularstellen in Tunis und Moskau.

Niederlande

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG

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

Die Richtlinie 2002/58/EG wurde insbesondere durch das geänderte Telekommunikationsgesetz *(Telecommunicatiewet)*, das am 19. Mai 2004 in Kraft trat, in niederländisches Recht umgesetzt.[2] Andere Rechtsvorschriften, die diese Richtlinie zum Teil 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.

B. Bedeutende Rechtsprechung und wichtige spezifische Themen

Die Arbeit der niederländischen Datenschutzbehörde (*College Bescherming Persoonsgegevens* - CBP) umfasste während des Jahres 2006 zahlreiche verschiedene Bereiche und Themen. In diesem Bericht werden vier dieser Bereiche besonders hervorgehoben: Recht, Sicherheit und Kontrolle, umfangreiche Verarbeitung personenbezogener Daten, Verhütung und Ermittlung von Betrug sowie Internet. Zu jedem dieser Bereiche wird mindestens eine Entwicklung dargelegt.

1. Justiz, Freiheit und Sicherheit

Terrorfahndung

In den vergangenen Jahren haben Polizei- und Justizbehörden erweiterte Befugnisse zur Bekämpfung des Terrorismus erhalten. Die niederländische Datenschutzbehörde CBP beriet den Justizminister und das Parlament zum Vorschlag für ein Gesetz, das die zulässigen Methoden für die Ermittlung und Bekämpfung terroristischer Straftaten erweitern soll. Die Datenschutzbehörde kritisierte insbesondere die mangelnde Stichhaltigkeit der Argumente für die Notwendigkeit der vorgeschlagenen Maßnahmen. Unter den vorgeschlagenen Maßnahmen befindet sich die Möglichkeit, die Ermittlungen bei bestimmten Gesellschaftsgruppen auszudehnen. Da die kritischen Anmerkungen der Datenschutzbehörde unbeachtet blieben, hat sie auf Ersuchen des Senatspräsidenten den Justizausschuss des Senats weiterhin zu Maßnahmen beraten, die notwendig wären, um zwischen der Überwachung der Datenverarbeitung und der Erweiterung der Befugnisse von Polizei- und Justizbehörden einen Ausgleich zu schaffen.

Themenverarbeitung

Das neue Gesetz über die Verarbeitung von polizeilichen Daten, das eine grundlegende Überarbeitung des Gesetzes über Polizeiregister (*Wet politieregisters*) umfasst, wird sich zweifellos auf den Datenschutz auswirken. Eine der wichtigsten Änderungen ist die Einführung der so genannten „Themenverarbeitung". Bei einer Themenverarbeitung können die personenbezogenen Daten unverdächtiger Personen, gegen die kein angemessener Schuldverdacht (aufgrund bestimmter Sachverhalte und Umstände) vorliegt, in der Art einer Rasterfahndung systematisch und proaktiv verarbeitet werden. Die Datenschutzbehörde hat davor gewarnt, dass ohne zusätzliche Datenschutzmaßnahmen wie Verschlüsselung eine unverhältnismäßig größere Gefahr besteht, dass unbescholtene Bürger Gegenstand unbegründeter Polizeiaktionen werden. Weiterhin hat die Datenschutzbehörde die Notwendigkeit einer ständigen Kontrolle der Richtigkeit und Qualität von Polizeidaten hervorgehoben.

2. Umfangreiche Datenverarbeitung

Wegen der fortschreitenden technologischen

[1] Gesetz vom 6. Juli 2000 über Regelungen zum Schutz personenbezogener Daten *(Wet bescherming persoonsgegevens), Staatsblad van het Koninkrijk der Nederlanden* (Amtsblatt der Gesetze, Gesetzesverordnungen und Erlasse) 2000, 302. Eine nicht offizielle englische Übersetzung ist auf der Website der niederländischen Datenschutzbehörde verfügbar, www.dutchDPA.nl oder www.Dutch DPAweb.nl

[2] Gesetz vom 19. Oktober 1998 bezüglich der im Telekommunikationsbereich geltenden Regelungen (*Telecommunicatiewet* - Telekommunikationsgesetz), *Staatsblad van het Koninkrijk der Nederlanden* (Amtsblatt der Gesetze, Gesetzesverordnungen und Erlasse) 2004, 189.

Entwicklungen wird es für Behörden und Privatunternehmen immer einfacher, personenbezogene Daten im großen Stil zu verarbeiten. Dies kann zweckmäßig und lukrativ sein, es kann jedoch auch Personen schädigen, besonders wenn Fehler begangen werden. Es kommt entscheidend darauf an, dass neue Datenverarbeitungssysteme von Beginn an unter technischen und rechtlichen Gesichtspunkten optimal angelegt sind.

Das Bürgerservicenummer und die elektronische Gesundheitsakte

Die Einführung der Bürgerservicenummer *(Burger Service Nummer, BSN)* war in den vergangenen Jahren ein wiederholtes Thema. Ursprünglich war die Einführung für 2006 vorgesehen, sie wurde aber auf 2008 vertagt. Dann soll die Bürgerservicenummer stufenweise umgesetzt werden, zunächst anstelle der derzeitigen Sozialversicherungsnummer im Gesundheitswesen. Seit ihrer ersten Stellungnahme zu dem Vorschlag im Jahr 2004 diskutiert die Datenschutzbehörde mit dem zuständigen Minister und dem Parlament nach wie vor die Notwendigkeit, in wesentlichen Teilen der Gesetzgebung Sicherheitsvorkehrungen vorzusehen, um eine angemessene und gesetzeskonforme Verarbeitung personenbezogener Daten zu gewährleisten. Wenn in einem der Back Offices in Bezug auf die BSN ein Fehler begangen würde, könnte dies aufgrund der Vernetzung zahlreicher Verwaltungssysteme verheerende Auswirkungen für die betroffene Person haben. Das Gesetz sieht keinen angemessenen Schadenersatz bei Fehlern vor. Dadurch wird das Vertrauen geschwächt, das die Bürger in die Verarbeitung ihrer personenbezogenen Daten durch Regierung und Behörden haben sollten.

Im Gesundheitssektor wird die BSN zur Umsetzung der Elektronischen Gesundheitsakte verwendet. Die Datenschutzbehörde wirkt bei der Entwicklung dieser Akte tatkräftig mit. Die zentralen Themen sind die Gewährleistung einer ausgewogenen Verteilung der Verantwortlichkeiten, des Zugangs, der Sicherheit und der Überwachung.

Einheitliche Fahrkarte für alle Beförderungsarten

Die Regierung plant die Einführung einer einheitlichen Fahrkarte für alle öffentlichen Verkehrsmittel in den Niederlanden. Im Jahr 2006 äußerte sich die niederländische Datenschutzbehörde sehr kritisch gegenüber der von Beförderungsunternehmen geplanten Nutzung personenbezogener Fahrgastdaten zu Zwecken der Leistungserbringung und des Direktmarketings. Dies veranlasste das Parlament dazu, den zuständigen Minister zur Klärung der anstehenden Datenschutzfragen aufzufordern. Als Reaktion auf die Forderungen des Parlaments versuchte der Minister, mehrere Datenschutzprobleme in Absprache mit den Beförderungsunternehmen und der niederländischen Datenschutzbehörde zu lösen. Im Jahr 2007 wird die Datenschutzbehörde eine Beförderungsgesellschaft prüfen, die eine derartige einheitliche Fahrkarte für alle Beförderungsarten eingeführt hat, um herauszufinden, ob Maßnahmen zum Schutz personenbezogener Daten ergriffen wurden und, falls ja, welche dies sind.

3. Betrugsbekämpfung

Betrugsbekämpfung in der Sozialfürsorge

Um den Missbrauch öffentlicher Gelder zu verhindern, wollen immer mehr Gemeinden im Zusammenwirken mit anderen Einrichtungen die von ihren Kunden bei der Beantragung von Sozialhilfe bereitgestellten Informationen überprüfen. Zusätzlich dazu wird die Vernetzung mit anderen Datenbanken auch zunehmend als Mittel zur Betrugsbekämpfung eingesetzt. Als Reaktion auf diese Entwicklung verfasste die Datenschutzbehörde im Jahr 2006 einen Perspektivbericht über die Betrugsbekämpfung durch die Verknüpfung von Datenbanken, der Leitlinien für die Suche eines ausgewogenen Verhältnisses zwischen Betrugsbekämpfung und Schutz der Privatsphäre gibt.

Betrug bei Wohngeldzahlungen

Bei der Bekämpfung von Betrug bei Wohngeldzahlungen an Sozialhilfeempfänger können Stadtverwaltungen von den Versorgungsunternehmen Auskünfte über

die Nutzung von Gas, Wasser und Strom einholen. Zusätzlich dazu hatte eine Gemeindeverwaltung die Vernetzung der Verwaltung der Stadtreinigung mit der Verwaltung des Sozialamts geplant, um sich über die Bewohnerdichte eines Hauses zu informieren. Die Datenschutzbehörde hat diese Praxis für unzulässig befunden. Die Stadtverwaltung könne nicht nachweisen, dass diese Maßnahmen zusätzlich zu den bereits bestehenden Vorkehrungen, wie etwa Vor-Ort-Besuchen, notwendig seien. Die Verwaltung der Stadtreinigung werde zudem zu Fakturierungszwecken genutzt; eine weitere Nutzung zu Zwecken der Betrugsbekämpfung sei unzulässig.

Interventionsteams

Bei der Betrugsbekämpfung in der Sozialfürsorge arbeiten mehrere öffentliche Behörden in so genannten „Interventionsteams" zusammen. In einigen Fällen erheben diese Teams auch personenbezogene Daten von Bürgern durch Beobachtung, ohne dass die Betroffenen davon in Kenntnis gesetzt werden. Die Datenschutzbehörde schreibt den Behörden jedoch vor, die Bürger über diese Praxis sowie auch darüber, dass keine belastenden Daten gefunden wurden, zu informieren. Ein erneuertes Protokoll für diese Praxis wurde von der Datenschutzbehörde im Jahr 2006 genehmigt. Die Datenschutzbehörde bereitete zudem eine Untersuchung vor, die von mehreren Interventionsteams im Jahr 2007 durchgeführt werden sollte.

4. Internet

Veröffentlichungen im Internet

Die Datenschutzbehörde hat die Probleme mancher Personen im Alltag untersucht, die durch Veröffentlichungen über sie im Internet entstanden sind. Eine genaue Analyse dessen, was in Bezug auf die Veröffentlichung im Internet erlaubt und nicht erlaubt ist, hat sich angesichts der Komplexität der Materie als schwierig herausgestellt. Im Jahr 2006 hat die Datenschutzbehörde eine vorläufige Politik entwickelt, die auch darauf abzielt, für die Debatte über dieses Thema ein breiteres Publikum zu gewinnen. Diese Politik wurde in einem Bericht veröffentlicht, der anlässlich der Abschiedskonferenz des Datenschutzbeauftragten Jan Willem Broekema vorgestellt wurde. Gestützt auf die Diskussionen und Erfahrungen mit der provisorischen Politik im Jahr 2006 wird die Datenschutzbehörde Anfang 2007 Leitlinien zur Verarbeitung personenbezogener Daten in Internet-Veröffentlichungen herausgeben.

Personalisierte Internet-Dienste

Bei der Nutzung personalisierter Dienste im Internet, wie Gmail, stellen Dienstanbieter immer größere persönliche Datenspeicher zur Verfügung, einschließlich Informationen über Internet-Suchfunktionen, E-Mail-Inhalte oder sogar den Inhalt von Computerfestplatten. Die Weitergabe dieser Daten an Dritte, unter anderem auf der Grundlage von entsprechenden Anforderungen von Regierung und Behörden, könnte erhebliche Auswirkungen für die Einzelnen haben.

In einer öffentlichen Debatte, die von der Datenschutzbehörde und der Verbraucherorganisation organisiert wurde, räumte Google Europe ein, dass IP-Adressen in der Tat in vielen Fällen personenbezogene Daten darstellen, was bedeutet, dass auf sie die Datenschutzgesetze in vollem Umfang anwendbar sind. Die Datenschutzbehörde betonte, dass die Nutzung dieser Daten zu anderen Zwecken nur in bestimmten Fällen erlaubt sei, dass Betroffene über die Verwendung ihrer Daten angemessen informiert werden sollten und dass Nutzer ein Recht auf den Zugriff auf ihre Daten und deren Berichtigung haben. Schließlich und endlich müsse eine maximale Frist für die Speicherung personenbezogener Daten gewahrt werden.

Polen

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

Die Änderung des Telekommunikationsgesetzes (Gesetzblatt *(Dziennik Ustaw)* Nr. 171, Ziffer 1800) ist im Februar 2006 in Kraft getreten. Es handelt sich unter anderem um den Inhalt von Paragraf 165 Absatz 1 des Telekommunikationsgesetzes, durch den die Frist für die Speicherung von Verkehrsdaten von einem Jahr auf zwei Jahre verlängert wurde. Während der Gesetzesdebatte wurden auch Vorschläge für eine noch längere Speicherfrist eingebracht, jedoch nicht angenommen.

Im Jahr 2006 wurde mit der Umsetzung der Änderungen am Telekommunikationsgesetz begonnen, die unter anderem die Bestimmungen der Richtlinie 2002/58/EG vom 12. Juli 2002 des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sowie die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, umfassend in die polnische Rechtsordnung einbetten sollen. Die Arbeit an den geplanten Änderungen der Rechtsbestimmungen wird derzeit fortgesetzt. Diese Änderungen werden voraussichtlich 2007 verabschiedet.

B. Bedeutende Rechtsprechung

Privatsphäre von Personen des öffentlichen Interesses

Am 20. März 2006 stellte das Verfassungsgericht auf Ersuchen des Präsidenten des Obersten Verwaltungsgerichtshofes in Bezug auf die Beschränkung des Schutzes der Privatsphäre von Personen, die öffentliche Ämter bekleiden, fest, dass Paragraf 5 Absatz 2 Satz 2 des Gesetzes vom 6. September 2001 über den öffentlichen Zugang zu Informationen verfassungskonform ist. Paragraf 5 Absatz 2 besagt Folgendes: „Das Informationsrecht der Öffentlichkeit ist begrenzt, um die Privatsphäre natürlicher Personen oder das Geschäftsgeheimnis von Unternehmern zu wahren". Der angefochtene Satz besagt: „Die Begrenzung gilt nicht für Informationen über Personen, die öffentliche Ämter bekleiden, soweit diese Informationen mit der Erfüllung des Amtes in Verbindung stehen, einschließlich der Informationen über die Bedingungen für die Übertragung und Ausübung des Amtes und für den Fall, dass eine natürliche Person oder ein Unternehmer auf dieses Recht verzichtet."

Nach Auffassung des Gerichts kann die Privatsphäre unter bestimmten Bedingungen im öffentlichen Interesse Einschränkungen unterliegen. Eine solche Einschränkung muss jedoch behutsam und ausgewogen erfolgen und auf einer Abwägung der diesbezüglichen Argumente beruhen. Es sei daran erinnert, dass diese Interessen jeweils gleiches Gewicht haben.

Das Verfassungsgericht stellte fest, dass die angefochtene Bestimmung des Gesetzes über den öffentlichen Zugang zu Informationen nur für den Fall nicht verfassungskonform wäre, dass bei ihrer Anwendung die oben genannten Grundsätze verletzt werden würden. Dies bedeutet, dass die Informationen, die durch den öffentlichen Zugang zu Informationen offengelegt werden, nicht über das Maß hinausgehen dürfen, das für die Transparenz des öffentlichen Lebens gemäß den in einem demokratischen Rechtsstaat geltenden Normen notwendig ist. Die offengelegten Informationen dürfen daher das Recht auf Schutz der Privatsphäre im Kern nicht verletzen. «Veröffentlichte Informationen müssen somit stets relevant für die Beurteilung der Arbeitsweise der betreffenden Institution bzw. des betreffenden Amtsträgers sein.

Beschränkungen des Rechts auf freie Meinungsäußerung

Am 19. Oktober 2006 urteilte das Verfassungsgericht, dass Artikel 212 § 1 und 2 des Gesetzes vom 6. Juni 1997 (Strafgesetzbuch) verfassungskonform ist. Dieser Artikel besagt: „Wer eine andere Person, eine Gruppe von Personen, eine Institution, eine Rechtskörperschaft oder eine Organisationseinheit ohne Rechtspersönlichkeit verleumdet, indem er sie einer Handlung oder einer Eigenschaft bezichtigt, die sie in den Augen der Öffentlichkeit erniedrigen könnte oder zum Verlust des Vertrauens führen könnte, das zur Ausübung eines bestimmten Amtes, Berufes oder einer bestimmten Tätigkeit notwendig ist, wird mit einer Geldstrafe, einer Einschränkung der persönlichen Freiheit oder mit bis zu einem Jahr Gefängnis bestraft."

In seiner Urteilsbegründung betonte das Verfassungsgericht, dass die Rechte und Freiheiten der Bürger, wie Menschenwürde, Leumund und Privatsphäre, unter bestimmten Umständen gegenüber dem Recht auf freie Meinungsäußerung und der Pressefreiheit überwiegen, was Einschränkungen letzterer nach sich ziehen kann.

Der Umstand, dass der Gesetzgeber eine solche Handlung zugleich als Ausübung der freien Meinungsäußerung und als Herabwürdigung eines Dritten einstuft, ist verfassungsrechtlich nicht relevant.

Am 2. Oktober 2006 brachte die Strafkammer des Obersten Gerichtshofs in einem Urteil unmissverständlich zum Ausdruck, dass die strafrechtliche Haftung gemäß Paragraf 51 des Gesetzes über den Schutz personenbezogener Daten (Übermittlung von personenbezogenen Daten an unberechtigte Personen) für die Veröffentlichung von personenbezogenen Daten (z. B. Anschrift) in der Presse gemäß Paragraf 14 des Pressegesetzes beim Chefredakteur oder verantwortlichen Herausgeber liegt, der gesetzlich verpflichtet ist, den Schutz dieser Daten zu gewährleisten.

Bei der Analyse der Beziehungen zwischen dem Gesetz über den Schutz personenbezogener Daten und dem Pressegesetz, dessen Paragraf 4 Absatz 6 vorsieht, dass es verboten ist, Informationen und Daten über das Privatleben ohne Einwilligung des Betroffenen zu veröffentlichen, sofern kein unmittelbarer Bezug zur öffentlichen Tätigkeit einer bestimmten Person besteht, konzentrierte sich der Oberste Gerichtshof auf die in Paragraf 3 Buchstabe a Absatz 2 des Gesetzes über den Schutz personenbezogener Daten enthaltene Auslegung der Presseklausel. Gemäß dieser Regelung ist die Presseklausel, mit Ausnahme der Bestimmungen von Artikel 14-19 des Gesetzes über den Schutz personenbezogener Daten, nicht auf journalistische Tätigkeit in der Presse im Sinne des Pressegesetzes oder auf literarische oder künstlerische Tätigkeiten anwendbar, außer wenn die Ausübung des Rechts auf freie Meinungsäußerung und auf freie Verbreitung von Informationen die Rechte und Freiheiten des Datensubjekts grundlegend verletzen.

Der Oberste Gerichtshof betonte, dass der genannte Artikel 3a Absatz 2 keinen Hinweis auf Paragraf 51 enthalte, der auf die journalistische Tätigkeit für die Presse anwendbar sei, er legt jedoch fest, dass die Bestimmungen des Gesetzes für den Fall greifen, dass die Ausübung der Informationsfreiheit die Rechte und Freiheiten des Datensubjekts in erheblicher Weise einschränkt. Dagegen ist es nach Ansicht des Gerichtshofs offensichtlich, dass die Verletzung der Datenschutzbestimmungen durch die Weitergabe von Daten an unbefugte Personen – ein Straftatbestand – einen schweren Verstoß gegen das Recht auf Schutz der Privatsphäre darstellt. Im Hinblick auf ein solches Verhalten gilt die Bestimmung von Paragraf 51 Absatz 1 auch für die journalistische Tätigkeit im Pressebereich. Der Oberste Gerichtshof stellte fest, dass der Chefredakteur gemäß Paragraf 36 Absatz 1 des Gesetzes über personenbezogene Daten verpflichtet ist, für den Schutz personenbezogener Daten gegen Weitergabe an unbefugte Personen zu sorgen. Er ist daher die Person, die zum Schutz personenbezogener Daten jeder Person

verpflichtet ist, auf die sich das von seiner Redaktion veröffentlichte journalistische Material bezieht. Ein Verstoß gegen diese gesetzliche Verpflichtung birgt Merkmale einer strafbaren Handlung im Sinne von Paragraf 51 Absatz 1 des Gesetzes über den Schutz personenbezogener Daten, das die Übermittlung von personenbezogenen Daten an unbefugte Personen durch die zu ihrem Schutz verpflichteten Personen unter Strafe stellt.

Gesundheitsdaten

Am 5. August 2006 wies das Verwaltungsgericht der Woiwodschaft Warschau eine Klage gegen die Entscheidung des Generalinspektors für den Schutz personenbezogener Daten ab und schloss sich der Auffassung Generalinspektors an, dass die Übermittlung der Gesundheitsdaten des Beschwerdeführers an einen Arzt und eine medizinische Universität zum Zwecke der Ausfertigung eines außergerichtlichen ärztlichen Gutachtens über den Gesundheitszustand des Beschwerdeführers sowie die Verarbeitung dieser Daten während der Vorbereitung dieses Gutachtens notwendig gewesen sei, um das Recht des Beschwerdeführers auf gerichtlichen Schutz durchzusetzen. Als Rechtsgrundlage führte es Paragraf 27 Absatz 2 Punkt 4 des Gesetzes an. Das Gericht billigte ferner die Aussage des Generalinspektors, wonach es nicht im Ermessen der Datenschutzbehörde liege, zu beurteilen, dass der Arzt, der die Stellungnahme über den Gesundheitszustand ausarbeitete, dabei spezifische andere Bestimmungen verletzte, denen zufolge der Arzt ein Gutachten über den Gesundheitszustand ausfertigen kann, nachdem er eine Person selbst gründlich untersucht hat.

