

11. Jahresbericht

der Art. 29

Datenschutzgruppe



1830-6462

11. 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 2007

Angenommen am 24. Juni 2008

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

© Europäische Gemeinschaften, 2008

Die Wiedergabe ist unter Angabe der Quelle gestattet.

INHALT

Vorwort des Vorsitzenden der Art. 29 Datenschutzgruppe	5
1. Fragen, zu denen die Art. 29 Datenschutzgruppe Stellung genommen hat.	9
1.1. Transfer von Daten in Drittländer	10
1.2. Elektronische Kommunikation, Internet und neue Technologien	12
1.3. Buchhaltung, Verlagswesen und Finanzangelegenheiten	12
1.4. personenbezogene Daten	13
1.5. Biometrie & Gesundheit Daten	13
1.6. Rechtsdurchsetzung	14
1.7. Verbraucher	14
1.8. Binnenmarkt-Informationssystem	15
2. Die wichtigsten Entwicklungen in den Mitgliedstaaten	17
Österreich	18
Belgien	20
Bulgarien	28
Republik Zypern	31
Tschechische Republik	33
Dänemark	36
Estland	39
Finnland	43
Frankreich	47
Deutschland	55
Griechenland	57
Ungarn	60
Irland	63
Italien	65
Lettland	74
Litauen	77
Luxemburg	81
Malta	84
Niederlande	86
Polen	90
Portugal	93
Rumänien	96
Slowakei	101
Slowenien	106
Spanien	114
Schweden	121
Vereinigtes Königreich	125
3. Aktivitäten der Europäischen Union und der Gemeinschaft	127
3.1. Die Europäische Kommission	128
3.2. Der Europäische Gerichtshof	131
3.3. Der Europäische Datenschutzbeauftragte	132

4. Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum.....137

Island..... 138

Liechtenstein..... 142

Norwegen..... 145

5. Mitglieder und Beobachter der Art. 29 Datenschutzgruppe.....149

Mitglieder der Art. 29 Datenschutzgruppe im Jahr 2007..... 150

Beobachter der Art. 29 Datenschutzgruppe im Jahr 2007.....155

VORWORT DES VORSITZENDEN DER ART. 29 DATENSCHUTZGRUPPE

Die technologischen und wirtschaftlichen Entwicklungen führen zu einer immer umfangreicheren Verarbeitung personenbezogener Daten in immer komplexeren IT-Systemen. Gleichzeitig trägt die intensiviertere Zusammenarbeit zwischen den Mitgliedstaaten der Europäischen Union entscheidend dazu bei, dass personenbezogene Daten grenzüberschreitend verarbeitet werden, etwa im Zusammenhang mit der europäischen Dienstleistungsrichtlinie.

Auch Initiativen des Rates oder der Kommission zur Verbesserung der Bekämpfung von Terrorismus und schwerer Kriminalität wirken sich auf die Verarbeitung personenbezogener Daten im Binnenmarkt aus, etwa dann, wenn – entsprechend der Richtlinie 2006/24/EG – Telekommunikationsdaten von den Anbietern von Internet- und Telekommunikationsdiensten auf Vorrat gespeichert werden müssen oder wenn Fluggesellschaften zur Weitergabe von Passagierdaten verpflichtet werden, die sie für die Erbringung ihrer Dienstleistungen erheben und speichern.

Deshalb kann es nicht verwundern, dass sich die europäischen Datenschutzbehörden auch im Jahr 2007 zahlreichen Herausforderungen stellen mussten. Sie haben dabei viele wichtige Aufgaben bewältigt. So verabschiedete die Art. 29 Datenschutzgruppe insgesamt 17 Stellungnahmen. Außerdem erarbeitete und veröffentlichte sie weitere Dokumente zu wichtigen datenschutzrechtlichen Fragen.

Von besonderer Bedeutung war die heftig umstrittene Verarbeitung von Passagierdaten, die die Fluglinien für Strafverfolgungszwecke sammeln müssen. Die Art. 29 Datenschutzgruppe begleitete die Verhandlungen zu einem neuen PNR-Abkommen zwischen der EU und den USA kritisch und hielt sich mit ihrer Kritik auch nicht zurück, als die Kommission im November 2007 ihr eigenes Modell vorstellte, das die Einführung eines ähnlichen PNR-Systems in der EU vorsieht.

Die Art. 29 Datenschutzgruppe leistete einen wichtigen Beitrag zur Interpretation des Begriffs „personenbezogene Daten“ im Sinne der Richtlinie 95/46/EG. Sie befasste sich mit dem schwierigen, aber wichtigen Thema „Binding Corporate Rules“ (BCR), um den Koordinierungsprozess zwischen den Datenschutzbehörden zu beschleunigen. Nach langwierigen Debatten konnte sie die wegen des Zugriffs von US-Behörden auf Daten über den internationalen Zahlungsverkehr in die Kritik geratene Gesellschaft „SWIFT“ überzeugen, ihre Art der Datenverarbeitung und -übermittlung durch Einrichtung eines neuen Datenverarbeitungszentrums in Europa zu ändern.

Im folgenden soll auf einige Schwerpunktthemen näher eingegangen werden:

Zu den wichtigsten Aktivitäten der Art. 29 Datenschutzgruppe im Berichtsjahr gehörte der 1. Datenschutztag am 28. Januar, dem Jahrestag der Verabschiedung der Europarat-Konvention 108 im Jahre 1981.

Dieser Tag wurde gemeinsam von EU-Datenschutzbehörden und dem Europarat ausgerufen. Zusammen mit Parlamentariern, Politikern und Nicht-Regierungs-Organisationen gab es Aktionen in ganz Europa. Im Zentrum all dieser Bestrebungen standen die Unterrichtung der europäischen Bürgerinnen und Bürger, die Bewusstseinsförderung bei Jugendlichen und die Analyse der Herausforderungen für einen effektiven Datenschutz. Tage der offenen Tür, Podiumsdiskussionen, Zusammenkünfte mit hochrangigen Regierungsvertretern und eine umfangreiche Medienberichterstattung unterstrichen die Wichtigkeit des Datenschutzes angesichts der neuesten Vorschläge der EU und der Initiativen der Wirtschaft, die die Privatsphäre unserer Bürger bedrohen.

Eine gründliche Evaluierung aller Aktionen zum Europäischen Datenschutztag mit dem Ziel, Anregungen und Erfahrungen zwischen den Datenschutzbehörden auszutauschen und Vorbilder aufzuzeigen, wird uns helfen, im Jahr 2008 und in den folgenden Jahren noch besser zu werden.

Mit der Erarbeitung und Verabschiedung der Stellungnahme über personenbezogene Daten (**WP 136**) hat die Art. 29 Datenschutzgruppe einen bedeutsamen Beitrag zur einheitlichen Interpretation und harmonisierten Anwendung eines Schlüsselbegriffs der Richtlinie 95/46/EG geleistet. Unterschiedliche Auslegungen, was unter personenbezogenen Daten zu verstehen ist, könnten die Rechtssicherheit gefährden und den freien Datenverkehr behindern. Das Arbeitspapier, das als Leitfaden für alle dienen soll, die sich mit der Erfassung und Verarbeitung personenbezogener Daten befassen, muss als Meilenstein in der Arbeit der Art. 29 Datenschutzgruppe angesehen werden. Es wird sich unter anderem dann in vielen zukünftigen Diskussionen als nützlich erweisen, wenn es um die Möglichkeiten zur Verwendung und zur Re-Identifizierung anonymisierter Daten geht.

Nach einer teilweise heftig, aber konstruktiv geführten Debatte zwischen der Kommission und dem Rat über die Grundprinzipien des Übereinkommens und nach einem gut besuchten Workshop, der im März 2007 gemeinsam mit dem LIBE-Ausschuss des Europaparlaments ausgerichtet wurde, erfolgte im Juli 2007 die Unterzeichnung des dritten PNR-Übereinkommens zwischen der EU und den USA.

In ihrem Arbeitspapier **WP 138**, das am 17. August 2007 verabschiedet wurde, begrüßte die Arbeitsgruppe die Tatsache des Abschlusses eines neuen, langfristigen Übereinkommen als Rechtsgrundlage für die Übermittlung von Passagierdaten, womit eine Rechtslücke vermieden wurde. Sie äußerte aber auch deutliche Kritik über das zu niedrige in dem Abkommen vorgesehene Datenschutzniveau. Da das neue Übereinkommen viele Fragen offen lässt, hat sich die Art. 29 Datenschutzgruppe sowohl an die Kommission als auch an den Rat gewandt und ihre Hoffnung zum Ausdruck gebracht, dass zumindest diese Fragen geklärt werden können.

Hinsichtlich des von der Kommission am 6. November 2007 vorgelegten Vorschlags zu einem EU-PNR-System konnte die Art. 29 Datenschutzgruppe nur ihre erhebliche Enttäuschung zum Ausdruck bringen (**WP 145**). Der Vorschlag ist zu eng an das zuvor unterzeichnete EU-US PNR-Übereinkommen angelehnt. Die Kommission konnte aus Sicht der Datenschutzbehörden – insbesondere nach Verabschiedung der Richtlinie 2004/82/EG (API-Richtlinie) – einen dringenden Bedarf für ein solches zusätzliches System nicht darlegen. Die API-Richtlinie verpflichtet bereits die Fluglinien zur Erfassung der in den Pässen der Passagiere enthaltenen Daten, die – abgesehen für Zwecke der Grenz- und Einwanderungskontrolle – auch für Strafverfolgungszwecke genutzt werden können. Die Art. 29 Datenschutzgruppe vertritt die Ansicht, dass ungeachtet der vielen noch zu behebenden Mängel in dem Vorschlag zuerst einmal eine gründliche Evaluierung der API-Richtlinie durchgeführt werden muss, um festzustellen, ob Passagierdaten wirklich ein nützliches Hilfsmittel im Kampf gegen Terrorismus und schwere Kriminalität sind.

Die Art. 29 Datenschutzgruppe forderte deswegen den Rat auf, mit allen Stellen, die sich mit der Erhebung und Verarbeitung von Passagierdaten befassen, insbesondere Fluglinien, Betreibern von Computer-Reservierungssystemen, dem Europaparlament und den Datenschutz- und Verbraucherschutzorganisationen in einen Dialog zu treten, um datenschutzfreundliche Lösungen zu finden, die für alle Interessengruppen akzeptabel sind, und die deren berechtigten Belange berücksichtigen.

Bedeutsam war auch die Verabschiedung des Arbeitspapiers **WP 130** über die Verarbeitung personenbezogener Daten in den elektronischen Krankenakten von Krankenhäusern, Ärzten und Gesundheitsbehörden. Angesichts der Wichtigkeit dieses Bereichs und aufgrund der Tatsache, dass besonders sensible Daten erhoben und verarbeitet werden, hielt es die Art. 29 Datenschutzgruppe für unerlässlich, ein entsprechendes Bewusstsein zu fördern und Leitlinien für alle Beteiligten herauszugeben. Nach der Veröffentlichung des Dokuments in einem so genannten „Konsultationsverfahren“ erhielt die Art. 29 Datenschutzgruppe zahlreiche Kommentare, die im Jahr 2008 erörtert werden sollen und gegebenenfalls berücksichtigt werden.

Die Art. 29 Datenschutzgruppe schloss die „Gemeinsame Durchsetzungsaktion“ der Datenschutzbehörden der Mitgliedstaaten im Krankenversicherungsbereich durch die Veröffentlichung eines Abschlussberichts auf ihrer Webseite ab. Zum ersten Mal haben alle Datenschutzbehörden der EU systematisch bei der Untersuchung und Prüfung eines Wirtschaftsbereichs zusammengearbeitet, der fast alle EU-Bürgerinnen und -Bürger betrifft und in dem große Mengen personenbezogener, größtenteils sensibler Daten erhoben und verarbeitet werden. Angesichts des Ergebnisses der Untersuchung wird die Art. 29 Datenschutzgruppe in den kommenden Jahren weiterhin die Umsetzung der Richtlinie 95/46/EG in anderen Bereichen prüfen.

Vom 15. bis zum 17. Oktober 2007 fand – diesmal organisiert vom US-Handelsministerium und der Federal Trade Commission – die dritte Safe Harbor Konferenz in Washington statt. Die Konferenz unterstrich erneut die Wichtigkeit, welche die Art. 29 Datenschutzgruppe, die Kommission und die beteiligten US-Behörden den Beziehungen zwischen der EU und den USA im Bereich des Datenschutzes zumessen. Die Teilnehmer hielten die Fortsetzung und Vertiefung einen solchen Dialogs vor allem angesichts des ständig zunehmenden Personen- und Warenverkehrs zwischen den beiden Kontinenten für unbedingt erforderlich. Angesichts der zunehmenden Herausforderungen müssen dabei sowohl die sich ändernden politischen als auch die technologischen Entwicklungen berücksichtigt werden. Alle Teilnehmer bestätigten, dass die Safe Harbor Konferenz das richtige Forum ist, um ein tieferes Verständnis für das Datenschutzsystem der jeweils anderen Seite zu entwickeln, und um gemeinsame rechtliche und tatsächliche Grundlagen zur Gewährleistung eines effektiven Schutzes personenbezogener Daten zu schaffen.

Die Art. 29 Datenschutzgruppe einigte sich zudem auf ein Verfahren zur Beschleunigung der Genehmigungsabläufe für verbindliche Regeln über den Umgang mit personenbezogenen Daten in international agierenden Unternehmen und Konzernen (Binding Corporate Rules – BCR). Trotz einiger Fortschritte auf diesem Gebiet bleibt noch viel zur Verbesserung der aktuellen Koordinierung zwischen den Datenschutzbehörden zu tun. Die Art. 29 Datenschutzgruppe wird deshalb ihren Dialog mit der Wirtschaft intensivieren, um eine weitere Optimierung der Abläufe zu erreichen.

Außerdem verabschiedete die Art. 29 Datenschutzgruppe auf Bitte der Kommission Stellungnahmen über das Binnenmarkt-Informationssystem der EU (**WP 140**) und über das Kooperationssystem für Verbraucherschutz (**WP 139**). Die in den Dokumenten angesprochenen Fragen werden für die zukünftige Arbeit der Arbeitsgruppe von großer Bedeutung sein.

Insgesamt war auch das Jahr 2007 weltweit von der Tendenz geprägt, dass staatliche Stellen und Unternehmen zunehmend in die Privatsphäre der Bürgerinnen und Bürger eindringen, eine Tendenz, die sich auch in den Folgejahren nicht abzuschwächen scheint. Deshalb ist es äußerst wichtig, dass sich die Gesellschaft dieser Gefahren bewusst wird und darauf angemessen reagiert. Die Art. 29 Datenschutzgruppe wird auch weiterhin nach Kräften dazu beitragen, das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten.

Dies ist der letzte Tätigkeitsbericht, den ich als Vorsitzender der Art. 29 Datenschutzgruppe abgebe, denn meine zweite Amtszeit endet im Februar 2008. Ich möchte mich deshalb bei allen Kolleginnen und Kollegen bedanken, die zu den Ergebnissen der gemeinsamen Arbeit beigetragen haben. Besonders erwähnen möchte ich hier Prof. José Luis Piñar Mañas, der von Februar 2004 bis Februar 2007 als stellvertretender Vorsitzender die Art. 29 Datenschutzgruppe geleitet hat, und Alex Türk, den Präsidenten der CNIL, der diese Aufgabe im April 2007 übernommen hat. Mein besonderer Dank gilt dem Sekretariat unter Leitung von Referatsleiter Alain Brun, das unsere Arbeit hervorragend begleitet und unterstützt hat und all denjenigen Mitarbeiterinnen und Mitarbeitern der nationalen Datenschutzbehörden, die im Hintergrund zu dem Gelingen unserer Arbeit beigetragen haben.



Peter Schaar

Kapitel 1

Fragen, zu denen die Art. 29 Datenschutzgruppe¹ Stellung genommen hat

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/2007_de.htm

1.1. TRANSFER VON DATEN IN DRITTLÄNDER

1.1.1. Passagierdaten/PNR

Stellungnahme 2/2007 (WP 132) zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden

Diese Stellungnahme und die Anhänge dazu (häufig gestellte Fragen und Musterinformationsblatt) sind für Reisebüros, Fluggesellschaften und sonstige Organisationen bestimmt, die Fluggästen Reisedienste für Flüge in die und aus den Vereinigten Staaten anbieten. Die Stellungnahme und die Anhänge ändern und ersetzen die Stellungnahme vom 30. September 2004 (WP97). Die Übermittlung von PNR-Daten an amerikanische Behörden ist derzeit durch das Interimabkommen vom 16. Oktober 2006 geregelt. 2007 sollen die Verhandlungen über ein neues Abkommen beginnen². Diese Stellungnahme soll beraten und darüber informieren, wer welche Informationen wie und wann vorzulegen hat. Die Informationen sind den Fluggästen beim Kauf eines Flugscheins und bei der Bestätigung des Flugs vorzulegen. Die Stellungnahme enthält Ratschläge dazu, wie die Informationen über Telefon, im persönlichen Gespräch und über das Internet zu erteilen sind.

Die Art. 29 Datenschutzgruppe hat Musterinformationsblätter ausgearbeitet (Anhänge zu dieser Stellungnahme), um es den Organisationen und Agenturen zu erleichtern, ihrer Informationspflicht nachzukommen, und um sicherzustellen, dass in der gesamten Europäischen Union einheitlich informiert wird.

Stellungnahme 5/2007 (WP 138) zum Folgeabkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika vom Juli 2007 über die Verarbeitung von Fluggastdatensätzen (Passenger

Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security

Die Stellungnahme befasst sich mit den Auswirkungen des neuen dritten Abkommens über die Übermittlung von Fluggastdatensätzen (PNR-Daten) an das US-Heimatschutzministerium (DHS) auf die Grundrechte und Grundfreiheiten und speziell auf das Recht der Fluggäste auf Schutz ihrer Daten. Mit der Einigung auf ein neues langfristiges Abkommen wurde eine Rechtsgrundlage für die Übermittlung von Fluggastdaten geschaffen. Die Datenschutzgruppe hat die Bekämpfung des internationalen Terrorismus und des weltweiten organisierten Verbrechens stets als notwendiges und legitimes Anliegen betrachtet, das Unterstützung verdient. Für eine Beschneidung der Grundrechte und Grundfreiheiten von Personen einschließlich ihres Rechts auf Achtung ihrer Privatsphäre und Schutz ihrer personenbezogenen Daten muss es jedoch gute Gründe geben, wobei abzuwägen ist zwischen dem notwendigen Schutz der öffentlichen Sicherheit auf der einen und anderen öffentlichen Interessen wie dem Datenschutz auf der anderen Seite.

Gemeinsame Stellungnahme (WP145) zu dem von der Kommission am 6. November 2007 vorgelegten Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken

In der Stellungnahme soll untersucht werden, inwieweit sich der Kommissionsvorschlag vom 6. November 2007 für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken auf die Grundrechte und Grundfreiheiten auswirkt. Der Vorschlag ist dem von der EU und den USA im Juli 2007 unterzeichneten PNR-Abkommen nachempfunden, das viele Ähnlichkeiten mit dem vorliegenden Vorschlag aufweist. Die datenschutzrechtlichen Bedenken, die die Art. 29 Datenschutzgruppe in Bezug auf das PNR-Abkommen geäußert hat, decken sich in einigen Punkten mit den in dieser Stellungnahme geäußerten Bedenken. Ebenfalls berücksichtigt sind die Feststellungen der Gruppe in der Stellungnahme 9/2006 vom 27. September 2006 zur Richtlinie 2004/82/EG des Rates, die ebenfalls eine Regelung zur Übermittlung von

²Das neue Abkommen wurde am 23. Juli 2007 in Brüssel und am 26. Juli 2007 in Washington unterzeichnet. Beschluss 2007/551/GASP/JI des Rates vom 23. Juli 2007, ABl L 204 vom 4.8.2007, S.16 Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, ABl L 204 vom 4.8.2007, S.18 http://europa.eu.int/eur-lex/lex/JOhtml.do?year=2007&serie=L&textfield2=204&Submit=Search&_submit=Search&ihtmlang=de

Fluggastdaten durch Fluggesellschaften an staatliche Stellen enthält. Allerdings muss bei einer europäischen Fluggastdatenregelung die Beschneidung von Grundrechten und Grundfreiheiten wohlbegründet sein und es muss das richtige Gleichgewicht zwischen dem Schutz der öffentlichen Sicherheit einerseits und der Beschränkung des Rechts auf Schutz der Privatsphäre andererseits gefunden werden.

1.1.2. Verbindliche unternehmensinterne Vorschriften (BCR)

Empfehlung 1/2007 (WP 133) über das Antragsformular für Genehmigungen von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten

Die Datenschutzrichtlinie 95/46/EG ermöglicht den Transfer personenbezogener Daten außerhalb des EWR nur dann, wenn das Drittland ein „angemessenes Schutzniveau“ für die Daten vorsieht (Art. 25) oder wenn der Verantwortliche für die Verarbeitung der Daten angemessene Sicherheitsmaßnahmen in Bezug auf den Schutz der personenbezogenen Daten ergreift (Art. 26). Verbindliche unternehmensinterne Verhaltensregeln (VUV, engl.: „Binding Corporate Rules, BCR“) sind einer der Wege, auf denen solche angemessenen Sicherheitsmaßnahmen (Art. 26) „von einer Gruppe von Unternehmen in Bezug auf Übermittlungen innerhalb der Gruppe“³ demonstriert werden können, obwohl VUV als Instrumente nicht in der Datenschutzrichtlinie 95/46/EG ausdrücklich aufgelistet sind. Die Nutzung von VUV als Rechtsgrundlage für internationale Übermittlungen aus dem EWR hinaus erfordert die Zustimmung jeder einzelnen der EWR-Datenschutzbehörden, aus deren Land die Daten übermittelt werden sollen.

1.1.3. Jersey

Stellungnahme 8/2007 (WP 141) zum Umfang des Schutzes personenbezogener Daten in Jersey

Die Kanalinseln umfassen fünf Hauptinseln – Jersey, Guernsey, Alderney, Herm und Sark - und liegen vor

der Nordwestküste Frankreichs in der St.–Malo-Bucht im Ärmelkanal. Verfassungsrechtlich sind sie in die Bailiwicks (Selbstverwaltungsgebiete) Guernsey und Jersey unterteilt. Das Bailiwick Jersey ist ein Schutzgebiet des Vereinigten Königreichs. Das Vereinigte Königreich ist zuständig für die internationalen Angelegenheiten und die Verteidigung von Jersey. Die Insel Jersey genießt Unabhängigkeit in Bezug auf ihre internen Angelegenheiten, einschließlich des Bereichs Datenschutz. Jersey gehört zum Zollgebiet der Europäischen Gemeinschaften. Für Handelsbeziehungen zwischen Jersey und Drittländern gelten der Gemeinsame Zolltarif, Abschöpfungen und andere Bestimmungen für Agrareinfuhren. Zwischen Jersey und der Gemeinschaft herrscht freier Warenverkehr. Gemeinschaftsvorschriften aus anderen Bereichen, einschließlich Datenschutzvorschriften, gelten allerdings nicht. Zum Zeitpunkt der Umsetzung der Richtlinie durch das Vereinigte Königreich erklärten die Behörden von Jersey, dass diese Vorschriften in Jersey nicht angewendet werden, und führten eine eigene Datenschutzregelung ein. Gemäß Artikel 299 des Vertrags zur Gründung der Europäischen Gemeinschaft ist die Richtlinie für Jersey nicht gültig, so dass Jersey im Sinne der Artikel 25 und 26 der Richtlinie als Drittland gilt.

1.1.4. Färöer

Stellungnahme 9/2007 (WP 142) zum Umfang des Schutzes personenbezogener Daten auf den Färöern

Die Färöer liegen im Nordatlantik. Sie bestehen aus 18 Inseln. Die Inseln sind administrativ in sieben Verwaltungsbezirke mit etwa 120 Kommunen unterteilt. Die Färöer bilden zusammen mit Dänemark und Grönland das Königreich Dänemark. Das Königreich ist eine konstitutionelle Monarchie. Gemäß dem Autonomiegesetz von 1948 sind die Inseln ein selbstverwaltetes Gemeinwesen innerhalb des Königreichs Dänemark. Das Autonomiegesetz unterteilt sämtliche Politikbereiche in zwei Hauptgruppen: Die allgemeinen Angelegenheiten fallen in die Zuständigkeit des Königreichs, die besonderen (färöischen) Angelegenheiten fallen in die Zuständigkeit der autonomen färöischen Verwaltung und Gesetzgebung. Die Regelungen auf den Färöern hinsichtlich personenbezogener Daten basieren auf vom

³ Siehe Arbeitsdokument WP 74, Abschnitt 3.1: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm

färöischen Parlament erlassenen Gesetzen sowie auf Gesetzen zur Regelung „allgemeiner Angelegenheiten“. Das Datenschutzgesetz wurde 2001 vom färöischen Parlament verabschiedet und wird von der färöischen Datenschutzbehörde durchgeführt.

Das dänische Datenschutzgesetz gilt nur für die Datenverarbeitung durch Organe und Einrichtungen des Königreichs (wie Polizei, Staatsanwaltschaft, Bezirksgefängnis sowie Gefängnis- und Bewährungswesen, Hoher Kommissar der Färöer, Datenverarbeitung im Bereich des Familienrechts sowie kirchliche Behörden). Da das dänische Datenschutzgesetz⁴ auf der Richtlinie beruht, gehen wir davon aus, dass dieses Gesetz zumindest angemessenen Schutz hinsichtlich der Verarbeitung personenbezogener Daten bietet. Die genannten Bereiche sind deshalb in der vorliegenden Stellungnahme nicht berücksichtigt worden

1.2. ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

Stellungnahme 1/2007 (WP 129) zum Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden

Die Europäische Kommission hat am 1. September 2006 ein Grünbuch über Detektionstechnologien und ihre Anwendung durch Strafverfolgungs-, Zoll- und andere Sicherheitsbehörden (KOM(2006) 474) angenommen („Grünbuch“). Ziel des Grünbuchs ist es, auf europäischer Ebene eine Diskussion über Detektionstechnologien anzuregen und „konstruktive Beiträge und konkrete Vorschläge“ zu sammeln, um mit vereinten Kräften bei den Detektionstechnologien, die hier im weitesten Sinne zu verstehen sind, voranzukommen. Die Datenschutzgruppe ist zusammen mit anderen Interessierten eingeladen worden, sich an der Konsultation zu beteiligen.

⁴ Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten. Dieses Gesetz dient zur Umsetzung der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Welche konkreten Schritte und Maßnahmen folgen werden, wird sich anhand der Antworten auf die im Grünbuch angesprochenen Fragen und der weiteren Beiträge zum Grünbuch entscheiden. Einzelne Schritte könnten schon beizeiten unternommen werden, je nachdem, welche Prioritäten sich im Laufe der Konsultation ergeben. So könnte eine Taskforce eingesetzt werden, die Maßnahmen in bestimmten Bereichen ausarbeitet, falls die Konsultationsteilnehmer ein entsprechendes Interesse bekunden. Der Taskforce könnten Vertreter aus verschiedenen mitgliedstaatlichen Behörden und Sachverständige aus dem Privatsektor angehören.

1.3. BUCHHALTUNG, VERLAGSWESEN UND FINANZANGELEGENHEITEN

8. Richtlinie über Abschlussprüfungen, Stellungnahme 10/2007 (WP 143) der Art. 29 Datenschutzgruppe

Am 15. Februar 2007 prüfte die Datenschutzgruppe ein Arbeitsdokument der GD Binnenmarkt über die Weiterleitung von Arbeitsunterlagen, die Abschlussprüfungen betreffen und personenbezogene Daten enthalten, an Aufsichtsbehörden von Drittstaaten. In dem betreffenden Arbeitsdokument wird der rechtliche Rahmen auf EU-Ebene erläutert, der durch die Richtlinie 2006/43/EG über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen⁵ (so genannte 8. Richtlinie) geschaffen worden ist. Die 8. Richtlinie regelt die Voraussetzungen für die Tätigkeit der Abschlussprüfer und führt eine unabhängige öffentliche Aufsicht für diesen Berufsstand auf Ebene der Mitgliedstaaten ein. Die Richtlinie enthält darüber hinaus besondere Bestimmungen für die Zusammenarbeit zwischen den Aufsichtsorganen der Mitgliedstaaten und den zuständigen Behörden von Drittländern. Die Zusammenarbeit soll sich auch auf den gegenseitigen Zugang zu Arbeitspapieren und sonstigen Dokumenten europäischer Prüfungsgesellschaften erstrecken.

⁵ Amtsbl. L 157 vom 9.6.2006, S. 57.

1.4. PERSONENBEZOGENE DATEN

Stellungnahme 4/2007 (WP 136) zum Begriff „personenbezogene Daten“

Die Datenschutzgruppe ist sich der Notwendigkeit einer gründlichen Analyse des Begriffs „personenbezogene Daten“ bewusst. Die Informationen über die gegenwärtige Praxis in den EU-Mitgliedstaaten deuten auf gewisse Unsicherheiten und Unterschiede in Bezug auf wichtige Aspekte dieses Begriffs hin, die das bestimmungsgemäße Funktionieren des bestehenden Datenschutzrahmens in verschiedenen Zusammenhängen beeinträchtigen könnten. Das Ergebnis dieser Analyse, die sich auf ein zentrales Element für die Anwendung und Auslegung der Datenschutzbestimmungen konzentriert, hat unweigerlich tiefgreifende Auswirkungen auf eine Reihe wichtiger Aspekte und ist von besonderer Bedeutung für Themen wie Identitätsmanagement im Zusammenhang mit elektronischen Behördendiensten (E-Government), Online-Gesundheitsfürsorge (E-Health) und der RFID-Technik.

Mit ihrer Stellungnahme will die Datenschutzgruppe eine gemeinsame Verständnisgrundlage für den Begriff „personenbezogene Daten“, die Situationen, in denen nationale Datenschutzgesetze anzuwenden sind, und die Art ihrer Anwendung schaffen. Bei der Erarbeitung einer gemeinsamen Definition für den Begriff „personenbezogene Daten“ wird der Rahmen für den Geltungsbereich der Datenschutzbestimmungen abgesteckt. Außerdem werden Leitlinien für die Anwendung nationaler Datenschutzbestimmungen auf typische Situationen erarbeitet, wie sie in ganz Europa auftreten. Dadurch trägt die Art. 29 Datenschutzgruppe entsprechend ihrem Mandat zur einheitlichen Anwendung dieser Regelwerke bei.

1.5. BIOMETRIE & GESUNDHEIT DATEN

Arbeitspapier (WP 131) Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA)

Das Arbeitspapier der Art. 29 Datenschutzgruppe zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA) gibt eine Interpretationshilfe zu den auf EPA-Systeme anwendbaren Datenschutzbestimmungen und erläutert einige der allgemeinen Grundprinzipien. Es liefert darüber hinaus konkrete Hinweise zu den Anforderungen, die bei der Einrichtung von EPA-Systemen an den Datenschutz gestellt werden müssen, und zu den Schutzmechanismen, die diese Systeme bieten müssen.

Die Datenschutzgruppe geht zunächst auf die allgemeinen Datenschutzbestimmungen im Zusammenhang mit EPA-Systemen ein. Ausgehend von dem generellen Verbot der Verarbeitung personenbezogener Gesundheitsdaten in Artikel 8 Absatz 1 der Datenschutzrichtlinie 95/46/EG beschäftigt sie sich mit der Anwendbarkeit der Ausnahmeregelungen von Artikel 8, Absätze 2, 3 und 4 auf EPA-Systeme und plädiert dabei für eine enge Auslegung dieser Vorschriften. Des Weiteren stellt die Datenschutzgruppe Überlegungen zu einem geeigneten Rechtsrahmen für EPA-Systeme an und gibt Empfehlungen zu elf Themenkomplexen ab, bei denen der Bedarf an speziellen Maßnahmen zum Schutz der Daten eines Patienten und eines jeden Einzelnen besonders deutlich wird.

Stellungnahme Nr. 3/2007 (WP 134) zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen (KOM(2006) 269 endg.)

Vor dem Hintergrund der gemeinsamen Visumpolitik und einer verstärkten Integration der Auslandsvertretungen

der Mitgliedstaaten soll mit dem aktuellen Vorschlag zur Änderung der Gemeinsamen Konsularischen Instruktion die Rechtsgrundlage für die obligatorische Erfassung biometrischer Identifikatoren von Personen, die ein Visum beantragen, geschaffen und die Organisation der Auslandsvertretungen geregelt werden. Die Annahme einer Verordnung zur Änderung der Gemeinsamen Konsularischen Instruktion zur Aufnahme biometrischer Identifikatoren ist eine „Voraussetzung“ für die Anwendung des Visa-Informationssystems (VIS)⁶, da diese Verordnung „den Rechtsrahmen für die Erfassung der erforderlichen biometrischen Identifikatoren vorgibt“.

Das Visa-Informationssystem wird eingerichtet, wenn die Verordnung des Europäischen Parlaments und des Rates über das VIS und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt, die die entsprechenden Regelungen für dieses System enthält, über die aber derzeit noch beraten wird, in Kraft getreten ist. Der Aufbau einer zentralen Datenbank mit Daten zu Visumantragstellern, einschließlich Fingerabdrücken und digitalisierten Gesichtsbildern, sowie Daten zu Gruppenreisenden und zu Personen, die in den Zielländern der Antragsteller als Gastgeber fungieren, soll zu den grundlegenden Voraussetzungen für die Umsetzung einer gemeinsamen Visumpolitik und die Verwirklichung der Ziele gemäß Artikel 61 des Vertrags zur Gründung der Europäischen Gemeinschaft (EGV), insbesondere des freien Personenverkehrs in einem Raum der Freiheit, der Sicherheit und des Rechts, gehören.

1.6. RECHTSDURCHSETZUNG

Bericht 1/2007(WP 137) über die erste gemeinsame Durchsetzungsmaßnahme: Bewertung und zukünftige Schritte

In ihrem ersten Bericht über die Durchführung der Datenschutzrichtlinie (KOM(2003) 265 endgültig) forderte die Europäische Kommission die Art. 29 Datenschutzgruppe (WP29) auf, „die Frage der besseren Durchsetzung insgesamt periodisch zu erörtern ... und zu erwägen, sektorale Untersuchungen auf EU-Ebene durchzuführen

und die diesbezüglichen Normen anzugleichen“. Das Ziel dieser Aktivitäten besteht darin, Informationen über den Grad der Durchführung zu sammeln und die Sektoren dabei zu unterstützen, mit möglichst geringem Aufwand eine bessere Rechtsbefolgung zu erzielen.

Dementsprechend beauftragte die Gruppe die Taskforce Rechtsdurchsetzung (Enforcement Task Force – ETF) im Juni 2004 damit, Überlegungen zu einer EU-Strategie und zu Durchsetzungskriterien anzustellen. Im November 2004 verpflichtete sich die WP29 in ihrer Entschließung zum Thema Rechtsdurchsetzung (WP101), „proaktive Strategien zur Rechtsdurchsetzung zu entwickeln [und] Durchsetzungsmaßnahmen voranzutreiben“ und legte sechs Kriterien zur Ermittlung eines für gemeinsame Durchsetzungsmaßnahmen geeigneten Sektors fest.

Die in WP101 definierte Kombination von Kriterien legte die Wahl eines Sektors mit hochgradig harmonisierten Aktivitäten und großem Einfluss in Bezug auf den Schutz personenbezogener Daten nahe. Aus diesem Grund beschloss die WP29, sich bei ihrer ersten gegenseitig abgestimmten Intervention auf private Krankenversicherungen und insbesondere auf die Erbringung von Krankenversicherungsleistungen zu konzentrieren.

1.7. VERBRAUCHER

Stellungnahme 6/2007 (WP 139) zu Datenschutzfragen im Zusammenhang mit dem Kooperationssystem für Verbraucherschutz

Gegenstand dieser Stellungnahme der Art. 29 Datenschutzgruppe („Datenschutzgruppe“) sind die datenschutzrelevanten Fragen im Zusammenhang mit dem Kooperationssystem für Verbraucherschutz der Europäischen Kommission („Kooperationssystem“). Dabei handelt es sich um eine von der Europäischen Kommission betriebene Datenbank, die auf der Grundlage der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden („Verordnung über die Zusammenarbeit im Verbraucherschutz“) eingerichtet wurde, um den Informationsaustausch zwischen den Verbraucherschutzbehörden der Mitgliedstaaten und der Kommission zu ermöglichen.

⁶ Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (KOM (2004) 835 endg.), von der Kommission am 28. Dezember 2004 vorgelegt.

Dieser Stellungnahme liegt ein entsprechendes Ersuchen des Leiters des Referats B-5 „Durchsetzung und Rechtsschutz“ der Generaldirektion Gesundheit und Verbraucherschutz („GD SANCO“) an das Sekretariat der Arbeitsgruppe vom 30. März 2007 zugrunde.

1.8. BINNENMARKT- INFORMATIONSSYSTEM

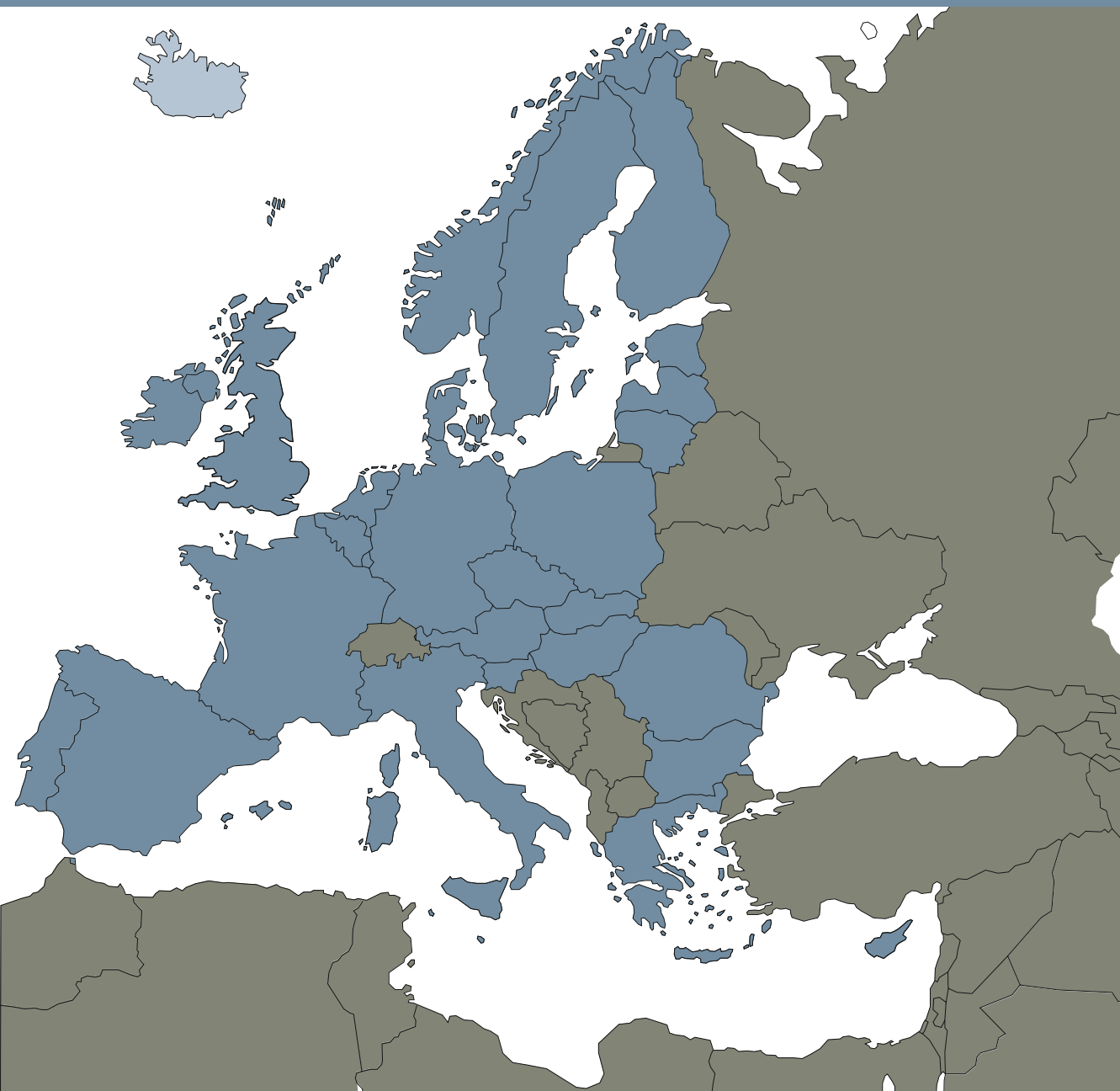
Stellungnahme 7/2007 (WP 140) zu Fragen des Datenschutzes im Zusammenhang mit dem Binnenmarkt-Informationssystem

Das Vorhaben, ein computergestütztes System als Hilfsmittel für den Informationsaustausch hinsichtlich personenbezogener Daten einzurichten, gibt Anlass zu erheblichen Bedenken in Bezug auf die Grundrechte von Einzelpersonen, insbesondere auf das Recht auf Privatsphäre.

Aufgrund der Komplexität des Binnenmarkt-Informationssystems (Internal Market Information System – IMI) und der verschiedenen damit verbundenen Fragen ersuchte die GD Binnenmarkt der Europäischen Kommission die Art. 29 Datenschutzgruppe um ihre Stellungnahme. Der Schwerpunkt der Stellungnahme der Art. 29 Datenschutzgruppe liegt auf denselben Aspekten, die in den Dokumenten „Issue Paper on Data Protection in IMI“ (Themenpaper über den Datenschutz im IMI; D-4784) und „General Overview“ (Allgemeine Übersicht; D-1804) behandelt werden. Zweck dieser Stellungnahme ist es, die Auswirkungen des IMI hinsichtlich personenbezogener Daten, die durch die Richtlinie 95/46/EG („Datenschutzrichtlinie“) und die Verordnung (EG) Nr. 45/2001 („Datenschutzverordnung“) geschützt werden, zu analysieren.

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 über die Vorratsspeicherung von Daten 2006/24/EG** wurde noch nicht umgesetzt. Im Frühjahr 2007 wurde ein Entwurf verschickt, der sehr kritisch aufgenommen wurde. Auch die Datenschutzkommission, die eine Kontrollfunktion ausüben sollte, legte einen negativen Kommentar zu dem Entwurf vor. Bisher wurde noch kein neuer Entwurf verschickt.

B. Bedeutende Rechtsprechung

Ein Bürger wollte von seiner österreichischen Bank wissen, welche seiner persönlichen Daten von SWIFT an die US-Behörden übermittelt worden waren. Die Datenschutzkommission wies die Beschwerde, die er erhoben hatte, als die Bank ihm nicht die gewünschte Auskunft gab, ab und erklärte, SWIFT habe unabhängig gehandelt und sei selbst dafür zuständig, diese Information zu erteilen (Rechtssache Nr. K121.245/0009-DSK/2007).

Ein Patient hatte mit einem Arzt eine Meinungsverschiedenheit über die Art der erforderlichen Behandlung. Der Arzt schrieb eine kurze Notiz, in der er den Vorfall beschrieb. Diese enthielt eine Bemerkung über den emotionalen Zustand des Patienten, die der Patient für unangemessen hielt. Er verlangte die Löschung dieser Bemerkung, und zwar auf der Grundlage des Rechts auf Berichtigung von Daten. Das Krankenhaus (als der für die Datenverarbeitung Verantwortliche) lehnte dies ab, und die Datenschutzkommission wies die Beschwerde ab und erklärte, die Information sei insofern korrekt, als sie die Darlegung und den persönlichen Eindruck des Arztes von diesem Vorfall darstelle (Rechtssache Nr. K121.246/0008-DSK/2007).

Ein österreichischer Bürger beging in der Schweiz einen Verkehrsverstoß. Die österreichischen Behörden halfen ihren Schweizer Kollegen durch die Übermittlung persönlicher Daten, ihn zu identifizieren. Der Bürger reichte bei der Datenschutzkommission eine Beschwerde ein, die abgewiesen wurde. Er focht diese Entscheidung vor dem Verwaltungsgerichtshof (VwGH) an. Er machte unter

anderem geltend, dass der Datenschutzkommission die von Artikel 28 der Richtlinie 95/46/EG verlangte Unabhängigkeit fehle. Der Verwaltungsgerichtshof wies all seine Argumente zurück und bestätigte, dass die Datenschutzkommission im Einklang mit den einschlägigen EU-Rechtsvorschriften organisiert sei (Entscheidung VwGH Zl. 2006/06/0322).

Für Rechtsprechung über Videoüberwachung siehe den Eintrag unter „Wichtige spezifische Themen“.

C. Wichtige spezifische Themen

Videoüberwachung

Fragen in Bezug auf Videoüberwachung stehen nach wie vor ganz oben auf der Agenda der Datenschutzkommission. 2007 erteilte die Kommission in mehreren Fällen die Erlaubnis. In einem Fall ging es um Videoüberwachung des U-Bahn-Netzes der öffentlichen Verkehrsgesellschaft Wiener Linien GmbH & Co. KG. Die Gesellschaft wollte Videoüberwachung als Hilfsmittel gegen Vandalismus und zum Schutz ihrer Mitarbeiter und Fahrgäste einsetzen. Die Kommission erteilte eine befristete Genehmigung, die am 30. Juni 2009 ausläuft. Nach Ablauf dieser Frist muss die Wiener Linien GmbH & Co. KG die positiven Auswirkungen der Videoüberwachung nachweisen, bevor die Genehmigung verlängert wird.

Dieser Punkt und die Meldung einer Videoüberwachung in großen Wohnblöcken waren Gegenstand zahlreicher Diskussionen.

Die Medien haben umfassend über das Thema Videoüberwachung berichtet, und auch von den Bürgern wird es aufmerksam verfolgt.

Kreditmeldungen

In den letzten Jahren sind die österreichischen Mobiltelefonanbieter, neben anderen Unternehmen, dazu übergegangen, die Kreditwürdigkeit jedes neuen Kunden zu überprüfen. Dies hat dazu geführt, dass zahlreiche Beschwerden von Bürgern eingingen, deren Antrag aufgrund einer negativen Meldung abgelehnt wurde. Die Datenschutzkommission hat sich in diesem Zusammenhang mit einer Reihe von Fragen befasst. Das Verhalten von Evidenzzentralen gegenüber Datensubjekten, die

ihre Rechte auf Zugang, Berichtigung und Löschung ausüben, wurde oftmals als unbefriedigend beurteilt. Ein weiteres in Angriff zu nehmendes Thema war die Genauigkeit der Daten.