Vereinigungen

Am 6. Juli 2006 wies das Verwaltungsgericht der Woiwodschaft Warschau eine Klage gegen die Entscheidung des Generalinspektors für den Schutz personenbezogener Daten in Bezug auf die Rechtmäßigkeit der Verarbeitung personenbezogener Daten der Tochter des Beschwerdeführers und die Auskunft über seine familiäre Situation durch eine bestimmte Vereinigung ab.

Das Gericht teilte die Auffassung des Generalinspektors, dass der Beschwerdeführer bei Abschluss eines Vertrages mit der genannten Vereinigung über das Sammeln von Spenden mit dem Ziel, seiner kranken Tochter zu helfen, der Vereinigung gleichzeitig die Genehmigung zur Verarbeitung ihrer Daten auf der Website und in anderen Informations- und öffentlichkeitswirksamen Materialien der Vereinigung erteilte. Die Vereinigung war daher berechtigt, sowohl Informationen über die Tochter, die an sie weitergegeben wurden, als auch Informationen über die familiäre Situation des Beschwerdeführers zu verarbeiten, um Spenden für die Hilfe bei der Rehabilitation, Behandlung, Beschaffung von Arzneimitteln, Ausrüstung usw. zu erhalten. Das Gericht hielt es für offensichtlich, dass, um die Situation einer Person zu bestätigen, die von der Vereinigung Hilfe erwartete, die bei dieser Hilfeleistung eigentlich nur als Mittler auftritt, der Nachweis zu erbringen war, dass die Empfängerin diese Hilfe auch tatsächlich benötigte. Die Glaubwürdigkeit der Hilfeempfängerin musste zweifellos im Hinblick auf ihre gesundheitliche, familiäre und finanzielle Situation überprüft werden. Gleichzeitig stimmte das Gericht mit dem Generalinspektor darin überein, dass die in Frage gestellte Zuverlässigkeit der Erfüllung des Vertrages durch die Vereinigung nicht von einer Verwaltungsbehörde beurteilt werden kann, da es sich dabei um zivilrechtliche Fragen handelt.

C. Wichtige spezifische Themen

Am 30. und 31. Januar 2006 stattete eine Gruppe von EU-Sachverständigen gemäß dem Mandat, das ihr durch den Beschluss des Ständigen Ausschusses Schengener Durchführungsübereinkommen der Arbeitsgruppe „Schengen-Bewertung" übertragen wurde, Polen einen Besuch ab, um eine regelmäßige Bewertung der Umsetzung des Schengen-Besitzstands in Polen vorzunehmen.

Der Auftrag war von besonderer Bedeutung, denn eine günstige Beurteilung war für den Beitritt Polens zum Schengener Informationssystem notwendig.

Während ihres Aufenthalts in Polen untersuchten die Sachverständigen rechtliche und sachliche Vorkehrungen der polnischen Datenschutzbehörde bei der Wahrnehmung ihrer Aufgaben als Kontrollinstanz gemäß Art. 114 Absatz 1 des Übereinkommens zur Durchführung des Schengener Abkommens.

Aus dem vorgelegten Bericht geht hervor, dass Polen für den Beitritt zum Schengener Abkommen in Bezug auf den Schutz personenbezogener Daten gut vorbereitet ist. So wurde insbesondere festgestellt, dass die Rechtsstellung und Arbeitsweise des Generalinspektors für den Schutz personenbezogener Daten die reibungslose Wahrnehmung der Aufgabe als Kontrollinstanz gewährleistet.

Es sei darauf hingewiesen, dass der Generalinspektor an den weiteren Vorbereitungen für den polnischen Beitritt zum Schengener Abkommen tatkräftig mitwirkt.

Im Rahmen künftiger Tätigkeiten führte der Generalinspektor Inspektionen in ausgewählten Konsulaten durch und wies die Behörden, die künftig Zugang zum SIS haben werden, auf die Notwendigkeit einer ordnungsgemäßen Erfüllung der Auskunftspflicht gegenüber Datensubjekten hin.

Im Jahr 2006 war das größte Problem in Verbindung mit Beschwerden im Banksektor ebenso wie in den Vorjahren die Übermittlung von Daten, die bei der Kreditsicherungsgesellschaft BIK S.A. *(Biuro Informacji Kredytowej)* und der polnischen Bankenvereinigung ZBO *(Związek Banków Polskich)* gespeichert werden. Zur dieser Speicherung sind die Banken gemäß den Bestimmungen des Bankgesetzes verpflichtet. In den meisten Fällen forderten die Beschwerdeführer, die Datenübermittlung für gesetzwidrig zu erklären und sie aus diesen Dateien zu löschen. In einigen Fällen erwies sich die weitere Speicherung und Verarbeitung von Daten des Beschwerdeführers durch die BIK S.A. als unbegründet, da dieser seine Verbindlichkeiten gegenüber der Bank beglichen hatte. Daher wurde die Löschung dieser Daten angeordnet. In den meisten Fällen dieser Art wurde jedoch der Antrag, eine Datenüberübermittlung dieser Art als gesetzwidrig einzustufen, abgelehnt, da die Verbindlichkeit des Beschwerdeführers gegenüber der Bank zum Zeitpunkt der Urteilsfindung Bestand hatte.

Was Rechtssachen zum Bereich Telekommunikation anbelangt, hat sich der Generalinspektor für den Schutz personenbezogener Daten mit Problemen wie der Verarbeitung von Verkehrsdaten befasst. Der Generalinspektor leitete administrative Schritte ein und hielt einen Mobilfunkbetreiber dazu an:

1) seiner Verpflichtung nachzukommen, Teilnehmer darüber zu informieren, mit wem sie die Verträge über Telekommunikationsdienste gemäß Telekommunikationsgesetz abschließen, d. h. im Einzelnen über: a) den Umfang der Verarbeitung von Verkehrsdaten und die Möglichkeiten, diesen Umfang zu beeinflussen, b) die Kategorien der zu Zwecken der Kostenermittlung und Zahlungen verarbeiteten Verkehrsdaten und den Zeitraum, in dem die Daten verarbeitet werden können, c) die Art von Verkehrsdaten, die zu Zwecken der Vermarktung von Telekommunikationsdiensten verarbeitet werden, die Bereitstellung von Mehrwertdiensten und den Zeitraum der Verarbeitung;

2) die Aufnahme einer getrennten Klausel in den Vertrag über die Einwilligung eines Teilnehmers, seine Verkehrsdaten zum Zwecke der Vermarktung von Telekommunikationsdaten zu verarbeiten und solche Daten zum Zwecke der Bereitstellung von Mehrwertdiensten zu verarbeiten, sowie dem Teilnehmer die Möglichkeit anzubieten, jede der oben genannten Zweckbestimmungen einzeln abzulehnen oder anzunehmen.

Eine der in den Medien breit kommentierten Rechtssachen des Jahres 2006 betraf eine Unternehmen, das an Kunden eines bekannten Telekommunikationsbetreibers Rechnungen versandte, die denen des Betreibers ähnelten.

Gleichzeitig mit den Rechnungen versandte diese Rechtspersönlichkeit Verträge, auf deren Grundlage personenbezogene Daten in das Internet-Telefonbuch eingetragen werden sollten. Der Generalinspektor informierte die Strafverfolgungsbehörden über eine hier möglicherweise vorliegende Straftat wegen der ungesetzlichen Verarbeitung personenbezogener Daten, der versäumten Registrierung des Dateiarchivierungssystems und der mangelnden Erfüllung der Auskunftspflicht.

Eines der Probleme in Verbindung mit Internet-Transaktionen war, dass mehr Daten als notwendig erhoben wurden. Dieses Problem trat zum Beispiel in Unternehmen auf, die die Registrierung von Internet-Domainnamen anboten, und die dabei personenbezogene Daten von Kunden mittels Kopie ihrer Ausweisdokumente erhoben. Diese Dokumente bergen Angaben wie Erscheinungsbild, Familienname, Name der Eltern und in den älteren Fassungen den Personenstand. Es sei darauf hingewiesen, dass keine Voraussetzungen gegeben waren, die die Verarbeitung der zusätzlichen Daten in den Ausweisdokumenten gerechtfertigt hätten, und dass die Balance zwischen den Rechten des Datensubjekts über seine Daten, und den Interessen des für die Datenverbeitung Veranwortlichen stets gewahrt bleiben muss.

Portugal

A) Umsetzung der Richtlinien 95/46/EG und 2002/58/EG

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

Die Richtlinie 2002/58/EG wurde per Gesetzesdekret 7/2004 (nur Artikel 13) und per Gesetz 41/2004 vom 18. August 2004 in nationales Recht umgesetzt.

Im Jahr 2006 traten einige Gesetze zu Datenschutzthemen in Kraft, insbesondere das Gesetz 51/2006 über den Einsatz der Videoüberwachung und anderer elektronischer Systeme zur Beobachtung des Verkehrsflusses, von Vorkommnissen und Übertretungen im Straßenverkehr. Dieses Gesetz räumt den Autobahnbetreibern die Möglichkeit zur Installation dieser Systeme ein und erteilt den Strafverfolgungsbehörden die Erlaubnis zur Datenverarbeitung.

Das neue Modell für den Reisepass wurde ebenfalls eingeführt; es umfasst biometrische Daten. Die Datenschutzbehörde *(Comissão Nacional de Protecção de Dados* - CNPD) gab zu beiden Gesetzen ihre Stellungnahme ab.

Die portugiesische Datenschutzbehörde CNPD wurde auf gesetzliche Anordnung als eine der für die Anwendung von Artikel 4 der Verordnung (EG) 2006/2004 vom 27. Oktober 2004 zuständige Behörde beauftragt, die Zusammenarbeit der Verbraucherschutzbehörden bei Spam (Werbemüll) zu gewährleisten.

B) Bedeutende Rechtsprechung

Wir möchten eine Entscheidung des Obersten Gerichtshofs vom Februar 2006 über den Einsatz der Videoüberwachung am Arbeitsplatz hervorheben. «Nach der Berufung einer Gewerkschaft ordnete der Oberste Gerichtshof in Portugal die Entfernung fast aller Videokameras an, da sie einen unverhältnismäßigen Eingriff in die Privatsphäre der Arbeitnehmer am Arbeitsplatz darstellten. Videoüberwachung am Arbeitsplatz ist gemäß dem Arbeitsgesetzbuch aus Sicherheitsgründen zulässig, darf aber nicht als Mittel zur Leistungskontrolle der Arbeitnehmer genutzt werden. In dem untersuchten Fall produzierte das Unternehmen Arzneimittel, und es gab Indizien dafür, dass Substanzen gestohlen wurden, die die öffentliche Gesundheit gefährden könnten. Der Gerichtshof vertrat die Auffassung, dass die Arbeitnehmer nicht einer ständigen „polizeilichen Maßnahme" ausgesetzt werden sollten. Diese Entscheidung des Obersten Gerichtshofs war sehr wichtig, da sie im Grenzfall dem Schutz der Privatsphäre Vorrang einräumt. Die Entscheidung ist zudem maßgeblich für die Intervention der Datenschutzbehörde bei der Beurteilung der Verhältnismäßigkeit der Verarbeitung von Videoüberwachungsdaten.

Ein weiteres wichtiges Urteil des Jahres 2006 fällte der Oberste Verwaltungsgerichtshof in einem durch den staatlichen Apothekenverband *(Associação Nacional de Farmácias)* angestrengten Berufungsverfahren gegen eine Entscheidung der Datenschutzbehörde, in dem der Zentrale Verwaltungsgerichtshof bereits positiv entschieden hatte.

Die Situation geht zurück auf das Jahr 1999, als die Datenschutzbehörde *(Comissão Nacional de Protecção de Dados* - CNPD) dem staatlichen Apothekenverband die Genehmigung für die Verarbeitung einer großen Zahl an personenbezogenen Daten auf nationaler Ebene untersagte, einschließlich aller Arzneimittel, die von jeder einzelnen Person gekauft wurden, eines Verzeichnisses aller Ärzte und ihrer Rezepte sowie weiterer Informationen über das Gesundheitssystem. Nach Ansicht der Datenschutzbehörde CNPD gab es zu jenem Zeitpunkt keine rechtliche Grundlage im portugiesischen Datenschutzgesetz, und es war eindeutig unverhältnismäßig, dass der Verband diese sensiblen Daten verarbeitete.

Der Oberste Verwaltungsgerichtshof schloss sich der Entscheidung der Datenschutzbehörde an.

Es gab weitere kleinere Rechtssachen in Verbindung mit Klagen gegen Sanktionsentscheidungen der Datenschutzbehörde, insbesondere hinsichtlich der Verhängung von Geldbußen bei versäumter Meldung und bei Verweigerung der Einsichtnahme in Daten aus Videoüberwachungssystemen. Im Jahr 2006 hielt der Trend zu einer klaren Mehrheit von Gerichtsentscheidungen zugunsten der Datenschutzbehörde CNPD an.

C) Wichtige spezifische Themen

1. Stellungnahmen zu Gesetzentwürfen

Gemäß dem Datenschutzgesetz müssen Gesetzentwürfe, die Fragen zum Datenschutz enthalten, auf nationaler wie auch internationaler Ebene der Datenschutzbehörde CNPD zur Stellungnahme unterbreitet werden.

Im Jahr 2006 gab die CNPD 46 Stellungnahmen ab, von denen einige in EU-Organen in Bearbeitung befindliche Rechtsvorschriften betrafen, wie der Rahmenbeschluss über den Austausch von Informationen in Vorstrafenregistern, das Prinzip der Verfügbarkeit oder das Abkommen EU/USA über Fluggastdatensätze.

Die Datenschutzbehörde gab zudem Stellungnahmen zur Umsetzung der Richtlinie 2004/52/EG über elektronische Mautsysteme und der Richtlinie 2005/28/EG über Leitlinien der guten klinischen Praxis für zur Anwendung beim Menschen bestimmte Prüfpräparate ab. Im Zusammenhang mit weiteren inländischen Rechtsvorschriften äußerte sich die Datenschutzbehörde zu mehreren wichtigen Angelegenheiten mit engem Bezug zum Datenschutz, wie zur Videoüberwachung in Taxis, zur Offenlegung einer Liste der Steuersünder, zum elektronischen Reisepass, zur Fahrtüchtigkeit unter Einfluss von Alkohol und psychoaktiven Drogen, zum Personalausweis (Bürgerkarte), zur Fahndungsdatenbank, zur Staatsangehörigkeitsregelung, zur Einreise von Ausländern in das Staatsgebiet, ihrem Aufenthalt sowie ihrer Ausreise, zur öffentlichen Bereitstellung elektronischer Briefkästen und zum Gesundheitswesen.

2. Front Office

Im Jahr 2006 eröffnete die portugiesische Datenschutzbehörde ein so genanntes Front Office, also eine Geschäftsstelle mit Publikumsverkehr, die ausschließlich dazu dient, Datensubjekte und für die Datenverarbeitung Verantwortliche entweder persönlich oder schriftlich bei der Behandlung von Auskunftsersuchen und beim Einreichen von Meldungen und anderen Unterlagen zu unterstützen. Gleichzeitig schaltete die Datenschutzbehörde eine spezielle Rufnummer frei, die so genannte „Privacy-Line" (+351 (0)21 393 00 39), unter der die breite Öffentlichkeit Rat suchen kann. Auskunftsersuchen können per Telefon, E-Mail, Fax, schriftlich oder auf der Website eingereicht werden.

Durch die Öffnung eines Front Office konnte die Arbeit besser eingeteilt und das Leistungsangebot sowie die Antwortzeit konnten optimiert werden.

3. Zugang von Versicherungsunternehmen zu Gesundheitsdaten von Verstorbenen

Die portugiesische Datenschutzbehörde CNPD erhält im Zusammenhang mit Lebensversicherungsverträgen zahlreiche Anfragen in Bezug auf Gesundheitsdaten von verstorbenen Personen. Die Versicherungsunternehmen wollen auf diese Gesundheitsdaten zugreifen, um die Versicherungsprämien des Verstorbenen an die berechtigten Empfänger auszuzahlen.

Die Datenschutzbehörde veröffentlichte im Jahr 2001 Leitlinien über den Zugang von Dritten zu Gesundheitsdaten. Demnach sind Versicherungsunternehmen ausschließlich befugt, Auskunft über die Todesursache einzuholen, sofern keine weiter gefasste Einwilligung des Datensubjekts vorliegt. Weitere Anfragen betrafen den Zugang von Versicherungsgesellschaften zu Gesundheitsdaten auf der Grundlage von Vertragsklauseln, die vom Verstorbenen unterzeichnet wurden. Die Datenschutzbehörde evaluierte die Situation und kam zu dem Schluss, dass diese Vertragsklauseln keine spezielle und gut informierte Einwilligung von

Seiten des Datensubjekts darstellten. Nach dieser Beurteilung empfahl die Datenschutzbehörde den Versicherungsunternehmen eine eigenständige Vertragsklausel mit einer gesonderten Unterschrift, die das Datensubjekt / den Versicherungsantragsteller über den Zweck des Zugangs und die Einholung seiner Einwilligung speziell informiert. Nach Ansicht der Datenschutzbehörde sollten Versicherungsunternehmen jedoch nur Zugang zu Angaben über die Ursache und Entwicklung jener Krankheit erhalten, die den Tod verursachte, und nicht zu allen Gesundheitsdaten. Letzteres hatten die Versicherungsgesellschaften gewünscht, um überprüfen zu können, ob eine arglistige Täuschung vorliegt, durch die eine Ausschüttung der Versicherungssumme hinfällig wäre. Diese Überlegungen können nachgelesen werden unter www.cnpd.pt

4. Arbeitssicherheit

Im Jahr 2006 verabschiedete die portugiesische Datenschutzbehörde CNPD eine Standardgenehmigung für die Verarbeitung von Gesundheitsdaten von Arbeitnehmern zu Zwecken der Arbeitssicherheit. Der Arbeitgeber hat keinen Zugang zu den allgemeinen Gesundheitsdaten der Arbeitnehmer, sondern nur zu den spezifischen Angaben, die der Betriebsarzt bereitstellt, etwa „arbeitsfähig" oder „nicht arbeitsfähig".

Ferner beurteilte die Datenschutzbehörde Angaben zu Alkohol- und Drogentests, die nur auf in manchen Berufen regelmäßig zulässig sind, falls ein lebensbedrohliches Risiko besteht.

Sicherheitsvorkehrungen und Fristen für die Datenspeicherung wurden ebenso behandelt wie die ausgelagerte Datenverarbeitung durch Fremdunternehmen. Diese Standardgenehmigung zielt darauf ab, den für Datenverarbeitung Verantwortlichen in diesem Bereich Anleitung zu geben und die Mitarbeiter über ihre Rechte aufzuklären. Die Standardgenehmigung ist auf unserer Website verfügbar, unter www.cnpd.pt.

Slowakei

A. Umsetzung der Richtlinie 95/46/EG sowie andere Entwicklungen in der Gesetzgebung

Umsetzung der Richtlinie 95/46/EG

Im Februar 2006 fanden zweitägige Gespräche zwischen dem Vertreter der Europäischen Kommission und der slowakischen Behörde zum Schutz personenbezogener Daten (*Úrad na ochranu osobných údajov* – ÚOOÚ; im Folgenden: die „Datenschutzbehörde") zur Beurteilung der Harmonisierung zwischen dem geänderten slowakischen Gesetz über den Schutz personenbezogener Daten und der Richtlinie 95/46/EG statt. Es handelte sich um das erste bilaterale Treffen nach dem Beitritt zur Europäischen Union. Ziel war die vollständige Angleichung der slowakischen Gesetzeslage an die Anforderungen der Richtlinie.

Im Januar 2007 erhielt die slowakische Datenschutzbehörde ÚOOÚ einen Bericht der Generaldirektion Justiz, Freiheit und Sicherheit der Europäischen Kommission, in dem die Datenschutzlage in der Slowakei als zufriedenstellend beurteilt wird. «Gesetz Nr. 428/2002 Coll. über den Schutz personenbezogener Daten wurde durch Gesetz Nr. 90/2005 Coll. (im Folgenden: „Datenschutzgesetz") geändert, und die slowakische Datenschutzbehörde ÚOOÚ wird ihren Aufgaben trotz beschränkter Finanz- und Personalressourcen nachkommen.

Im Datenschutzbereich war in der Slowakei eine positive Entwicklung zu verzeichnen. Zwar sind noch weitere Schritte zur Steigerung der institutionellen Unabhängigkeit der Datenschutzbehörde erforderlich, doch andere wichtige Fragen – wie die Finanzausstattung der Behörde, ihre Zuständigkeiten und ihre Verankerung in der Verfassung – konnten durch die Umsetzung der entsprechenden Änderungen am Datenschutzgesetzt bereits geklärt werden, so dass die vollständige Harmonisierung mit der Datenschutzrichtlinie deutlich näher gerückt ist.

Es sollten weitere Änderungen am Datenschutzgesetz vorgenommen werden, um der Datenschutzbehörde umfangreichere Untersuchungsbefugnisse zu verleihen. Die entsprechenden Empfehlungen der Europäischen Kommission werden in eine Neuformulierung des Gesetzes einfließen, die im Jahresverlauf 2007 erfolgen wird.

Weitere Entwicklungen in der Gesetzgebung

Im Rahmen der vorgeschriebenen Einbindung in das Gesetzgebungsverfahren gab die Datenschutzbehörde 156 Stellungnahmen zu Gesetzentwürfen, Gesetzen, Erlassen und Verordnungen der slowakischen Regierung ab. Der Großteil der beurteilten Gesetzentwürfe kam aus dem Innenministerium, dem Gesundheitsministerium und dem Finanzministerium.

Im Allgemeinen wurden die Empfehlungen der Datenschutzbehörde berücksichtigt. Lediglich beim Bankengesetz gab es einen Konflikt um die Formulierung über den Zeitraum für die Datenspeicherung, in dem das Parlament dem Vorschlag des Finanzministeriums den Vorzug gab. Gemäß der neuen Formulierung müssen die Aufzeichnungen aus der Überwachung von Bankräumlichkeiten nach 12 Monaten vernichtet werden.

Auf Anregung der Datenschutzbehörde wurde eine wichtige Änderung am Gesetz über das öffentliche Gesundheitswesen vorgenommen. Die Datenschutzbehörde setzte durch, dass die in Arztberichten enthaltenen personenbezogenen Daten im Gesetz ausdrücklich genannt werden.