Eine Evidenzzentrale machte geltend, sie sei für einen Teil des Beurteilungsprozesses nicht der für die Datenverarbeitung Verantwortliche, da die Unternehmen, die diese Meldungen bestellt hatten, lediglich die Rohdaten genommen und diese unter ihrer eigenen Kontrolle in ein Scoring-System eingegeben hatten. Die Datenschutzkommission entschied, dies treffe tatsächlich zu und die Unternehmen seien für diesen Teil des Systems selbst die für die Datenverarbeitung Verantwortlichen. Die Entscheidung der Kommission wurde vor dem österreichischen Verfassungsgerichtshof angefochten.

Darüber hinaus hat die Datenschutzkommission Schritte zur Festlegung von Unternehmensregeln für Evidenzdatenbanken ergriffen, vor allem für eine große Datenbank namens „Konsumentenkreditevidenz“.



Belgien

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

Anlässlich des 15-jährigen Bestehens des Gesetzes vom 8. Dezember 1992 über den Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten (im Folgenden „Privatsphäre-Gesetz“), das die Richtlinie 95/46/EG umsetzt, hat die Kommission zum Schutz der Privatsphäre (im Folgenden „belgische Kommission“ oder „die Kommission“) eine mit Anmerkungen versehene Fassung⁷ dieser Rechtsvorschrift ausgearbeitet. Dieser Kommentar enthält für jeden Artikel des Gesetzes eine Reihe von – normativen oder auf die Rechtsprechung bezogenen – Verweisen, die als nützlich erachtet werden, um diese Bestimmungen wieder in ihren Kontext zu stellen, richtig zu verstehen und zu interpretieren. Vor allem die europäischen Gesetzestexte (sowohl der Europäischen Union als auch des Europarates), die Stellungnahmen der Gruppe 29 und die Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte gehören zu den Quellen, die in diesem Referenzleitfaden erwähnt werden. Im Übrigen hat die belgische Kommission diesen Jahrestag zum Anlass genommen, eine Zwischenbilanz über die in diesen 15 Jahren geleistete Arbeit, die Perspektiven und künftigen Herausforderungen zu ziehen und bestimmte aktuelle Fragen auf einer akademischen Sitzung im Parlament zu erörtern.

Gesetz über die elektronische Kommunikation

Im Laufe des Jahres 2007 hat sich die belgische Kommission mit einem Vorschlag zur Änderung des Gesetzes vom 13. Juni 2005 über die elektronische Kommunikation (Stellungnahme 18/2007 vom 27. April 2007) befasst, das die Richtlinie 2002/58/EG (M.B., 20. Juni 2005) in belgisches Recht umsetzt. Auch wenn dieser Vorschlag letztlich gescheitert ist, sind die darin angeregten Änderungen erwähnenswert, da sie darauf abzielten, den Schutz der Privatsphäre bei der Erbringung von Lokalisierungsservices per Handy zu verbessern: einerseits, indem den Benutzern des Geräts die gleichen Garantien bezüglich des Schutzes ihrer Privatsphäre eingeräumt werden wie

den Abonnenten (obligatorische vorherige Unterrichtung des Benutzers, bei jeder Lokalisierungsanfrage obligatorische Unterrichtung über die Aktivierung des Services direkt auf dem Handy und Recht des Endbenutzers, die Services zu annullieren), und andererseits, indem diese Schutzmaßnahmen auf minderjährige Kinder ab 12 Jahren ausgedehnt werden (Erhalt ihrer Zustimmung zusätzlich zu der ihrer gesetzlichen Vertreter). Doch wie gesagt, wurde das Gesetz vom 13. Juni 2005 nicht in oben stehendem Sinne geändert.

Gesetz zur Regelung der Installation und des Einsatzes von Überwachungskameras

Dem vorigen Jahresbericht war zu entnehmen, dass die Frage der Videoüberwachung 2006 zu den wichtigsten Anliegen sowohl des Gesetzgebers als auch der belgischen Kommission zählte.

Nach langen Diskussionen und einer Reihe von Anhörungen der von dieser Problematik betroffenen Akteure – darunter die belgische Kommission – wurde am 1. März 2007 das Gesetz zur Regelung der Installation und des Einsatzes von Überwachungskameras (im Folgenden das Kamera-Gesetz – M.B., 31. Mai 2007) verabschiedet. Diese sektorale Rechtsvorschrift regelt speziell die Bildverarbeitung zu Überwachungszwecken. Allerdings ist diese letztere ohne ausdrückliche Ausnahmen nach wie vor gültig. Die großen Linien dieser neuen Vorschrift lassen sich folgendermaßen zusammenfassen:

Das Kamera-Gesetz gilt für jedes ortsfeste oder mobile Überwachungssystem, das zum Zweck der Überwachung bestimmter Orte angebracht und benutzt wird. Die Installation und der Einsatz von Überwachungskameras, die durch besondere Rechtsvorschriften geregelt werden (Privatdetektive, Sicherheit von Fußballwettkämpfen) sowie die Installation und der Einsatz von Kameras, die am Arbeitsplatz die Sicherheit und Gesundheit, den Schutz der Güter des Unternehmens, die Kontrolle des Produktionsprozesses und die Kontrolle der Arbeit gewährleisten sollen, sind aus seinem Geltungsbereich ausgeschlossen.

Das Kamera-Gesetz unterscheidet zwischen drei Arten von Orten (nicht geschlossene Orte, der Öffentlichkeit zugängliche geschlossene Orte und der Öffentlichkeit nicht zugängliche geschlossene Orte): Für jede Art von

⁷Dieses Dokument ist in Form einer CD-Rom bei der Kommission erhältlich. Es kann auch auf ihrer Internet-Site heruntergeladen werden.

Ort gelten gesonderte Regeln, sowohl im Hinblick auf die Prozedur der Installation der Überwachungskamera als auch auf ihren Einsatz.

Nur für die Anbringung einer Überwachungskamera an einem offenen Ort muss vorher eine positive Stellungnahme der lokalen politisch Verantwortlichen sowie eine positive Stellungnahme der lokalen Polizeidienststellen eingeholt werden, die bestätigt, dass eine Sicherheits- und Effizienzanalyse durchgeführt wurde und dass die geplante Installation den Grundsätzen der Datenschutzbestimmungen entspricht. Die Beurteilung der Verhältnismäßigkeit wird im Übrigen davon abhängen, in welcher Art von Ort die Kamera angebracht wird (gefilmte Bilder, Zugang zu den Daten, Empfänger der Daten, Aufbewahrung der Daten, Anzahl von Geräten). Beispielsweise müssen die Kameras im öffentlichen Raum derart angebracht werden, dass private Orte (wie Eingänge oder Fenster von Privatgebäuden) nicht von ihnen erfasst werden. Des Weiteren gilt für Kameras im öffentlichen Raum, dass das Ansehen von Bildern in Realzeit nur unter der Kontrolle von Verwaltungs- oder Gerichtsbehörden zulässig ist, damit die Polizeidienste bei Verstößen, Beschädigung oder Beeinträchtigung der öffentlichen Ordnung sofort eingreifen können.

Um seiner Informationspflicht nachzukommen, muss der für die Verarbeitung Verantwortliche ein Piktogramm anbringen, das auf die Kameraüberwachung hinweist. Jeder Einsatz versteckter Kameras ist verboten (*Siehe Stellungnahme 22/2007 vom 13. Juni 2007 zum Vorentwurf eines Königlichen Erlasses zur Festlegung der Art, auf die auf das Vorhandensein einer Kameraüberwachung hinzuweisen ist, vorgelegt in Durchführung des Gesetzes vom 21. März 2007 zur Regelung der Installation und des Einsatzes von Überwachungskameras*).

Schließlich muss der für die Verarbeitung Verantwortliche, wenn er an gleich welchem Ort eine Überwachungskamera installieren will, den belgischen Ausschuss mittels eines speziell zu diesem Zweck erstellten Formulars (spezifische thematische Erklärung) über seinen Beschluss unterrichten. Darüber hinaus muss jede Installation von Kameras an einem geschlossenen Ort gleichzeitig auch den lokalen Polizeidienststellen mitgeteilt werden.

Einsetzung sektoraler Ausschüsse

Innerhalb der belgischen Kommission eingerichtete sektorale Ausschüsse wachen darüber, dass die Verarbeitung personenbezogener Daten, die in verschiedenen spezifischen Sektoren (soziale Sicherheit, öffentliche Stellen usw.) vorgenommen wird, die Privatsphäre nicht beeinträchtigt. Einige von ihnen haben die Befugnis, bestimmte Arten der Verarbeitung zu gestatten. Diese Ausschüsse setzen sich einerseits aus Mitgliedern der belgischen Kommission und andererseits aus Experten zusammen, die aufgrund ihrer praktischen Kenntnis des betreffenden Sektors ausgewählt werden. Im Jahr 2007 haben mehrere dieser Ausschüsse ihre Arbeit in dieser paritätischen Zusammensetzung aufgenommen und eine steigende Zahl von Genehmigungsanträgen erhalten.

Übermittlung von Gesundheitsdaten

In dem Jahresbericht 2006 wurde auch erwähnt, dass Anfang 2007 ein Gesetzesentwurf zur Schaffung eines sektoralen Ausschusses für soziale Sicherheit und Gesundheit verabschiedet werden sollte. Gemäß dem *Gesetz vom 15. Januar 1990 zur Errichtung und Organisation einer Zentralen Datenbank der sozialen Sicherheit*, wie geändert am 1. März 2007, wurden die Befugnisse des sektoralen Ausschusses, bis dahin für den Bereich der sozialen Sicherheit zuständig, auf bestimmte Arten der Verarbeitung personenbezogener Gesundheitsdaten ausgedehnt. Die neue Abteilung „Gesundheit“ dieses Ausschusses hat die Aufgabe, die Übermittlung von Gesundheitsdaten zu genehmigen, vorausgesetzt, diese Übermittlung ist gesetzlich erforderlich. Ferner hat sie die Aufgabe, die Einhaltung der durch das Gesetz oder kraft des Gesetzes über den Schutz der Privatsphäre in Bezug auf Verarbeitung dieser Daten festgelegten Bestimmungen zu überwachen.

B. Bedeutende Rechtsprechung

Es gibt unserer Meinung nach keine besonders relevanten gerichtlichen Entscheidungen, die hier zu erwähnen wären.

C. Wichtige spezifische Themen

Allgemeine Einleitung

Die bereits 2005 und 2006 festgestellte Tendenz, Daten zu zentralisieren und zu verknüpfen, hat sich 2007 fortgesetzt. Wie in den Vorjahren hat die belgische Kommission in ihren im Laufe dieses Jahres vorgelegten Stellungnahmen besonderes Gewicht auf die folgenden zwei Punkte gelegt: die notwendige Beachtung des Prinzips der Kompatibilität zwischen den Dateien, um systematische Datenkreuzungen zu vermeiden, und die notwendige Transparenz dieser Arten der Verarbeitung gegenüber den Bürgern und die Aufrechterhaltung einer gewissen Datenkontrolle durch alle. Diese Grundsätze wurden vor allem angesichts der Zunahme von Projekten für elektronische Verwaltung (siehe den Abschnitt „Öffentlicher Sektor“) erneut bekräftigt.

Auch wenn sie nicht durchweg erfolgreich waren, sollten doch gewisse Legislativinitiativen erwähnt werden, da sie darauf abzielten, einen klaren Rechtsrahmen für die Verarbeitung besonders sensibler Daten, wie beispielsweise solche, die in die nationale Polizeidatenbank aufgenommen werden sollen, oder für die Verarbeitung von Daten, auf die immer häufiger zurückgegriffen wird (wie etwa Steuerdaten), bereitzustellen. Bei dieser Gelegenheit hat die belgische Kommission auch an bestimmte grundlegende Prinzipien erinnert.

Wie im Jahr 2006 hat die belgische Kommission die Beachtung der für den Datenschutz geltenden Rechtsvorschriften durch die Gesellschaft SWIFT untersucht. Auch die Beachtung dieser Vorschriften durch die Unternehmen im Rahmen der Einrichtung interner Warnsysteme (Whistleblowing) oder bei der Übermittlung personenbezogener Daten ins Ausland (beispielsweise durch die Annahme verbindlicher Unternehmensvorschriften) wurde von ihr aufmerksam geprüft.

Schließlich hat die belgische Kommission bestimmte Standpunkte und Empfehlungen in Bezug auf neue Technologien wie Digitalfernsehen und andere interaktive Medien, sowie in Bezug auf die Verbreitung von Bildern im Allgemeinen und im schulischen Bereich im Besonderen formuliert.

Diese verschiedenen Aspekte, die die Tätigkeit der belgischen Kommission im Jahr 2007 geprägt haben, werden im Folgenden ausführlich beschrieben.

Polizei- und Sicherheitssektor

Nationale Polizeidatenbank: Mit ihrer Stellungnahme 12/2007 vom 21. März 2007 hat die belgische Kommission die Verordnungsinitiative zur Festlegung der Bedingungen, unter denen die Polizeidienste im Rahmen der ihnen übertragenen Aufgaben personenbezogene Daten und Informationen sammeln und verarbeiten dürfen, positiv aufgenommen. Sie hat dieses Projekt nach Maßgabe der Anforderungen – insbesondere in Bezug auf Voraussagbarkeit und Verhältnismäßigkeit – der europäischen Menschenrechtskonvention (EMRK) und der Rechtsprechung des für die Überwachung ihrer Anwendung zuständigen Gerichtshofes geprüft. Die Kommission hat ihrer Stellungnahme allerdings Bedingungen hinzugefügt, da sie der Ansicht war, dass die Anforderungen von Artikel 8 der EMRK in mehreren Punkten nur summarisch erfüllt waren. Sie hat zwar erklärt, sich der praktischen Probleme in Verbindung mit der Strukturierung und Kategorisierung der Gesamtheit der gesammelten oder den Polizeidiensten übermittelten Rohdaten und -informationen bewusst zu sein, aber es doch vor allem für notwendig gehalten, diese Informationssysteme so genau wie möglich zu begrenzen, damit der Bürger die Möglichkeit hat, in vernünftigen Maße vorzusehen, was in ihnen enthalten sein könnte und aus welchen Gründen.

Öffentlicher Sektor

Verarbeitung von Daten durch die Finanzverwaltung: Die Kommission hat sich auch mit der Initiative befasst, die darauf abzielt, bestimmte Arten der Verarbeitung personenbezogener Daten, die sowohl innerhalb der Finanzverwaltung – von ihren verschiedenen Dienststellen – als auch im Rahmen der externen Beziehungen, die diese Verwaltung mit anderen öffentlichen und privaten Organisationen unterhält, vorgenommen werden, zu regulieren. Die Textentwürfe, die ihr zur Stellungnahme vorgelegt wurden, waren darauf ausgerichtet, einerseits die aktuelle Praxis der Finanzverwaltung mit dem Privatsphäre-Gesetz in Einklang zu bringen und andererseits einen Rechtsrahmen sowohl für die globale und integrierte Informatisierung der Finanzverwaltung als auch für den Einsatz automatisierter

Entscheidungshilfe-Tools im Rahmen des Kampfs gegen Steuerhinterziehung bereitzustellen. Insbesondere war Folgendes vorgesehen: (1) Schaffung eines Registers mit einem „einheitlichen Dossier“ für jeden Steuerzahler (natürliche und/oder juristische Person); (2) die Ausführung der Datenverarbeitung mittels eines automatisierten Entscheidungshilfe-Tools (Datenlager – *datawarehouse*) zur Erkennung von Risiken und Risikogruppen von Objekten und Subjekten, die mit der totalen oder teilweisen Nichtbeachtung der Steuergesetze zusammenhängen (*datamining*), sowie (3) beim Föderalen Öffentlichen Dienst Finanzen eingehende und ausgehende Datenströme, die an andere Behörden und Berufsgruppen gerichtet sind oder von diesen stammen.

In ihren Stellungnahmen zu dieser Initiative hat die belgische Kommission vor allem die folgenden Elemente hervorgehoben (*Stellungnahmen 01/2007 vom 17. Januar 2007 und 16/2007 vom 11. April 2007 zum Vorentwurf des Gesetzes über bestimmte Arten der Verarbeitung personenbezogener Daten durch den Föderalen Öffentlichen Dienst Finanzen*):

- Jeder Austausch von Daten, die zu unterschiedlichen Zwecken erhoben werden – selbst innerhalb der Finanzverwaltung –, darf nicht als vereinbar betrachtet werden, sondern muss, bevor er tatsächlich stattfindet, gemäß Artikel 4 des Privatsphäre-Gesetzes auf seine Vereinbarkeit hin geprüft werden. Diese Bestimmung sieht ausdrücklich vor, dass Daten später nicht auf eine Weise verarbeitet werden dürfen, die sich mit den Zwecken, zu denen sie ursprünglich erhoben wurden, nicht vereinbaren lässt, wobei alle relevanten Faktoren zu berücksichtigen sind, insbesondere die vernünftigen Einschätzungen der Betroffenen und die Rechtsvorschriften. Ein internes Genehmigungsverfahren im Anschluss an die Prüfung durch einen *Ad-hoc*-Ausschuss kann dies nicht ersetzen;
- die Kommission stimmt zu, dass zwischen administrativen Verwaltungsaufgaben und Aufgaben im Zusammenhang mit Kontrolle, Eintreibung und Streit-sachen unterschieden wird. Diesbezüglich stellt sie klar, dass die Beschreibung dieser Zwecke auf der Basis eines funktionellen Kriteriums und nicht auf der Basis eines Verfahrenskriteriums erfolgen müsste;
- selbst wenn Steuerdaten als solche nach der belgischen Gesetzgebung nicht als „sensible Daten“ im *strengen Wortsinn* gelten, werden sie oftmals – und zu Recht – als solche betrachtet, da sie erhebliche Auswirkungen auf das Privatleben eines jeden Bürgers haben;
- die Kommission ist der Auffassung, dass derartige Sondervorschriften – im Prinzip – mit dem Privatsphäre-Gesetz in Einklang stehen müssen. Wenn sich aus speziellen Gründen Ausnahmen von den Basisvorschriften zum Schutz personenbezogener Daten als notwendig und gerechtfertigt erweisen, müssten diese Ausnahmen im Privatsphäre-Gesetz selbst aufgeführt werden;
- auch wenn die Kommission keine Einwände gegen die Schaffung und Verwendung einer sektoralen Steuernummer hat, stellt sie sich doch gewisse Fragen bezüglich der Verwendung dieser Steuernummer im Rahmen der externen Beziehungen der Finanzverwaltung und der Risiken, dass eine solche Nummer *de facto* zu einer zweiten universellen Identifizierungsnummer wird. Die allgemeine Verwendung dieser Steuernummern wird die Verwendung der nationalen Registernummer, die nach belgischem Recht von einem kraft seiner Genehmigungsbefugnis für die Überwachung ihrer Verwendung gemäß dem Privatsphäre-Gesetz zuständigen Ausschuss kontrolliert wird, nicht ersetzen können;
- die Kommission ist nicht gegen die Einrichtung einer internen Kontrolle innerhalb einer Organisation oder eines öffentlichen Dienstes. Ganz im Gegenteil begrüßt sie die Schaffung eines internen Ausschusses zur Überwachung der „internen Einhaltung“ des Datenschutzes, unbeschadet ihrer externen Kontrollbefugnis und der ihrer sektoralen Ausschüsse;
- was die Dauer und die Bedingungen für die Aufbewahrung der Daten betrifft, verlangt die Kommission eine regelmäßige Evaluierung der Notwendigkeit, sie aufzubewahren, und der Bedingungen dieser Aufbewahrung. Sie empfiehlt eine obligatorische und regelmäßige Evaluierung der Notwendigkeit, diese Daten aufzubewahren, und zwar vor Ablauf der maximalen Frist, da die Daten gelöscht werden müssen, sobald festgestellt wird, dass sie nicht mehr exakt, relevant oder notwendig sind. Die Kommission hat ferner empfohlen, nach jeder Evaluierung eine klare Trennung zwischen den für die laufenden Tätigkeiten notwendigen Daten und den Daten vorzunehmen, die gegebenenfalls archiviert werden sollen;

- schließlich begrüßt die Kommission die spezifische Verfahrenskontrolle für die Verwendung des *datawarehouse* und der Datamining-Methoden, die in dem Gesetzesvorschlag vorgesehen sind, da diese Kontrolle Garantien bietet, mit denen sich verhindern lässt, dass diese Hilfsmittel auf untransparente und unverhältnismäßige Weise eingesetzt werden: Vor jeder Entschlüsselung oder beim Eingeben zusätzlicher Daten in das *datawarehouse* ist dem internen Kontrollausschuss ein Bericht zur Stellungnahme vorzulegen, dem gemäß eine Abwägung der Interessen und eine Prüfung der Notwendigkeit vorgenommen werden müssen. Zusätzlich zu dieser Verfahrenskontrolle hat die Kommission empfohlen, einen *Ad-hoc* Dienst (dritte Vertrauenspartei) für die Entschlüsselung/Verschlüsselung der Daten einzurichten. Dieser Regelungsentwurf wurde jedoch nicht angenommen.

Automatisierte Entscheidungen: Im Rahmen der zu diesem Regelungsentwurf abgegebenen Stellungnahmen wie auch zu anderen Gelegenheiten hat die Kommission außerdem nachdrücklich darauf hingewiesen, dass es unbedingt erforderlich ist, das Verbot zu beachten, Entscheidungen, die rechtliche Auswirkungen auf eine Person haben oder diese erheblich betreffen, ausschließlich auf Basis einer automatisierten Datenverarbeitung zu fällen. Die Kommission zeigt sich gleichermaßen wachsam, ob es sich nun um eine Entscheidung handelt, die darauf zielt, einer betroffenen Person einen automatischen Vorteil einzuräumen – beispielsweise durch Maßnahmen zur administrativen Vereinfachung –, oder um eine Entscheidung im Rahmen der Kontrolle oder der Bekämpfung von Steuerhinterziehung. Selbst wenn sie gesetzlich gestattet ist, muss eine derartige Entscheidungsfindung mit angemessenen Garantien verknüpft sein, die gewährleisten, dass die betroffene Person eine gewisse Kontrolle über ihre Daten behält.

Im Rahmen ihrer Beurteilung des oben kommentierten spezifischen Projekts zur Regelung von Datenverarbeitung durch die Finanzverwaltung gelangt die Kommission zu dem Schluss, dass die Datenverarbeitung und die Entscheidungsfindungen – etwa die Entscheidung, eine bestimmte Person einer Steuerprüfung zu unterziehen – nicht ausschließlich auf Basis der aus dem

datawarehouse resultierenden Informationen erfolgen dürfen.

In einer Stellungnahme zu einem Projekt bezüglich der automatischen Anwendung von Höchstpreisen für die Strom- und Erdgasversorgung für Kunden mit geringem Einkommen – basierend auf einer Koppelung der Daten der Energielieferanten und der Daten der Sozialversicherung – erinnert die Kommission an dieses Verbot und an die notwendige Beachtung des Prinzips der Verhältnismäßigkeit und empfiehlt, ein System der stillschweigenden Zustimmung einzuführen.

Kopplung – Zwischenorganisation: Die an die belgische Kommission und ihre sektoralen Ausschüsse gerichteten Anfragen zur Genehmigung der Übermittlung von Datenströmen zeigen auch, dass mehrere öffentliche Einrichtungen zwecks administrativer Vereinfachung – teils aber auch zu Kontrollzwecken – zunehmend daran interessiert sind, die Daten ein und desselben Bürgers zu koppeln (wie in dem oben stehenden Beispiel bezüglich der automatischen Gewährung eines Vorzugstarifs). Die Daten, die in diesem Rahmen am häufigsten angefordert werden, beispielsweise um ein Recht oder einen an Einkommensbedingungen geknüpften Vorteil zu gewähren, sind die Daten über die finanzielle Lage der betroffenen Person. Dieser zunehmende Rückgriff auf gekoppelte Daten hat die belgische Kommission veranlasst, die Mitwirkung einer Zwischenorganisation (*trusted third party*) zu empfehlen, die hinsichtlich ihrer Unabhängigkeit alle Garantien bietet, um von den betroffenen Personen als vertrauenswürdig erachtet zu werden (*Siehe Stellungnahme 02/2007 vom 17. Januar 2007 zum Entwurf eines Königlichen Erlasses zur Festlegung der Regeln, nach denen bestimmte Krankenhausdaten dem für die Volksgesundheit zuständigen Ministerium zu übermitteln sind*).

Spätere Verarbeitung zu statistischen und wissenschaftlichen Zwecken: Die Rolle einer Zwischenorganisation im Rahmen der späteren Verarbeitung von Daten zu historischen, statistischen und wissenschaftlichen Zwecken wurde ebenfalls genau dargelegt. So hat die Kommission klargestellt, welche Garantien die Hochschulwelt bezüglich der Verarbeitung personenbezogener Daten zu statistischen und wissenschaftlichen Zwecken beizubringen hat, wenn ein Wissenschaftler einen Antrag auf Zugang zu den innerhalb der Finanzverwaltung

verfügbaren Katasterdaten stellt (*Stellungnahme 32/2007 vom 7. November 2007 zur Verwendung von Katasterdaten zu statistischen und wissenschaftlichen Forschungszwecken*). Bei dieser Gelegenheit hat sie auch an ihre Rechtsprechung – und die ihrer sektoralen Ausschüsse – in Bezug auf die Verwendung der einheitlichen nationalen Nummer erinnert. Um die Interessen der Forscher an der Erhebung personenbezogener Daten zu wissenschaftlichen oder statistischen Forschungszwecken gegen die der Bürger an der Kontrolle der Verwendung ihrer Daten abzuwägen, empfiehlt die Kommission eine Arbeitsmethode, bei der die oder der Verantwortliche für die Verarbeitung der Datenbank, der die Stichprobe der zu befragenden Personen entnommen wurde, den ersten Kontakt mit den betroffenen Personen selbst herstellt, um sie um ihre Zustimmung zur Mitwirkung an der geplanten Erhebung zu bitten (*Stellungnahme 16/2006 vom 14. Juni 2006 bezüglich der Bedingungen für die Übermittlung von Daten aus dem nationalen Register im Rahmen einer (wissenschaftlichen) Untersuchung*).

Privatsektor

SWIFT: Die Verarbeitung personenbezogener Daten durch die Gesellschaft SWIFT und insbesondere ihre Übermittlung an die Vereinigten Staaten und ihre Abfrage durch das amerikanische Schatzamt (UST) mit dem erklärten Ziel, den Terrorismus zu bekämpfen, waren 2006 Gegenstand von zwei Stellungnahmen der belgischen Kommission. Darin gelangte die Kommission zu dem Schluss, dass die belgische Gesellschaft sich mehrere – strafrechtlich sanktionierte – Verstöße gegen das Privatsphäre-Gesetz hat zuschulden kommen lassen. Das ganze Jahr 2007 hindurch hat die Kommission die Entwicklung dieser Frage und die Maßnahmen, die von der Gesellschaft SWIFT ergriffen wurden, um ihre Tätigkeit mit den belgischen Vorschriften in Einklang zu bringen, aufmerksam verfolgt. Zu diesem Zweck hat sie gegenüber dieser Gesellschaft ein Empfehlungsverfahren eingeleitet. Zum Zeitpunkt der Abfassung dieses Berichts war dieses Verfahren noch nicht abgeschlossen.

Verbindliche Unternehmensregeln (Binding Corporate Rules – BCR): Das Privatsphäre-Gesetz verleiht dem König die Befugnis, nach Stellungnahme der belgischen Kommission die nicht dem Gesetz entsprechende internationale Übermittlung von Daten an ein Drittland auf Basis verbindlicher Unternehmensregeln, die bezüglich

des Datenschutzes ausreichende Garantien bieten, zu gestatten. Das Unternehmen General Electric (GE) hat beschlossen, für seine grenzüberschreitenden Ströme von Daten über seine Arbeitnehmer auf diese Form der Kontrolle zurückzugreifen. Gemäß seinen Regeln verpflichtet sich GE, den Föderalen Öffentlichen Dienst Justiz (das Justizministerium) und die belgische Kommission zu unterrichten, wenn eine ausländische Rechtsverpflichtung die Übermittlung von Daten vorschreibt, es sei denn, diese Information wird von dieser Behörde ausdrücklich verboten. Auch wenn die Kommission diese Unterrichtungspflicht – die übrigens auch von der Gruppe 29 in ihrem WP 128 über die oben erwähnten Arten der Datenverarbeitung durch SWIFT befürwortet wird – begrüßt, ist sie der Ansicht, (1) dass die damit verknüpfte Ausnahme auf ein Verbot ausschließlich durch die für die Überwachung der Einhaltung des Gesetzes zuständigen Behörden beschränkt werden muss, (2) dass dieses Verbot eine Rechtsgrundlage haben müsste und (3) dass es zeitlich begrenzt sein müsste. Im Übrigen macht die Kommission ihre positive Stellungnahme davon abhängig, dass die auf die individuelle Zustimmung des Arbeitgebers gegründete Ausnahme vom Widerspruchsrecht abgeschafft wird und die für den Datenschutz zuständigen Behörden die Möglichkeit eines Audits vorsehen (*Stellungnahme 13/2007 vom 21. März 2007 zum Entwurf eines Königlichen Erlasses, der die Übermittlung an einen Staat zulässt, der kein Mitglied der Europäischen Gemeinschaft ist und der kein angemessenes Niveau des Schutzes der personenbezogenen Daten der Mitarbeiter des Unternehmens General Electric gewährleistet*).

Whistleblowing: Aus dem Bericht 2006 ging hervor, dass die belgische Kommission im Anschluss an zahlreiche Fragen und Informationsanfragen in Bezug auf die Einführung beruflicher Ethikgrundsätze in Unternehmen (whistleblowing) eine *Empfehlung zur Vereinbarkeit beruflicher Warnsysteme mit dem Privatsphäre-Gesetz* verabschiedet hatte. Auf diese Empfehlung gestützt, hat die belgische Kommission 2007 die Einrichtung eines beruflichen Warnsystems beim flämischen Ombudsman, der im Zusammenhang mit den von Personalmitgliedern des flämischen öffentlichen Dienstes erstatteten Anzeigen von Unregelmäßigkeiten Untersuchungen durchführen darf, positiv aufgenommen.

Neue Technologien

Digitalfernsehen: Nach einer Stellungnahme zur digitalen Übertragung „traditioneller“ Fernsehdienstleistungen unter Ausschluss anderer vom Digitalfernsehen gebotener Möglichkeiten (zum Beispiel im Bereich der Interaktivität) formuliert die Kommission die folgenden Feststellungen:

- Die automatisierte Verarbeitung von Digitalfernseh-Daten durch die Fernsehanbieter muss als „Verarbeitung personenbezogener Daten“ betrachtet werden;
- was die Rechtmäßigkeit der Verarbeitung anbelangt, ist die Kommission der Ansicht, dass sich der Digitalfernsehanbieter, um die Sammlung personenbezogener Daten zu begründen, entweder auf die Zustimmung der betroffenen Person oder auf die Notwendigkeit berufen könnte, im Hinblick auf die Ausführung des von der betroffenen Person abgeschlossenen Verteilungsvertrags eine derartige Verarbeitung vorzunehmen, beispielsweise zu Fakturierungszwecken. Die Kommission schließt hingegen in jedem Fall aus, dass das berechnete Interesse des Fernsehanbieters gegenüber dem Schutz der Privatsphäre des betroffenen Verbrauchers überwiegt (Artikel 5f des Privatsphäre-Gesetzes – Artikel 7f der Richtlinie 95/46/EG);
- in der Stellungnahme werden die Bedeutung des Finalitätsprinzips und die Effektivität der Rechte der betroffenen Person besonders unterstrichen;
- schließlich befürwortet die Kommission die Annahme eines Verhaltenskodex speziell für diesen Sektor.

(Stellungnahme 06/2007 vom 7. Februar 2007 zum Digitalfernsehen und zum Schutz der Privatsphäre)

Interaktive Formen des Medienkonsums: In ihrer Stellungnahme 29/2007 vom 19. September 2007 zu den neuen Formen des Medienkonsums beleuchtet die belgische Kommission die neuen Gefahren für die Privatsphäre, die mit diesen neuen Formen des Medienkonsums einhergehen, insbesondere wenn sie interaktiv sind, und vor allem mit dem interaktiven Fernsehen: Benutzerprofilierung, Manipulation der Benutzer, Verlust des Rechts auf anonymen Medienkonsum und Verlust des Rechts auf Information, kulturelle Vielfalt und Pluralität der Medien. Was die Profilierung betrifft, unterstreicht die Stellungnahme die Tatsache, dass die Erbringung der Dienstleistung und die Profilierung zwei verschiedene

Finalitäten darstellen. Eine (spätere) Verarbeitung von Daten zu Profilierungszwecken ist daher nur zulässig, wenn die betroffene Person ihr zweifelsfrei zugestimmt hat. Es wird wichtig sein, zu kontrollieren, ob die Freiheit dieser Zustimmung beachtet wird: Eine Ablehnung der Profilierung darf nicht dazu führen, dass die betroffene Person von der Dienstleistung ausgeschlossen wird oder ganz allgemein keine Möglichkeit mehr hat, auf diese neuen Formen des Medienkonsums zuzugreifen.

Empfehlung bezüglich der Übertragung von Bildern

Im Allgemeinen: Angesichts der zunehmenden Übertragung von Bildern mithilfe von und auf immer zahlreicheren und vielfältigeren Trägern hat die belgische Kommission die Initiative ergriffen und eine Empfehlung zu diesem Thema abgegeben. Der interessierte Leser wird auf diese Empfehlung verwiesen (*Initiativempfehlung 02/2007 vom 28. November 2007 zur Übertragung von Bildern*).

Im schulischen Bereich: Auf der Grundlage der herausgearbeiteten Prinzipien hat die belgische Kommission eine Stellungnahme zur Übertragung von Fotos Minderjähriger im schulischen Bereich abgegeben. Tatsächlich nehmen derartige Übertragungen zu, entweder indem Klassenfotos auf die Internet-Site der Schule gestellt werden oder durch die Veröffentlichung von Einzelfotos. Die Kommission weist darauf hin, dass die Prinzipien des Privatsphäre-Gesetzes ohne Einschränkung auf diese Verarbeitung personenbezogener Daten anzuwenden sind. Sie schließt in der Tat die Anwendbarkeit der Ausnahmen, die für Datenverarbeitung zu journalistischen Zwecken vorgesehen sind, aus.

Im Prinzip wird die Zustimmung der „betroffenen Personen“ zu einer derartigen Verarbeitung personenbezogener Daten erforderlich sein. Wenn es sich um einen Minderjährigen ohne Urteilsvermögen handelt, wird diese Zustimmung bei seinen rechtmäßigen Vertretern zu beantragen sein. Wenn es sich um einen urteilsfähigen Minderjährigen handelt, empfiehlt die Kommission, den Minderjährigen einzubeziehen und seine eigene Zustimmung sowie die seiner rechtmäßigen Vertreter zu verlangen.

Die Kommission unterscheidet im Übrigen zwischen gezielten und nicht gezielten Fotos. Eine stillschweigende Zustimmung könnte vorausgesetzt werden, wenn im Rahmen der Berichterstattung über ein bestimmtes Ereignis ein *nicht gezieltes Foto* aufgenommen wird (Gruppenfoto bei einem Schulfest, Veröffentlichung in einer Schülerzeitung). Doch auch in diesem Fall müssen die betroffenen Personen über die Aufnahme des Fotos, aber auch über seinen Endzweck und die Art der geplanten Veröffentlichung informiert werden. Die Verwendung derartiger Fotos zwecks Werbung für die Schule ist ausgeschlossen. Solche Fotos dürfen die Ehre und den guten Ruf nicht angreifen. Im Übrigen dürfen keinerlei überflüssige personenbezogenen Daten das Foto begleiten. Diese Vorsichtsmaßnahme ist umso strenger zu beachten, wenn sensible Daten enthüllt werden.

Für die *gezielten Fotos* (zum Beispiel Einzelporträt) ist die vorherige Zustimmung nach Inkenntnissetzung der betroffenen Person – vor allem über die Ausübung ihrer Informations-, Zugangs-, Richtigstellungs- und Ablehnungsrechte – erforderlich, und zwar für jede Art von aufgenommenen Bildern und Übertragungsweisen. In Anwendung des Prinzips der Verhältnismäßigkeit empfiehlt die belgische Kommission ferner, dass die Internet-Veröffentlichung in Fällen, in denen sie zur Information von Eltern und Schülern bestimmt ist, auf einem Teil der Site erfolgt, zu dem nur sie Zugang haben, beispielsweise durch die Eingabe eines Passwortes.

Neue Internet-Site der belgischen Kommission zum Schutz der Privatsphäre

Anlässlich des ersten europäischen Datenschutztages hat die belgische Kommission ihre neue Internet-Site eröffnet, deren Inhalt sehr viel reichhaltiger ist als in der vorigen Version. Diese Site ist darauf ausgelegt, sowohl die Erwartungen der informationssuchenden Bürger zu erfüllen, als auch den Bedürfnissen eines in Bezug auf den Schutz personenbezogener Daten versierten Publikums gerecht zu werden. Sämtliche Stellungnahmen, Empfehlungen und Genehmigungen, auf die in dem vorliegenden Beitrag verwiesen wird, liegen unter der Adresse <http://www.privacycommission.be> vor.



Bulgarien

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 vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr wurde 2006 durch die Änderungen des Gesetzes über den Schutz personenbezogener Daten (GSPD) vollständig in bulgarisches Recht umgesetzt.

Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurde umgesetzt durch das Telekommunikationsgesetz, das im Staatsanzeiger, Ausgabe 41/2007, bekannt gemacht wurde.

2007 wurde die Verordnung Nr. 1/2007 über das Mindestniveau technischer und organisatorischer Maßnahmen und die zugelassene Art des Schutzes personenbezogener Daten, erlassen gemäß Art. 23, Absatz 5 des GSPD, verabschiedet und in Ausgabe 25/2007 des Staatsanzeigers veröffentlicht. Diese Verordnung legt das Mindestniveau technischer und organisatorischer Maßnahmen bei der Verarbeitung personenbezogener Daten und die zugelassene Art des Schutzes fest.

Neue Vorschriften über die Tätigkeit der Kommission für den Schutz personenbezogener Daten (KSPD), in Übereinstimmung mit Art. 9, Abs. 2 des GSPD, wurden in Ausgabe 25/2007 des Staatsanzeigers bekannt gegeben. Die Vorschriften regeln die Themen, die Funktionen und die Tätigkeit der KSPD; sie zielen auf die strikte Umsetzung des GSPD und auf die Einführung klarer Regeln für die für die Verarbeitung personenbezogener Daten Verantwortlichen und für Datensubjekte.

B. Bedeutende Rechtsprechung

Die typischen Fälle von Verletzungen der Richtlinie 95/46/EG und des GSPD betrafen 2007 die illegale Verarbeitung personenbezogener Daten von natürlichen

Personen ohne deren Zustimmung und ohne vorherige Meldung durch die für die Datenverarbeitung Verantwortlichen bezüglich der verarbeiteten Kategorien der personenbezogenen Daten und der Zwecke, für die sie verarbeitet wurden, der Empfänger ihrer personenbezogenen Daten und des Rechts natürlicher Personen auf Zugang zu ihren personenbezogenen Daten.

Die KSPD behandelte Beschwerden in Bezug auf die Verarbeitung personenbezogener Daten, die über die spezifischen, streng festgelegten gesetzlichen Zwecke hinausging, sowie die weitere Verarbeitung auf eine nicht mit diesen Zwecken übereinstimmende Weise. In diesen Fällen wurden Daten illegal auf Vorrat gespeichert, um sie für andere Zwecke, einschließlich Direktmarketing, zu benutzen. Nach der Erfahrung der KSPD kann man davon ausgehen, dass natürliche Personen besonders empfindlich sind, wenn es um die Weitergabe bestimmter Kategorien ihrer personenbezogenen Daten, meist in Bezug auf ihre Gesundheit, geht, aber dies waren 2007 keine typischen Fälle.

2007 ist die Zahl der Beschwerden in Bezug auf die Verarbeitung personenbezogener Daten zwecks Direktmarketing oder Videoüberwachung ohne Inkennzeichnung und Zustimmung der natürlichen Personen erheblich zurückgegangen.

Was die Verbreitung personenbezogener Daten im Internet betrifft, zeigt die Arbeit der KSPD, dass personenbezogene Daten in den meisten Fällen mithilfe der Registrierung auf Websites gesammelt werden und natürliche Personen derartige Daten aus freien Stücken verfügbar machen.

2007 gab die KSPD Stellungnahmen zu Fragen in Verbindung mit der legalen Verarbeitung personenbezogener Daten durch die für die Verarbeitung personenbezogener Daten Verantwortlichen ab. Stellungnahmen wurden sowohl von für die Verarbeitung personenbezogener Daten Verantwortlichen als auch von natürlichen Personen bezüglich ihrer Rechte gemäß dem GSPD angefordert. Abgegeben wurden Stellungnahmen in Bezug auf die legale Verarbeitung persönlicher Identifikationsnummern (PIN), die Verarbeitung personenbezogener Daten zu statistischen Zwecken, Voraussetzungen für die legale Verarbeitung

personenbezogener Daten von Kunden von Unternehmen, die öffentliche Dienstleistungen erbringen, und das Fotokopieren von Personalausweisen von Bankkunden.

Im Anschluss an die Änderungen des GSPD im Jahr 2006 und die Verabschiedung des neuen Artikels 36a des GSPD traf die Kommission Entscheidungen im Hinblick auf die Übermittlung personenbezogener Daten sowohl an die Mitgliedstaaten der Europäischen Union als auch an Drittländer. In Fällen, in denen die für die Verarbeitung personenbezogener Daten Verantwortlichen personenbezogene Daten an andere für Datenverarbeitung Verantwortliche auf dem Territorium von Drittländern außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums übermitteln, traf die KSPD ihre Entscheidung erst nach Beurteilung der Frage, ob in dem betreffenden Drittland ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet war. Diese Beurteilung stützt sich auf Kriterien wie die Art der bereitgestellten Daten; die Dauer der Datenverarbeitung; Zweck der Bereitstellung von personenbezogenen Daten; die Benachrichtigung der natürlichen Personen, deren Daten bereitgestellt werden, über die Zwecke dieser Bereitstellung und die Empfänger der Daten in dem Drittland; das Zugangsrecht der natürlichen Person und die Möglichkeit zur Berichtigung oder Löschung in Fällen, in denen die Verarbeitung dem GSPD nicht entspricht; unter der Voraussetzung, dass in dem Drittland für Datenschutz gesorgt wird und Maßnahmen für die Möglichkeit einer Entschädigung des Schadens vorgesehen sind, den die natürliche Person aufgrund der illegalen Verarbeitung erleidet. 2007 betrafen die Anträge, die von für die Verarbeitung personenbezogener Daten Verantwortlichen gemäß Art. 36a des GSPD an die KSPD gerichtet wurden, die Übermittlung personenbezogener Daten von ernannten Arbeitnehmern mit einem Arbeitsvertrag an die für die Datenverarbeitung Verantwortlichen mit dem Alleinbesitz des Kapitals von getrennten, in Drittländern ansässigen Unternehmen gemäß Art. 1, Punkt 14 der Zusatzklauseln des GSPD. Ferner wurden Anträge von für Datenverarbeitung Verantwortlichen gestellt, deren Tätigkeit die Auswahl von Personal und die Anwerbung von Seeleuten für Fahrten unter einer fremden Flagge beinhaltet.

C. Wichtige spezifische Themen

Im Januar begann die Durchführung eines Twinning-Projekts BG/2005/IB/OT/02 im Rahmen des PHARE-Programms BG2005/017-586.03.01: Weitere Verstärkung der Verwaltungskapazität der bulgarischen Kommission für den Schutz personenbezogener Daten und die Schaffung der Rahmenbedingungen für die Umsetzung des Gesetzes über den Schutz personenbezogener Daten.

Das Twinning-Projekt wurde in fünf Abschnitte unterteilt: 1. Analyse des Rechtsrahmens; 2. Aufbau der Institutionen; 3. Informationssystem der KSPD; 4. Bearbeitung von Beschwerden und Kontrollen; 5. Strategien und Methoden zur Sensibilisierung der Öffentlichkeit für die Tätigkeit der KSPD.

Das Projekt umfasste 42 Aktivitäten, die sein Hauptziel betreffen: Aufbau der Institutionen und damit zusammenhängende Investitionen in die bulgarische KSPD, um mehr Effizienz und eine bessere Arbeitsweise der Aktivitäten in Bezug auf den Schutz personenbezogener Daten in dem Land zu erreichen, und zwar durch die Übernahme und Umsetzung bewährter Verfahren der EU zur Vorbeugung von Verletzungen des Schutzes personenbezogener Daten sowie zu ihrem optimalen Schutz.

Die Aktivitäten betrafen verschiedene Bereiche des Schutzes personenbezogener Daten: Telekommunikation, Innenministerium, Justiz, Gesundheit, Versicherung, Direktmarketing, Banken, Videoüberwachung, E-Regierung usw.

Die Umsetzung der Aktivitäten im Rahmen des Twinning-Projekts wurde im Februar 2008 abgeschlossen.

Das PHARE-Programm BG2005/017-586.03.01 sieht die Umsetzung eines Durchführungsvertrags vor. Der Vertrag wird voraussichtlich Ende Februar unterzeichnet.

Jeden Monat werden Monitoring-Berichte über das Projekt erstellt, wodurch Schutz und effektive Kontrolle gewährleistet sind.

Im Jahr 2007 wurde ein Web-basiertes Informationssystem für die Registrierung der für die Verarbeitung personenbezogener Daten Verantwortlichen entwickelt, das folgende Möglichkeiten bietet:

1. Ausfüllen des Antragsformulars in einem speziellen Abschnitt der Website der KSPD – www.cdpd.bg
2. Bestätigung der eingetragenen Daten mit und ohne Verwendung einer elektronischen Signatur.
3. Registrierung der zugelassenen für die Verarbeitung personenbezogener Daten Verantwortlichen (VPDV) im KSPD-Register „Register der VPDV und der von ihnen geführten Register“ mit einem einmaligen Erkennungscode.
4. Das Register ist öffentlich, und der Zugang dazu erfolgt über die Website der KSPD – www.cdpd.bg
5. Empfang, auf der E-Mail-Adresse der registrierten VPDV, der offiziellen Bestätigung, dass sie in dem System registriert sind, sowie des Benutzernamens und Passworts für den Zugang zu ihrem eigenen Profil, mit dem sie Aktualisierungen zu Veränderungen, die bei den angegebenen Umständen aufgetreten sind, vornehmen können.
6. Zugänglichkeit von Daten aus dem öffentlichen Register, sowohl für die registrierten VPDV als auch für alle interessierten Parteien, die jederzeit über die neuen Aktivitäten und den neuen Status der Organisationen informiert werden können.