B. Bedeutende Rechtsprechung

Im Jahresverlauf 2006 gelangten drei Datenschutzfälle vor Gericht: In zwei Fällen wurde gegen Entscheidungen der Datenschutzbehörde wegen Verstoßes gegen das Datenschutzgesetz geklagt, und in einem Fall verklagte ein Schweizer Staatsbürger die Datenschutzbehörde wegen angeblicher Untätigkeit, nachdem seine personenbezogenen

Daten auf der Website einer Zeitung veröffentlicht worden waren.

Im ersten Fall hatte eine Bank bereits vor dem Inkrafttreten der entsprechenden Rechtsgrundlage bestimmte Maßnahmen gegen Kunden durchgeführt. Im Rahmen eines Vergleichs zwischen der Datenschutzbehörde und dem betreffenden Kreditinstitut entschied das Gericht auf Einstellung des Verfahrens.

Im zweiten Fall erließ die Datenschutzbehörde eine Anordnung gegen die Übermittlung von personenbezogenen Daten von einer privaten Einrichtung an eine neu gegründete andere private Einrichtung, da nach Auffassung der Datenschutzbehörde dafür keine vertragliche Grundlage bestand. Das Gericht befand die Anordnung der Datenschutzbehörde für unbegründet.

In der dritten Sache dauerte das Verfahren zum Zeitpunkt der Abfassung des vorliegenden Berichts noch an. In Kürze wird die Entscheidung des Obersten Gerichtshofes der Slowakischen Republik über die Frage erwartet, ob die Datenschutzbehörde – die Beklagte im vorliegenden Verfahren – gesetzlich verpflichtet gewesen wäre, gegen die Veröffentlichung von bereits andernorts veröffentlichten personenbezogenen Daten des Klägers auf der Website einer slowakischen Zeitung vorzugehen.

C. Wichtige spezifische Themen

Im Jahr 2006 gingen bei der Datenschutzbehörde 102 Beschwerden von Datensubjekten und sonstigen natürlichen Personen ein, die ihre im Datenschutzgesetz niedergelegten Rechte unmittelbar verletzt sahen. Von sonstigen Rechtssubjekten kamen zwölf Beschwerden wegen Verstößen gegen das Datenschutzgesetz. 82 Verfahren wurden von Amts wegen eingeleitet. Diese 196 Beschwerden und Verfahren stellen gegenüber 2005 eine Steigerung um 55% dar.

In Jahresverlauf 2006 führte die Inspektionsabteilung 96 Inspektionen und so genannte „Aufforderungen zur Erläuterung" durch, und es ergingen 70 verbindliche Anordnungen.

In Umsetzung der Regierungsentschließung Nr. 558/2008 über die vorläufige Stellungnahme der Slowakei für den Evaluationsbericht hinsichtlich der Konformität der Datenschutzbestimmungen mit den Anforderungen des Schengen-Besitzstandes führte die Datenschutzbehörde Inspektionen in den Konsularabteilungen der diplomatischen Vertretungen der Slowakei in der Ukraine, Weißrussland und der Russischen Föderation sowie im slowakischen Außenministerium durch.

Verarbeitung der personenbezogenen Daten der Kunden einer privaten Versicherungsgesellschaft

Die Datenschutzbehörde beschäftigte sich mit der Verletzung der Rechte der Kunden einer privaten Versicherungsgesellschaft. Die Untersuchung des Falls wurde durch die Veröffentlichung eines Artikels in einer überregionalen Tageszeitung angestoßen. Es hatte sich eine Person an die Zeitung gewandt, der per E-Mail eine Datenbank mit personenbezogenen Daten von circa 20.000 Kunden einer Autoversicherung zugegangen war: Personenkennzahl, Fabrikat und Modell des Fahrzeugs sowie die Höhe der im Jahr 2005 geleisteten Beiträge der einzelnen Personen zur gesetzlich vorgeschriebenen KFZ-Haftpflichtversicherung. Der Empfänger verfügte über keine Zugriffsberechtigung auf diese riesige Datenbank, sondern hatte die E-Mail aufgrund eines Fehlers der zuständigen Person bei der Versicherungsgesellschaft erhalten. Glücklicherweise sorgte die Person, welche die Zeitung informierte, für die Sicherheit der bei ihr eingegangenen personenbezogenen Daten. Da die Datenschutzbehörde feststellte, dass es zu keinem Missbrauch der Daten gekommen war, verzichtete sie auf die Verhängung einer Geldbuße.

Verarbeitung von personenbezogenen Daten im Rahmen der Beherbergung von Ausländern

Die Datenschutzbehörde befasste sich mit mehreren Fällen der mutmaßlich gesetzwidrigen Verarbeitung der personenbezogenen Daten von Ausländern, die sich besuchsweise in der Slowakei aufhielten. Eine Reihe von für die Datenverarbeitung Verantwortlichen erhoben die personenbezogenen Daten von Ausländern auf gesetzwidrigem Wege, indem sie ohne Zustimmung der Datensubjekte die Personaldokumente fotokopierten. Andere für die Datenverarbeitung Verantwortliche verarbeiteten bei Hotelbuchungen mehr personenbezogene Daten als für diesen Zweck erforderlich. Zu den Daten, deren Verarbeitung im Rahmen der Beherbergung unnötig war, zählten beispielsweise: Beruf, Angaben zum Arbeitgeber, Personenkennzahl und Geburtsort. Die Datenschutzbehörde erließ eine Anordnung, damit sich dies in Zukunft nicht wiederholt.

Verarbeitung der Krankenakte eines Patienten während des Transports

Die Datenschutzbehörde befasste sich mit einem Fall, in dem die personenbezogenen Daten eines Patienten während seiner Verlegung in ein anderes Krankenhaus unzureichend geschützt wurden. Die Krankenakte des Patienten wurde in die Obhut eine Krankenwagenfahrers gegeben, der die Akte auf das Fahrzeugdach legte und vergaß, sie vor dem Losfahren wieder herunterzunehmen. Gemäß dem Gesetz über das Gesundheitswesen und Dienstleistungen in dessen Umfeld liegt die Haftung für den Schutz von Krankenakten zur Gänze beim Gesundheitsdienstleister in seiner Funktion als für die Datenverarbeitung Verantwortlicher des betreffenden Informationssystems. Es wurde festgestellt, dass kein Vertrag über die Verarbeitung von personenbezogenen Daten durch einen mit der Datenverarbeitung Beauftragten (in diesem Fall: mit dem Krankentransportunternehmen) vorlag. Daher betrachtete die Datenschutzbehörde den Gesundheitsdienstleister als den für die Datenverarbeitung Verantwortlichen des betreffenden Informationssystems, der somit umfassend für den Verlust der Krankenakte haftet. Die Datenschutzbehörde hat das Gesundheitsministerium über den Fall informiert und zum Erlass einer einheitlichen Verordnung für sämtliche medizinischen Einrichtungen aufgefordert, die diesen Leitlinien für den ordnungsgemäßen Umgang mit Krankenakten in derartigen Situationen an die Hand geben soll.

Pensionsfonds

Die Datenschutzbehörde leitete ein Verfahren wegen der gesetzwidrigen Verbreitung von personenbezogenen Daten durch den für die Datenverarbeitung Verantwortlichen eines Pensionsfonds ein. Aufgrund des Gesetzes über kapitalgebundene Rentenversicherungen sind die Pensionsfonds nun verpflichtet, die Versicherten in regelmäßigen Abständen über ihren Kontostand zu informieren. In der Praxis versandten die Pensionsfonds an Versicherte, die eine solche Auskunft verlangten, per E-Mail einen Kontoauszug. Dabei kam es zuweilen vor, dass ein Versicherter einen Auszug mit den personenbezogenen Daten eines anderen Versicherten erhielt. Die Untersuchung ergab, dass der für die Datenverarbeitung Verantwortliche die Kontoauszüge als unverschlüsselte Datei im Anhang von E-Mails verschickt hatte. Bei der serienweisen Abarbeitung kam es zu Verwechslungen der E-Mail-Adressen bzw. der Anhänge.

Internationale Zusammenarbeit

Im Rahmen des Aufbaus von Partnerschaften mit anderen mittel- und osteuropäischen Datenschutzbehörden fand eine Reihe von Gesprächen statt:

- Im März 2006 wurde in der Tschechischen Republik ein zweitägiges Treffen mit Vertretern der tschechischen Datenschutzbehörde ÚOOÚ abgehalten. Dabei wurden unterschiedliche Themen erörtert, darunter der derzeitige Stand des

Schutzes der Privatsphäre bei der Kommunikation zwischen der öffentlichen Verwaltung und den Bürgern, die Vorbereitungen für den Beitritt zum Schengener Abkommen, die Durchführung der Überwachungsaufgaben im SIS sowie das Verhältnis zwischen den Kontrollbehörden, den Inspektionsaufgaben und dem grenzüberschreitenden Datenfluss. Hauptergebnis des Treffens war die Verabschiedung eines gemeinsamen Memorandums über Kooperation. Die Beziehungen zwischen den Partnerbehörden wurden als sehr gut eingestuft, besser als der europäische Standard, besonders dank der gemeinsamen Geschichte, der problemlosen sprachlichen Verständigung und im Hinblick auf die zu klärenden Fragen.

- Im Juli 2006 fanden in Bratislava zweitätige Gespräche mit Vertretern der kroatischen Datenschutzbehörde statt. Hauptthemen waren die Durchführung der Kontroll- und Inspektionsaufgaben der Behörden sowie Fragen der internen organisatorischen Abläufe.

- Auch in Rumänien wurden Gespräche geführt, bei denen der Leiter der slowakischen Datenschutzbehörde die Partner über die slowakische Gesetzgebung zum Zugang zu Daten der öffentlichen Verwaltung, zum Zugriff auf der Geheimhaltung unterliegende Akten und zur Meldung von Dateisystemen, die personenbezogene Daten enthalten, informierte.

Slowenien

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

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

Am 30. November 2005 verabschiedete die Nationalversammlung das Gesetz über den Datenschutzbeauftragten[2], das am 31. Dezember 2005 in Kraft trat. Mit diesem Gesetz wurde das Amt des Datenschutzbeauftragten *(Informacijska pooblaščenec)* eingerichtet, d. h. die beiden bisherigen Ämter (Inspektionsbehörde für den Schutz personenbezogener Daten und Beauftragter für den Zugang zu Informationen der öffentlichen Verwaltung) wurden in eine neue, eigenständige und unabhängige Einrichtung mit klaren Aufgaben und Befugnissen überführt. Der Datenschutzbeauftragte nahm seine Tätigkeit am letzten Tag des Jahres 2005 auf und übernahm die Aufgaben, Zuständigkeiten und Mitarbeiter der beiden genannten Vorgängerbehörden.

Der Datenschutzbeauftragte ist zuständig für:

- Entscheidung über eine Beschwerde gegen eine Entscheidung, mit der eine Einrichtung einen Antrag auf Zugriff verweigert oder ablehnt oder das Zugriffsrecht oder die Wiederverwendung öffentlicher Informationen in einer anderen Weise verletzt, sowie im Rahmen derartiger Beschwerdeverfahren auch für die Überwachung der Umsetzung des Gesetzes zur Regelung des Zugangs zu Informationen der öffentlichen Verwaltung und der zugehörigen Durchführungsverordnungen;
- Inspektion und Überwachung der Umsetzung des Gesetzes und sonstiger Regelungen zum Schutz und zur Verarbeitung personenbezogener Daten sowie zur Übermittlung von personenbezogenen Daten aus Slowenien, sowie die Erfüllung anderer, in diesen Regelungen festgelegten Pflichten;
- Entscheidung über die Beschwerde einer Einzelperson, wenn der für die Datenverarbeitung Verantwortliche deren gemäß den Bestimmungen des Gesetzes über den Schutz personenbezogener Daten gestellten Antrag auf Datenzugriff, d. h. einen Auszug, eine Liste, eine Prüfung, eine Bestätigung, eine Informationen, eine Erklärung, ein Transkript oder eine Kopie, ablehnt;
- Einreichung eines Antrags an das Verfassungsgericht der Republik Slowenien zur Prüfung der Verfassungsmäßigkeit von Gesetzen, sonstigen Verordnungen und allgemeinen Gesetzen, die zur Ausübung der öffentlichen Gewalt erlassen wurden, wenn die Frage der Verfassungsmäßigkeit und Rechtmäßigkeit in Verbindung mit einem von ihm eingeleiteten Verfahren (in Fällen des Zugriffs auf Daten der öffentlichen Verwaltung bzw. des Schutzes von personenbezogenen Daten) auftaucht.

Der Datenschutzbeauftragte ist außerdem ein Amtsträger, der Verletzungen ahnden muss: Ihm obliegt die Überwachung des Gesetzes über den Datenschutzbeauftragten und des Gesetzes über den Schutz personenbezogener Daten.

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

Der Datenschutzbeauftragte nimmt regelmäßig an Sitzungen der EU-Arbeitsgruppen teil, die sich mit dem Schutz personenbezogener Daten befassen, sowie an Treffen von Datenschutzbehörden der EU-Mitgliedstaaten, die im Rahmen der Richtlinie 95/46/EG abgehalten werden (Artikel-29-Datenschutzgruppe, sowie die Arbeitsgruppen, die sich mit der Verarbeitung personenbezogener Daten bei Europol und Eurojust befassen). Innerhalb der

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

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

Artikel-29-Datenschutzgruppe hat der slowenische Datenschutzbeauftragte auch einen Vertreter in zwei Unterausschüssen – ITF und SWIFT.

Die Richtlinie 2002/58/EG wurde durch Änderungen am Gesetz über elektronische Kommunikation in slowenisches Recht umgesetzt[3], das am 9. April 2004 angenommen wurde und am 1. Mai 2004 in Kraft trat. Kapitel 10 des Gesetzes reguliert insbesondere den Schutz personenbezogener Daten sowie den Schutz der Privatsphäre und der Vertraulichkeit in elektronischen Kommunikationen.

Am 28. November 2006 wurde in Slowenien das Gesetz zur Änderung des Gesetzes über elektronische Kommunikation[4] verabschiedet, das die Richtlinie 2006/24/EG zur Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, umsetzt. Das Gesetz, das am 27. Dezember 2006 in Kraft trat, sieht vor, dass alle slowenischen Anbieter von Telekommunikationsdienstleistungen (Internetzugang, E-Mail, Telefon, Mobiltelefon usw.) sämtliche Verkehrsdaten ihrer Kunden für einen Zeitraum von zwei Jahren speichern müssen. Die gesetzlichen Bestimmungen über die Vorratsspeicherung von Telefondaten sollen am 15. September 2007 in Kraft treten, während die Regelungen über die Datenspeicherung bei Internetzugang, E-Mail und Internettelefonie (VoIP) am 15. März 2009 rechtswirksam werden sollen.

Der Datenschutzbeauftragte muss zudem die Durchführung des Schengener Abkommens gemäß dessen Artikel 128 überwachen. Dabei überwacht eine unabhängige Einrichtung die Übermittlung personenbezogener Daten, um die Einhaltung des Übereinkommens zu gewährleisten.

B. Bedeutende Rechtsprechung

Das Datenschutzgesetz definierte auch Bedingungen, unter denen biometrische Maßnahmen zu genehmigen 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 von vertraulichen Daten und Geschäftsgeheimnissen als unbedingt notwendig erweisen. In solchen Fällen müssen die für biometrische Maßnahmen Verantwortlichen der Überwachungsbehörde eine vorherige Beschreibung der geplanten biometrischen Maßnahmen und die Gründe für deren Einführung übermitteln. Der Gebrauch biometrischer Maßnahmen ist nur nach dem Erhalt der Einwilligung seitens der Behörde zur Verwendung biometrischer Maßnahmen erlaubt. Hier kam es jedoch 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 Datenschutzbeauftragte, dass solche für Datenverarbeitung Verantwortliche der Aufsichtsbehörde eine Beschreibung der biometrischen Maßnahmen und die Gründe für ihre Einführung übermitteln müssen, und sie erst dann befugt sind, diese weiter zu gebrauchen, wenn sie die entsprechende Entscheidung der Behörde erhalten haben.

Im Jahr 2006 erließ der Datenschutzbeauftragte insgesamt neun Entscheidungen zur Ausführung biometrischer Maßnahmen, von denen vier juristische Personen des privaten Rechts und fünf juristische Personen des öffentlichen Rechts betrafen, wobei alle Betroffenen aus den Bereichen Banken, Gesundheitswesen bzw. Telekommunikation stammten. Anträge auf Genehmigung der Ausführung biometrischer Maßnahmen wurden in zwei Fällen gebilligt, in zwei weiteren Fällen geschah dies nur zum Teil und in fünf Fällen wurden sie abgelehnt. Der Datenschutzbeauftragte genehmigte den Einsatz der biometrischen Fingerabdruck-Identifizierung beim Zugang von Mitarbeitern zu geschützten Produktionsbereichen und bei der Individualisierung von Bankkarten und anderen

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

[4] Staatliches Amtsblatt der Republik Slowenien, Nr. 129/2006

Visitenkarten in Form von Chipkarten zur allgemeinen Nutzung sowie bei Überprüfungen des Zugangs von Mitarbeitern zu Systembereichen mit Betriebsgeheimnissen (Aufzeichnungen über Kartenbesitzer, Finanztransaktionen, Kartenbetrugsfälle usw.). Der Datenschutzbeauftragte 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 Geschäftstätigkeit 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.

Aufgrund festgestellter Unregelmäßigkeiten musste eine der verantwortlichen Rechtspersonen die Nutzung aller biometrischen Datenlesegeräte einstellen, die davor verwendet wurden, um die Anwesenheit der Mitarbeiter am Arbeitsplatz zu überprüfen.

Im Jahr 2006 traf der Datenschutzbeauftragte mehrere Entscheidungen, über die in den nationalen Medien umfassend berichtet wurde:

1. Eine Entscheidung in Bezug auf ein geringfügiges Vergehen einer Bekleidungsfirma im Einzelhandel, die Geschäftsräume in ihrem Kaufhaus, insbesondere Umkleidekabinen, per Video überwachen ließ, was einen Verstoß gegen das Gesetz zum Schutz personenbezogener Daten darstellt, das die Videoüberwachung in Umkleidekabinen, Aufzügen und Toiletten untersagt. Bei der Untersuchung stellte sich heraus, dass Videobänder gespeichert wurden und dass der Zugang zum Videoüberwachungssystem nicht auf geeignete Weise geschützt war, während es gleichzeitig keine Belege für die Speicherung auf Wechseldatenträgern gab. Der Datenschutzbeauftragte veranlasste den Urheber zur sofortigen Beendigung der Videoüberwachung in den Umkleidekabinen, was auch unverzüglich geschah. Zusätzlich dazu verhängte der Datenschutzbeauftragte eine Geldbuße wegen Verstoßes gegen gesetzliche Bestimmungen, da der Urheber einen schwerwiegenden Verstoß gegen die Privatsphäre und Würde der Personen, die die fraglichen Umkleidekabinen nutzen, verübte und folglich ihre Grundrechte auf persönliche Würde, Sicherheit und Privatsphäre verletzte.

2. Eine Entscheidung wegen eines geringfügigen Vergehens einer Verlagsgesellschaft, die in ihrer Wochenzeitung Namen von 86 Mitarbeitern eines Konkurrenzunternehmens mit dem höchsten Netto- und Bruttoeinkommen veröffentlichte, das heißt personenbezogene Daten von 86 Beschäftigten illegal verwendete, verarbeitete und der Öffentlichkeit preisgab, und zwar ohne gesetzliche Grundlage und ohne die persönliche Einwilligung der Betroffenen zur Verarbeitung dieser Daten. Der betreffende Fall betraf die Verarbeitung personenbezogener Daten von Mitarbeitern des Privatsektors, die im Gesetz über Arbeitsbeziehungen ausführlicher geregelt ist[5].

Gemäß den Bestimmungen des genannten Gesetzes sowie des Gesetzes über den Schutz personenbezogener Daten hätte die Zeitung Daten über die Gehälter von Beschäftigten nur für den Fall veröffentlichen können, dass dies für die Wahrnehmung der Rechte und Pflichten aufgrund der Beschäftigungsbeziehungen oder in Verbindung mit den Beschäftigungsbedingungen oder mit der ausdrücklichen Einwilligung des Einzelnen notwendig gewesen wäre.

Die Öffentlichkeit der Höhe von Bezügen wurde ausschließlich für den öffentlichen Sektor festgelegt[6], mit dem ausdrücklichen Zusatz, dass öffentliche Handelsgesellschaften und Handelsgesellschaften, deren Mehrheitseigentümer der Staat ist (wie im Falle der Verlagsgesellschaft), in diesem Sinne nicht unter den öffentlichen Sektor fallen.

[5] Staatliches Amtsblatt der Republik Slowenien, Nr. 42/2002 und 79/2006

[6] Staatliches Amtsblatt der Republik Slowenien Nr. 56/2002 *(Zakon o sistemu plač v javnem sektorju)*.

Die Wochenzeitung berief sich auf die Meinungsfreiheit und das öffentliche Interesse, übersah jedoch die Regelung in Paragraf 3 Artikel 15 der Verfassung und Artikel 10 der Europäischen Menschenrechtskonvention, der zufolge Menschenrechte und Grundfreiheiten aufgrund der Rechte anderer eingeschränkt sind. Darüber hinaus wurde die Meinungsfreiheit bereits zuvor durch das Mediengesetz eingeschränkt[7], wonach die Wochenzeitung nur für den Fall berechtigt gewesen wäre, die strittigen Daten entgegenzunehmen und zu veröffentlichen, dass eine solche Handlung eine schwere Straftat oder unmittelbare Gefahr für das Leben und das Eigentum von Menschen abwenden könnte, was in dieser Angelegenheit nicht gegeben war. Die Datenveröffentlichung verstieß gegen die in der Verfassung verbrieften Rechte auf persönliche Würde, Sicherheit und Privatsphäre, ferner gegen die Persönlichkeitsrechte sowie gegen das Recht auf den Schutz personenbezogener Daten.