Derzeit befindet sich das System im letzten Versuchsstadium und wird innerhalb des lokalen Netzwerks der KSPD eingesetzt. Voraussichtlich wird es Anfang 2008 allen VPDV über die Website der KSPD – www.cdpd.bg – zugänglich sein.



Republik Zypern

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

Richtlinien 95/46/EG und 2002/58/EG:
Keine neuen Entwicklungen zu melden.

Am 31. Dezember 2007 wurde im Staatsanzeiger der Republik ein Gesetz mit dem Titel „Vorratsspeicherung von Telekommunikationsdaten für die Zwecke der Untersuchung schwerer Straftaten“ veröffentlicht.

Mit diesem Gesetz wurden die Vorschriften der Richtlinie 2006/24/EG vom 15. März 2006 über die Vorratsspeicherung von Daten umgesetzt.

Der Zeitraum für die Vorratsspeicherung von Daten wurde auf sechs Monate festgelegt.

Schwere Straftaten wurden als Straftaten definiert, die nach dem Strafgesetzbuch oder jedem anderen Gesetz als Verbrechen gelten oder für die eine Haftstrafe von fünf Jahren oder mehr verhängt wird.

Nach dem Gesetz ist der Zugang zu auf Vorrat gespeicherten Telekommunikationsdaten nur dann zulässig, wenn ein Präsident eines Bezirksgerichts oder ein führender Amtsrichter eine entsprechende Weisung erteilt, nachdem ein Polizeiermittler mit Zustimmung des Generalstaatsanwaltes einen Antrag auf einen solchen Zugang gestellt hat.

Es gibt eine ausdrückliche Vorschrift, nach der die Vorratsspeicherung oder Offenlegung des Inhalts der Kommunikation verboten ist.

Telekommunikationsdaten, die aufgrund einer gerichtlichen Weisung an die entsprechende Behörde weitergegeben wurden, müssen binnen 10 Tagen ab dem Weitergabedatum vernichtet werden, wenn der Generalstaatsanwalt der Republik der Ansicht ist, dass sie nicht mit der Begehung einer schweren Straftat zusammenhängen.

In anderen Fällen werden die Daten gemäß einer vom Polizeichef vorgeschriebenen und von der Aufsichtsbehörde genehmigten Methode vernichtet.

Der Kommissar für den Schutz personenbezogener Daten wurde zur Aufsichtsbehörde für den Zweck der Überwachung der Umsetzung des Gesetzes bestimmt.

Die Aufsichtsbehörde ist befugt, Audits vorzunehmen und Beschwerden zu prüfen und dem Generalstaatsanwalt der Republik einen Fall vorzulegen, wenn eine Verletzung eine Straftat darstellen könnte.

Laut einer Erklärung der Republik Zypern werden die Vorschriften des Gesetzes über die Vorratsspeicherung von Telekommunikationsdaten in Bezug auf Internet-Zugang, Internet-Telefonie und E-Mail am 15. März 2009 in Kraft treten.

B. Bedeutende Rechtsprechung

Nachdem im März 2007 in einer Tageszeitung ein Bericht über die Situation im alten Nicosia General Hospital (nach seinem Umzug in ein neues Gebäude) veröffentlicht wurde, beschloss der Kommissar, eine Untersuchung durchzuführen.

Die Untersuchung ergab, dass in gewissen Teilen des alten Krankenhauses Dokumente zurückgelassen worden waren, die personenbezogene Patientendaten enthielten, und dass der Zugang zu den Räumlichkeiten trotz der Anwesenheit von Wächtern am Krankenseingang nicht kontrolliert wurde und jeder Zugang zu den Gebäuden und allen darin befindlichen Dokumenten hatte, einschließlich der Personen, die im Krankenhaus Reparaturen ausführten.

Die Vertreter des Gesundheitsministeriums, das für den Umzug des Krankenhauses verantwortlich war, gaben Erklärungen bezüglich der Sicherheitsmaßnahmen und der in den alten Räumlichkeiten zurückgelassenen Daten ab.

Danach wurden Maßnahmen ergriffen, um das unbefugte Betreten der Räumlichkeiten zu verhindern, und

die darin befindlichen Dokumente wurden an einen sicheren Ort gebracht und/oder vernichtet.

Unter Berücksichtigung aller mit dem Fall verbundenen Umstände und der Tatsache, dass die Anweisungen des Kommissars befolgt wurden, wurde dem Generaldirektor des Ministeriums eine Geldstrafe in Höhe von C£1 500 auferlegt.

Ein Spam-Fall, bei dem es um den Versand unerwünschter Mitteilungen zu den Ergebnissen von Pferderennen an Mobiltelefone ging, wurde untersucht, nachdem beim Kommissar eine Reihe von Beschwerden eingegangen war. Die Nachrichten wurden (von mehreren Nummern) mithilfe vorbezahlter Telefonkarten verschickt. Die Sender dieser Nachrichten haben unsere Briefe und Fragen nie beantwortet, und im Anschluss an das vorgeschriebene Verfahren hat der Kommissar eine Entscheidung erlassen, die ihnen eine Geldstrafe in Höhe von C£2 000 auferlegt.

C. Wichtige spezifische Themen

Im Grundbuchamt wurde ein Audit vorgenommen, um festzustellen, wie das Amt seine verschiedenen Verarbeitungsoperationen ausführte.

Das Audit wurde auf Basis eines Fragebogens durchgeführt und ergab Folgendes:

- Die Informationen, die Datensubjekten bezüglich der Verarbeitung ihrer Daten erteilt wurden, waren nicht ausreichend/zufriedenstellend.
- Das Amt sammelte Daten von Dritten und versäumte es, die Datensubjekte entsprechend zu informieren.
- Städtischen und anderen Kommunalbehörden wurden zwecks Erhebung von Grundsteuern Daten über die Besitzer von Immobilien übergeben, ohne dass die Besitzer darüber informiert wurden.
- In gewissen von dem Amt verwendeten Dokumenten werden zu viele und irrelevante Informationen gesammelt.
- Die Mitarbeiter des Amtes, die mit der Verarbeitung personenbezogener Daten befasst sind, haben keinerlei Informationen/Schulung in Bezug auf das Datenschutzgesetz und auch keine schriftlichen oder anderen Anleitungen im Hinblick auf ihre diesbezüglichen Verpflichtungen erhalten.

Die Ergebnisse des Audits wurden dem Amt mitgeteilt, und wir überwachen derzeit die Schritte, die es unternimmt, um den Anweisungen des Kommissars Folge zu leisten.

Die Beschäftigten einer Kommunalbehörde beschwerten sich beim Kommissar darüber, dass von ihnen verlangt wird, sich die Fingerabdrücke abnehmen zu lassen, um zu kontrollieren, wann sie an ihrem Arbeitsplatz ankommen und ihn wieder verlassen.

Im Rahmen der Prüfung dieser Beschwerde erklärte die betreffende Kommunalbehörde, sie habe sich für diese Methode entschieden, weil die zuvor angewendete Methode (Lochen einer Karte) missbraucht worden sei (die Beschäftigten vernichteten ihre Karten oder lochten die Karten anderer Beschäftigter) und diese Methode wirksamer sei und Missbrauch ausschließe. Die Behörde führte dem Kommissar auch das zur Abnahme der Fingerabdrücke eingesetzte System vor. Nach Erwägung aller Argumente und der ihm vorgelegten Informationen entschied der Kommissar, dass die Abnahme von Fingerabdrücken zur Überprüfung der Anwesenheit der Beschäftigten unter diesen Umständen gesetzlich nicht zulässig sei, und forderte die Behörde auf, diese Praktik einzustellen und alle bereits gesammelten Fingerabdrücke zu vernichten.

Da dem Kommissar noch andere Beschwerden und Fragen in Bezug auf das Sammeln/die Verwendung der Fingerabdrücke von Beschäftigten zwecks Überprüfung ihrer Anwesenheit am Arbeitsplatz vorgelegt wurden, hat der Kommissar Anleitungen zur Sammlung von Fingerabdrücken für diesen Zweck erlassen (die auf unsere Website gestellt wurden) und darauf hingewiesen, dass ihre Sammlung für den oben genannten Zweck *prima facie* gegen das Gesetz verstößt und nur in sehr außergewöhnlichen/spezifischen Fällen angewendet werden sollte.



Tschechische Republik

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

Die grundlegende Rechtsvorschrift im Bereich des Schutzes personenbezogener Daten ist das Gesetz Nr. 101/2000 Coll. über den Schutz personenbezogener Daten und Änderungen einiger damit zusammenhängender Gesetze, das am 1. Juni 2000 in Kraft getreten ist. Das Amt für den Schutz personenbezogener Daten (ASPD) wurde auf der Grundlage der Vorschriften dieses Gesetzes errichtet und ist mit weitreichenden Befugnissen ausgestattet; unter anderem kann es bei Gesetzesverstößen Maßnahmen ergreifen und direkt Geldbußen verhängen und ist außerdem unabhängig. Das Gesetz hat die Richtlinie 95/46/EG im Wesentlichen in tschechisches Recht umgesetzt. 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 erwähnten Richtlinie in Einklang gebracht.

Die Richtlinie 2002/58/EG wurde 2004 teilweise umgesetzt durch das Gesetz Nr. 480/2004 Coll. über bestimmte Dienstleistungen der Informationsgesellschaft, das besondere Vorschriften zu unerbetenen Nachrichten enthält und für das ASPD neue, wirksame Befugnisse bei der Bekämpfung von „Werbenachrichten“ (Spams) vorsieht. Anschließend wurde diese Richtlinie 2005 im Wesentlichen durch das Gesetz Nr. 127/2005 Coll. über elektronische Kommunikation umgesetzt, das gleichzeitig eine Reihe anderer Richtlinien aus dem „Telekommunikationspaket“ implementiert.

2007 gab es in der grundlegenden Datenschutzgesetzgebung die zwei folgenden Entwicklungen:

- geringfügige Änderung des Datenschutzgesetzes Nr. 101 für die Zwecke des Eintritts der Tschechischen Republik in das Schengen-Gebiet (Gesetz Nr. 101 wurde durch Gesetz Nr. 170/2007 Coll. geändert), und
- Einleitung eines Verfahrens zur Änderung des Gesetzes Nr. 127 über elektronische Kommunikation aufgrund der Notwendigkeit, die Richtlinie Nr. 2006/24/EG über die Vorratsspeicherung von Daten in nationales

Recht umzusetzen; dieses Verfahren ist noch nicht abgeschlossen.

B. Bedeutende Rechtsprechung

Gemäß den Rechtsvorschriften der Regierung der Tschechischen Republik ist das ASPD die beauftragte Stelle, der die Entwürfe der relevanten Gesetze und anderen Vorschriften im Rahmen der interministeriellen Verfahren zur Stellungnahme vorzulegen sind, also bevor der Entwurf dem Parlament vorgelegt wird. 2007 nahm das ASPD zu einer Reihe von Rechtsvorschriften Stellung.

Die Umsetzung der Richtlinie über die Vorratsspeicherung von Daten wird, neben der Änderung des Gesetzes über elektronische Kommunikation (siehe oben), die Einführung von Änderungen an einigen anderen Gesetzen, hauptsächlich dem Polizeigesetz Nr. 283/1991 Coll., erforderlich machen. Das Polizeigesetz wird ohnehin aus anderen Gründen geändert. Der Entwurf ist beim ASPD auf harsche Kritik gestoßen, und das Verfahren ist noch nicht abgeschlossen.

Die langfristigen Vorbereitungen für den Eintritt der Tschechischen Republik in das Schengen-Gebiet erreichten 2007 ihren Höhepunkt. Am 1. September 2007 wurde das Schengen-Informationssystem versuchsweise in Betrieb genommen. Ende September 2007 wurde die Evaluierungsmission der dafür eingesetzten Experten mit positiven Ergebnissen beendet. Im Rahmen der Vorbereitungen mussten mehrere Gesetze geändert werden, vor allem:

- Gesetz Nr. 283/1991 Coll. (geändert), über die Polizei der Tschechischen Republik;
- Gesetz Nr. 141/1961 Coll. (geändert), über Strafgerichtsverfahren (Strafordnung);
- Gesetz Nr. 326/1999 Coll. (geändert), über den Aufenthalt von Ausländern auf dem Hoheitsgebiet der T. R.;
- Gesetz Nr. 325/1999 Coll. (geändert), über Asyl;
- Gesetz Nr. 361/2000 Coll. (geändert), über Verkehr auf dem Straßennetz;
- Gesetz Nr. 56/2001 Coll. (geändert), über die Bedingungen für den Verkehr von Fahrzeugen auf dem Straßennetz.

Der Status des ASPD als unabhängiges Aufsichtsorgan für das Schengen-Informationssystem wurde endgültig bestätigt. Schließlich bekräftigte die Entscheidung des Rates 2007/801/EG vom 6. Dezember 2007 die volle Anwendung der Schengen-Regelungen in neun Ländern, einschließlich der Tschechischen Republik.

C. Wichtige spezifische Themen

Die vom ASPD im Jahr 2007 **durchgeführten Kontrollen** umfassten insgesamt 112 abgeschlossene Kontrollverfahren. Bei der Mehrzahl der von unabhängigen Prüfern und deren Kontrollteams durchgeführten Überprüfungen handelte es sich um *Ad-hoc*-Kontrollen, d. h. der Überprüfung von Veranlassungen und Beschwerden seitens Privatpersonen. Lediglich rund 15 % der Kontrollen wurden im Rahmen des Jahresplan für Kontrollaktivitäten durchgeführt, wobei derartige Kontrollaktionen in der Regel sehr viel komplexer sind und ein breiteres Spektrum an Datenverarbeitungsmerkmalen und -aspekten abdecken.

Der Jahresplan für Kontrollaktivitäten 2007 konzentrierte sich auf 5 allgemeine Bereiche:

1. Informationssysteme der öffentlichen Verwaltung, mit besonderen Auswirkungen auf Datenverarbeitung in Verbindung mit Informationen über den Besitz natürlicher Personen (z. B. das Grundbuch);
2. Verarbeitung personenbezogener Daten im Rahmen von Überwachungssystemen (Kameraanlagen), mit besonderen Auswirkungen auf Überwachungssysteme in Bildungsanstalten, Gesundheitseinrichtungen und Gemeindeverwaltungen;
3. Bereitschaft der Tschechischen Republik zum Eintritt in das Schengen-Gebiet, insbesondere als Follow-up zu den Ergebnissen der Experten-Evaluierungsmission 2006;
4. Verkehrssysteme – besondere Aufmerksamkeit wurde der Überwachung von Fahrzeugbewegungen im Straßenverkehr, z. B. im Zusammenhang mit dem Einzug von Mautgebühren, gewidmet;
5. Verarbeitung personenbezogener Daten in der Verwaltung von Staatsanwalts- und Justizbehörden.

Die oben erwähnten Kontrollaktivitäten umfassen nicht die Tätigkeiten in Bezug auf **unerbetene Werbenachrichten** („Marketing-Spams“). 2007 erhielt das ASPD 1 569

Beschwerden und andere Anfragen in Bezug auf diesen spezifischen Bereich; die damit verbundenen Kontrollaktionen betrafen 515 Unternehmen, von denen 466 angewiesen wurden, Maßnahmen zu ergreifen. Weiteren 71 wurden Geldstrafen auferlegt.

Wie im Vorjahr lassen sich die am häufigsten auftretenden Probleme folgendermaßen zusammenfassen:

- Viele der kontrollierte 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.
- Praktisch keine der Mitteilungen wurde ausdrücklich als Werbenachricht kenntlich gemacht. Die Mitteilungen tragen alle möglichen Arten von Bezeichnungen: Newsletter, Information, Nachrichten usw. Das Gesetz über gewisse Dienste der Informationsgesellschaft schreibt jedoch vor, dass eine Werbenachricht „klar und deutlich“ als solche kenntlich gemacht werden muss.
- 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.
- Manche Anbieter elektronischer Dienste gehen davon aus, dass das Anklicken eines Kontrollkästchens auf dem Registrierungsformular im entsprechenden 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 Passwort geschützt ist.
- 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.

Zusätzlich zu seinen standardmäßigen Überwachungsaktivitäten hat das ASPD große Anstrengungen im Bereich von **Kommunikationsaktivitäten** unternommen: Die tschechische Datenschutzbehörde (DSB) und das Ministerium für Bildung, Jugend und Sport haben ein spezifisches *Bildungsprogramm* für Sekundarschullehrer entwickelt, das aus einem vierstündigen Kurs besteht und den Schutz der Privatsphäre und personenbezogener Daten im Kontext grundlegender Menschenrechte zum Thema hat. Ferner wurde in Zusammenarbeit mit dem tschechischen Fernsehen ein *unterhaltsamer Film* gedreht, der 13 Episoden umfasst und vier Monate lang zur Hauptsendezeit ausgestrahlt wurde.

Nicht zuletzt wurde am Datenschutztag ein *Jugendwettbewerb* mit dem Titel „Meine Privatsphäre! Nicht gucken, nicht schnüffeln“ gestartet, der im April 2007 ausgewertet wurde. In diesem Kontext waren Jugendliche aus zwei Altersgruppen aufgerufen, in literarischer oder grafischer Form zum Ausdruck zu bringen, was sie unter den Begriffen Schutz der Privatsphäre und Schutz personenbezogener Daten verstehen. Am 1. Juni 2007, dem 7. Jahrestag der Einrichtung der tschechischen DSB, wurden die Preise den Gewinnern im Rahmen des Internationalen Filmfestivals für Kinder und Jugendliche in der Stadt Zlín überreicht.

Am 11. Dezember 2007 vergab die Datenschutzbehörde der Gemeinschaft Madrid den „Europäischen Preis für Best-Practice im Datenschutz in europäischen öffentlichen Diensten“ an das ASPD.



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 verabschiedet und trat am 1. Juli 2000 in Kraft. Die englische Fassung des Gesetzes kann auf folgender Adresse abgerufen werden:
<http://www.datatilsynet.dk/english/the-act-on-processing-of-personal-data/>

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, Paragraph 6 (vgl. 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 im Telekommunikationsmarkt (vgl. Durchführungsverordnung Nr. 780 vom 28. Juni 2007);
- die Durchführungsverordnung Nr. 1031 vom 13. Oktober 2006 über die Bereitstellung elektronischer Kommunikationsnetze und Dienstleistungen;
- Kapitel 71 der Zivilprozessordnung, (vgl. Durchführungsverordnung Nr. 1261 vom 23. Oktober 2007);
- Paragraph 263 des Strafgesetzbuches, (vgl. Durchführungsverordnung Nr. 1260 vom 23. Oktober 2007).

Gemäss Artikel 57 des Gesetzes über den Schutz personenbezogener Daten ist die Stellungnahme der dänischen Datenschutzbehörde (DSB) einzuholen, wenn Verordnungen, Rundschreiben oder ähnliche allgemeine Richtlinien für den Schutz der Privatsphäre in Zusammenhang mit der Datenverarbeitung herausgegeben werden. Dies gilt auch für Gesetzesentwürfe. Die DSB hat zu verschiedenen Gesetzen und Regelungen, die Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz haben, Stellung bezogen.

2007 legte das Justizministerium einen Gesetzentwurf für die Sicherheit bei bestimmten Sportveranstaltungen vor (Hooligan-Register).

Die Gesetzesvorlage sieht die polizeiliche Sperrung einer Person vor, falls sich diese einer Straftat im Zusammenhang mit einer spezifischen Sportveranstaltung schuldig gemacht hat und Anlass zur Vermutung besteht, dass die Person, falls nicht gesperrt, innerhalb des von der Sperrung betroffenen Gebiets neue Straftaten begehen würde.

Einer gesperrten Person wäre der Besuch bestimmter Sportveranstaltungen und der Aufenthalt innerhalb 6 Stunden vor und 6 Stunden nach der Veranstaltung untersagt, wobei sich die Person in einem Umkreis von 500 Metern von diesen Sportveranstaltungen nicht bewegen dürfte. Nach dem Gesetzentwurf sollte die Sperrung für einen bestimmter Zeitraum von nicht mehr als 2 Jahren gelten.

Nach dem Gesetzentwurf sollte die Polizei personenbezogene Daten über gesperrte Personen an Sportclubs übermitteln, um auf diesem Weg die Sperrung verstärkt durchzusetzen. Die an die Sportclubs übermittelten personenbezogenen Daten würden Namen und Fotos enthalten.

Der DSB zufolge gibt der Gesetzentwurf Anlass zu Bedenken, was den Schutz der Privatsphäre der Datensubjekte betrifft. Die DSB bezweifelte, dass die vorgeschlagene Verarbeitung sensibler Daten im Hinblick auf die in dem Gesetzesvorschlag beschriebenen Zwecke angemessen wäre.

Die DSB wies darauf hin, dass das vorgeschlagene Gesetz es ermöglichen würde, sensible Daten über die Datensubjekte zu verarbeiten, auch wenn diese nur einer Straftat beschuldigt würden.

Die DSB betonte ferner, dass der Gesetzesvorschlag dazu führen könne, sensible Daten an einen breiteren Personenkreis zu übermitteln und somit das Risiko erhöhe, dass Daten entgegen dem Gesetz über die Verarbeitung personenbezogener Daten verarbeitet würden.

Im letzten Entwurf des Gesetzesvorschlags ist der Gesetzgeber auf viele der von der DSB geäußerten Bedenken eingegangen. Der Gesetzesvorschlag ist bisher jedoch noch nicht verabschiedet worden.

B. Bedeutende Rechtsprechung

Die DSB wurde gebeten, eine Stellungnahme abzugeben zur Forderung des ATP⁸ (Arbejdsmarkedets Tillægspension), personenbezogene Daten an Drittländer zu übermitteln, vgl. Paragraf 27 (4) des Gesetzes über die Verarbeitung personenbezogener Daten.

Die DSB wurde darüber informiert, dass das ATP Ende 2006 über fast 4,5 Millionen Mitglieder und ungefähr 150 000 Beitrag zahlende Arbeitgeber sowohl aus dem privaten als auch aus dem öffentlichen Sektor verfüge.

Die vom ATP verarbeiteten personenbezogenen Daten umfassten Informationen über Namen, Adresse, sonstige Kontaktinformationen, Personenstandsregisternummer, Arbeitgeber, Beruf und Ausbildung.

Vor allem aus Gründen der Liefersicherheit wollte das ATP Daten über Mitglieder und Beitrag zahlende Arbeitgeber an Datenverarbeiter in Indien und Südafrika übermitteln.