3. Eine Entscheidung in Bezug auf ein geringfügiges Vergehen einer Zeitung wegen der Veröffentlichung von Autopsieberichten über drei Minderjährige, die nach einem Vorfall in einer Diskothek ums Leben kamen. Wie im vorausgegangenen Fall berief sich der Urheber auf die Meinungsfreiheit und das öffentliche Interesse. Diese Rechte konnten jedoch nicht die Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Privatsektor sein, vor allem bei medizinisch sensiblen Daten, wie den personenbezogenen Daten der Verstorbenen, deren Handhabung durch das Gesetz über den Schutz personenbezogener Daten besonders geregelt ist. Die Verarbeitung der personenbezogenen Daten erfolgte zudem nicht im Einklang mit dem ursprünglichen Zweck. Die Autopsieberichte wurden nämlich zur Verwendung im Strafverfahren gegen den Diskothekenbesitzer verfasst, und nicht zur Veröffentlichung in den Medien.

Der Datenschutzbeauftragte untersuchte ferner die Rechtmäßigkeit der Verarbeitung personenbezogener Daten bei klinischen Studien zu Arzneimitteln, das Verfahren für den Schutz personenbezogener Patientendaten und das Verfahren für den Zugriff auf solche Daten. Im Hinblick auf die vorherige Einholung einer individuellen schriftlichen Erklärung des Patienten zur Teilnahme an den klinischen Studien wurden keine Unregelmäßigkeiten festgestellt. Es wurde jedoch aufgezeigt, dass keine Kataloge über Archivierungssysteme für personenbezogene Daten mit Angaben zu den klinischen Studien angelegt wurden, dass keine Aufzeichnungen über die Zugriffe auf Archive mit Patientendaten geführt wurden und dass keine Maßnahmen zu Gewährleistung der Nachverfolgbarkeit getroffen wurden. Bei der Inspektion stellte die betreffende medizinische Einrichtung die Zuständigkeit der Datenschutzbehörde in dem betreffenden Fall in Frage. Es wurden Aussagen von medizinrechtlichen Gutachtern angeführt, denen zufolge die Datenschutzbehörde die Einwilligung der Patienten einholen müsse, bevor sie personenbezogene Daten sichte. Diesen medizinrechtlichen Gutachtern zufolge würden die Ärzte, indem sie den staatlichen Inspektoren die geforderten Unterlagen zeigen, gegen den Kodex für ärztliche Ethik verstoßen und dadurch die Vertraulichkeit zwischen Arzt und Patienten untergraben. Aus dem genannten Grund lehnte die medizinische Einrichtung die Überprüfung und Aushändigung schriftlicher Einwilligungen der Patienten ab und setzte das Verfahren trotz der unmissverständlichen Bedeutung dieser gesetzlichen Bestimmungen (Paragraf 2 und 8 des Gesetzes über den Datenschutzbeauftragten und Paragraf 51 und 52 des Gesetzes über den Schutz personenbezogener Daten) aus, wonach der Schutz personenbezogener Daten und die Durchführung der Bestimmungen des Gesetzes über den Schutz personenbezogener Daten und sonstiger Regelungen zum Schutz oder zur Verarbeitung solcher Daten in der alleinigen Zuständigkeit des Datenschutzbeauftragten als nationale Behörde für den Datenschutz liegt.

Im Hinblick auf eine gütliche Lösung in dieser Angelegenheit schlug das Ministerium für öffentliche Verwaltung vor, die ärztlichen Unterlagen von einem gerichtlich bestellten Sachverständigen prüfen zu lassen. Trotz der umfassenden gesetzlichen

[7] Staatliches Amtsblatt der Republik Slowenien, Nr. 110/2006

Zuständigkeit des Datenschutzbeauftragten für die inhaltliche Prüfung von Archivierungssystemen mit personenbezogenen Daten unabhängig von ihrer Vertraulichkeit oder Geheimhaltung stimmte der Datenschutzbeauftragte der vorgeschlagenen Lösung zu.

Im Jahr 2006 reichte der Datenschutzbeauftragte zwei Anträge auf eine gerichtliche Nachprüfung ein:

1. Die richterliche Nachprüfung von Absatz 7 und 8 Paragraf 128 Luftfahrtgesetz[8], das Bewegungen von Personen auf dem Gelände des öffentlichen Flughafens sowie im Bereich der Flugverkehrskontrolle regelt. Nach Auffassung des Datenschutzbeauftragten ist die betreffende Bestimmung mit den Artikeln 2, 15 und 38 der Verfassung und mit Artikel 8 der Europäischen Menschenrechtskonvention nicht vereinbar. Daher empfahl er die Aufhebung dieser Bestimmung und die Aussetzung ihrer Inkraftsetzung, bis das Verfassungsgericht seine endgültige Entscheidung getroffen hat.

Der betreffende Artikel stellt in seiner jetzigen Form einen schweren Verstoß gegen das in der Verfassung verankerte Recht auf den Schutz personenbezogener Daten dar, da er darauf abzielt, eine unangemessen hohe Zahl von personenbezogenen Daten zu erfassen, eine Tatsache, die im Hinblick auf das öffentliche Interesse und die öffentliche Sicherheit weder vernünftig noch angemessen erscheint, die beide Wesensmerkmale einer demokratischen Gesellschaft sind. Im Luftfahrtgesetz fehlt eine zur Gewährleistung der Rechtssicherheit der betroffenen Personen hinreichend klare Definition des Zwecks der Erfassung oder Verarbeitung personenbezogener Daten. Darüber fehlt im Luftfahrtgesetz die geforderte explizite Aufzählung der zu verarbeitenden personenbezogenen Daten, sondern es werden vielmehr nur Beispiele für zu erfassende personenbezogene Daten geliefert.

Obwohl das Gesetz an sich vorsieht, personenbezogene Daten direkt bei den Betroffenen mit ihrer ausdrücklichen Einwilligung einzuholen, sollte die Einrichtung solcher Archivierungssysteme für personenbezogene Daten dem Verhältnismäßigkeitsprinzip unterliegen. Es widerspricht nämlich dem Grundsatz der Verhältnismäßigkeit, Daten über den Zeitraum des Aufenthalts, Studiums oder Besuchs im Ausland, Daten über geringfügige Vergehen und schwebende Strafverfahren, erlassene Disziplinarmaßnahmen sowie Art und Umfang von eingegangenen finanziellen Verpflichtungen zu erheben. Die Forderung, sensible personenbezogene Daten offenzulegen, die über den ursprünglichen Zweck der Erhebung hinausgehen (Alkohol- und Drogenmissbrauch, psychische Probleme und Erkrankungen), ist ebenfalls verfassungswidrig.

2. Richterliche Nachprüfung von Paragraf 1 Artikel 96, Paragraf 2 Artikel 98, Artikel 100, Paragraf 5 und 6 von Artikel 103 und Paragraf 1 von Artikel 114 des Gesetzes über das Grundstückskataster[9], das u. a. die Erfassung von Grundstücken, den Grundstückskataster, die Herausgabe von Daten sowie andere Immobilien betreffende Fragen regelt. Die betreffenden Bestimmungen des Gesetzes regeln die Erhebung mehrerer Arten von personenbezogenen Daten, liefern jedoch diesbezüglich keine konkrete Zweckbestimmung, weshalb das Gesetz ungenau, zu breit gefasst und unscharf definiert ist. Ohne gesetzliche Zweckbestimmung der Datenerhebung kann weder die Art noch der Umfang der für die Verarbeitung notwendigen Daten festgelegt werden.

Darüber hinaus sollen die erhobenen personenbezogenen Daten gemäß Artikel 114 des Gesetzes über die Erfassung der Grundstücke in den Grundstückskataster aufgenommen werden, der Bestandteil der staatlichen Archive ist. Die Umstand, dass die gesetzlichen Bestimmungen keine eindeutige Zweckbestimmung für die Nutzung personenbezogener Daten definieren, bewirkt, dass diese Daten veröffentlicht und allen möglichen Zwecken genutzt werden könnten, was eindeutig der Verfassung widersprechen würde.

[8] Staatliches Amtsblatt der Republik Slowenien, Nr. 18/2001, 110/2002, 49/2006, 79/2006

[9] Staatliches Amtsblatt der Republik Slowenien, Nr. 47/2006

Gemäß Artikel 100 wird der Grundstückskataster zusätzlich zu den Daten aus der Volkszählung daher auch durch andere Datenbanken ergänzt. Eine solche Bündelung der Daten in einem einheitlichen öffentlichen Grundstücksregister ist unter dem Gesichtspunkt des Schutzes personenbezogener Daten unvertretbar. Mit anderen Worten: Das Gesetz über den Schutz personenbezogener Daten legt einen dezentralen Ansatz für Registerarchive mit personenbezogenen Daten nahe. Im Hinblick auf die Anzahl der in den öffentlich zugänglichen Grundstückskataster aufgenommenen personenbezogenen Daten weist der Datenschutzbeauftragte darauf hin, dass die vorgeschlagene Lösung dem Grundsatz der Verhältnismäßigkeit nicht entspricht. Es sei nicht nur unangemessen, eine übermäßig hohe Zahl an personenbezogenen Daten zu erheben, sondern vor allem auch, sie zu veröffentlichen und darüber hinaus in einem einheitlichen, öffentlich zugänglichen Archiv zusammenzuführen. Die Veröffentlichung solcher Daten verstößt gegen den Verfassungsgrundsatz der Unantastbarkeit privaten Eigentums. Ferner besteht eine reale Gefahr, dass Einzelne solche öffentlich zugänglichen Daten für verschiedene, nicht näher bestimmte Verwendungszwecke nutzen, was unter dem Gesichtspunkt der Rechtssicherheit nicht zu vertreten ist.

C. Wichtige spezifische Themen

Das 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. Dies bedeutet: über die Ausführung einer Videoüberwachung einen förmlichen Beschluss zu fassen, 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 zahlreichen Beschwerden bei der Behörde führt.

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

Eines der fortbestehenden Hauptprobleme im Bereich der personenbezogenen Daten ist auf die Tatsache zurückzuführen, dass die meisten für die Datenverarbeitung Verantwortlichen der Datenschutzbehörde bisher noch keine 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 zu den Dateisystemen der für die Datenverarbeitung Verantwortlichen in der Republik Slowenien, Informationen über die von den einzelnen für die Datenverarbeitung Verantwortlichen verwalteten Dateisystemen, Typen von in den einzelnen Dateisystemen enthaltenen personenbezogenen Daten, den Verarbeitungszweck usw. einzusehen.

Anfang 2006 hatten nur ungefähr 1.000 für Datenverarbeitung Verantwortliche (in Slowenien gibt es ungefähr 140.000) die von ihnen verwalteten Registersysteme für personenbezogene Daten gemeldet. Den gesetzlichen Bestimmungen zufolge sollten die für Datenverarbeitung Verantwortliche ihre Daten bis spätestens am 1. Oktober 2006 übermitteln. Nach dieser Frist erließ der Datenschutzbeauftragte Bußgelder gegen die verantwortlichen juristischen Personen. Das Register beinhaltet den Großteil der für die Datenverarbeitung Verantwortlichen des öffentlichen Sektors, wohingegen ein erheblicher Teil der für die Datenverarbeitung Verantwortlichen des privaten Sektors sich über ihre Meldepflichten offenbar noch nicht im Klaren sind.

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. Im Jahr 2006 gab der Datenschutzbeauftragte insgesamt 616 Stellungnahmen zur Rechtslage ab.

Im gleichen Jahr führten die staatlichen Inspektoren für den Schutz personenbezogener Daten (ab April 2006 sind beim Datenschutzbeauftragten sieben Inspektoren beschäftigt) 230 Inspektionen durch, davon 87 im öffentlichen und 143 im privaten Sektor.

Spanien

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

- Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates wurde durch das Gesetz 15/1999 vom 13. Dezember 1999 über den Schutz personenbezogener Daten in spanisches Recht umgesetzt (*Ley Orgánica de Protección de Datos de Carácter Personal* - LOPD)[1].

Im gesamten Jahresverlauf 2006 arbeitete die spanische Datenschutzbehörde weiter an der Vorbereitung der Allgemeinen Durchführungsverordnung zum Gesetz über den Schutz personenbezogener Daten, das derzeit den formalen Weg durch die Instanzen des Justizministeriums beschreitet. Die Verabschiedung wird für das erste Halbjahr 2007 erwartet.

Während des Jahres 2006 wurden folgende Verordnungen mit Relevanz für den Datenschutz genehmigt:

1. Gesetz 7/2006 über den Schutz der Gesundheit und die Bekämpfung des Dopings im Sport

Dieses Gesetz regelt die Verarbeitung von Daten über Doping und Gesundheit im Sport. Aufgrund seiner Auswirkungen für das Grundrecht auf den Schutz personenbezogener Daten richtete die spanische Datenschutzbehörde (*Agencia Española de Protección de Datos* - AEPD) ihr besonderes Augenmerk darauf, sicherzustellen, dass geeignete Sicherheitsvorkehrungen getroffen werden, um einen Verstoß gegen dieses Recht zu unterbinden. Der Gesetzestext beschränkt die Datenverarbeitung auf die ermittelten und benannten Zwecke, für die eine Genehmigung vorliegt, so dass die Informationen nur zur Dopingkontrolle oder Anzeige solcher Straftaten verwendet werden können. Gleichermaßen sind Dopingkontrolleure zur Verschwiegenheit verpflichtet. Auf besonders geschützte Daten haben sie nur begrenzten Zugriff, und um den Zugang zu bestimmten Bereichen zu schützen, sind die Daten zu trennen. Für die neue Gesundheitskarte für Sportler sind Sicherheitsmaßnahmen auf hohem Niveau erforderlich.

2. Gesetz 29/2006 vom 26. Juli 2006 über Garantien und den vernünftigen Umgang mit Arzneimitteln und sonstigen Medizinprodukten.

Dieses Gesetz regelt u. a. klinische Studien von Arzneimitteln, ärztliche Verschreibungen sowie die Zusammenarbeit verschiedener öffentlicher und privater Einrichtungen im Hinblick auf den vernünftigen Umgang mit Arzneimitteln, einschließlich der sich im Rahmen dieser Zusammenarbeit ergebenden Datenübermittlungen. In einem Bericht aus dem Jahr 2005 stellte die AEPD eine Reihe von Überlegungen in diesem Zusammenhang an: Unter anderem wurde auf die Notwendigkeit verwiesen, die Bedürfnisse zu ermitteln und die Fälle zu benennen, in denen für die Verarbeitung und Weitergabe von Daten aus dem elektronischen Verschreibungssystem keine Einwilligung des Datensubjekts erforderlich ist. Ferner wurde betont, dass die Veröffentlichung der Ergebnisse einer klinischen Studie ausnahmslos nach der Abtrennung von den personenbezogenen Daten der Datensubjekte erfolgen muss, sowie dass grundsätzlich sämtliche Datenverarbeitungen an die Grundsätze des Datenschutzgesetzes angepasst werden müssen.

3. Leitlinie 1/2006 der spanischen Datenschutzbehörde vom 8. November 2006, über die Verarbeitung personenbezogener Daten im Rahmen der Überwachung mit Kamera- oder Videokamerasystemen

Mit dieser Leitlinie zielt die AEPD darauf ab, die zu Zwecken der Überwachung vorgenommene Bildverarbeitung an die Grundlagen des Datenschutzgesetzes anzupassen und die Rechte von Personen zu gewährleisten, deren Bilder mit derartigen Verfahren verarbeitet werden. Dies schließt sowohl personenbezogene Daten aus, die für den Heimgebrauch aufgenommen

[1] ES: https://www.agpd.es/upload/Canal_Documentacion/legislacion/Estatal/Ley%2015_99.pdf
EN: https://www.agpd.es/upload/Ley%20Org%E1nica%2015-99_ingles.pdf

werden, als auch die Bildverarbeitung seitens der staatlichen Sicherheitskräfte und seitens privater Sicherheitsdienste in Ausführung ihrer regulären Aufgaben, wobei diese durch andere spezifische Rechtsvorschriften geregelt ist und ebenfalls die im Datenschutzgesetz 15/1999 festgelegten Garantien respektieren muss. Der Anwendungsbereich dieser Leitlinie umfasst die Aufnahme, das Sammeln, die Übermittlung, die Aufbewahrung und die Speicherung von Bildern, einschließlich ihrer Vervielfältigung oder Ausstrahlung in Echtzeit, sowie die Verarbeitung der zugehörigen personenbezogenen Daten. Die Installation von Kameras oder Videokameras wird nur dann für zulässig befunden, wenn der Zweck der Überwachung nicht ohne unverhältnismäßig hohen Aufwand durch andere Mittel erfüllt werden kann, die in die Privatsphäre des Einzelnen und sein Recht auf den Schutz personenbezogener Daten weniger eingreifen. Die Leitlinie sieht ferner vor, das Informationsrecht zu garantieren, sowie dass in allen Fällen eine im Verhältnis zum angestrebten Zweck unangemessene Datenverarbeitung zu vermeiden ist.

4. Gesetz 16/2006 vom 26. Mai 2006 über das Statut des Nationalen Mitglieds von Eurojust und die Beziehungen zur Europäischen Union

Im Jahresverlauf 2006 konnte die spanische Datenschutzbehörde AEPD außerdem verschiedene Gesetzesinstrumente mit Relevanz für den Datenschutz erstellen, indem sie von ihrer Rechtsabteilung Berichte mit verbindlichem Charakter ausarbeiten ließ. Zu den wichtigsten in Bearbeitung befindlichen Vorschlägen gehören folgende:

- Gesetzentwurf über biomedizinische Forschung
- Gesetzentwurf gegen Gewalt, Rassismus, Fremdenhass und Intoleranz im Sport
- Gesetzentwurf über die Aufbewahrung von Daten über elektronische Kommunikationen
- Gesetzentwurf über die Aufbewahrung von Polizeidatenbanken über DNS-Identifikationsmerkmale
- Gesetzentwurf über die elektronische Verwaltung

- Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

Diese Richtlinie wurde durch das Gesetz 32/2003 vom 3. November 2003 über Telekommunikation in spanisches Recht umgesetzt. Die Ausführungsbestimmungen liefert der Königliche Erlass 424/2005 vom 15. April 2005, der die Bedingungen für die Bereitstellung elektronischer Kommunikationsdienste, den allgemeinen Dienst und den Schutz der Nutzer festlegt.

B. Bedeutende Rechtsprechung

Gemäß Artikel 48 (2) des Datenschutzgesetzes beenden die Entscheidungen durch den Direktor den Verwaltungsweg. Deshalb können die genannten Entscheidungen, auch nach dem Einreichen eines Widerspruchs bei der Behörde, über die Verwaltungsgerichtsbarkeit angefochten werden. Im Jahr 2006 ergingen 120 Urteile des Verwaltungsgerichtshofs. In fünf Fällen erkannte der Oberste Gerichtshof im Interesse der Vereinheitlichung der Rechtsprechung auf Abweisung oder Nichtigkeit von Berufungsanträgen. Dieser Bericht bezieht sich ausschließlich auf solche Urteile, in denen bei kontroversen Fragen Präzedenzfälle geschaffen wurden und Aspekte des Datenschutzes zum Tragen kommen, die eine komplexe Auslegung erfordern.

- Meldung der Eintragung in eine Datei säumiger Schuldner

Die Missachtung der Pflicht, einem Datensubjekt eine schriftliche Bestätigung über seine Aufnahme in eine Datei über eine Vermögensliquidation auszustellen, führt zu keiner Bestrafung des für die Dateiverarbeitung Verantwortlichen, wenn dieser sich an die entsprechende von der Datenschutzbehörde herausgegebenen Verordnung gehalten hat (der zufolge die Meldung seitens des Unternehmens, das die Datei säumiger Schuldner verarbeitet, ausreichend

war) und wenn die Datenschutzbehörde anschließend die Kriterien geändert hat. Eine solche Veränderung der Kriterien, aufgrund deren die Meldung dann als unzureichend eingestuft wurde, darf nicht rückwirkend zu Strafzwecken angewandt werden.

- E-Mail-Adressen sind personenbezogene Daten

Die E-Mail-Adresse einer Person ist eine personenbezogene Angabe, unabhängig davon, ob der Name oder die Adresse mit dem tatsächlichen Vor- und Nachnamen des Inhabers, seinem Land oder der Firma, bei der er arbeitet, übereinstimmen. Dies ergibt sich aus dem Umstand, dass es möglich ist, eine Person durch einen einfachen Vorgang zu identifizieren, weil die elektronische Postadresse an einen spezifischen Domainnamen geknüpft ist und es daher ausreichen würde, den Server zu konsultieren, der diesen Dienst verwaltet.

- Unzulässige Zweckbestimmungen

In seinem Urteil vom April 2006 vertrat das Gericht die Auffassung, dass Öffentlichkeit des Gerichtswegs nicht bedeutet, dass die Gesamtheit der in Gerichtsverfahren in einer Vollstreckungsphase verarbeiteten Dateien durchgesehen und der breiten Öffentlichkeit völlig frei und unterschiedslos zur Verfügung gestellt werden können, sondern vielmehr, dass der Begriff der Öffentlichkeit Beschränkungen unterliegt, ausgenommen bei öffentlichen Anhörung von Datensubjekten. Die betreffenden Gerichtsverfahren dürfen entschieden nicht als öffentlich zugängliche Quellen betrachtet werden.

- Grundsatz der Datenqualität

Dem Gericht legte fest, dass der Grundsatz der Datenqualität einzuhalten ist, wenn personenbezogene Daten in eine Solvenz- und Vermögensakte eingetragen werden. Bei der Überprüfung der betreffenden Daten auf ihren Wahrheitsgehalt ist die erforderliche Sorgfalt zu wahren. Gegen diesen Grundsatz wird zu dem Zeitpunkt verstoßen, ab dem fehlerhafte Daten in eine Akte eingetragen werden, die Informationen Dritter über die Nichterfüllung von Zahlungsverpflichtungen beinhaltet. Zum Zeitpunkt der Informationsübermittlung an eine Solvenzakte muss der für die Datenverarbeitung Verantwortliche mit größter Sorgfalt darüber wachen, dass die Solvenzdaten, die übermittelt werden sollen, wahrheitskonform sind. Sollte der für die Datenverarbeitung Verantwortliche nach der Meldung von einem Datenfehler Kenntnis erlangen, muss er diese innerhalb einer angemessenen Frist berichtigen und die notwendigen Maßnahmen einleiten, um zu verhindern, dass die fehlerhafte Mitteilung durch Weiterverarbeitung offizielle Form annimmt.