Die DSB wies das ATP auf den Paragraf 41 (4) des Gesetzes über die Verarbeitung personenbezogener Daten hin, der Folgendes besagt: „Im Hinblick auf Daten, die für die öffentliche Verwaltung erzeugt werden und für fremde Staaten von besonderem Interesse sind, werden Maßnahmen ergriffen, um sicherzustellen, dass sie im Kriegsfall oder unter ähnlichen Umständen beseitigt oder vernichtet werden können.“

Nach einem Briefwechsel mit dem ATP gelangte die DSB zu dem Schluss, dass Paragraf 41 (4) es dem ATP untersagte, personenbezogene Daten an Indien und Südafrika zu übermitteln.

Die DSB unterstrich die Art der verarbeiteten personenbezogenen Daten und die Menge der vom ATP verarbeiteten Daten (die praktisch die gesamte Bevölkerung Dänemarks abdecken).

Ferner wies die DSB darauf hin, dass bei der Verabschiedung des Gesetzes über die Verarbeitung personenbezogener Daten sowohl personenbezogene Daten aus dem zentralen Personenstandsregister als auch personenbezogene Daten über die Ausbildung von Bürgern vom Gesetzgeber als Informationen bezeichnet wurden, die durch den Paragraf 41 (4) abgedeckt werden.

C. Wichtige spezifische Themen

2005 beschloss der dänische Justizminister, eine Expertengruppe einzusetzen, um die bestehenden Gesetze über Fernsehüberwachung zu bewerten und eine Grundlage zu schaffen, auf der entschieden werden kann, wo die Grenze zwischen dem Bedarf an Sicherheit und Verbrechensvorbeugung und dem Recht des Bürgers auf Privatsphäre zu ziehen ist.

Dieser Beschluss beruhte unter anderem auf einer aktuellen Stellungnahme der DSB, die auf eine Reihe bedenklicher Aspekte im Zusammenhang mit der gemeinsamen Durchsetzung des Gesetzes über Fernsehüberwachung und des Gesetzes über die Verarbeitung personenbezogener Daten hinwies.

Auf Grundlage der Stellungnahme der Expertengruppe, zu der die DSB Stellung bezog, verabschiedete das dänische Parlament am 1. Juni 2007 ein neues Gesetz.

Die Hauptbestandteile des Gesetzes sind:

- Möglichkeit für Finanzinstitute, Kasinos, Hotels, Restaurants, Einkaufszentren und Einzelhandelsgeschäfte, ihre eigenen Eingänge und die Fassaden der Gebäude mit Kameras überwachen zu lassen. Die Überwachung von Bereichen, die sich unmittelbar neben Eingängen und Fassaden befinden und die normalerweise als Zugangs- oder Fluchtwege zu und/oder von eigenen Eingängen benutzt werden oder benutzt werden könnten, darf nur dann von Finanzinstituten, Kasinos, Hotels, Restaurants, Einkaufszentren und Einzelhandelsgeschäften veranlasst werden, wenn sie

⁸ Unabhängige Einrichtung, durch das Gesetz Nr. 46 vom 7. März 1964 zu dem Zweck errichtet, Zusatzrenten an Lohnempfänger usw. zu zahlen.

zur Vorbeugung von Straftaten eindeutig notwendig ist.

- Änderung des Datenschutzgesetzes, das nun jede Verarbeitung personenbezogener Daten in Verbindung mit Fernsehüberwachung umfasst und spezifische Vorschriften über die Vorratsspeicherung von Daten (30 Tage, falls die Daten nicht für einen spezifischen Fall erforderlich sind) und die Weitergabe von Daten (die nur gestattet ist, wenn das Datensubjekt ausdrücklich zugestimmt hat, wenn die Weitergabe gesetzlich vorgeschrieben ist oder wenn die Daten zu Ermittlungszwecken an die Polizei weitergegeben werden) enthält.
- Es ist nicht erforderlich, der DSB Datenverarbeitungen in Verbindung mit Fernsehüberwachung zu melden.
- Die DSB ist für die Beaufsichtigung der Datenverarbeitung in Verbindung mit Fernsehüberwachung durch private Prüfer zuständig.

In ihrer Stellungnahme, die vor der Verabschiedung des neuen Gesetzes durch das dänische Parlament vorgelegt wurde, befürwortete die DSB den Vorschlag, dass es nur bestimmten Gruppen von Unternehmen gestattet sein sollte, in begrenzten Bereichen Fernsehüberwachung einzusetzen, und dass die Überwachung zum Zweck der Verbrechensvorbeugung eindeutig erforderlich sein muss.

Die DSB betonte, dass der Gesetzentwurf zu einer steigenden Verarbeitung personenbezogener Daten führen würde und auch die Personen betreffen würde, die sich in den überwachten Bereichen bewegen.

Im Zusammenhang mit den erweiterten Möglichkeiten zur Veranlassung von Fernsehüberwachung wies die DSB auf die Notwendigkeit angemessener Schutzvorkehrungen hin, wie etwa die Einführung von Regelungen zur Vorratsspeicherung und zur Datenübermittlung.

Im Hinblick auf Tonaufzeichnungen im Zusammenhang mit Fernsehüberwachung verlangte die DSB, im Rahmen der Verabschiedung des neuen Gesetzes über diesen Punkt nachzudenken, da das aktuelle Gesetz im Gegensatz zum Datenschutzgesetz die Verarbeitung personenbezogener Daten in Verbindung mit Tonaufzeichnungen nicht abdeckt.

Die DSB befürwortete die Empfehlung, dass die DSB nicht über Fernsehüberwachung unterrichtet werden sollte, einerseits aufgrund der Überlegungen zu den erforderlichen Mitteln, andererseits weil die DSB in diesem Fall dafür verantwortlich wäre, alle Datenkontrolleure (öffentliche wie private) zu beaufsichtigen, die personenbezogene Daten im Zusammenhang mit Fernsehüberwachung verarbeiten.



Estland

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

Die Entwicklung, die im letzten Berichtszeitraum in diesem Bereich stattgefunden hat, war die Fertigstellung der Gesetzesentwürfe für das Gesetz über den Schutz personenbezogener Daten (im Folgenden GSPD) und das Gesetz über die Information der Öffentlichkeit (im Folgenden GlÖ); die Verabschiedung der Änderungen dieser Gesetze und ihr teilweises Inkrafttreten dürfen als die wichtigsten Entwicklungen des aktuellen Zeitraums betrachtet werden. Während des kommenden Berichtszeitraums sollen zwei wichtige Gesetze endgültig umgesetzt werden.

Änderungen in der Art und Weise, wie personenbezogene Daten eingestuft werden, und die Einbeziehung biometrischer Daten in die Kategorie sensibler Daten sind die Hauptmerkmale des GSPD, das am 15. Februar 2007 verabschiedet wurde und 2008 vollständig in Kraft tritt. Überdies gehört dazu der erhöhte Schutz bei der Verarbeitung personenbezogener Daten, d. h. Änderungen in Rechtsvorschriften über die Verarbeitung personenbezogener Daten, die für legale öffentliche Verwendung verfügbar gemacht werden, Vorschriften zur Verarbeitung personenbezogener Daten für Forschungs- oder Regierungsstatistiken sowie die Einsetzung eines offiziellen Verantwortlichen für den Schutz personenbezogener Daten.

Seit dem 1. Januar 2008 besteht die Kategorie private personenbezogene Daten nicht mehr. Personenbezogene Daten werden nun in „sensible personenbezogene Daten“ und „personenbezogene Daten“ unterteilt. Mit der Aufhebung der Kategorie private personenbezogene Daten entfällt auch die oben erwähnte Verpflichtung, die Verarbeitung dieser Daten zu melden.

Seit dem 1. Januar 2008 werden biometrische Daten, vor allem Fingerabdrücke, Handtellerabdrücke und Irisabbildungen, als sensible personenbezogene Daten behandelt, und der Begriff Daten in Bezug auf genetische Informationen wurde durch „genetische Daten“ ersetzt.

Eine der gesetzlichen Änderungen sieht vor, dass eine Person das Recht hat, die Beendigung der Weitergabe und jeder anderen Verwendung von personenbezogenen Daten, die in gesetzlich zulässiger Weise für öffentliche Verwendung bestimmt wurden, zu verlangen. Folglich wird eine Person die Kontrolle über die weitere Verwendung dieser Daten nach ihrer Weitergabe behalten, was nach dem früheren Gesetzestext nicht möglich war.

Seit dem 1. Januar 2008 regelt das GSPD die Erhebung personenbezogener Daten zwecks Solvenzeinschätzung. Während es bis zu diesem Punkt den geltenden Normen entsprach, war die Frist für die Erhebung solcher Daten nicht speziell festgelegt. Ab dem 1. Januar 2008 dürfen personenbezogene Daten über Zahlungsverzug nur noch binnen drei Jahren ab der Nichterfüllung der Verpflichtungen verarbeitet und an Dritte weitergegeben werden. Die Daten im Kreditregister dürfen also nicht älter als drei Jahre sein. Ältere Daten werden aus dem Register entfernt. Diese Änderung soll im Wesentlichen sicherstellen, dass jeder Verarbeiter die Grundlage für die Verarbeitung der Daten sichert und gewährleistet, dass Verträge, Vereinbarungen und andere Dokumente den gesetzlichen Anforderungen nicht zuwiderlaufen. Die Anforderungen bezüglich der Zustimmung des Datensubjekts haben sich ebenfalls geändert.

Künftig kann eine Person die Verarbeitung von Daten verbieten, wenn die Rechtsgrundlage für ihre Offenlegung und Verarbeitung nicht geprüft werden kann.

Eine Person kann die weitere Verarbeitung nur dann nicht verbieten, wenn die ursprüngliche Offenlegung zu journalistischen Zwecken (das Gesetz enthält diesbezüglich neue Vorschriften) oder auf gesetzlicher Grundlage (zum Beispiel Datenbanken, die nur Regierungsstellen zugänglich sind) erfolgt ist.

B. Bedeutende Rechtsprechung

Fall 1: Offenlegung personenbezogener Daten auf der Website der Regierung der Stadt Tallinn

Eine Privatperson wandte sich an die Datenschutzbehörde und verlangte eine Erklärung für folgenden Sachverhalt: Auf welcher gesetzlichen Grundlage wurde der Name ihres Kindes im Register der Rechtsakte der

Regierung der Stadt Tallinn, zu dem die Öffentlichkeit Zugang hat, offen gelegt? Die Person führte an, man habe personenbezogene Daten offen gelegt, zu denen Dritte nur beschränkt Zugang haben sollten.

Die Datenschutzbehörde wandte sich diesbezüglich an die Regierung der Stadt Tallinn und erklärte den Beamten ihren Standpunkt. Die Datenschutzbehörde nahm schriftlich zu der Offenlegung personenbezogener Daten in Rechtsakten der Regierung der Stadt Tallinn Stellung und verlangte, auf Basis der Beschwerde einer Privatperson, die Beseitigung des Namens des Kindes dieser Privatperson aus dem Register der Rechtsakte, das auf der Website der Regierung der Stadt Tallinn veröffentlicht wird. Nach Kenntnisnahme dieses Standpunkts unterließ es die Regierung der Stadt Tallinn, den Namen des Kindes bis zum angegebenen Datum aus dem Register zu entfernen.

Dem Gesetz über die Organisation der lokalen Regierung zufolge dürfen bestimmte Daten von ländlichen Gemeinden oder Städten offen gelegt und jedem zugänglich gemacht werden, und zwar gemäß dem gesetzlich vorgeschriebenen Verfahren und den Gesetzen der ländlichen Gemeinde oder der Stadt. Doch dem gleichen Gesetz zufolge dürfen diejenigen Daten, deren Veröffentlichung gesetzlich verboten ist, nicht offen gelegt werden.

Gemäß §1 des GSPD besteht der Zweck dieses Gesetzes darin, die Grundrechte und -freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten im Einklang mit öffentlichen Interessen zu schützen. Bei der Verarbeitung personenbezogener Daten müssen sich die leitenden Verarbeiter und zugelassenen Verarbeiter personenbezogener Daten von den Prinzipien der Zweckmäßigkeit und der Minimalität (§6 (3) des GSPD) und der Unverletzbarkeit der Privatsphäre leiten lassen.

Die Datenschutz-Inspektion macht geltend, dass der Name einer Person an sich nicht als private personenbezogene Daten zu betrachten ist, aber dass der Name einer Person mit zusätzlichen Informationen auch private personenbezogene Daten darstellen kann. Unter dem Gesichtspunkt des Schutzes der Grundrechte ist es äußerst wichtig, dass personenbezogene Daten nur

in dem Maße verarbeitet werden, wie es für bestimmte, im Voraus festgelegte Zwecke erforderlich ist.

Dem Gesetz über die Information der Öffentlichkeit (GIÖ) zufolge sollte, falls die Gewährung des Zugangs zu Daten zur Offenlegung von Daten führt, die nur für den Dienstgebrauch bestimmt sind, sichergestellt werden, dass nur auf den Teil der Daten oder des Dokuments, für den keine Zugangsbeschränkungen gelten, zugegriffen werden kann (§ 38 (2) des GIÖ).

Die Datenschutzbehörde hat der Stadtregierung Folgendes erklärt: Nach dem Beispiel von Artikel 1 (1) und Erwägung 10 der Präambel der europäischen Datenschutzrichtlinie 95/46/EG legt die Gesetzesvorlage des GSPD den Schwerpunkt auf die genaue Angabe des Zwecks, auf die Notwendigkeit, die Grundrechte und Grundfreiheiten der Bürger zu schützen, und vor allem auf das Recht auf die Unverletzbarkeit der Privatsphäre. Dies besagt jedoch nicht, dass es ein absolutes Recht auf den Schutz personenbezogener Daten und die Unverletzbarkeit der Privatsphäre gibt, sondern unterstreicht lediglich, dass bei der Verarbeitung personenbezogener Daten in Grenzfällen immer der Interpretation gefolgt werden sollte, nach der die Unverletzbarkeit der Privatsphäre Vorrang vor möglichen öffentlichen Interessen hat.

Der Konflikt zwischen dem Schutz der Privatsphäre und der Notwendigkeit, Daten offen zu legen, tritt klar zutage, wenn Daten auf dem Internet offen gelegt werden. Aufgrund des GIÖ und des GSPD ist es verboten, private personenbezogene Daten und sensible personenbezogene Daten offen zu legen (ausgenommen in gesetzlich vorgeschriebenen Fällen). Nicht sensible Daten dürfen erst nach Abwägung der damit verbundenen konkurrierenden Interessen offen gelegt werden: Wenn die Offenlegung gegen die Unverletzbarkeit der Privatsphäre des Datensubjekts verstieße, dürfen nicht sensible Daten der Öffentlichkeit nicht zugänglich gemacht werden. An dieser Stelle ist anzumerken, dass die Beschränkungen nur für den Zugang für die breite Öffentlichkeit gelten.

Auf der Basis der vorangehenden Darlegungen gelangte die Datenschutz-Inspektion zu dem Schluss, dass die Regierung der Stadt Tallinn die Prinzipien der Minimalität

und Zweckmäßigkeit verletzt hat, da die Offenlegung der Daten auf dem Internet angesichts des angegebenen Zweckes nicht verhältnismäßig ist und gegen die Unverletzbarkeit der Privatsphäre verstößt.

Die Datenschutz-Inspektion erließ eine Weisung an die Regierung der Stadt Tallinn, mit der diese verpflichtet wurde, den Namen des Kindes der Privatperson aus dem Register der Rechtsakte zu entfernen. Diese Weisung wurde am 15. Januar 2007 auf der Website der Regierung der Stadt Tallinn veröffentlicht.

Fall 2: Kreditregister

Zwischen der Privatperson H. R. und Hansapank wurde ein so genannter „Ego“-Mietkaufvertrag geschlossen, und so konnte H.R. einen Kredit in Anspruch nehmen. Er verpflichtete sich im Übrigen, Hansapank diesen Kredit vertragsgemäß in monatlichen Raten zurückzuzahlen. H. R. kam seiner vertraglichen Rückzahlungspflicht nicht nach.

Daraufhin schlossen Hansapank und H. R. einen Schuldenvertrag für die Rückzahlung der aus dem „Ego“-Mietkaufvertrag hervorgegangenen Schulden. H. R. versäumte es mehrmals, den im Rahmen des oben erwähnten Vertrags aufgenommenen Schuldenbetrag zurückzuzahlen.

Gemäß Abschnitt 88 (2) (4) des Gesetzes über Kreditinstitutionen, dem „Ego“-Mietkaufvertrag und dem Schuldenvertrag machte Hansapank H. R.s Schulden auf der Website von AS Krediidinfo publik.

2006 zahlte H. R. seine Schulden bei der Hansapank zurück und verlangte die Entfernung seiner Daten aus dem Kreditregister.

Anschließend reichte H. R. bei der Datenschutz-Inspektion eine Beschwerde ein. Die Datenschutz-Inspektion erließ eine Weisung an Hansapank: Laut der Beschwerde des Datensubjekts hatte er keine Erlaubnis zur Veröffentlichung seiner personenbezogenen Daten auf der Website von AS Krediidinfo gegeben. Da Hansapank die Zwecke der Datenverarbeitung weder in dem Vertrag noch, nach Wissen der Datenschutz-Inspektion, in irgendeinem anderen Dokument in Verbindung mit dem Datensubjekt genau angegeben hatte, wird auf

Basis des Prinzips, dass im Falle einer Streitigkeit davon auszugehen ist, dass ein Datensubjekt der Verarbeitung der mit ihm verbundenen personenbezogenen Daten nicht zugestimmt hat (Abschnitt 12 (5) des GSPD), die Veröffentlichung von Daten durch Hansapank ohne Zustimmung des Datensubjekts als Datenverarbeitung betrachtet.

Die Verfügung erlegte der Bank die Verpflichtung auf, die illegale Veröffentlichung von H. R.s personenbezogenen Daten zu beenden. Hansapank kam dieser Verpflichtung nach, schickte aber der Datenschutz-Inspektion ihren Einspruch zu. Die Datenschutz-Inspektion stimmte dem Einspruch nicht zu, und daraufhin brachte Hansapank den Fall vor Gericht.

Das Verwaltungsgericht von Tallinn entschied in seinem Urteil vom 17.04.2007, dass die Weisung in ihrer Schlussfolgerung im Wesentlichen gerechtfertigt und legitim war.

Am 14. Mai 2007 legte Hansapank beim Berufungsgericht von Tallinn Berufung ein.

C. Wichtige spezifische Themen

Zum ersten Mal in diesem Zeitraum formulierte die Datenschutz-Inspektion ihre eigene Initiative in Bezug auf Prioritäten im Bereich von Aufsichtsaktivitäten für das Jahr. Sie wählte sieben Themen aus, die zu diesem Anlass eingehend behandelt wurden, und für jedes dieser Themen veröffentlichte die Inspektion auf ihrer Website, in den Medien oder auf einem den Interessengruppen zugänglichen Sender eine Stellungnahme oder ein Anleitungsdokument. Diese Initiative ging aus der Organisation selbst hervor, und die Datenschutzbehörde hat die Themen ausgewählt, die nach Ansicht der Beamten der Inspektion im Bereich des Schutzes personenbezogener Daten und der Information der Öffentlichkeit am problematischsten oder schwer zu interpretieren sind.

Auf der Grundlage der Themen nahm die Datenschutzbehörde Untersuchungen und, falls erforderlich, Kontrollen vor und erstellte anhand der Ergebnisse Leitlinien/Anleitungsdokumente, die auf der Website der Datenschutz-Inspektion veröffentlicht wurden.

Für den erwähnten Zeitraum wurden im Bereich der Aktivitäten folgende Prioritäten ausgewählt: Übermittlung personenbezogener Daten an Drittländer; Gefahren oder Möglichkeiten im Bereich der Web-Suche; Zulässigkeit der Aufnahme von Telefongesprächen; Offenlegung personenbezogener Daten in den Rechtsdokumenten von Kommunalregierungen; Verarbeitung personenbezogener Daten im Rahmen des Projekts ID-Ticket; Kinder und ihre Rechte bei der Verarbeitung personenbezogener Daten und schließlich die Zusammensetzung personenbezogener Daten bei der Ausstellung von Kundenkarten.

Im Folgenden wird ein kurzer Überblick über zwei interessante Stellungnahmen gegeben:

Verarbeitung personenbezogener Daten im Rahmen des Projekts ID-Ticket

Laut dem Gesetz über Ausweispapiere ist der wichtigste und einzig obligatorische Personalausweis in Estland die ID-Karte. Das von der Datenschutz-Inspektion veröffentlichte Dokument „Verarbeitung personenbezogener Daten im Rahmen des Projekts ID-Ticket“ untersucht die Verwendung der ID-Karte als Nachweis für den Einkauf von Dienstleistungen, zum Beispiel bei der Benutzung des Tallinner ID-Ticket-Systems, wobei der Schwerpunkt auf der Datenverarbeitung in derartigen Systemen liegt.

Die Leitlinien sind hauptsächlich für die Öffentlichkeit und für private Organisationen bestimmt, die Informationssysteme einrichten möchten, die die ID-Karte als Nachweis des Rechtes, eine Dienstleistung oder ein Produkt zu erhalten, benutzen. Die Datenschutz-Inspektion formulierte sieben Empfehlungen auf der Grundlage der Prinzipien des Schutzes personenbezogener Daten.

Die Datenschutz-Inspektion legte dar, dass das System, das auf der in Tallinn verwendeten ID-Karte zum Erwerb des Rechts, öffentliche Verkehrsmittel zu benutzen, beruht, mit den Prinzipien des GSPD übereinstimmt. Die Datenschutz-Inspektion begrüßt Initiativen, die erlauben, den Anwendungsbereich der ID-Karte zu erweitern, und gleichzeitig die Rechte der Bürger auf den Schutz relevanter personenbezogener Daten unter allen Gesichtspunkten berücksichtigen.

Kinder und ihre Rechte bei der Verarbeitung personenbezogener Daten

Die Datenschutz-Inspektion analysierte die Verarbeitung der personenbezogenen Daten von Kindern in verschiedenen alltäglichen Bereichen. Die veröffentlichten Informationen basieren auf wesentlichen internationalen Rechtsinstrumenten über Kinderrechte, auf einheimischen Normen in relevanten Bereichen, auf den Ergebnissen der durchgeführten Kontrollen und auf Verhaltensmustern in verschiedenen Umgebungen, die in der Praxis zum Einsatz kommen. Nach dem Kinderschutzgesetz werden Personen unter 18 Jahren als Kinder betrachtet. Das Dokument enthält eine rechtliche Argumentation über die Verarbeitung der personenbezogenen Daten eines Kindes und das Recht eines Kindes auf die Unverletzbarkeit der Privatsphäre.

Ein separater Abschnitt untersucht Fragen im Zusammenhang mit Web-Kameras an Schulen. Dank der Technologie können Eltern ihre Kinder 24 Stunden am Tag überwachen, und der Bedarf an Videoüberwachung beruht auf Sicherheitserwägungen. Gleichzeitig beeinträchtigt die Videoaufzeichnung jeder Art von Daten die Grundrechte einer Person.

Die Inspektion empfahl in ihrem Dokument, dass die Überwachung der Handlungen der Kinder einerseits gegenüber dem Recht des Kindes auf Privatsphäre verhältnismäßig sein und andererseits auf öffentlichen Interessen wie Sicherheit, Verbrechensvermeidung usw. basieren muss.

Darüber hinaus werden in dem veröffentlichten Dokument die Bereiche untersucht, die die Veröffentlichung der Noten der Kinder und die Veröffentlichung ihrer Daten auf dem Internet betreffen. Ferner wurde dem Zeigen von Kindern in den Medien mehr Aufmerksamkeit gewidmet.