- Besonders geschützte Daten

Die elektronische Verarbeitung von Daten über die Mitgliedschaft in einer politischen Partei gibt Aufschluss über die Weltanschauung einer Person, weshalb ihre Einwilligung notwendig ist. Die öffentliche Rolle eines Datensubjekts, das einer politischen Partei angehört, oder ihre gegenüber der Datenschutzbehörde angeführte Ernennung in ein öffentliches Amt, stellen keine hinreichende Begründung für die Nicht-Einholung einer solchen Einwilligung dar. Die Verwendung von Daten über die Weltanschauung einer Person kann u. U. ebenfalls bestraft werden, gleichgültig zu welchem Zweck diese Verwendung erfolgt und selbst wenn eine solche Offenlegung von privaten Daten unabsichtlich geschieht.

- Verstoß gegen den Grundsatz der Einwilligung

Die Verwendung von Daten, auch durch einen Dritten, nachdem ihr Besitzer das Recht auf Löschung ausgeübt hat, stellt einen Verstoß gegen die Verpflichtung dar, eine Einwilligung einzuholen. Das Gericht befand, dass eine Partei, die nicht Inhaber der Datei ist (da diese von einer anderen Partei geliefert wurde), aufgrund der Verwendung der Daten diese einer Verarbeitung unterzieht, was die Einwilligung durch das Datensubjekt erforderlich macht.

C. Wichtige spezifische Themen

1. Transparenz:

- Vor dem Parlament

1.a) Erscheinen des Direktors der Datenschutzbehörde vor dem Parlament

- Erscheinen vor der Kommission des Ministeriums für Bildung und Wissenschaft zum Gesetzentwurf zur Bekämpfung des Dopings im Sport

Im Juni 2006 legte der Direktor der AEPD vor dem Parlament die Überlegungen der Datenschutzbehörde zu dem vor der Verabschiedung stehenden Gesetzentwurf über den Schutz der Gesundheit und die Bekämpfung des Dopings im Sport dar. Während seines Vortrags im Parlament betonte der Direktor der AEPD; dass der Gesetzentwurf, der spezielle Vorschriften zur Datenverarbeitung in den Bereichen Doping und Gesundheit im Sport beinhaltet, die Bemerkungen der juristischen Abteilungen hinsichtlich des Datenschutzgesetzes angemessen berücksichtigt. Insbesondere gilt dies für die Einhaltung des Grundsatzes der Zweckmäßigkeit und der Verschwiegenheitspflicht, ferner für die Bestimmung, dass die Informationen nur zur Dopingkontrolle oder zur Meldung diesbezüglicher Tatbestände genutzt werden dürfen sowie für den Umstand, dass Personen oder Instanzen, die Dopingkontrollaktivitäten durchführen, eine Verschwiegenheitspflicht auferlegt wird. Für den Zugriff auf besonders geschützte Daten wurden zudem spezifische Beschränkungen festgelegt.

- Erscheinen vor dem Verfassungsausschuss zur Vorlage des Jahresberichts 2005

Am 11. Oktober 2006 stellte der Direktor der spanischen Datenschutzbehörde AEPD auf eigenes Ersuchen dem Parlament den Jahresbericht 2005 vor. In seinem Vortrag wies er darauf hin, dass die Angaben des Jahresberichts der Behörde auf eine zunehmend verbreitete Kenntnis der „Datenschutzkultur" bei Unternehmen und Bürgern in Spanien hinweisen. Ferner führte er aus, dass immer häufiger Forderungen nach Maßnahmen laut werden, um eine effiziente Anwendung der im Datenschutzgesetz vorgesehenen Garantien zu gewährleisten. Der Direktor berichtete über die steigende Anzahl der Zugriffe, Berichtigungen, Löschungen und Einwände von Bürgern, eine Tatsache, die verdeutliche, dass sich die Bürger dafür interessieren, welche Informationen über sie gespeichert werden, und dass sie in vielen Fällen deren Löschung wünschen. Die Zahlenangaben über die Tätigkeit der Behörde wurden ebenfalls aufgeschlüsselt: Hierzu gehört eine Zunahme der Einträge in das Allgemeine Datenschutzregister um 40%, eine um 42% gestiegene Anzahl der Bußgeldverfahren sowie deutlich vermehrte Anfragen seitens der Bürger.

2. Durchführung

2.a) System für Telematikmeldungen an die Datenschutzbehörde (*Notificaciones Telemáticas a la AEPD* - NOTA)

Im Juli 2006 stellte die Datenschutzbehörde AEPD das System für Telematikmeldungen (NOTA) vor. Es ist das erste elektronische Verwaltungssystem, das von der Behörde bereitgestellt wird. Ziel dieses Systems, das sowohl von öffentlichen als auch von privaten Einrichtungen genutzt werden kann, ist es, die Dateimeldepflichten zu erleichtern und zu vereinfachen. Mit NOTA können drei Datentypen gemeldet werden: durch telematische Mittel unter Einsatz der elektronischen Signatur, mit im NOTA-System ausgefüllten Ausdrucken (auf denen sich ein automatisch lesbarer Stempel zur beschleunigten Erfassung befindet) sowie im XML-Format über Internet, mit oder ohne anerkanntes Signaturzertifikat.

Auf der Website der Behörde[1] können für die Datenverarbeitung Verantwortliche ein Dateneingabeformular für das Allgemeine Datenschutzregister (*Registro General de Protección de Datos* – RGPD) benutzen, das mit dem neuen System von 13 auf 3 Seiten gekürzt wird:

[1] www.agpd.es

I. Je nach Art des für die Datenverarbeitung Verantwortlichen (öffentliche oder private Einrichtung) kann eine neu erstellte Datei gemeldet werden sowie eine bereits im Allgemeinen Datenschutzregister RGPD eingetragene Datei geändert oder gelöscht werden.
II. Die zuvor ausgefüllte vereinfachte Meldung oder die Standardmeldung ermöglicht die Meldung solcher Dateien für folgende Einsatzbereiche: Kunden, Personalverwaltung, Löhne, Wohnungseigentümergemeinschaften, Patienten, Register der verschreibungspflichtigen Arzneimittel von Privatapotheken, Mitarbeiterkarteien, Verwaltung von Erhebungen, Finanzverwaltung sowie Kontrolle des Zugriffs auf Dateien der öffentlichen Verwaltung.
III. Die Standardmeldung dient zur Meldung jeder anderen Dateiart.

2.b) Förderung von Präventivmaßnahmen: Sektorielle Inspektionen 2006

Im Jahresverlauf 2006 führte die AEPD von Amts wegen sektorielle Inspektionen bei nicht-universitäten geregelten Bildungseinrichtungen durch. Dabei wurden über 60 staatliche und private Schulen in Spanien untersucht. Diese amtlichen Inspektionen sind rein präventiv ausgerichtet, da sie, ohne auf eine Bestrafung abzuzielen, die Bildungseinrichtungen prüfen, auf die Pflicht zur Einhaltung der betreffenden Bestimmungen des Datenschutzgesetzes hinweisen, etwaige Defizite aufzeigen und Empfehlungen zu deren Berichtigung geben. Zur Durchführung dieses von Amts wegen durchgeführten sektoriellen Inspektionsplans wurde die Verarbeitung der Daten über Schüler und Familien durch verschiedene Abteilungen und Dienste von Schulen untersucht, unter anderem Aspekte wie Einschreibungsformulare und Antragsverfahren, Art der erfassten Daten und Dokumente, Art der Daten in der Schulakte, Datenverarbeitung durch ärztliche und beratende Dienste in den Schulen sowie von solchen Bildungseinrichtungen festgelegte Sicherheitsvorkehrungen für den Datenschutz.

2.c) Förderung der Selbstregulierung

- Verhaltenskodizes

Im Jahresverlauf 2006 wurden bei der Datenschutzbehörde folgende Verhaltenskodizes registriert, die den Datenschutz sowohl im öffentlichen als auch im privaten Sektor selbst regulieren.

2.c.1) Standardcode für den Datenschutz bei der VERAZ-PERSUS-Datei

VERAZ-PERSUS ist eine so genannte „Opt-in-Datei", in die sich jede Person entweder selbst oder durch ihren gesetzlichen Vertreter eintragen lassen kann, um die betrügerische Verwendung ihrer personenbezogenen Daten durch Dritte zum Nachteil ihrer Identität, Zahlungsfähigkeit oder Vermögenswerte zu verhindern. Bei der Nutzung dieser Datei treffen die Einrichtungen die notwendigen Zusatzvorkehrungen gemäß Kriterien der Sorgfalt und der Vertraulichkeit, um sicherzustellen, dass die Person, die den Vorgang bei den betreffenden Organisationen beauftragt, der tatsächliche Inhaber der auf freiwilliger Basis eingetragenen Identitätsdaten ist. Der Standardcode schafft die Voraussetzungen für die Organisation und das System für den Betrieb der VERAZ-PERSUS-Datei, deren Benutzer umfangreichere Garantien in Anspruch nehmen können als jene, die in üblichen Datenschutzvorschriften enthalten sind.

2.d) Untersuchung nach Meldungen von Bürgern – insbesondere zum Telekommunikationssektor

Der Telekommunikationssektor war 2006 der Sektor mit der größten Anzahl von Beschwerden. Auf ihn entfallen ungefähr 35% aller Meldungen, die zu Geldstrafen in Höhe von mehreren Millionen Euro führten. Diese Situation besteht bereits seit mehreren Jahren und beruht auf einer aggressiven Geschäftspolitik verschiedener Telekommunikationsbetreiber im Zuge der Liberalisierung des Sektors, im Bestreben, den eigenen Marktanteil zu Lasten des früheren Monopolunternehmens zu vergrößern.

Diese Praktiken veranlassten einige Betreiber dazu, Telekommunikationsdienste auf den Namen von Kunden zu registrieren, die diese Dienste bei Wettbewerbern bestellt hatten, was eine betrügerische Verarbeitung von personenbezogenen Daten ohne Einwilligung des Datensubjekts darstellt. In den meisten Fällen dieser Art weigern sich die Kunden, die auf betrügerische Weise registrierten Dienste zu zahlen. Daraufhin trägt der Betreiber die Kundendaten in Dateien säumiger Zahler ein, die zwischen Telekommunikationsgesellschaften und Banken ausgetauscht werden, wodurch zukünftig Bestellungen solcher Dienste gesperrt werden, was eindeutig einen erheblichen Nachteil für den Verbraucher darstellt.

Die spanische Datenschutzbehörde AEPD bestraft diese Praxis seit mehreren Jahren, was für einige Betreiber Geldstrafen von über einer Million Euro in einem einzigen Geschäftsjahr mit sich bringt. Als ein Ergebnis davon wandten sich 2006 zwei wichtige Betreiber, die mit einer Geldstrafe belegt worden waren, an die AEPD und bekundeten ihre Absicht, die Datenschutzgesetze zu erfüllen. Beide Betreiber gaben an, dass sie ihre Vertragsabschlussverfahren geändert und daher die besagten Praktiken beendet hätten, und dass sie sich nun freiwillig einer Prüfung der neuen Verfahren durch AEPD-Inspektoren unterziehen wollten. Diese Prüfungen wurden Ende 2006 durchgeführt, und es wird erwartet, dass die Zahl der Meldungen im Jahresverlauf 2007 allmählich zurückgeht.

3. Verbreitung der Datenschutzkultur und Kooperationsvereinbarungen mit anderen Behörden

3.a) Erste Europäische Datenschutzkonferenz

Im März 2006 organisierte die spanische Datenschutzbehörde (*Agencia Española de Protección de Datos* - AEPD) – mit Unterstützung der Stiftung des Bankhauses BBVA (*Fundación BBVA*) und des Verbands der spanischen Industrie und Handelskammern (*Consejo Superior de Cámaras de Comercio, Industria y Navegación de España*) – die Erste Europäische Datenschutzkonferenz, an der mehr als 300 Experten für internationale politische, institutionelle und unternehmerische Fragen teilnahmen. Ziel der Konferenz war die Diskussion der für den Datenschutz relevanten Auswirkungen bei Angelegenheiten wie Finanztätigkeit, Bekämpfung von Terrorismus und organisierter Kriminalität, Betrugsbekämpfung und Verwaltungstransparenz. Zu diesem Zweck wurde die Konferenz in vier Blöcke untergliedert:

I. Datenschutz, Privatsektor und Finanztätigkeit
II. Datenschutz und -sicherheit
III. Umsetzung und Bedeutung der Datenschutzrichtlinie
IV. Transparenz, Datenschutz und Telekommunikation

Verbindliche unternehmensinterne Vorschriften (*Binding Corporate Rules* - BCR), Rechtsinstrumente zur Terrorismusbekämpfung und ihre Auswirkungen auf den Schutz der Privatsphäre, Identitätsdiebstahl, ubiquitäres Computing sowie Auswirkungen neuer Entwicklungen im Bereich Telekommunikation auf den Schutz der Privatsphäre waren einige der diskutierten Themen.

3.b) Empfehlungen für Internetnutzer

Durch die Umsetzung der Richtlinie 2002/58/EG erhielt die Datenschutzbehörde AEPD Zuständigkeiten für den Schutz der Rechte und Garantien von Nutzern im Bereich der elektronischen Kommunikation. Im Rahmen dieser Zuständigkeiten und anlässlich des Internet-Tages im Mai 2006 verabschiedete die spanische Datenschutzbehörde einen *Leitfaden mit Empfehlungen für Internetnutzer*. In diesem Leitfaden stellte die Datenschutzbehörde AEPD fest, dass es, obwohl neue Technologien unverzichtbarer Bestandteil in der Entwicklung einer modernen Gesellschaft sind, vorrangig ist, ein Umfeld des Vertrauens zu schaffen, damit unter den Bürgern der Informationsgesellschaft die Nutzung des Internets gefördert und die Entstehung einer Datenschutzkultur entwickelt

werden. Dieser Leitfaden umfasst Empfehlungen betreffend Surfen im Internet, Gebrauch von E-Mails, Bekämpfung von Viren und Social Engineering (Phishing), elektronischen Geschäftsverkehr und elektronische Bankdienstleistungen oder Instant-Messenger-Services sowie Gesprächsforen im Internet (Chatrooms). Ferner sei auf Regelungen hingewiesen, die speziell auf die Internetnutzung durch Minderjährige, den Einsatz der IP-Telefonie oder den Dateitausch, beispielsweise durch Peer-to-Peer-Instrumente, abzielen.

3.c) Zusammenarbeit mit der Datenschutzbehörde von Andorra

Die Datenschutzbehörden von Spanien und Andorra unterzeichneten 2006 eine Absichtserklärung mit dem Ziel, die Zusammenarbeit zwischen beiden Institutionen in Gang zu setzen und gemeinsame Aktionen durchzuführen, die darauf abzielen, das Recht auf Datenschutz in beiden Ländern zu fördern. Zur Entwicklung dieser Zusammenarbeit verpflichteten sich die beiden Behörden, in gemeinsamen Aktionen Rechte und Pflichten in Datenschutzfragen zu verbreiten und sich gegenseitig bei der Anwendung und Auslegung der Datenschutzvorschriften in ihren jeweiligen Ländern zu unterstützen. Außerdem erörterten sie die mögliche gemeinsame Durchführung von Studien, Untersuchungen oder Berichten zu dem Thema sowie die Zusammenarbeit mit ihren jeweiligen Regierungen mit dem Ziel, effiziente Garantien in Datenschutzfragen, vor allem im Hinblick auf internationale Datenübermittlungen, zu erreichen.

4. Aktivitäten von Spanien in Bezug auf das lateinamerikanische Datenschutznetz

Im Mai 2006 versammelten sich die Vertreter der 12 Mitgliedsländer des Lateinamerikanischen Datenschutznetzes in Santa Cruz de la Sierra, Bolivien.

Während des Treffens erstellten die Teilnehmer Arbeitsdokumente, die beim nächsten Treffen des Netzwerks im ersten Halbjahr 2007 zur Verabschiedung vorgelegt werden sollen. Die Erstellung der Dokumente erfolgte in den vier themenzentrierten Arbeitsgruppen, die anlässlich der 4. Lateinamerikanischen Datenschutzkonferenz eingerichtet wurden, die im Jahr 2005 in Mexiko stattfand: „Impulse für Gesetzgebung und Harmonisierung“„Das Online-Netzwerk“„Selbstregulierungsinstrumente“ und„Verarbeitung von Gesundheitsdaten“.

In diesen Dokumenten wurden insbesondere folgende Schlüsse gezogen:

- Es ist notwendig, Maßnahmen zu ergreifen, die in allen lateinamerikanischen Ländern ein angemessenes Datenschutzniveau garantieren. Die gegenseitige Angleichung der Rechtsvorschriften zwischen den Ländern Lateinamerikas ist zu gewährleisten, damit der für eine reibungslose Entwicklung der Marktwirtschaft erforderliche Informationsfluss ermöglicht werden kann.

- Ärztliche Aufzeichnungen zur Gesundheitsbetreuung müssen alle Daten umfassen, die für eine genaue Kenntnis des tatsächlichen, aktuellen Gesundheitszustands notwendig sind. Zugriff, Nutzung, Ablage, Aufbewahrung und Übermittlung diesbezüglicher Gesundheitsdaten erfordern zusätzliche Sicherheitsvorkehrungen und müssen Grundsätze in Bezug auf die persönliche Würde, die Willensfreiheit, den Schutz der Privatsphäre sowie den Schutz personenbezogener Daten beachten. Diese Grundsätze der persönlichen Einwilligung können jedoch Einschränkungen im Interesse des Gemeinwohls unterliegen, die allerdings einer gesetzlichen Regelung bedürfen. Weiterhin müssen die Gesundheitssysteme für die notwendige Mobilität sorgen, indem sie Systeme einrichten, die Gesundheitsinformationen zwischen den verschiedenen Einrichtungen, Zentren und Diensten des Gesundheitssystems austauschen, so dass bei Reisen innerhalb jedes Landes eine angemessene Gesundheitsbetreuung gewährleistet werden kann.

- Selbstregulierungsinitiativen als Ergänzung zum bestehenden gesetzlichen Rahmen, der bereits von staatlicher Seite vorgegeben ist, können den Schutz personenbezogener Daten fördern. Aufgrund dessen wird für Gesetzestexte zum Datenschutz die Aufnahme von klaren Bestimmungen zur Förderung von Selbstregulierungsmechanismen, zur Steigerung ihres Bekanntheitsgrads und zur Festlegung wirksamer Maßnahmen für den Umgang mit Regelverstößen empfohlen.
- Schließlich wurde das Online-Netzwerk-Projekt vorgestellt, das die breite geografische Streuung der Mitglieder des Lateinamerikanischen Datenschutznetzes überwinden helfen soll. In erster Linie soll durch dieses Projekt für das Lateinamerikanische Datenschutznetz ein virtuelles Instrument geschaffen werden, mit dem es seine Aktivitäten weiterentwickeln und vermitteln, das Grundrecht auf Datenschutz in Lateinamerika verbreiten und ein System für den Informationsaustausch zwischen den Mitgliedern konfigurieren kann.

Schweden

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

In Schweden wurde die EU-Richtlinie 95/46/EG durch das Datenschutzgesetz (1998:204) umgesetzt, das am 24. Oktober 1998 in Kraft trat. Das Datenschutzgesetz wird durch die Datenschutzverordnung ergänzt, die am gleichen Tag in Kraft trat. Das Gesetz findet wie die Richtlinie auf die automatisierte ebenso wie auf die manuelle Datenverarbeitung Anwendung. Jedoch gelten die grundsätzlichen Regelungen zur Datenverarbeitung und zum erlaubten Zeitraum einer solchen Verarbeitung hinsichtlich manueller Datenverarbeitungen, die vor dem Inkrafttreten des Datenschutzgesetzes begonnen wurden, erst ab dem 1. Oktober 2007. Das Gesetz gilt zwar grundsätzlich für die Verarbeitung personenbezogener 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 speziellen Gesetze und Beschlüsse wurde der Richtlinie Rechnung getragen.

In den beiden vorhergehenden Jahresberichten der Artikel-29-Datenschutzgruppe (von 2004 und 2005) wurde der Bericht des mit der Überprüfung des Datenschutzgesetzes befassten Untersuchungsausschusses präsentiert. Der Untersuchungsausschuss schlug Änderungen am Datenschutzgesetz in Form von Ausnahmen von den Datenhandhabungsregeln vor. Nach eingehender Prüfung des Vorschlags des Untersuchungsausschusses legte die Regierung (das Justizministerium) am 16. März 2006 dem Parlament einen Gesetzentwurf zur Änderung des Datenschutzgesetzes vor. Im Mai verabschiedete das Parlament die Regierungsvorlage, so dass ab 1. Januar 2007 hinsichtlich der Verarbeitung personenbezogener Daten ein so genanntes „Missbrauchsmodell" gelten wird. Die Änderungen führen Ausnahmen von den Datenhandhabungsregeln des Datenschutzgesetzes ein. Diese Ausnahmen beziehen sich auf die alltägliche Verarbeitung von personenbezogenen Daten in unstrukturiertem Material (wie z. B. beim Erstellen von fortlaufendem Text mit Textverarbeitungsprogrammen oder im Internet). Das „Missbrauchsmodell" bezieht sich auf die Verarbeitung personenbezogener Daten, die keinem Satz von personenbezogenen Daten angehören (bzw. dafür bestimmt sind), der in eine bestimmte Struktur gebracht worden ist, um die Datensuche bzw. die Datenzusammenstellung wesentlich zu erleichtern. Für die Verarbeitung von personenbezogenen Daten, die von den Datenhandhabungsregeln ausgenommen sind, gilt eine einzige einfache Regel: Die Datenverarbeitung ist nicht erlaubt, wenn sie einen unangemessenen Eingriff in die Privatsphäre darstellt. Die Datenhandhabungsregeln des Datenschutzgesetzes gelten weiterhin für die Verarbeitung von strukturierten Daten, etwa bei der Verarbeitung von Daten in Registern personenbezogener Daten, sowie für unstrukturiertes Material, das Teil eines Registers personenbezogener Daten ist.

Die EU-Richtlinie 2002/58/EG wurde mit Inkrafttreten des Gesetzes über die elektronische Kommunikation (2003:389) am 1. Juli 2003 in schwedisches Recht umgesetzt. In Kapitel 6 dieses Gesetzes stehen Datenschutzregeln für den elektronischen Kommunikationssektor. Die Einhaltung der Datenschutzbestimmungen des Gesetzes wird von der Überwachungsbehörde für das Post- und Telekommunikationswesen (Post- och telestyrelsen - PTS) kontrolliert. 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.

Nach der Annahme der EG-Richtlinie über die Vorratsdatenspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektroni-

scher Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, betraute der schwedische Justizminister im Mai 2006 einen Untersuchungsausschuss mit der Überprüfung der innerstaatlichen Rechtsvorschriften auf diesem Gebiet, um gemeinsam mit den Dienstanbietern die erforderlichen Änderungen vorzuschlagen. Die Untersuchung wurde Ende August 2006 begonnen, der Bericht wird für 2007 erwartet. Die Datenschutzbehörde ist in diesem Untersuchungsausschuss vertreten.

Im letztjährigen Bericht teilte die Datenschutzbehörde mit, dass verschiedene Untersuchungsausschüsse zahlreiche Vorschläge unterbreitet haben, die darauf abzielen, die Bekämpfung von Verbrechen zu erleichtern. Diese Vorschläge würden verschärfte Zwangsmaßnahmen seitens der Polizei sowie umfangreichere Möglichkeiten zur Erhebung und Aufzeichnung personenbezogener Daten mit sich bringen. Während der letzten zwei Jahre wurden nicht weniger als 20 verschiedene Vorschläge hinsichtlich Kontrolle und Überwachung vorgelegt, und diese Fragen wurden im Jahresverlauf 2006 detailliert erörtert. Zwei Gesetzentwürfe – der Gesetzentwurf zum verstärkten Gebrauch von Zwangsmaßnahmen zur Verhinderung von Schwerverbrechen (2005/06:177) und der Gesetzentwurf zu geheimen Abhörmaßnahmen im Inneren von Gebäuden (2005:06:178) – wurden 2006 ins Parlament eingebracht, ruhen allerdings zum Zeitpunkt der Abfassung des vorliegenden Berichts. Ein Vorschlag aus dem Jahr 2005 zum Zugang zu elektronischer Kommunikation bei der Aufklärung von Verbrechen soll im Juni 2007 ins Parlament eingebracht werden. Im Dezember 2006 präsentierte die Regierung einen Vorentwurf für ein Gesetz, der vorsieht, den gesamten grenzübergreifenden drahtgestützten Datenverkehr einer Signalüberwachung durch die Funküberwachungsbehörde der Streitkräfte (*Försvarets radioanstalt* - FRA) zu unterwerfen.

Im September präsentierte ein Untersuchungsausschuss, der mit der Überprüfung der Regelungen zu Patientenakten und sonstiger Bereiche des Gesundheitswesens beauftragt war, einen Vorschlag für eine einheitliche Regelung des Umgangs mit personenbezogenen Daten im Gesundheitswesen. Dazu wurde ein umfassendes neues Patientendatengesetz vorgeschlagen. Der Vorschlag kann als Teil des laufenden Prozesses für ein engeres Zusammenwirken der verschiedenen Akteure im Gesundheitswesen sowie für eine leichtere Orientierung der Patienten angesehen werden. Der Vorschlag wurde zur Beratung vorgelegt und wird derzeit seitens der Regierung geprüft.

B. Bedeutende Rechtsprechung

Im Juni 2005 entschied die Datenschutzbehörde in einem Fall zum so genannten „Amt zur Bekämpfung von Urheberrechtspiraterie" (*Svenska antipiratbyrån*, im Folgenden: das „Amt"), einer Schutzgemeinschaft verschiedener privatwirtschaftlicher Unternehmen. Das „Amt" hatte eine Vielzahl von Einzelinformationen, insbesondere IP-Adressen, in Verbindung mit der Verbreitung von urheberrechtlich geschütztem Material per *Filesharing* über das Internet gesammelt. Die Datenschutzbehörde hatte die Verarbeitung von personenbezogenen Daten seitens des „Amt" untersucht und dabei herausgefunden, dass ein Teil der seitens des „Amts" 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 – außer bei Vorliegen einer Ausnahmegenehmigung der Datenschutzbehörde – einzig und allein den zuständigen Behörden gestattet, personenbezogene Daten zu verarbeiten, die Rechtsverletzungen und strafbare Handlungen betreffen. Dagegen handelte es sich nach Auffassung des „Amts" bei der durchgeführten Verarbeitung um keine Verarbeitung von personenbezogenen Daten im Sinne des Datenschutzgesetzes. Was die gesammelten IP-Adressen anbelangt, so hatte das „Amt" keinen Zugriff auf die personenbezogenen Daten zur Zuordnung zwischen den Abonnenten von Internetzugängen und bestimmten IP-Adressen. In ihrer Entscheidung vom Juni 2005 befand die

Datenschutzbehörde allerdings – unter Bezugnahme auf die Vorarbeiten zum Datenschutzgesetz -, dass die in diesem Fall verarbeiteten Daten sehr wohl als personenbezogene Daten zu betrachten sind. In ihrer Entscheidung vom Juni 2005 wies die Datenschutzbehörde das „Amt" zur Einstellung der Datenverarbeitung an, da es keinen Antrag auf eine Ausnahmegenehmigung gestellt hatte. Das „Amt" klagte gegen diese Entscheidung vor dem Verwaltungsgericht Stockholm, das die Klage mit Urteil vom 27. Dezember 2006 abwies. Dagegen legte das „Amt" beim Verwaltungsberufungsgericht Rechtsmittel ein, der Fall ist noch anhängig.

Nach der Entscheidung der Datenschutzbehörde vom Juni 2005 beantragte das „Amt" dann für sich eine Ausnahmegenehmigung 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 seitens ihrer Teilnehmer zu informieren und zivilrechtliche Klagen gegen sie anzustrengen. Im Oktober 2005 entschied die Datenschutzbehörde, eine solche Ausnahmegenehmigung zu dem durch Abschnitt 21 des Datenschutzgesetzes begründeten Verbot zu erteilen. Die Ausnahmegenehmigung galt bis 31. Dezember 2006. Die Datenschutzbehörde hat die Ausnahmegenehmigung inzwischen verlängert, so dass das „Amt" derzeit befugt ist, personenbezogene Daten zu strafbaren Handlungen zu verarbeiten.

C. Wichtige spezifische Themen

Druckschriften

Sämtliche Druckschriften der Datenschutzbehörde stehen auf ihrer Website zum kostenlosen Herunterladen bereit. *Magazin DIrekt* ist eine Vierteljahreszeitschrift mit Berichten, Nachrichten und Kommentaren. Bestimmte Aufsichtstätigkeiten werden in Form von spezifischen oder thematischen Projekten durchgeführt und abschließend in Berichten dokumentiert. Im Jahresverlauf 2006 wurden zwei derartige Berichte veröffentlicht: *Wie gehen Inkassobüros mit Beschwerden um?* und *So sollten Versicherungsgesellschaften sensible personenbezogene Daten verarbeiten*. Die Behörde hat auch andere Druckschriften veröffentlicht, wie etwa die Informationsbroschüren *Informationssicherheit* und *Ortungstechnologie im Arbeitsleben*.

Im Bereich der Selbstregulierungen innerhalb bestimmter Branchen hat die Datenschutzbehörde eine Stellungnahme zur vorgeschlagenen Endfassung des Verhaltenskodex über die Verarbeitung personenbezogener Daten bei der Wohnraumvermietung abgegeben, der u. a. von der schwedischen Hausbesitzervereinigung und vom schwedischen Mieterbund gemeinsam ausgearbeitet wurde. Im Jahr 2006 bat die Bauwirtschaft die Datenschutzbehörde um eine Stellungnahme zum Entwurf für einen Verhaltenskodex zur Verarbeitung personenbezogener Daten in dieser Branche. Durch den Verhaltenskodex soll der Schwarzarbeit ein Riegel vorgeschoben werden. Ein weiteres Ziel ist die Gewährleistung des freien Wettbewerbs im Baubereich. Ein erstes Treffen mit Branchenvertretern ist für Anfang 2007 angesetzt.

Im Juni 2006 beschloss die Regierung eine neue E-Government-Strategie. Eines der Ziele dieser Strategie lautet, dass die öffentliche Verwaltung bis 2010 über ein effizientes Datenmanagement verfügen wird, das sowohl einen einfachen Informationszugriff ermöglicht als auch dem Datenschutz und der Datensicherheit angemessen Rechnung trägt. Ein weiteres Ziel ist es, bis 2010 in vielen Bereichen der öffentlichen Verwaltung Effizienzsteigerungen durch die Einführung von elektronischen Fallbehandlungssystemen (*Case-Handling Systems* – CHS) zu erzielen. Im Jahr 2006 beauftragte die Regierung die Datenschutzbehörde mit einem Beitrag zur Entwicklung effizienter E-Government-Dienste, unter besonderer Berücksichtigung des Rechts auf Schutz der Privatsphäre. Zu diesem Zweck beschloss die Datenschutzbehörde eine detaillierte Untersuchung von E-Government-Projekten der Lokalverwaltungen.

Im Jahresverlauf 2006 führte die Datenschutzbehörde auch eine Kommunikationsübung mit dem Titel „Steht dein Bild im Internet?“ durch. Mit dieser Übung sollten junge Menschen zum Nachdenken darüber angeregt werden, wozu ein Fehler im Internet führen kann. Außerdem sollten Leitlinien vermittelt werden, was im Internet zulässig ist, und was nicht. Die Datenschutzbehörde produzierte ein fünfteiliges Hörspiel mit jungen Schauspielern über typische Probleme auf Websites: Mobbing, Veröffentlichung von Fotos und die angeblich 13-jährige Lisa, bei der es sich in Wahrheit um den 53-jährigen Bengt handelt. Diese Geschichten wurden auf einigen Jugendfestivals verbreitet: In den Toiletten wurden Tonwiedergabegeräte installiert, die sich automatisch einschalteten, sobald eine Person den Raum betrat. Die Geschichten dauerten jeweils 60 bis 90 Sekunden. Auch bei weiteren Veranstaltungen wurden diese Tonwiedergabegräte eingesetzt, und inzwischen können die Kurzhörspiele auch auf einer von der Datenschutzbehörde eingerichteten speziellen Website angehört werden.

Vereinigten Königreichs

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

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 in britisches Recht überführt und am 11. Dezember 2003 rechtswirksam.

B. Bedeutende Rechtsprechung

Im Jahr 2006 gab es keine bedeutende Rechtsprechung bei den Gerichten des Vereinigten Königreichs, die sich auf die Richtlinien 95/46/EG bzw. 2002/58/EG bezogen hätte.

C. Wichtige spezifische Themen

Im Mai 2006 unterbreitete der britische Datenschutzbeauftragte *(Information Commissioner)* dem Parlament einen Sonderbericht *(What Price Privacy? – Privatsphäre um welchen Preis?)* über den gesetzwidrigen Handel mit vertraulichen personenbezogenen Daten. Dieser Bericht enthüllte die Machenschaften einer breitgefächerten Branche, die sich auf den illegalen Handel mit personenbezogenen Daten wie Adressen, Telefonnummern aus früheren Telefonverzeichnissen, Vorstrafenregistern und Bankverbindungen spezialisiert hat. Private Ermittler und Fahnder lieferten solche Informationen unter anderem an Journalisten und an Kreditinstitute, die Schuldner ausfindig machen möchten. Der Datenschutzbeauftragte machte auf das geringe Strafmaß aufmerksam, das für dieses Vergehen droht, und forderte Haftstrafen von bis zu zwei Jahren, um eine entsprechende Abschreckungswirkung zu gewährleisten.

Im Dezember veröffentlichte der Datenschutzbeauftragte eine Überprüfung der Folgemaßnahmen zu diesem Bericht, in der er die Antworten der Regierung sowie von öffentlichen und privaten Einrichtungen vorstellte. In diesem Bericht nannte er auch namentlich die Zeitungen, bei denen Journalisten personenbezogene Angaben von einem Privatermittler entgegennahmen, was einen Verstoß gegen Paragraf 55 des Datenschutzgesetzes darstellt.

Im November organisierte der Datenschutzbeauftragte in London die 28. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre (kurz: Internationale Datenschutzkonferenz) zum Thema Überwachungsgesellschaft. Das Surveillance Studies Network legte einen speziell in Auftrag gegebenen „Bericht zur Überwachungsgesellschaft" vor, der den Umfang der Rückverfolgung und Aufzeichnung menschlicher Aktivitäten und Bewegungen jetzt und in zehn Jahren bewertete. Die Konferenz bot weiterhin Beiträge aus einem breiten Spektrum von Rednern aus den Bereichen der Rechtsberufe, Regierungen, Wissenschaft, Unternehmen und Strafverfolgung. In der nicht-öffentlichen Sitzung des Datenschutzbeauftragten stellte die französische Datenschutzbehörde CNIL eine Initiative zum Thema „Datenschutz vermitteln und effektiver gestalten" vor, die auch vom britischen Datenschutzbeauftragten und vom Europäischen Datenschutzbeauftragten mitgetragen wird. Alex Türk (Präsident der CNIL) berichtete, dass die schnellen Technologiefortschritte und die Entwicklung neuer Gesetze zur Terrorismusbekämpfung Herausforderungen darstellen, denen sich die Datenschutzbehörden stellen müssen.

Für das Jahr 2006 leitete der britische Datenschutzbeauftragte eine Neubeurteilung seines Konzepts des Informationsaustauschs im öffentlichen Sektor ein. Die Leitlinien des Datenschutzbeauftragten für den Umgang mit personenbezogenen Daten, die bei der Erhebung und Verwaltung der Gemeindesteuer *(Council Tax)* gespeichert werden, wurden überarbeitet. Demnach wir der Datenschutzbeauftragte von

seinen Durchsetzungsbefugnissen keinen Gebrauch machen, außer wenn stichhaltige Indizien für ungerechtes Handeln vorliegen oder ungerechtfertigte Nachteile für einzelne Personen entstanden sind. Diese Empfehlungen sollen die lokalen Gebietskörperschaften zur optimalen Nutzung der von ihnen gespeicherten Informationen anspornen, während zugleich die Interessen der Datensubjekte geschützt werden. Darüber hinaus hat der Datenschutzbeauftragte die Arbeit an einem Rahmenkodex für Informationsaustausch aufgenommen, der den Mitarbeitern des öffentlichen Sektors bei ihren Entscheidungen in Bezug auf den Austausch personenbezogener Daten Leitlinien an die Hand geben soll. Eine Gruppe von praxiserfahrenen IT-Fachleuten aus Institutionen wie den Sozialdiensten, dem Gesundheitssektor und der Polizei wird bei der Ausarbeitung dieses Kodex hinzugezogen.

Im Jahr 2006 unterrichtete der Datenschutzbeauftragte die nachstehenden parlamentarischen Ausschüsse:

- den Bildungsausschuss des schottischen Parlaments – Gesetzentwurf über den Schutz gefährdeter Gruppen in Schottland

- Schottisches Parlament, Unterausschuss Recht – Konsultation (Pädophile Sexualstraftäter)

- Oberhaus *(House of Lords)*, Sonderausschuss, Unterausschuss F Europäische Union (Innere Angelegenheiten) – Erhebung zur Entwicklung der zweiten Generation des Schengener Informationssystems (SIS II)

Im Jahr 2006 antwortete der Datenschutzbeauftragte auf folgende Konsultationen:

- Verkehrsministerium – Übermittlung von Daten der Fahrzeughalter aus den britischen Fahrzeugregistern

- Amt für Verfassungsangelegenheiten – Konsultation zur Zunahme der Straftaten gemäß Paragraf 55 Datenschutzgesetz (1998).

- Kraftfahrzeugstelle *(Driver and Vehicle Licensing Agency)* – Datenübermittlung und Datenvorratsspeicherung

- Zoll- und Finanzbehörde *(Her Majesty's Revenue and Customs)* – Konsultation über den Verhaltenskodex zur Offenlegung von personenbezogenen Daten im Rahmen des Terrorismusbekämpfungsgesetzes *(Anti-terrorism, Crime and Security Act)*

- Innenministerium *(Home Office)* – Untersuchung zum Schutz elektronischer Daten

- Innenministerium *(Home Office)* – Neue Befugnisse zur Bekämpfung des organisierten Verbrechens und der Finanzkriminalität

- Innenministerium *(Home Office)* – Konsultation zur Regelung der Ermittlungsbefugnisse (Regulation of Investigatory Powers Act Pt III)

- Housing Corporation (Dachgesellschaft der gemeinnützigen Wohnungsunternehmen) - Bekämpfung der Obdachlosigkeit

- Projekt „Information Sharing Index" – Children Act 2004: Regelungen für den englischen „Information Sharing Index", eine geplante Datenbank mit Angaben zu allen in England wohnhaften Kindern und Jugendlichen unter 18 Jahren, um sie besser gegen Missbrauch zu schützen. Rechtsgrundlage ist das Kindergesetz von 2004.

- **Amt für Lokalverwaltung *(Office of Communities and Local Government)*** – Kommunale Verwaltungen werden darauf vorbereitet, gemeinnützige Wohnungsverwaltungen mit Aufgaben zur Bewältigung asozialer Verhaltensweisen zu betrauen

- **Walisische Versammlung *(Welsh Assembly)*** – *„Making the Connections?"* („Stimmen die Verbindungen?"), eine Anhörung zur Festlegung von Kernstandards für die Kundenorientierung im öffentlichen Dienst von Wales

Kapitel 3

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. DIE EUROPÄISCHE KOMMISSION

Arbeitsdokument der Kommissionsdienststellen SEK (2006)95 vom 20. Januar 2006 über die Umsetzung der Entscheidung der Kommission hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG und 2002/16/EG)

Dieses Dokument enthält die Ergebnisse der Funktionsbeurteilung über die mit den Kommissionsentscheidungen 2001/497/EG[1] und 2002/16/EG[2] eingeführten Standardvertragsklauseln. Die Gesamtbeurteilung ergab keinerlei erhebliche Probleme im Zusammenhang mit dem Gebrauch dieser Vertragsklauseln, abgesehen von der Notwendigkeit, bestimmte Aspekte zu klären, um die Verwendung zu erleichtern. Der Bericht zeigt ferner auf, dass die Mitgliedstaaten nur über wenige Informationen hinsichtlich der Verwendung der Vertragsklauseln verfügen. Die Kommissionsdienststellen sind der Ansicht, dass eine verbesserte Überwachung seitens der Mitgliedstaaten beim Erkennen potenzieller Probleme hilfreich sein wird. Die Kommissionsdienststellen würden es außerdem begrüßen, wenn als Alternative zur Nutzung von Ausnahmen in verstärktem Maße Standardvertragsklauseln zur Anwendung gelangen würden. Sie weisen auch auf die zunehmende Bekanntheit der Standardvertragsklauseln hin.

Abkommen vom 19. Oktober 2006 zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records - PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (US-Ministerium für Heimatschutz)

Dieses auf den Artikeln 24 und 28 des Unionsvertrags beruhende Abkommen ersetzt die vorherige Angemessenheitsentscheidung und das internationale Abkommen in derselben Sache, das durch die Entscheidung des Europäischen Gerichtshofs vom 30. Mai 2007 wegen mangelnder Rechtsgrundlage für nichtig erklärt wurde. Das neue Abkommen stützt sich darauf, dass die US-Behörden (DHS – *Department of Homeland Security*, US-Ministerium für Heimatschutz) an ihrer Umsetzung der Verpflichtungen festhalten, und geht davon aus, dass das DHS ein angemessenes Schutzniveau gewährleistet. Das Abkommen schafft eine Rechtsgrundlage für die Übermittlung von personenbezogenen Daten („PNR-Daten") und deren Verarbeitung durch das DHS. Es ist als Interimslösung gedacht, bis zum Inkrafttreten eines an seine Stelle tretenden Abkommens, im Prinzip spätestens zum 31. Juli 2007.

Konferenz über internationale Übermittlungen von personenbezogenen Daten vom 23. und 24. Oktober 2006; gemeinsame Veranstaltung der Artikel-29-Datenschutzgruppe (unabhängige EU-Beratergruppe für den Schutz von personenbezogenen Daten und der Privatsphäre) und der Internationalen Handelsbehörde (ITA, International Trade Administration) des US-Wirtschaftsministeriums (Department of Commerce)

Die Konferenz wurde von der Kommission gemeinsam mit der Artikel-29-Datenschutzgruppe und dem US-Wirtschaftsministerium *(Department of Commerce)* abgehalten. Der Schwerpunkt der Konferenz lag auf internationalen Übermittlungen personenbezogener Daten. Es handelte sich um eine Anschlussveranstaltung zur 2005 in Washington abgehaltenen Konferenz über so genannte „Sichere Häfen" *(safe harbors)*. Die Konferenz widmete diesem Thema fünf Workshops: Im Einzelnen ging es dabei um *safe-harbor*-Programme für Datenübermittlungen in die USA, Vertragsklauseln, verbindliche unternehmensinterne Vorschriften sowie um Ausnahmen, unter denen trotz eines mangelnden Schutzniveaus bzw. trotz fehlender spezifischer Garantien hinsichtlich der Datenverarbeitung internationale Datenübermittlungen vorgenommen werden können. Geschlossen wurde die Konferenz mit einem Workshop zu weltweiten Übermittlungen personenbezogener Daten. Der Teilnehmerkreis der Konferenz umfasste internationale Datenschutzexperten sowie Vertreter von Universitäten, Forschungsinstituten, privaten Organisationen und Datenschutzbehörden aus der

[1] ABl. EU L 181, 4.7.2001, S. 19

[2] ABl. EU L 6, 1.2.2002, S. 52

EU und aus Drittländern. Die Anschlussveranstaltung zu dieser Konferenz wird 2007 in Washington stattfinden. Der ständige Dialog im Datenschutzbereich sollte zu einer Vertiefung der transatlantischen Beziehungen führen und die Herausbildung einer demokratischen Informationsgesellschaft fördern, in welcher der Schutz personenbezogener Daten gewährleistet ist.