Kurz gesagt hat die Datenschutzbehörde den Standpunkt eingenommen, dass der Schutz der Privatsphäre von Kindern auf zwei Aspekten basieren sollte: Verantwortlichkeit und Bewusstsein.



Finnland

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

Der 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 über personenbezogene Daten (523/1999), das am 1. Juni 1999 in Kraft getreten ist, Gesetzeskraft verliehen. Dieses Gesetz wurde am 1. Dezember 2000 revidiert, als Vorschriften über die Entscheidungsfindung der Kommission und die Festlegung, wie verbindlich diese Entscheidungen in Fragen bezüglich der Übermittlung personenbezogener Daten an Drittländer außerhalb der Europäischen Union gemäß der Datenschutzrichtlinie sind, darin einbezogen wurden.

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.

Mit dem Gesetz über Datenschutz im Bereich elektronische Kommunikation (516/2004), das am 1. September 2004 in Kraft getreten ist, wurde die Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG) umgesetzt. Der Zweck des Gesetzes besteht darin, die Vertraulichkeit und den Schutz der Privatsphäre in der elektronischen Kommunikation zu gewährleisten und die Informationssicherheit in der elektronischen Kommunikation sowie die ausgewogene Entwicklung eines breiten Spektrums elektronischer Kommunikationsdienste zu fördern.

Die Verantwortung für die Durchsetzung des Gesetzes wurde aufgeteilt, so dass das Mandat des Büros des Datenschutzombudsmanns Folgendes beinhaltet: Regulierung der Verarbeitung von Ortungsdaten, Regulierung des Direktmarketings, Regulierung der Katalogisierungsdienste und Regulierung des Informationsrechts der Benutzer.

Diesbezüglich ist anzumerken, dass der Staatsanwalt laut Strafgesetzbuch verpflichtet ist, den Datenschutzombudsmann zu Rate zu ziehen, bevor er im Fall einer Verletzung der Vertraulichkeit in der elektronischen Kommunikation Anklage erhebt.

B. Bedeutende Rechtsprechung

Der Gerichtshof der Europäischen Gemeinschaften befasst sich mit der Veröffentlichung von Daten über Erwerbseinkommen

Eine finnische Firma veröffentlichte jährlich das Erwerbseinkommen von mehr als einer Million Finnen und gab die Daten für die Zwecke eines SMS-Dienstes an eine andere Firma weiter. Diese Informationen wurden dann gegen eine Gebühr als eine SMS-Werbekdienstleistung an die Öffentlichkeit weitergegeben.

Der Datenschutzombudsmann forderte die zuständige Datenschutzbehörde auf, die Veröffentlichung dieser Informationen über Erwerbseinkommen zu verbieten. Die Datenschutzbehörde hat die Kompetenz, die illegale Verarbeitung personenbezogener Daten zu untersagen. Im Gegensatz zur Ansicht des Datenschutzombudsmanns akzeptierten die Datenschutzbehörde und das Verwaltungsgericht, das sich nach der Behörde mit der Angelegenheit befasste, die Interpretation, nach der es sich hier um die Verarbeitung personenbezogener Daten zu journalistischen Zwecken handelt, auf die das Gesetz über personenbezogene Daten im Prinzip nicht angewendet wird. Die Angelegenheit wird derzeit am Obersten Verwaltungsgericht behandelt. Am 8. Februar 2007 forderte das Oberste Verwaltungsgericht beim Gerichtshof der Europäischen Gemeinschaften ein vorläufiges Urteil an. Der Gerichtshof hat daraufhin für den 12. Februar 2008 eine Anhörung zu dieser Angelegenheit angesetzt. Das Oberste Verwaltungsgericht wird seine Entscheidung auf Basis des vorläufigen Urteils treffen.

Das Oberste Verwaltungsgericht weist eine Bank an, das Recht auf vollständigen Zugang umzusetzen

Im Februar 2007 stimmte das Oberste Verwaltungsgericht der Interpretation des finnischen Gesetzes durch den Datenschutzombudsmann zu, nach der sich das Recht auf Zugang auch auf Daten über die

eigenen Kredittransaktionen eines Kunden und die darauf angewendeten Zinssätze erstreckt.

Die Bank hatte geltend gemacht, dass Transaktionsangaben und Zinssatzdaten kein Teil der Kundendatendateien seien, da die Mikrofilme mit diesen Daten getrennt von der Kundendatendatei gespeichert werden. Dem Datenschutzombudsmann zufolge ist diese Ansicht jedoch unrichtig, da der Umfang der personenbezogenen Datendatei durch ihre Verwendung bestimmt wird. Nach dem Gesetz über personenbezogene Daten gehören Daten, die im Rahmen einer gleichen Aufgabe verarbeitet werden, zu der gleichen personenbezogenen Datendatei (logische Datendatei), selbst wenn einzelne Teile der Datendatei (Sub-Register) getrennt gespeichert werden. Da der Zweck der Verwendung der Zinsdaten, wie der anderen Daten über X, im Management einer Kundenbeziehung bestehe, seien alle Daten Teil der gleichen Datendatei. Ob sie nun technisch gesehen zusammen oder getrennt gespeichert werden, wurde als unerheblich betrachtet.

Authentifizierung des Kunden in Schnellkreditfirmen

Die Nachfrage nach Schnellkrediten über Handy oder Internet ist in Finnland dramatisch gestiegen. Schätzungsweise gibt es hier gegenwärtig 50 bis 60 Schnellkreditfirmen. Die unzulängliche Authentifizierung von Personen, die einen Schnellkredit beantragen, hat zu einer Reihe von Fällen geführt, in denen der Kredit im Namen einer anderen Person aufgenommen wurde, ohne dass sich diese dessen bewusst war.

In vielen dieser Schnellkreditfirmen basiert die Authentifizierung des Kreditantragstellers ausschließlich auf der von dem Antragsteller angegebenen Sozialversicherungsnummer und auf den Registrierungsdaten des Telekommunikationsunternehmens. Wenn diese Daten sich als richtig erweisen, geht man davon aus, dass der Antragsteller der- bzw. diejenige ist, für den er/sie sich ausgibt. Unzulängliche Authentifizierung hat zu Identitätsdiebstahl geführt. Die Schwierigkeiten bei der Authentifizierung werden durch die Tatsache erschwert, dass dem Kreditgeber keine spezielle Verpflichtung auferlegt wurde, den Antragsteller eines Schnellkredits zu identifizieren.

Im März 2007 forderte der Datenschutzombudsmann die zuständige Datenschutzbehörde auf, eine Schnellkreditfirma anzuweisen, ihr Authentifizierungsverfahren für Kreditantragsteller zu ändern. Der Datenschutzombudsmann verlangte, dass Kreditgeber ihre Kunden identifizieren, um die Richtigkeit aller verarbeiteten personenbezogenen Daten sicherzustellen. Die Auffassung der Datenschutzbehörde wird eine noch allgemeinere Bedeutung haben, da einer vom Datenschutzombudsmann in Auftrag gegebenen Erhebung zufolge fast alle Unternehmen in diesem Bereich ein ähnliches, auf mangelhafter Identifizierung beruhendes System anwenden. Die Entscheidung könnte sich auch auf andere Geschäftsbereiche auswirken.

C. Spezifische Themen

Gesetz über Kreditinformation

Das neue Gesetz über Kreditinformation ist am 1. November 2007 in Kraft getreten. Das Gesetz bündelt Rechtsvorschriften zu Kreditinformationen über Kunden, Unternehmen und relevantes Unternehmenspersonal. Es beinhaltet Vorschriften über Daten, die in Kreditauskunftsregistern gespeichert werden sollen, und den Speicherzeitraum dieser Daten. Das neue Gesetz legt die Zwecke, für die Kreditinformationen über Verbraucher offen gelegt und verwendet werden dürfen, genauer fest.

Nach dem neuen Gesetz überwacht der Datenschutzombudsmann auch die Verarbeitung von Kreditinformationen über Unternehmen. Von den Anbietern von Kreditinformationen wird erwartet, dass sie vertrauenswürdig sind und bewährte Verfahren im Bereich der Kreditinformation anwenden. Derzeit können Informationen über Zahlungsunterbrechungen, die von Behörden bestätigt und von den Gläubigern gemeldet werden, sowie die Einstufungen der Kreditwürdigkeit von natürlichen Personen und Unternehmen in den Kreditauskunftsregistern gespeichert werden.

Informationen über sämtliche Zahlungsverzüge werden für einen im Voraus festgelegten Zeitraum in den Kreditauskunftsregistern gespeichert. Diese Speicherfristen werden durch das neue Gesetz genauer

festgelegt und in manchen Fällen verkürzt. Während einerseits die Zahlung der Schuld die Speicherfrist verkürzen kann, kann diese Frist andererseits auch verlängert werden, wenn die natürliche Person oder das Unternehmen erneut in Zahlungsverzug gerät.

Das neue Gesetz wird außerdem Unternehmen gestatten, ihre Kreditinformationen zu prüfen und Irrtümer zu berichtigen. Derartige Rechte wurden zuvor nur natürlichen Personen eingeräumt. Die Anbieter von Kreditinformationen müssen als angemessenen Ausgleich auch Verbrauchern Kreditinformationen erteilen. Auf diese Weise soll Verbrauchern ermöglicht werden, die Zuverlässigkeit ihrer Vertragspartei besser zu beurteilen.

Gesetz über die elektronische Verarbeitung von Sozialhilfe- und Patientendaten

Das Gesetz über die elektronische Verarbeitung von Sozialhilfe- und Patientendaten trat am 1. Juli 2007 in Kraft. Derzeit wird in Finnland eine landesweite Patientendatenbank aufgebaut, die vom gesamten Gesundheitsversorgungssektor genutzt werden soll. Die Datenbank wird vom finnischen Sozialversicherungsinstitut errichtet und soll zwischen 2008 und 2011 schrittweise in Betrieb genommen werden.

Die Datenbank umfasst Dienste für die Speicherung, Archivierung und Übermittlung von Patientenunterlagen und Rezepten. Die Reform soll die Zusammenarbeit zwischen verschiedenen Parteien im Bereich der Sozialhilfe und Gesundheitsversorgung verbessern und die elektronische Übermittlung von Daten von einer Partei zur anderen ermöglichen, wenn der Patient dem zustimmt.

In erster Linie geht es darum, die Sicherheit bei der Verarbeitung von Sozialhilfe- und Patientendaten und der Produktion von Gesundheitsdiensten auf eine Weise zu verbessern, die für Patienten sowohl sicher als auch effektiv ist. Darüber hinaus bietet das neue Gesetz Patienten auch die Möglichkeit, auf ihre eigenen Daten zuzugreifen und ihren Gebrauch betreffende Daten zu protokollieren, beispielsweise indem sie sie online ansehen.

Alle öffentlichen Anbieter von Gesundheitsversorgung sollen beginnen, die Datensystemdienste zu nutzen. Private Anbieter von Gesundheitsversorgung sind verpflichtet, sich dem System anzuschließen, wenn die Langzeitspeicherung ihrer Patientendaten elektronisch erfolgt.

Gesetz über elektronische Rezepte

Das neue Gesetz über elektronische Rezepte trat am 1. April 2007 in Kraft. Die neue Rechtsvorschrift legt die Anforderungen für ein elektronisches Rezeptsystem und seine Umsetzung fest. Nach dem Gesetz können Rezepte elektronisch erstellt und über Datennetze direkt an das Landes-Rezeptzentrum weitergeleitet werden, das dem Apotheker dann die Informationen zukommen lässt, die er braucht, um die verschriebene Arznei abzugeben.

Die Ärzte müssen ihre Patienten über die Verwendung elektronischer Rezepte unterrichten und ihnen schriftliche Anweisungen zu dem Arzneimittel und seiner Verwendung geben. Der Patient hat das Recht, das elektronische Rezept abzulehnen. In diesem Fall erhält er bzw. sie ein herkömmliches, auf Papier geschriebenes Rezept. Da alle elektronischen Rezepte in dem Rezeptzentrum gespeichert werden, können die Patienten jederzeit die Gültigkeit ihrer Rezepte und die Menge der noch nicht abgegebenen Arznei überprüfen, ohne die ursprünglichen Rezepte aufbewahren zu müssen. Für die Führung des Rezeptzentrums und der Rezeptarchive wird das finnische Sozialversicherungsinstitut zuständig sein. Die Rezepte werden 30 Monate lang im Rezeptzentrum aufbewahrt. Danach sollen sie an das Rezeptarchiv übermittelt werden.

Wenn alle Rezepte für einen Patienten elektronisch erstellt wurden, kann ein Arzt, Zahnarzt, Apotheker oder qualifizierter Chemiker auf der Grundlage der im Rezeptzentrum befindlichen Daten (und mit Zustimmung des Patienten) die Medikamente, die einem Patienten insgesamt verschrieben wurden, und potenzielle Medikamenteninteraktionen prüfen. Die Patienten haben auch das Recht, Informationen darüber zu erhalten, wer die sie betreffenden Daten im Rezeptzentrum oder Rezeptarchiv verarbeitet oder eingesehen hat.

Empfehlungen der Arbeitsgruppe über Biobanken

Laut dem am 12. Oktober 2007 veröffentlichten Bericht einer vom Ministerium für Soziales und Gesundheit eingesetzten Arbeitsgruppe macht der umfassendere Gebrauch sowohl bereits vorhandener als auch künftiger Sammlungen menschlicher Gewebeproben zu medizinischen Zwecken die Überwachung der Tätigkeiten, bessere Kommunikation, einheitlichere Verfahren und Qualitätskriterien erforderlich.

Die Arbeitsgruppe empfahl, in Finnland Biobanken zu errichten (dezentralisiertes System). Die Hauptaufgabe einer Biobank würde darin bestehen, menschliche biologische Proben und daraus abgeleitete oder sie betreffende Informationen für künftige Untersuchungen zu erfassen, zu verwalten und aufzubewahren. Eine Biobank kann entweder selbst Proben erfassen, oder es können zu Forschungszwecken angelegte Probensammlungen von anderswo in die Biobank aufgenommen werden.

Nach dem Vorschlag der Arbeitsgruppe würde ein Probenspender um seine Zustimmung zur Übermittlung seiner bzw. ihrer Proben an die Biobank gebeten werden. Die Zustimmung würde darauf basieren, dass dem Spender der allgemeine Zweck der Biobank bekannt ist. Probenspender haben das Recht, zu wissen, was mit ihren Proben geschehen soll, und die Möglichkeit, auf ihre Verwendung Einfluss zu nehmen, ist durch die allgemeine Meldepflicht, die Transparenz der Tätigkeiten und die Überwachung der Handlungen der Biobank durch die Behörden sichergestellt. Die Übermittlung bereits vorhandener, zum Zweck der Diagnose und Behandlung von Krankheiten entnommener Diagnose- und Forschungsproben an eine Biobank ist entweder mit Zustimmung des Probenspenders möglich oder, wenn die Erneuerung der Zustimmung unangemessen schwierig ist, mit einer Genehmigung der nationalen Behörde für medizinisch-rechtliche Angelegenheiten.

Daten über Biobanken werden in einem Biobank-Register gesammelt, das zusammen mit den spezifischen Biobank-Registern der Probensammlungen ein Datensystem bildet, zu dem sowohl Forscher als auch die breite Öffentlichkeit Zugang haben.



Frankreich

A. Gesetzgebung

1. Verordnung vom 25. März 2007

Frankreich hat die europäische Richtlinie vom 24. Oktober 1995 durch das Gesetz vom 6. August 2004 über die Abänderung des Gesetzes vom 6. Januar 1978 umgesetzt. Die erste Durchführungsverordnung zu diesem neuen Gesetz wurde am 20. Oktober 2005 verabschiedet; sie enthielt insbesondere Bestimmungen bezüglich der Ernennung von Ansprechpartnern zum „Datenschutz“ innerhalb von Unternehmen und Verwaltungen. Durch eine am 25. März 2007 verabschiedete Änderung dieser Verordnung wurden insbesondere verfahrenstechnische Klarstellungen hinzugefügt.

- Information der Personen im Falle der Übermittlung ihrer Daten an Länder außerhalb der Europäischen Union

Die Verordnung vom 25. März 2007 sieht vor, dass Personen, deren Daten an Länder außerhalb der Europäischen Union übermittelt werden, nicht nur über diese Übermittlung informiert werden müssen, sondern genauer gesagt über das Land, in dem der Empfänger seinen Sitz hat, den Zweck der Übermittlung, die Kategorie der personenbezogenen Daten, die Gegenstand der Übermittlung sind, und über das Schutzniveau, das von dem außerhalb der Europäischen Union befindlichen Drittland geboten wird. Ferner sieht die Verordnung vor, dass die Übermittlung, falls sie im Anschluss an die Erhebung personenbezogener Daten ins Auge gefasst wird, erst nach einer Frist von fünfzehn Tagen nach Erhalt oben stehender Informationen durch die betroffene Person erfolgen darf.

- Zugangsrecht-Verfahren

In der Durchführungsverordnung vom 25. März 2007 werden die Bedingungen der Ausübung des Zugangsrechts genau dargelegt. Die Beantragung eines Zugangsrechts kann per Post oder an Ort und Stelle eingereicht werden, wobei die betreffende Person sich gegenüber dem für die Verarbeitung Verantwortlichen gültig ausweisen muss. Wenn der Antrag an Ort und Stelle gestellt wird und es nicht möglich

ist, ihm umgehend nachzukommen, muss der Antrag stellenden Person eine datierte und unterschriebene Empfangsbestätigung ausgehändigt werden. Nach der Verordnung ist der für die Verarbeitung Verantwortliche verpflichtet, dem Antrag der betreffenden Person binnen zwei Monaten nach seinem Empfang nachzukommen. Nach Ablauf dieser Zweimonatsfrist wird das Ausbleiben einer Antwort des für die Verarbeitung Verantwortlichen als Weigerung betrachtet.

2. Stellungnahme zum Verordnungsentwurf zur Anwendung von Artikel 6 des Gesetzes vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft, mit dem die Richtlinie 2000/31/EG in französisches Recht umgesetzt wird

Artikel 6 des Gesetzes für das Vertrauen in die digitale Wirtschaft (LCEN) schreibt die Aufbewahrung der Daten vor, anhand derer sich die Personen, die an der Schaffung von Online-Inhalten mitgewirkt haben, identifizieren lassen.

Dieser Artikel verpflichtet Hosting-Anbieter und Internetzugang-Anbieter zur Aufbewahrung der Daten, anhand derer sich die Personen, die an der Schaffung von Online-Inhalten (Blogs, persönliche Seiten, Anzeigen auf einer Auktionsseite usw.) mitgewirkt haben, identifizieren lassen, zwecks eventueller Übermittlung an die Justizbehörden und an die mit dem Kampf gegen den Terrorismus betrauten Dienste.

Die CNIL (Nationale Datenschutzbehörde Frankreichs) hat kürzlich einen Verordnungsentwurf geprüft, in dem die betroffenen Datenkategorien und ihre Aufbewahrungsdauer festgelegt werden. Diese Verordnung, begleitet von der Stellungnahme der CNIL, dürfte in Kürze veröffentlicht werden.

B. Rechtsprechung

1. Vielfalt

Nach der Veröffentlichung ihrer ersten Empfehlungen zu dem Thema im Juli 2005 hat die CNIL ihre Reflexion vertieft und mehr als sechzig Anhörungen vorgenommen: Wissenschaftler, Statistiker, Gewerkschaftsorganisationen, Vertreter der großen Religionen, Vereinigungen, qualifizierte Persönlichkeiten, Unternehmensleiter ... Diese Anhörungen haben gezeigt, dass

es sehr vielfältige und teils abweichende Meinungen zu diesem Thema gibt und es schwierig ist, in diesem Bereich einen Konsens zu erreichen.

Dennoch gelangt die CNIL zu folgender Feststellung: Frankreich muss seinen Statistikapparat verbessern, und von nun an müssen Lösungen gefunden werden, um das Wissen über unsere Gesellschaft voranzubringen, um auf diese Weise Diskriminierungen besser bekämpfen zu können.

Zu diesem Zweck hat die CNIL im Mai 2007 ihre zehn Empfehlungen veröffentlicht, die für ihren Pragmatismus, ihre Ausgewogenheit und ihren Ehrgeiz gelobt wurden. Im Folgenden die Kernelemente dieser Empfehlungen:

- Es ist unerlässlich, Wissenschaftlern einen einfacheren Zugang zu Personaldateien, administrativen Dateien und öffentlichen Statistikbanken zu ermöglichen, dies selbstverständlich unter Beachtung des Datenschutzes.
- Um die Realität der erlebten Diskriminierung zu messen, ist es ferner notwendig, Erhebungen durch Fragebögen nahe an den betroffenen Personen zu entwickeln. Da sie fakultativ sind, auf Selbstauskunft beruhen und die Antworten vertraulich sind, muss es möglich sein, Fragen über die Staatsangehörigkeit und den Geburtsort der Personen, aber auch ihrer Eltern zu stellen. Es ist auch wichtig, dass die Personen, die sich diskriminiert fühlen, die Kriterien – Aussehen, Sprache, Name usw. – angeben, auf denen diese Diskriminierung ihrer Meinung nach beruht.
- Im Übrigen kann die Analyse von Vornamen und Nachnamen unter bestimmten Bedingungen – das heißt, wenn sie nicht zu einer Einstufung in „ethno-rassische“ Kategorien führt – nützlich sein, um eventuelle diskriminierende Praktiken zu erkennen.
- Diesbezüglich steht die CNIL der Schaffung eines „ethno-rassischen“ Referenzsystems sehr zurückhaltend gegenüber. Die große Mehrheit der angehörten Personen lehnt eine solche Nomenklatur entschieden ab. Gefahr der Verstärkung von Stereotypen, von Stigmatisierung, ungewisse Klassifizierung, nicht wissenschaftlich, reduzierend, ungenau ... all diese Gründe erklären die derzeitige Zurückhaltung und rechtfertigen eine sehr vorsichtige Haltung gegenüber diesem Thema. Die CNIL war insbesondere der Ansicht, dass

die Grundsatzentscheidung, eine solche Nomenklatur zu schaffen, falls sie benutzt wird, unbedingt – und insbesondere für öffentliche Statistiken und Volkszählungen – vom Gesetzgeber getroffen werden muss, und zwar unter der Aufsicht des Verfassungsrates.

- Schließlich ist es notwendig, das Datenschutzgesetz zu ändern, um einen besseren Schutz der Personen und ihrer sensiblen Daten zu gewährleisten, indem der wissenschaftliche Charakter der Untersuchungen garantiert und die Kontrolle der CNIL über diese Untersuchungsdateien, für die die Zustimmung der Personen allein nicht ausreichen würde, verstärkt wird.

Im Anschluss an die Empfehlungen der CNIL haben Michèle Tabarot und Sébastien Huyghe, beide Abgeordnete und Mitglieder der CNIL, eine Änderung zum Gesetzesentwurf über Einwanderungskontrolle, Eingliederung und Asyl vorgelegt, nach der Datenverarbeitungen, bei denen die rassische oder ethnische Herkunft der Personen für die Zwecke von Untersuchungen, die darauf abzielen, *„die Vielfalt der Herkunftsländer der Personen, die Diskriminierung und die Eingliederung zu messen“*, direkt oder indirekt erkennbar wird, der CNIL zur Genehmigung vorgelegt werden müssten. Um sich der wissenschaftlichen Qualität dieser Untersuchungen zu vergewissern, war vorgesehen, dass die CNIL einen per Verordnung eingesetzten Ausschuss anrufen kann. Um keine neue Struktur zu schaffen, war vorgesehen, auf den wissenschaftlichen Rat des Konzertierungsausschusses für Daten in Human- und Sozialwissenschaften zurückzugreifen, der in den Ministerien für Wirtschaft, Beschäftigung, nationale Bildung und Forschung eingerichtet wurde.