Arbeitsdokument der Kommissionsdienststellen SEK (2006)1520 vom 20. November 2006 über die Anwendung der Entscheidung der Kommission 2002/2/EG vom 20. Dezember 2001 gemäß Richtlinie 95/56/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten aufgrund des kanadischen Gesetzes über den Schutz personenbezogener Daten und elektronische Dokumentation (Personal Information Protection and Electronic Documentation Act)

Am 20. Dezember 2001 verabschiedete die Kommission ihre Entscheidung 2002/2/EG gemäß Art. 25 (6) der Richtlinie, in welcher sie erklärt, dass für die Zwecke des Art. 25 (2) der genannten Richtlinie Kanada als ein Staat betrachtet wird, der ein angemessenes Schutzniveau für personenbezogene Daten bietet, die aus der Europäischen Union an Empfänger übermittelt werden, die dem kanadischen Gesetz über den Schutz personenbezogener Daten und elektronische Dokumentation (PIPEDA – *Personal Information Protection and Electronic Documentation Act*) unterliegen.

Zweck des Arbeitsdokuments ist es, Ergebnisse zum Funktionieren der Entscheidung sowie etwaige Ergebnisse hinsichtlich einer etwaigen diskriminierenden Umsetzung zu präsentieren. Im Wesentlichen beruht es auf einer im Auftrag der Kommission durchgeführten Studie zur Analyse des Sachstandes in Kanada im Hinblick auf die Anwendung der Entscheidung. Auf der Grundlage dieser Studie sowie weiterer gesammelter Informationen gelangten die Kommissionsdienstellen zur Ansicht, dass das kanadische Gesetz über den Schutz personenbezogener Daten und elektronische Dokumentation (PIPEDA – *Personal Information Protection and Electronic Documentation Act*) nach wie vor ein angemessenes Schutzniveau für personenbezogene Daten im Sinne des Artikels 25 der Richtlinie bietet. Der in Artikel 3 der Entscheidung 2002/2/EG niedergelegte Vorbehalt, dass nämlich bei der Übermittlung von Daten in Länder außerhalb der Europäischen Union bestimmte Sicherheitsvorkehrungen erforderlich sind, wurde aufrechterhalten.

3.2. DER EUROPÄISCHER GERICHTSHOF

Urteil des Gerichtshofs (Große Kammer) vom 30. Mai 2006 über Fluggastdatensätze (Passenger Name Records – PNR; verbundene Rechtssachen C-317/04 und C-318/04): Das Gericht annulliert die Entscheidung des Rates über den Abschlusses eines Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Übermittlung und Verarbeitung von personenbezogenen Daten sowie die Entscheidung der Kommission über den angemessenen Schutz dieser Daten.

Das Gericht stellt fest, dass die Angemessenheitsentscheidung sich ausschließlich auf PNR-Daten bezieht, die an das United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten, CBP) übermittelt werden und dass es sich bei der Übermittlung von PNR-Daten an das CBP um Verarbeitungsoperationen mit Auswirkung auf die öffentliche Sicherheit und auf die Handlungen des Staates im Bereich des Strafrechts handelt, was durch Artikel 3 (2) der Richtlinie ausdrücklich aus dem Geltungsbereich der Richtlinie ausgeschlossen ist. Folglich fällt die genannte Entscheidung nicht in den Geltungsbereich der Richtlinie und wird ohne Beachtung sonstiger Einwände für nichtig erklärt.

Das Abkommen bezieht sich auf die gleiche Datenübermittlung wie die Angemessenheitsentscheidung, das heißt, auf Datenverarbeitungsoperationen, die aus dem Geltungsbereich der Richtlinie ausgeschlossen sind. Folglich bildet die Verbindung von Artikel 95

EG und von Artikel 25 der Richtlinie keine gültige Rechtsgrundlage für den Abschluss der Vereinbarung. Im Interesse der Rechtssicherheit belässt das Gericht die Angemessenheitsentscheidung und die Vereinbarung noch 90 Tage lang in Kraft, um eine ordnungsgemäße Beendigung zu ermöglichen.

3.3. DIE EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

Einleitung

Der Europäische Datenschutzbeauftragte (EDPS – European Data Protection Supervisor) ist ein unabhängiger Amtsträger, der die ordnungsgemäße Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen[3] der Europäischen Gemeinschaft überwacht. Der Europäische Datenschutzbeauftragte berät die Organe und Einrichtungen der Gemeinschaft auch bei Legislativvorschlägen, die Auswirkungen auf den Datenschutz haben könnten. Ferner arbeitet er mit den Datenschutzbehörden der Mitgliedstaaten sowie mit den Behörden in der dritten Säule der Europäischen Union (Polizei- und Justizkooperation in Strafsachen) zusammen, um konsequenten 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. Dabei handelt es sich um eine Zusammenfassung der einschlägigen Bestimmungen der Richtlinien 95/46 und 2002/58.

Der Europäische Datenschutzbeauftragte nahm seine Tätigkeit im Jahr 2004 auf. Die ersten zwei Jahre wurden auf den buchstäblichen Aufbau der Behörde und die Konsolidierung ihrer Aufgaben verwendet. Im Jahr 2006 konnte die Anzahl der verabschiedeten Stellungnahmen dann deutlich gesteigert werden. Damit kam die Zeit, sich auch der Beurteilung der Ergebnisse – d. h. der Richtlinienkonformität – zuzuwenden. Der allgemeine Eindruck lautet, dass die EU-Verwaltung in dieser Hinsicht Fortschritte gemacht hat und immer häufiger auf den Europäischen Datenschutzbeauftragten zukommt, um den Datenschutz in ihre alltägliche Praxis bei der Verarbeitung personenbezogener Daten sowie bei der Ausarbeitung neuer legislativer Texte zu integrieren.

Überwachung

Diese Aufgabe des Europäischen Datenschutzbeauftragten besteht darin, die gemeinschaftlichen Organe und Einrichtungen zu überwachen und dafür zu sorgen, dass sie die in der Verordnung 45/2001 festgeschriebenen Verpflichtungen für den Datenschutz einhalten. Die Entwicklung einer Datenschutzkultur in der EU-Verwaltung ist eine dringende Notwendigkeit. Der Europäische Datenschutzbeauftragte hat eine Lernphase bis zum Frühjahr 2007 einkalkuliert, nach der gegebenenfalls Maßnahmen zur Durchsetzung dieser Verpflichtungen eingeleitet werden. Die wichtigsten Elemente im Jahr 2006 waren:

- Die Anzahl an **Datenschutzbeauftragten** (DBA) in den Organen und Einrichtungen ist im Jahresverlauf kontinuierlich angestiegen. Der Europäische Datenschutzbeauftragte setzte seine Unterstützung für das Netz der Datenschutzbeauftragten fort und veranstaltete einen Workshop für neue Datenschutzbeauftragte. Es finden laufend bilaterale Evaluierungen der Fortschritte bei der Einhaltung der Meldepflichten in den großen Institutionen statt.
- Im Jahr 2006 wurden 54 **Stellungnahmen nach Vorabprüfung** zu risikobehafteten Verarbeitungssystemen herausgegeben. Davon betrafen 49 bestehende Systeme, die in Betrieb genommen wurden, bevor der Europäische

[3] Der Terminus „Organe und Einrichtungen" in Verordnung (EG) 45/2001 schließt auch die Gemeinschaftsagenturen ein. Ein umfassende Liste finden Sie unter folgender Verknüpfung: http://europa.eu/agencies/community_agencies/index_de.htm

Datenschutzbeauftragte seine Tätigkeit aufnahm bzw. bevor die Verordnung in Kraft trat. Die Vorabprüfungen betrafen vor allem die Verarbeitung personenbezogener Daten im Zusammenhang mit Personalbeurteilungen, Krankenakten, E-Monitoring, Disziplinarverfahren und Sozialdienstleistungen.

- Im Jahr 2006 gingen 52 **Beschwerden** ein, von denen 10 für zulässig befunden wurden und zu einer näheren Untersuchung Anlass gaben. Der Großteil der eingegangenen Beschwerden lag nach wie vor außerhalb der Überwachungszuständigkeiten des Europäischen Datenschutzbeauftragten und betraf beispielsweise Probleme auf mitgliedstaatlicher Ebene.
- Im November wurde eine Gemeinsame Absichtserklärung mit dem **Europäischen Bürgerbeauftragten** unterzeichnet, die einen Rahmen für das Vorgehen in Fällen liefert, die unter die Zuständigkeit beider Stellen fallen.
- Im Jahresverlauf 2006 wurde eine Reihe von **Untersuchungen** in verschiedenen Bereichen durchgeführt. Dazu zählte etwa eine bei der GD Wettbewerb der Europäischen Kommission. Dabei wurde im Auftrag der Kommission eine breit angelegte Branchenuntersuchung durchgeführt, bei der auch die Erhebung von Verbraucherdaten überprüft wurde. Eine weitere Untersuchung betraf die unterschiedlichen Rollen der Europäischen Zentralbank (EZB) im Zusammenhang mit dem Zugriff der US-Behörden auf das SWIFT-System (Mitteilungssystem für den internationalen Zahlungsverkehr). Der Europäische Datenschutzbeauftragte verlangte von der EZB, dafür zu sorgen, dass die europäischen Zahlungssysteme umfassend mit den europäischen Datenschutzgesetzen im Einklang stehen, und er wird die Entwicklungen im Jahresverlauf 2007 genau verfolgen.
- Der Europäische Datenschutzbeauftragte gab auch häufiger als in den Vorjahren Stellungnahmen zu **Verwaltungsakten** ab. Er leitete auf eigene Initiative eine Erhebung zur Praxis im Umgang mit persönlichen Dateien ein. Ferner leitete der Europäische Datenschutzbeauftragte Untersuchungen zur Übermittlung personenbezogener Daten an Drittländer und internationale Organisationen sowie zum Einsatz von Videoüberwachung in den Organen und Einrichtungen ein. Die Arbeit zu diesen wichtigen Themen wird 2007 fortgesetzt.
- Ebenfalls fortgesetzt wurde die Arbeit im Bereich des Dokuments **Zugang der Öffentlichkeit zu Dokumenten und Datenschutz**. Der Europäische Datenschutzbeauftragte trat in einem Fall vor dem Erstinstanzgericht auf und unterstützte dabei den Antrag des Klägers auf vollständige Offenlegung der verlangten Anwesenheitsliste durch die Kommission. Ein Entwurf des Arbeitsdokuments **E-Monitoring**, in dem es um Daten geht, die bei der Verwendung elektronischer Kommunikationsmittel (Telefon, E-Mail, Internet) anfallen, wurde an Datenschutzbeauftragte verteilt, um deren Anmerkungen und Reaktionen dazu zu sammeln. Außerdem wurde ein Workshop veranstaltet, um die Leitlinien des Dokuments zu testen.
- Die gemeinsam mit den Datenschutzbeauftragten der einzelnen Mitgliedstaaten durchgeführte Überwachung von **EURODAC** wurde im Jahresverlauf fortgesetzt. Der Europäische Datenschutzbeauftragte begann im September 2006 im Zusammenwirken mit deutschen und französischen Fachleuten ein detailliertes Sicherheitsaudit. Der Vorlage des endgültigen Berichts erfolgt bis Frühjahr 2007.

Beratung

Dem Europäischen Datenschutzbeauftragten kommt gegenüber der EU-Verwaltung eine Beraterrolle in sämtlichen Fragen des Schutzes personenbezogener Daten zu. Insbesondere gilt dies für Legislativvorschläge mit möglichen Auswirkungen auf den Datenschutz. Meilensteine des Jahres 2006 waren etwa:

- Weiterentwicklung der Beratungstätigkeit und Veröffentlichung einer **Aufstellung** der für 2007 vorgesehenen Schritte auf der Website im Dezember 2006.
- Die Veröffentlichung von 11 offiziellen **Stellungnahmen** zu unterschiedlichen Bereichen,

wie etwa Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, Visa (einschließlich des Zugriffsrechts auf das umfassende Visa-Informationssystem (VIS) für die Strafverfolgungsbehörden), Reisepässe, konsularische Instruktionen, Finanzangelegenheiten sowie eine zweite Stellungnahme zum Datenschutz in der dritten Säule.

- **Interventionen** in externe Entwicklungen mit Bezug zur Tätigkeit des Europäischen Datenschutzbeauftragten, wie etwa das Konzept der Interoperabilität, die Übermittlung von Fluggastdatensätzen nach dem PNR-Urteil des Europäischen Gerichtshofs, die Speicherung von Verbindungsdaten, der Abschluss des Rechtsrahmens für die zweite Generation des Schengener Informationssystems (SIS II) sowie die Verhandlungen im Rat über den Vorschlag für einen Rahmenbeschluss zum Schutz personenbezogener Daten in der dritten Säule.
- Beobachtung neuer **technologischer Entwicklungen**, wie etwa so genannte *Enabling Technologies* sowie Forschung und Entwicklung für den Schutz der Privatsphäre und den Datenschutz. Die Entwicklungen in Politik und Gesetzgebung wurden ebenfalls beobachtet, und zwar nicht nur im Zusammenhang mit den Bereichen Freiheit, Sicherheit und Recht, sondern darüber hinaus in weiteren Feldern, etwa durch eine Prüfung des Rechtsrahmens für den Schutz der Privatsphäre in elektronischen Kommunikationen.

Zusammenarbeit

Die Zusammenarbeit des Europäischen Datenschutzbeauftragten berührt nicht nur den Datenschutz im Rahmen der ersten Säule (EG-Vertrag), sondern beinhaltet auch die Kooperation mit nationalen Aufsichtsbehörden der dritten EU-Säule mit dem Ziel eines einheitlicheren Schutzes personenbezogener Daten. Meilensteine des Jahres 2006 waren etwa:

- Der Europäische Datenschutzbeauftragte arbeitete weiterhin eng mit der **Artikel-29-Datenschutzgruppe** zusammen und leistete einen aktiven Beitrag zu den drei von der Datenschutzgruppe herausgegebenen Stellungnahmen zur Übermittlung von Fluggastdatensätzen in die Vereinigten Staaten. Gute Synergieeffekte zwischen den Stellungnahmen der Datenschutzgruppe und dem Europäischen Datenschutzbeauftragten wurden im Jahresverlauf 2006 etwa bei der Vorratsspeicherung von Telekommunikationsdaten, bei den Unterhaltspflichten und bei der Prüfung der Richtlinie zum Schutz der Privatsphäre in der elektronischen Kommunikation erzielt.
- Im Zusammenwirken mit den Aufsichtsbehörden für die Informationssysteme **Schengen, Europol, Eurojust und für das Zollinformationssystem** setzte sich der Europäische Datenschutzbeauftragte weiterhin für ein hohes und einheitliches Datenschutzniveau ein. Dieses Ziel gewinnt angesichts der zahlreichen Vorschläge zum Austausch personenbezogener Daten im Rahmen der Strafverfolgung immer mehr an Bedeutung.
- Der Europäische Datenschutzbeauftragte nahm auch an der **Europäischen Konferenz sowie an der Internationalen Konferenz** zum Schutz der Privatsphäre und zum Datenschutz teil. Letztere war zur Gänze dem Thema „Die Überwachungsgesellschaft" gewidmet und mündete unter anderem in eine allgemein unterstützte Erklärung mit dem Titel „Communicating Data Protection and Making It More Effective" („Datenschutz vermitteln und wirksamer gestalten"; auch als „Londoner Initiative" bezeichnet). Als einer der Architekten der Initiative wird der Europäische Datenschutzbeauftragte auch an der Überwachung der Entwicklung im Jahresverlauf 2007 mitwirken.

Kapitel 4

Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

Island

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

Im Jahr 2007 wurde eine Reihe von Gesetzen, Verwaltungsregeln und -verordnungen verabschiedet. Die wichtigsten davon waren die Folgenden:

1. Gesetz Nr. 21/2006 zur Änderung des Gesetzes Nr. 47/1993 über die Beschäftigungs- und Niederlassungsfreiheit von EWR-Bürgern in Island sowie des Gesetzes Nr. 97/2002 über die Beschäftigtenrechte von Ausländern. Mit diesem Gesetz soll die Überwachung von Gesetzen hinsichtlich der Beschäftigtenrechte von Bürgern aus den neuen EU-Mitgliedstaaten (Tschechische Republik, Estland, Zypern, Lettland, Litauen, Ungarn, Malta, Polen, Slowakei und Slowenien) erleichtert werden. Dieses Gesetz sieht bis zum 1. Mai 2009 vor, dass Beschäftigte aus diesen Ländern durch ihre Arbeitgeber bei der Arbeitsverwaltung *(Vinnumálastofnun)* angemeldet werden müssen. Weitere Bestimmungen verpflichten den Arbeitgeber zur Vorlage bestimmter Dokumente, wie etwa des Arbeitsvertrags, bei dieser Behörde. Ferner gestattet das Gesetz die Verknüpfung der Daten über die genannten Beschäftigten zwischen der Arbeitsverwaltung, der Ausländerbehörde *(Útlendingastofnun)*, der Polizei und den Steuerbehörden. «Die isländische Datenschutzbehörde *(Persónuvernd)* kritisierte diese Bestimmung, so dass sich das Parlament zu einer Klärung entschloss. Nun heißt es in der Bestimmung, dass die Verknüpfung zu dem Zweck gestattet ist, herauszufinden, ob das Gesetz Nr. 97/2002 über die Beschäftigungsrechte von Ausländern eingehalten wird, dass die Verknüpfung innerhalb einer angegebenen Aufgabe erfolgen muss und dass keine permanente Verknüpfung der Daten erfolgen darf.

2. Gesetz Nr. 46/2006 zur Änderung des Polizeigesetzes Nr. 90/2006 sowie des Gesetzes Nr. 92/1989 über die Exekutivgewalt des Staates in den Bezirken Islands. Das Gesetz enthält eine Bestimmung, die eine rege Debatte auslöste. Diese Bestimmung betrifft die so genannte Untersuchungsabteilung innerhalb der Polizei. Die Debatte betraf die Frage, ob es sich dabei um einen Geheimdienst handeln würde. Da es jedoch keine Bestimmungen gibt, die dieser Abteilung irgendwelche weitergehenden Befugnisse verleihen würden als anderen Abteilungen der Polizei, sah die Datenschutzbehörde keinen Anlass zu besonderen Anmerkungen über die Gesetzesvorlage, die dann auch in dieser Form verabschiedet wurde.

3. Gesetz Nr. 53/2006 über die Erlangung von Beweisen bei mutmaßlichen Verletzungen geistiger Eigentumsrechte. Dieses Gesetz ermöglicht den Inhabern geistiger Eigentumsrechte das Einholen gerichtlicher Verfügungen zur Untersuchung der Verletzung der genannten Rechte. Die Untersuchungshandlungen müssen stets durch die zuständigen Staatsbeamten durchgeführt werden, die Inhaber der geistigen Eigentumsrechte erhalten aber gewisse Zugriffsrechte auf beschlagnahmtes Material und dürfen unter gewissen Auflagen bei den Untersuchungshandlungen anwesend sein.

4. Gesetz Nr. 64/2007 über Maßnahmen gegen Geldwäsche. Dieses Gesetz enthält Bestimmungen, welche die Finanzinstitute verpflichten, von ihren Kunden bei Transaktionen Identitätsnachweise zu verlangen, sowie Bestimmungen über die Verarbeitung personenbezogener Daten zur Bekämpfung von Geldwäsche. Das Gesetz löst Gesetz Nr. 80/1993 ab und beruht auf der Richtlinie 2005/60/EG zur Verhinderung und Untersuchung von Geldwäsche.

5. Verordnung Nr. 837/2006 zur elektronischen Überwachung. Diese Verordnung, die sich auf die elektronische Überwachung am Arbeitsplatz, in Schulen und in sonstigen Bereichen mit beschränktem Personenaufkommen bezieht, wurde durch die Datenschutzbehörde Persónuvernd aufgrund des Gesetzes Nr. 77/2000, Paragraf 37, erlassen.

Sie ersetzt die Verordnung Nr. 888/2004 und enthält unter anderem Bestimmungen dazu, wann elektro-

nische Überwachung überhaupt eingesetzt werden darf, wie lange die bei einer derartigen Überwachung aufgezeichneten Daten gespeichert werden dürfen, ferner Bestimmungen zur automatischen Überwachung (Scanning) der Internet-Nutzung am Arbeitsplatz, zur automatischen Erfassung der Fahrdaten von Beschäftigten, zur Überwachung der Arbeitsleistung, zur Pflicht des für die Überwachung Verantwortlichen, den betroffenen Datensubjekten Auskunft zu erteilen, sowie zur Pflicht des für die Überwachung Verantwortlichen, Regeln für die Überwachung niederzulegen, wenn die Überwachung in die Verarbeitung personenbezogener Daten mündet, d. h. wenn das erfasste Material gespeichert wird.

B. Bedeutende Rechtsprechung

Am 1. Juni 2006 erging ein Urteil des Obersten Gerichtshofs in einem Fall zur Veröffentlichung von E-Mails in einer Zeitung. Dabei ging es um die Frage, ob die Veröffentlichung von E-Mails einen Verstoß gegen die Bestimmungen des isländischen Strafgesetzbuchs zum Schutz der Privatsphäre darstellt, ferner um die Rechtmäßigkeit einer einstweiligen Verfügung gegen die weitere Verbreitung der E-Mail-Inhalte und gegen die weitere Herausgabe der Zeitung, in deren Besitz sich diese E-Mails befanden. Die E-Mails betrafen anstehende Anklagen gegen prominente isländische Geschäftsleute wegen mutmaßlich gesetzwidrigen Verhaltens. Nach Einschätzung der Zeitung hatten die Personen, zwischen denen die E-Mails ausgetauscht wurden, den Fall ins Rollen betracht, was durch die Veröffentlichung der E-Mails belegt werden sollte. Eine der Personen erwirkte die genannte einstweilige Verfügung und erstattete Anzeige gegen die Zeitung, da ihrer Ansicht nach eine Verletzung ihrer Privatsphäre und somit der genannten Bestimmungen des Strafgesetzbuchs vorlag. Der Oberste Gerichtshof schloss sich dieser Argumentation nicht an und verwies unter anderem darauf, dass die Vorwürfe gegen die Geschäftsleute zu einer regen öffentlichen Debatte Anlass gegeben hatten. Daher waren die E-Mails nach Einschätzung des Obersten Gerichts von öffentlichem Interesse. Somit setzte das Oberste Gericht die Verfügung außer Kraft und sprach die Zeitung vom Vorwurf des Verstoßes gegen das Strafgesetzbuch frei.

Am 21. Dezember 2006 entschied das Bezirksgericht Reykjavík gegen die Klage eines Bürgers, eine Entscheidung der Datenschutzbehörde Persónuvernd vom 27. Februar 2006 für nichtig zu erklären. Beim Kläger handelte es sich um einen Arzt der, laut der Entscheidung, auf die Patientenakte einer Person ohne deren Einwilligung zugegriffen hatte, um eine Gesundheitsbeurteilung für eine Versicherungsgesellschaft zu erstellen. Die Datenschutzbehörde Persónuvernd befand, dass es sich um einen gesetzwidrigen Zugriff handelte, da keine Einwilligung der betroffenen Person vorlag. Das Bezirksgericht Reykjavík schloss sich dieser Auffassung an.

C. Wichtige spezifische Themen

Eine der Hauptaufgaben der Datenschutzbehörde Persónuvernd im Jahre 2006 waren Inspektionen. Es wurden formelle administrative Entscheidungen hinsichtlich der Rechtmäßigkeit und der Sicherheit der Verarbeitung personenbezogener Daten bei den Sozialämtern von fünf Stadtgemeinden (darunter Reykjavík), bei drei Arbeitsämtern, bei der Gefängnisverwaltung und bei drei Gesundheitsämtern gefällt.

Liechtenstein

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

2006 traten folgende für den Datenschutz wichtige Gesetze in Kraft:

Die Verordnung vom 21. Februar 2006 über das Bearbeiten von Personendaten im Bereich des präventiven Staatsschutzes (Staatsschutz Datenschutzverordnung; StDSV) wurde durch die Regierung auf Grund der Verordnungskompetenz nach Art. 43 des Datenschutzgesetzes (DSG) erlassen. Art. 43 DSG sieht für die Bearbeitung von Personendaten in besonderen Be-reichen der Verbrechensbekämpfung (Terrorismus, gewalttätiger Extremismus, organisiertes Verbrechen und des verbotenen Nachrichtendienstes) sowie zur Gewährleistung der staatli-chen Sicherheit gewisse Ausnahmen von Bestimmungen des DSG vor, welche bis zum In-krafttretens eines Gesetzes, welches diese Bereiche regelt, vor. Diese Verordnung wurde in enger Zusammenarbeit mit dem Datenschutzbeauftragten ausgearbeitet. Die baldige Schaffung eines Gesetzes ist wichtig und dringend, damit wieder ein Gleichgewicht in den erwähnten Bereichen mit dem Recht auf Achtung der Privatsphäre hergestellt werden kann.

Das Gesetz vom 17. März 2006 über die elektronische Kommunikation (Kommunikationsge-setz; KomG), mit welchem unter anderem die Richtlinie 2002/58/EG umgesetzt wurde, trat in Kraft.

Das Heimatschriftengesetz (HSchG) vom 18. Dezember 1985 wurde zur Einführung der bio-metrischen Pässe in Umsetzung der Verordnung 2252/2004/EG über Normen für Sicher-heitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten geändert. Dabei war die Sicherheit der Daten ein Schwerpunkt der Landtagsdiskussion. Das Gesetz sieht vor, dass die Daten im Reisepass aufzunehmen sind (Art. 16a). Somit ist davon auszugehen, dass es zu keiner zentralen Speicherung der biometrischen Daten kommt, was aus Datenschutzsicht zu begrüssen ist. Ursprünglich war die Aufnahme der nationalen Kennnummer (PEID) ebenfalls geplant. Der Datenschutzbeauftragte argumen-tierte aus verschiedenen Gründen gegen die Aufnahme dieser Nummer in den Pass, vor allem, da sie sich bisher noch auf keine gesetzliche Grundlage stützen kann. Weiters sprachen keine zwingenden Gründe für die Aufnahme dieser Nummer in den Reisepass, so dass die Regierung schliesslich von dieser Idee Abstand nahm.

Das Personen- und Gesellschaftsrecht (PGR) wurde im Zusammenhang mit der Richtlinie 2003/58/EG in Bezug auf die Offenlegungspflichten von Gesellschaften bestimmter Rechts-formen (so genannte modernisierte Publizitätsrichtlinie) geändert, welche im Wesentlichen verlangt, dass die offenlegungspflichtigen Daten über ein Unternehmen über „eine Akte" e-lektronisch abrufbar sind, offen zu legende Dokumente elektronisch verfügbar sind, die Möglichkeit des elektronischen Geschäftsverkehrs mit der Registerbehörde realisiert wird und die gesetzlich vorgeschriebenen Bekanntmachungen auf einer zentralen elektronischen Plattform erfolgen und archiviert werden.

Insgesamt gab der DSB Stellungnahmen zu 23 Gesetzesvorhaben ab.

B. Bedeutende Rechtssprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Nachdem im Sommer bekannt geworden war, dass das US-Finanzministerium (UST) von der Society for Worldwide Interbank Financial Telecommunication (SWIFT) Zugang zu den in den USA gespeicherten Daten im Rahmen internationale Zahlungsanweisungen forderte und auch bekam, wurde dieses Thema rasch durch die Artikel 29 Arbeitsgruppe aufgenommen und auch in Liechtenstein ein Thema. Der DSB nahm in diesem Zusammenhang Kontakt mit dem Bankenverband auf

und wies auf die Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunica-tion (SWIFT), WP 128, und insbesondere die Pflicht der Finanzinstitute zur Information ihrer Kunden, hin. Diese komplexe Angelegenheit war bei Jahresende noch nicht abgeschlossen.

Die Prüfung der Umsetzung der erteilten Zugriffsbewilligungen im Rahmen der von der Lan-desverwaltung geführten Zentralen Personenverwaltung (ZPV) konnte nicht bis Jahresende abgeschlossen werden.[1] Weiterhin stellen sich grundsätzliche Fragen zur Beschaffenheit der ZPV (Verhältnismässigkeit der Datenbearbeitung, Protokollierung von Lesezugriffen, Lö-schung und Sperrung von Daten).

Information der Öffentlichkeit: Auf der Internetseite des Datenschutzbeauftragten www.sds.llv.li wurde über aktuelle und/oder wichtige Themen informiert. Davon sind vor allem die folgenden stichwortartig zu nennen: Neues Lernprogramm zur Datensicherheit und zum Datenschutz; Telefonieren mit Internettechnologie; Spyware; Hooliganismus, Fussball WM und Datenschutz; Geolokalisierung (Ortung) von Personen; Datenschutztipps für die Ferien; Dokumentenmanagementsysteme (DMS) und Datenschutz bei Suchmaschinen. Zur Problematik von Phishing Mails wurde eine Pressemitteilung verfasst.

Dazu wurde die Möglichkeit der Bestellung eines Newsletters über Neuigkeiten zum Datenschutz geschaffen.

Schliesslich wurden „Richtlinien über technische und organisatorische Massnahmen zur Gewährleistung der Datensicherheit" sowie „Richtlinien zur Bearbeitung von Personendaten durch Behörden" erstellt und in der Liechtensteinischen Juristen-Zeitung (LJZ) ein Aufsatz zum Thema „Die Einwilligung als zentrales Element des Datenschutzrechts" veröffentlicht.

[1] Siehe dazu bereits im 9. Jahresbericht.

Norwegen

A. Umsetzung der Richtlinie 95/46/EG

Bedeutende Änderungen in Datenschutzgesetzen bzw. Gesetzen zum Schutz der Privatsphäre

Keine nennenswerten.

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

Neues Gesetz über politische Parteien
Am 1. Januar 2006 ist ein neues Parteiengesetz in Kraft getreten. Unter Datenschutzgesichtspunkten betreffen die wichtigsten Bestimmungen die Einrichtung eines zentralen Registers und die Übermittlung von Angaben über finanzielle Zuwendungen von Privatpersonen an politische Parteien sowie das Verbot der Entgegennahme anonymer Spenden.

Eine Bemerkung der Datenschutzbehörde Datatilsynet in der Konsultationsrunde betraf folgenden Punkt:

„Privatpersonen können sehr wohl legitime Gründe dafür haben, dass sie ihren Namen in Verbindung mit einer Parteienspende nicht preisgeben wollen. Unsere Gesetzgebung sollte auch die Tatsache widerspiegeln, dass finanzielle Zuwendungen an politische Parteien eine Privatangelegenheit sein können."

Innerbetriebliche Hinweisgeber
Am 1. Januar 2007 traten neue Bestimmungen in Bezug auf innerbetriebliche Hinweisgeber im Berufsleben in Kraft. Den neuen Vorschriften zufolge müssen Wirtschaftsunternehmen zwar vorschriftsmäßige Lösungen für Hinweisgeber einführen, die Bestimmungen lassen nun jedoch Raum für eine anonyme Mitteilung. Die Routinen für Daten, Offenlegung, Speicherung usw. ergeben sich aus dem Gesetz über den Schutz personenbezogener Daten. Die neuen Bestimmungen greifen nicht wesentlich in die Datenschutzvorschriften ein, werden aber dennoch erwähnt, da Regelungen für innerbetriebliche Hinweisgeber ein Thema sind, das in der Artikel-29-Datenschutzgruppe häufig diskutiert wird.

Änderungen des Gesetzes über Kinderfürsorgedienste:
Aufgrund von Änderungen des Gesetzes über Kinderfürsorge, die am 1. Januar 2006 in Kraft traten, sind Angestellte privater Krisenzentren, die Zuschüsse erhalten, zur Offenlegung gegenüber den Kinderfürsorgebehörden verpflichtet, falls Grund zu der Annahme besteht, dass die in das Krisenzentrum gebrachten Kinder vernachlässigt werden. Die Datenschutzbehörde Datatilsynet lehnte diese Bestimmung energisch ab und vertritt die Ansicht, dass sie einen schweren Verstoß gegen die Privatsphäre von Personen darstellt, die ein Krisenzentrum in einer Notfallsituation kontaktieren.

Gesetz über die Arbeits- und Sozialverwaltung
NAV ist das Kürzel für die norwegische Arbeits- und Sozialbehörde (Arbeids- og velferdsforvaltningen). Sie wurde am 1. Juli 2006 im Zuge einer umfassenden Reform des Sozialsystems gegründet. Die NAV verwaltet eine sehr hohe Zahl sensibler Daten über fast jede in Norwegen wohnhafte Person, von der Geburt bis zum Tod. Das Gesetz führte zu Forderungen nach einem verbesserten Datenschutz, unter anderem im Bereich der gesetzlichen Geheimhaltungspflicht. Das schwierigste Problem ist, dass sich die Zahl der Personen mit Zugriff auf sensible personenbezogene Daten praktisch verdoppelt hat und keine angemessenen Beschränkungen für den Zugriff auf das IKT-System bestehen.

Rechtsvorschriften in Bezug auf das Gesundheitsregister der Streitkräfte wurden im Februar 2005 angenommen, traten aber erst am 24. April 2006 in Kraft. Das Gesundheitsregister der Streitkräfte kann u. a. personenbezogene Daten, Leistungs- und Gesundheitsdaten von Soldaten und Zivilbeschäftigten, sowie Daten über das physische und soziale Umfeld umfassen. Das Register birgt

eine erhebliche Zahl von Gesundheitsdaten über die Soldaten und Zivilbeschäftigten der Streitkräfte, ohne dass die Betroffenen ihre Einwilligung zu dieser Erfassung erteilt hätten.

Änderungen der Vorschriften für Familienbeihilfen
Schulen können nun angehalten werden, dem Nationalen Sozialversicherungsdienst Routineberichte zu übermitteln, wenn Schüler abwesend sind und ihre Abwesenheit möglicherweise auf einem Auslandsaufenthalt beruht. Diese Änderungen sind im April 2006 in Kraft getreten.

Am 1. Januar 2005 trat das **Registrierungsgesetz für Devisen** *(Valutaregisterloven)* in Kraft. Im Januar 2006 wurden Änderungen vorgeschlagen, die der Polizei erweiterte Befugnisse einräumen würden. Davor war der Datenzugriff nur in Verbindung mit bereits laufenden Ermittlungen zulässig. Das geänderte Gesetz sieht als Kriterium für den Zugriff vor, dass Behörden zur Prävention und Bekämpfung von Kriminalität Informationen benötigen.

Paragraf 7 des Staatsangehörigkeitsgesetzes erhielt einen neuen dritten Paragrafen, der für die Beantragung der norwegischen Staatsangehörigkeit nunmehr die Vorlage eines polizeilichen Führungszeugnisses vorschreibt. Die Datenschutzbehörde forderte eine Beurteilung der Frage, ob die Verletzung bestimmter Strafrechtsbestimmungen als weniger relevant betrachtet werden könnte. Dieser Forderung wurde jedoch nicht Folge geleistet. Das polizeiliche Führungszeugnis wird auch frühere Anschuldigungen und Anzeigen enthalten, sogar für den Fall, dass eine Anschuldigung oder Anzeige abgewiesen wurde und die Strafverfolgungsbehörden es verabsäumt haben, den Eintrag entsprechend zu aktualisieren. Erfreulicherweise wurde der Vorschlag, alle Behörden von der Geheimhaltungspflicht zu entbinden und sie zugleich zur Weitergabe von Daten zu verpflichten, falls die Einwanderungsbehörden Angaben zur Bearbeitung von Einbürgerungsanträgen benötigen, nicht verabschiedet.

B. Bedeutende Rechtsprechung

Keine nennenswerten Entscheidungen.

C. Wichtige spezifische Themen

Verkehrsüberwachung
Die Datenschutzbehörde Datatilsynet befasst sich weiterhin mit Fragen der neuen Infrastrukturen zur Überwachung des Straßenverkehrs und der öffentlichen Verkehrsmittel. Die Behörde stellt fest, dass einige EU-weit eingeführte Systeme, wie eCall, die Implementierung neuer Überwachungsanlagen voraussetzen würden. Zusätzlich dazu hat Norwegen vollautomatische Mautstationen eingerichtet, an denen RFID-Technologie zum Einsatz kommt. Diese Stationen machen eine anonyme Nutzung bestimmter Straßen sowie die anonyme Einfahrt in zwei norwegische Städte unmöglich.

Biometrik
Die Datenschutzbehörde Datatilsynet lehnte mehrere Anträge ab, die eine Verwendung biometrischer Merkmale für verschiedene Systeme zum Ziel hatten. Das Spektrum reichte von einem Garderobendienst bis hin zur Gebäudeüberwachung und zum Zugriff auf Datensysteme. Fünf Antragsteller wandten sich an den Beschwerdeausschuss der Datenschutzbehörde (Personvernnemnda), bis zur Abfassung des vorliegenden Berichts konnte vom Beschwerdeausschuss jedoch nur eine Beschwerde geregelt werden. Die Datenschutzbehörde Datatilsynet wird sich auch 2007 mit diesem Thema befassen.

Mangelhafter Schutz elektronischer Gesundheitsdaten
Die Datenschutzbehörde Datatilsynet führte 2006 in Zusammenarbeit mit der norwegischen Behörde für Gesundheitsaufsicht zwei Inspektionen in Krankenhäusern durch. Bei den Inspektionen sollte geprüft werden, ob die Gesundheitsdaten auf geeignete Weise geschützt werden. In beiden Krankenhäusern wurde ein mangelhafter Schutz sensibler Daten festgestellt. Der Zugriff der Mitarbeiter

auf Patientendaten überstieg das notwendige Maß, wodurch die Schweigepflicht bedroht wurde.

Strafandrohung für Child Grooming

Im Jahr 2006 schlug das Justizministerium vor, Handlungen, die den sexuellen Missbrauch von Kindern vorbereiten sollen („Child Grooming"), strafrechtlich zu ahnden. Die Datenschutzbehörde Datatilsynet erkundigte sich, ob neue polizeiliche Ermittlungsmethoden geplant wären, um diesem Vorschlag Folge zu leisten. Die Fahndung nach einer Person, die keine Straftat verübt hat, eine solche jedoch plant, kann die übermäßige Überwachung unschuldiger Personen nach sich ziehen.

Kapitel 5

Mitglieder der Art. 29 Datenschutzgruppe im Jahr 2006

MITGLIEDER DER ART. 29 DATENSCHUTZGRUPPE IM JAHR 2006

Österreich	**Belgien**
Frau Waltraut Kotschy Österreichische Datenschutzkommission Ballhausplatz 1 - AT - 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Herr Willem Debeuckelaere Kommission des Schutzes des Privatlebens (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32(0)2/213.85.40 Fax : +32(0)2/213.85.65 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Zypern	**Tschechische Republik**
Frau Goulla Frangou Kommissionsmitgliedes für Schutz persönlicher Daten (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 40, Themistokli Dervi str. Natassa Court, 3rd floor - CY - 1066 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) 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 Büro für Schutz persönlicher Daten (Ú ad pro ochranu osobních údaj) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-mail: posta@uoou.cz Website: http://www.uoou.cz/
Dänemark	**Estland**
Frau Janni Christoffersen Datenschutzagentur (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	Herr Urmas Kukk Estnisches Datenschutzinspektorat (Andmekaitse Inspektsioon) Väike - Ameerika 19 - EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 137 E-mail: info@dp.gov.ee Website: http://www.dp.gov.ee
Finnland	**Frankreich**
Herr Reijo Aarnio Büro des Datenschutzombudsmannes (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) 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 Nationale Kommission der Informatik und der Freiheiten (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +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 Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 - DE - 53117 Bonn Tel: +49 (0)1888 7799-0 Fax: +49 (0)1888 7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de Herr Alexander Dix (Vertreter der Bundesländer) Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4-10 - DE - 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Website: http://www.datenschutz-berlin.de	Herr Nikolaos Frangakis Hellenische Datenschutzbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Ampelokipi - GR - Athen Tel: +30 210 6475600 Fax: +30 210 6475628 E-mail: contact@dpa.gr Website: http://www.dpa.gr
Ungarn	**Irland**
Herr Attila Peterfalvi Datenschutzbeauftragte von Ungarn (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: http://abiweb.obh.hu/abi/	Herr Billy Hawkes Kommissionsmitglied des Datenschutzes (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tel: +353 57 868 4800 Fax:+353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie
Italien	**Lettland**
Herr Francesco Pizzetti Italienische Datenschutzaufsichtsbehörde (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	Frau Signe Plumina Data State Inspection (Datu valsts inspekcija) Kr. Barona 5-4, Riga, LV - 1050 Tel: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Website: http://www.dvi.gov.lv
Litauen	**Luxemburg**
Herr Algirdas Kunčinas Staatsdatenschutzinspektorat (Valstybinė duomenų apsaugos inspekcija) Žygimantų str. 11-6a - LT - 01102 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 Nationale Kommission für den Datenschutz (Commission nationale pour la Protection des Données - CNPD) 41, avenue de la Gare - LU - 1611 Luxembourg Tel: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Website: http://www.cnpd.lu

Malta	**Niederlande**
Herr Paul Mifsud Cremona Büro des Kommissionsmitgliedes des Datenschutzes (Office of the Data Protection Commissioner) 2, Airways House High Street - MT - SLM 1549 Sliema Tel: +356 2328 7100 Fax: +356 23287198 E-mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10 - NL - 2595 CL The Hague (Postbus 93374 - 2509 AJ The Hague) Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl
Polen	**Portugal**
Herr Michał Serzycki Generalinspektor für Schutz persönlicher Daten (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 70 86 Fax: +48 22 860 70 90 E-mail: kancelaria@giodo.gov.pl Website: http://www.giodo.gov.pl	Herr Luís Novais Lingnau da Silveira Nationale Kommission von Datenschutz (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa 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 Büro für den Schutz persönlicher Daten (Úrad na ochranu osobných údajov SR) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	Frau Natasa Pirc Musar Kommissionsmitglied der Informationen (Informacijski pooblaš̌enec) 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.ip-rs.si
Spanien	**Schweden**
Herr Artemi Rallo Lombarte Spanische Agentur des Datenschutzes (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6219/20 Fax: +34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Herr Göran Gräslund Dateninspektionsbehörde (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se Website: http://www.datainspektionen.se

Vereinigtes Königreich	**European Data Protection Supervisor**
Herr Richard Thomas Büro des Kommissionsmitgliedes der Informationen (Information Commissioner's Office) Wycliffe House Water Lane, SK9 5AF Wilmslow GB Tel: +44 1625 545745 Fax: +44 1625 524510 E-mail: Fuellen Sie bitte das Online-Kontaktformular auf unserer Website aus Website: http://www.ico.gov.uk	Herr Peter Hustinx Europäischer Datenschutzbeauftragter (European Data Protection Supervisor – EDPS) Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 63, BE - 1047 Brussels 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 2006

Island	**Norwegen**
Frau Sigrun Johannesdottir Datenschutzbehörde (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tel: +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Website: http://www.personuvernd.is	Herr Georg Apenes Dateninspektorat (Datatilsynet) P.O.Box 8177 Dep - NO - 0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E-mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Bulgarien**
Herr Philipp Mittelberger Stabsstelle für Datenschutz - SDS Kirchstrasse 8, Postfach 684 - LI -9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E-mail: info@sds.llv.li Website: http://www.sds.llv.li	Herr Krassimir Dimitrov Kommission für Schutz persönlicher Daten (Комисията за защита на личните данни) 1 Dondukov - BG - 1000 Sofia Tel: +359 2 940 2046 Fax: +359 2 940 3640 E-mail: kzld@government.bg Website: http://www.cdpd.bg
Rumänien	
Frau Georgeta Basarabescu Nationale Aufsichtsbehörde für persönliche Datenverarbeitung (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest 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
Herr Alain Brun Referatsleiterin Referat Datenschutz Generaldirektion Justiz, Freiheit und Sicherheit Europäische Kommission Büro: LX46 6/80 - BE - 1049 Brussels Tel: +32 2 296 53 81 Fax: +32 2 299 8094 E-mail: Alain.Brun@ec.europa.eu Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

NE-AC-08-001-DE-C
DOI 10.2758/15232

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 978-92-79-08198-9