Gegen diese Bestimmung wurde vor dem Verfassungsrat Einspruch erhoben.

Mit seiner Entscheidung vom 15. November 2007 hat sie der Rat für verfassungswidrig erklärt, da er die Ansicht vertrat, dass zwischen dieser Bestimmung und einem Gesetz über die Einreise und den Aufenthalt von Ausländern in Frankreich kein Zusammenhang besteht. In der Sache selbst hat der Rat folgendermaßen geurteilt: *„Auch wenn die zur Durchführung von Untersuchungen zur Messung der Vielfalt der Herkunftsländer der Personen, der Diskriminierung und der Eingliederung notwendigen*

Verarbeitungen objektive Daten betreffen können, dürfen sie nicht, ohne das in Artikel 1 der Verfassung festgeschriebene Prinzip zu verkennen, auf der ethnischen Herkunft oder der Rasse beruhen [...]“.

Diese Entscheidung lässt die Frage offen, welche Arten von Untersuchungen heute im Bereich der Messung der Vielfalt, der Diskriminierung und der Eingliederung vorgenommen werden dürfen. Die aktuellen Kommentare des Verfassungsrates in Bezug auf das Urteil, das er am 15. November 2007 gefällt hat, bringen Klarstellungen und legen nahe, dass er den Rückgriff auf ein ethno-rassistisches Referenzsystem ausschließt, Untersuchungen über das Gefühl der ethnischen Zugehörigkeit jedoch gestattet.

2. Verfolgung von Internet-Nutzern

Im Oktober 2005 hat die CNIL den Einsatz von vier Vorrichtungen zur Überwachung der „peer to peer“-Netze abgelehnt, den die für die Wahrnehmung und Zuteilung der Rechte im Musiksektor zuständigen Gesellschaften (SACEM, SDRM, SPPF und SCPP) vorgeschlagen hatten. Die vier Gesellschaften haben die Entscheidungen der CNIL vor dem Obersten Verwaltungsgericht angefochten, das sie am 23. Mai 2007 teilweise aufgehoben hat. Tatsächlich war das Gericht der Auffassung, dass die CNIL einen „Ermessensfehler“ begangen hat, als sie Verarbeitungen, deren Zweck darin besteht, die illegale Bereitstellung musikalischer Werke in den Netzwerken aufzuspüren und festzustellen, für unverhältnismäßig erklärte. Hingegen hat das Oberste Verwaltungsgericht die Analyse der CNIL bezüglich des Versands gezielter pädagogischer Botschaften an die Internet-Nutzer berücksichtigt. Es hat geurteilt, dass diese Versendungen illegal sind, da es sich hier nicht um einen Fall handelt, in dem die Internetzugang-Anbieter die Anschlussdaten der Internet-Nutzer aufbewahren dürfen.

Im Anschluss an diese Entscheidung hat die CNIL mit den betroffenen Wahrnehmungs- und Zuteilungsgesellschaften Kontakt aufgenommen, um ihre weiteren Absichten zu erfahren. Drei von ihnen (SACEM, SDRM, SCPP) haben den ungültigen pädagogischen Teil aus ihren Anträgen entfernen und sie dann erneut gestellt. So hat die CNIL, verpflichtet, aus der Entscheidung des Obersten Verwaltungsgerichts Konsequenzen

zu ziehen, diesen drei Gesellschaften im November 2007 gestattet, Verarbeitungen zur Aufspürung und Feststellung von Verstößen im Internet vorzunehmen. Die letzte der betroffenen Gesellschaften (die SPPF) hat ihren Antrag im Laufe des Monats Dezember 2007 erneuert. Der Einsatz dieser mit den drei anderen identischen Vorrichtung müsste Anfang 2008 genehmigt werden.

Parallel dazu hat das Pariser Berufungsgericht in zwei Entscheidungen von April und Mai 2007 geurteilt, dass die anlässlich der Aufspürung und Feststellung von Betrugshandlungen im Internet gesammelten IP-Adressen es nicht zulassen, nicht einmal indirekt, natürliche Personen zu identifizieren, und sie folglich keine personenbezogenen Daten sind. Besorgt über die Auswirkungen einer solchen Analyse auf den Schutz der Privatsphäre im Internet, hat sich die CNIL an das Justizministerium und den Staatsanwalt beim Kassationshof gewandt, um im Interesse des Gesetzes ein Rechtsmittel gegen diese beiden Entscheidungen einzulegen. Die CNIL hat darauf hingewiesen, dass die Datenschutzbehörden der Mitgliedstaaten der Europäischen Union in einer Stellungnahme vom 20. Juni 2007 daran erinnert haben, dass es sich bei der IP-Adresse durchaus um personenbezogene Daten handelt.

Im Übrigen hat die CNIL in den Räumlichkeiten von Dienstleistungsgesellschaften, die mit der Überwachung von „peer to peer“-Netzen befasst sind, mehrere Kontrollmissionen durchgeführt. Die Untersuchung der bei diesen Kontrollmissionen gesammelten Elemente müsste im ersten Quartal 2008 abgeschlossen sein.

In diesem Stadium ist ferner zu betonen, dass der Minister für Kultur und Kommunikation eine Mission ins Leben gerufen hat, die speziell damit beauftragt ist, *„Lösungen zur Bekämpfung von widerrechtlichem Herunterladen zu finden und legale Angebote von Werken zu entwickeln“*. Nach Ausführung dieser Mission hat Denis Olivennes im November 2007 mehrere Empfehlungen vorgelegt. Ihre Berücksichtigung durch die Regierung müsste zu legislativen und technischen Änderungen führen, zu denen die CNIL sich wird äußern müssen.

C. Arbeitsweise und Tätigkeiten der CNIL

1. Annahme von Beschlüssen

Im Jahr 2007 hat die CNIL im Rahmen von 25 Plenarsitzungen, 12 kleineren Gremien und 3 allgemeinen Ausschüssen 40 Mal getagt. Auf diesen Sitzungen wurden insgesamt 393 Beschlüsse angenommen (+ 30 % gegenüber 2006, + 600 % gegenüber 2003).

Diese Beschlüsse betreffen Stellungnahmen und Genehmigungen, die die CNIL im Rahmen ihrer verschiedenen Missionen – Beratung oder Gutachten a), Sanktionen b), Vereinfachung der vorausgehenden Formalitäten c) und deklaratorische Formalitäten (Genehmigung oder Ablehnung einer Genehmigung, Stellungnahme) d) – erteilt hat.

a) Beratung und Gutachten

2007 hat die CNIL 6 Stellungnahmen zu Gesetzes- oder Verordnungsentwürfen abgegeben, darunter eine Stellungnahme zu dem Entwurf einer Verordnung zur Anwendung von Artikel 6 des Gesetzes vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft, und betreffend die Aufbewahrung von Daten, welche die Identifizierung jeder natürlichen oder juristischen Person ermöglichen, die an der Schaffung eines Online-Inhalts mitgewirkt hat.

b) Vereinfachung der vorausgehenden Formalitäten

Die CNIL hat die in diesem Sinne durchgeführten Arbeiten fortgesetzt und Maßnahmen zur Vereinfachung der vorausgehenden Formalitäten, die bei ihren Diensten zu erledigen sind, verabschiedet. So hat sie vier einmalige Genehmigungen verabschiedet (darunter eine Genehmigung in Bezug auf den Einsatz automatisierter Verarbeitungen personenbezogener Daten im Zusammenhang mit der Verwaltung von Verstößen bei den Ordnungsbehörden der Bodentransportdienste und eine Genehmigungsänderung in Bezug auf Verarbeitungen personenbezogener Daten durch Finanzinstitutionen im Rahmen der Bekämpfung von Geldwäsche und Terrorismusfinanzierung) und zwei Stellungnahmen zu einer einmaligen Rechtsverordnung abgegeben.

Diese Vereinfachungen sind systematisch mit einer sehr genauen Rahmenregelung verknüpft. Sie gelten

nur, wenn die für die Verarbeitung Verantwortlichen sämtliche von der CNIL zu diesem Zweck aufgestellten Bedingungen einhalten.

c) Deklaratorische Formalitäten

Die CNIL hat 2007

- 214 Genehmigungen;
- 26 Genehmigungsverweigerungen und
- 22 Stellungnahmen zu sensiblen oder riskanten Verarbeitungen verabschiedet.

d) Sanktionen

Seit dem Gesetz vom 6. August 2004, mit dem das Datenschutzgesetz von 1978 geändert wurde, verfügt die CNIL über Sanktionsbefugnisse, die ihr erlauben, Geldstrafen in Höhe von 150 000 Euro (300 000 Euro im Wiederholungsfall) zu verhängen, wobei dieser Betrag 5 % des Umsatzes nicht überschreiten darf.

Insgesamt hat die CNIL 2007

- 9 Geldstrafen – zwischen 5 000 und 50 000 Euro – verhängt und
- 5 Verwarnungen und
- 101 Mahnungen ausgesprochen.

2. Verweise

Im Jahr 2007 war die CNIL im Übrigen mit 7 115 Fällen befasst (4 455 Beschwerden und 2 660 Anträge auf indirektes Zugangsrecht zu den Dateien der Polizei und der Gendarmerie). Am stärksten waren die folgenden Sektoren betroffen: *Bank-Kredit, kommerzielle Kundenwerbung, Arbeit, Telekommunikation*.

Diese Zahl ist gegenüber 2006 um 20 % gestiegen. Die CNIL erhält heute doppelt so viele Beschwerden wie vor zehn Jahren!

3. Bedeutsame Entwicklungen 2007

Schaffung eines Rahmens für biometrische Verfahren

Im Jahr 2007 hat die CNIL erstmals ein Stimmernennungssystem geprüft. Es handelte sich um eine Vorrichtung, deren Zweck darin bestand, die Verwaltung und Reinitialisierung der Passwörter, die benutzt werden, um auf das Informationssystem der Firma Michelin zuzugreifen, zu sichern und zu vereinfachen. Dieses Verfahren ermöglicht die automatische Erzeugung und Reinitialisierung der Passwörter. Bei dieser

Gelegenheit hat sich die CNIL insbesondere vergewissert, dass die Arbeitnehmer ausreichend informiert waren und alle Maßnahmen ergriffen wurden, um die Sicherheit der Daten zu gewährleisten und Risiken der Identitätsaneignung vorzubeugen.

Ferner hat die CNIL zum ersten Mal fünf Vorrichtungen geprüft, die auf der Erkennung des Venengeflechts der Finger basieren und dazu bestimmt sind, den Zugang zu Räumlichkeiten oder Informationssystemen zu kontrollieren. Im Anschluss an eine umfassende technische Begutachtung dieser Technologie ist die CNIL zu der Auffassung gelangt, dass das Venengeflecht nach dem aktuellen Stand der Technik ein biometrisches Merkmal ist, das keine Spuren hinterlässt und dessen Registrierung in einer Datenbank keine besonderen Risiken im Hinblick auf den Datenschutz birgt.

1997 hat sich die CNIL erstmals zu einer Vorrichtung auf Basis der Erkennung von Fingerabdrücken geäußert. Zehn Jahre später hielt sie es für notwendig, ihre Position genauer darzulegen. Sie wollte klarstellen, auf welche Kriterien sie sich im Wesentlichen stützt, um den Einsatz von Vorrichtungen, die auf der Erkennung von Fingerabdrücken (gespeichert in einem Lese-Vergleichs-Terminal oder einem Server) basieren, zu genehmigen oder abzulehnen.

Dieses Analyseraster beruht auf folgenden Feststellungen:

- der Fingerabdruck ist ein biologisches Merkmal mit „Spuren“. Jeder Mensch hinterlässt im Alltag zahlreiche Spuren seiner Fingerabdrücke, zum Beispiel auf einem Glas, einem Türgriff usw., die mehr oder weniger leicht zu verwerten sind;
- diese „Spuren“ können ohne Wissen der betroffenen Personen erlangt und insbesondere genutzt werden, um ihre Identität zu usurpieren (beispielsweise den erlangten Fingerabdruck benutzen, um eine Vorrichtung zur Erkennung von Fingerabdrücken zu täuschen).

Diese Besonderheiten und die damit verbundenen Risiken haben die CNIL bewogen, die Vorrichtungen je nach der Art der Speicherung der Fingerabdrücke zu unterscheiden:

- Speicherung auf einem Einzelträger (wie etwa Chipkarte oder USB-Schlüssel): Das Risiko ist begrenzt, da die Person die Kontrolle über ihre biometrischen Daten hat, die nicht benutzt werden können, um sie ohne ihr Wissen zu identifizieren.
- Speicherung in einem Lese-Vergleichs-Terminal oder auf einem Server: Das Risiko ist hoch, da die Person die Kontrolle über ihre Daten verliert, die im Besitz eines Dritten sind. Wird unbefugt in das System eingedrungen, kann man auf sämtliche Fingerabdrücke zugreifen.

Daher gestattet die Kommission den Einsatz von Vorrichtungen, die auf der Erkennung von Fingerabdrücken beruhen, verbunden mit der Speicherung in einer Datenbank, nur dann, wenn sie durch wesentliche Sicherheitserfordernisse gerechtfertigt sind und vier Anforderungen erfüllen:

- die Finalität der Vorrichtung muss auf die Zugangskontrolle einer begrenzten Zahl von Personen in einem genau festgelegten Bereich beschränkt bleiben, und es muss um Wichtigeres gehen als allein um das Interesse der jeweiligen Organisation, etwa die physische Unversehrtheit der Personen, der Güter und Einrichtungen oder auch die Unversehrtheit gewisser Informationen;
- Verhältnismäßigkeit: Es ist wichtig, zu wissen, ob das vorgeschlagene System dem festgelegten Zweck im Hinblick auf die Risiken, die es in puncto Schutz personenbezogener Daten birgt, gut oder so gut wie möglich entspricht;
- Sicherheit: Die Vorrichtung muss eine zuverlässige Erkennung und/oder Identifizierung der Personen ermöglichen und gleichzeitig alle Sicherheitsgarantien bieten, um eine unbefugte Preisgabe der Daten zu verhindern;
- Information der betroffenen Personen: Sie muss unter Beachtung des „Datenschutzes“ und gegebenenfalls des Arbeitsgesetzes erfolgen.

SWIFT-Affäre: Ausweg aus der Krise

Die amerikanische Presse hat im Juni 2006 die Existenz eines Programms zur Überwachung internationaler Banktransaktionen enthüllt, das die CIA kurz nach den Attentaten vom 11. September 2001 eingerichtet hat. Diesen Enthüllungen zufolge haben die CIA und das US-Finanzministerium seit Jahren Zugriff auf Millionen

von Daten, die von SWIFT, dem größten internationalen Nachrichtendienst im Banksektor (siehe Jahresbericht 2006), befördert werden.

Dieser Zugang, der im Namen des Kampfes gegen die Finanzierung des Terrorismus eingerichtet wurde, macht es möglich, nicht nur die Finanztransfers in die Vereinigten Staaten zu überwachen, sondern auch alle anderen Arten von Transaktionen, die von SWIFT durchgeführt werden, auch innerhalb der Europäischen Union. So werden der Betrag der Transaktion, die Währung, das Wertstellungsdatum, der Name des Empfängers, der Kunde, der die Finanztransaktion in Auftrag gegeben hat, sowie das Finanzinstitut dieses Kunden mitgeteilt. Offiziell zielt dieses Programm darauf ab, Personen zu identifizieren, die vermutlich mit Aktivitäten zur Finanzierung des Terrorismus zu tun haben. Befürchtungen, es könne zu anderen, weniger mit Sicherheit und mehr mit Wirtschaft zusammenhängenden Zielen benutzt werden, lassen sich jedoch nicht von der Hand weisen.

Die Koordinierungsgruppe der europäischen CNIL (Art. 29 Gruppe oder G29) hat in ihrer Stellungnahme vom November 2006 erklärt, die Gesellschaft SWIFT habe gegen die europäischen Datenschutzbestimmungen verstoßen, insbesondere indem sie bei der Einrichtung des Programms zur Überwachung der Bank- und Finanzdaten durch die amerikanischen Behörden behilflich war. Die Gruppe war ferner der Ansicht, dass die Finanzeinrichtungen in dieser Angelegenheit mitverantwortlich waren.

Ein Jahr später kann man von einem „Ausweg aus der Krise“ sprechen. Die G29 hat am 11. Oktober 2007 eine Pressemitteilung veröffentlicht, in der sie die erheblichen Fortschritte begrüßte, die SWIFT bei ihren Bemühungen, den Datenschutzprinzipien zu entsprechen, erreicht hat.

Abschluss der Verhandlungen zwischen Europa und den Vereinigten Staaten

Im Frühjahr 2007 haben die Europäische Kommission und der Rat mit der amerikanischen Regierung eine Reihe von Garantien ausgehandelt, um die Bestimmungen für die Nutzung der in der SWIFT-Datenbank in den USA gespeicherten Daten durch die amerikanischen

Behörden festzulegen. Diese Garantien betreffen die Beschränkung der Nutzung auf den Kampf gegen den Terrorismus, die Beachtung des Prinzips der Notwendigkeit, Aufbewahrungszeiträume von 5 Jahren und die Ernennung einer „renommierten europäischen Persönlichkeit“ (Jean-Louis Bruguière), die befugt ist, das korrekte Funktionieren des Überwachungsprogramms zu überprüfen. Diese politische Vereinbarung war Gegenstand einer Korrespondenz, die von der Europäischen Kommission veröffentlicht wurde.

Eine völlig neu strukturierte technische Architektur

Die gegenwärtige Architektur von SWIFT beruht auf dem Prinzip einer systematischen Kopie aller Nachrichten in den beiden Betriebszentren (das eine in den Niederlanden, das andere in den Vereinigten Staaten). Diese Nachrichten werden also, ungeachtet ihrer Herkunft und ihres Bestimmungsortes, derzeit 148 Tage lang im amerikanischen Betriebszentrum gespeichert.

Ende des Jahres 2009 wird diese Architektur jedoch durch die Einrichtung eines neuen Betriebszentrums in der Schweiz von Grund auf verändert. Die von Kunden europäischer Banken gesendeten Nachrichten werden systematisch in den beiden europäischen Zentren (Schweiz und Niederlande) kopiert werden und nicht mehr durch den amerikanischen Server laufen. Folglich werden insbesondere die Nachrichten, die Transfers innerhalb der Europäischen Union betreffen, von amerikanischer Seite nicht mehr überwacht. Die Nachrichten, die aus den Vereinigten Staaten stammen oder an sie gerichtet sind, werden systematisch im amerikanischen Betriebszentrum gespeichert.

Discovery

Die CNIL stellt fest, dass die Forderungen nach Weitergabe der personenbezogenen Daten, die sich, unter anderem, im Besitz der französischen Tochtergesellschaften amerikanischer Unternehmen befinden, die Gegenstand von „Discovery“-Verfahren vor amerikanischen Zivilgerichten oder von „pretrial discovery“ sind, in der letzten Zeit zugenommen haben. Es ist gang und gäbe geworden, dass die Unternehmen, die diesen Forderungen unterworfen sind, oder ihre ausländischen Töchter verpflichtet werden, die Kopien von Festplatten oder der elektronischen Post

bestimmter Mitarbeiter oder sogar ihres gesamten Personals weiterzugeben.

Im Übrigen können, in einem anderen rechtlichen Rahmen, bestimmte ausländische Behörden wie etwa die *Securities and Exchange Commission* (SEC) oder die *Federal Trade Commission* (FTC) kraft der ihnen übertragenen Ermittlungsbefugnisse von ausländischen Unternehmen ebenfalls die Vorlage von Dokumenten oder Schriftstücken verlangen. Diese Anordnungen können französische Unternehmen betreffen, je nachdem, ob es sich um Tochtergesellschaften amerikanischer Unternehmen handelt, die an der amerikanischen Börse notiert sind, oder ob sie direkt auf dem amerikanischen Markt tätig sind.

Hier stellen sich zahlreiche Fragen, vor allem in Bezug auf das Datenschutzgesetz.

Diese Ersuchen um Weitergabe können gegen die Datenschutzbestimmungen verstoßen, insbesondere im Hinblick auf die Information und die Zustimmung der Personen, die Verhältnismäßigkeit der vorgenommenen Verarbeitung und die Bedingungen der Übermittlung von Daten an Länder außerhalb der Europäischen Union.

Derartige Situationen werfen im Übrigen Probleme auf, die mit anderen Bereichen als „Datenschutz“ zusammenhängen, vor allem in Bezug auf internationale Rechtshilfe und den Schutz nationaler Wirtschaftsinteressen oder sogar nationaler Hoheitsrechte.

Aus Besorgnis über die aus diesen Pflichten erwachsenden Konsequenzen und die Weitergabe solcher Mengen von Daten im Hinblick auf die einschlägigen französischen und europäischen Vorschriften, haben mehrere französische oder ausländische, in Frankreich niedergelassene Unternehmen und Fachanwälte die CNIL über die Entwicklung dieses Phänomens unterrichtet.

Besorgnis erregend ist des Weiteren, dass diese Unternehmen auch Zweifel bezüglich des Schutzes ihrer industriellen und kommerziellen Geheimnisse äußern, wobei manche von ihnen von echten Befürchtungen im Bereich der Wirtschaftsinformation sprechen.

Angesichts der zunehmenden Zahl betroffener Unternehmen, die sich heute an die CNIL wenden, sah sich diese veranlasst, die Regierung auf diesen Punkt aufmerksam zu machen. In Kürze müssten interministerielle Erörterungen zu diesem Thema beginnen.

Zentrale Kredit- und Wohnungsdateien

Die Einrichtung von Dateien, die es einem gesamten Tätigkeitssektor (Krediteinrichtungen oder professionelle Vermieter) ermöglichen, Informationen über die Solvenzrisiken von Kreditnehmern oder Wohnungssuchenden zu erhalten, hat die CNIL angesichts der offensichtlichen Gefahr, dass die betroffenen Personen sozial ausgegrenzt werden, zu höchster Wachsamkeit veranlasst.

Bei der Einführung einer Kreditzentrale in Frankreich stellt sich vor allem die Frage der Rechtmäßigkeit und der Verhältnismäßigkeit, und zwar sowohl in Bezug auf Ethik und Verletzung der Privatsphäre als auch hinsichtlich Effizienz und Kosten. Die CNIL hat es seit jeher abgelehnt, in Ermangelung eines spezifischen Rechtsrahmens die Rechtmäßigkeit der Einrichtung einer solchen Zentrale anzuerkennen. Ihrer Ansicht nach ist nur der Gesetzgeber befugt, sich zum sozialen Nutzen einer „positiven Datei“ im Kreditsektor zu äußern und gegebenenfalls die Zwecke und den Inhalt dieser Datenbank genau zu bestimmen. Diesem Standpunkt entsprechend, hat sie sich geweigert, die Einrichtung einer Kreditzentrale durch das Unternehmen Experian zu genehmigen.

Im Übrigen hat sie es abgelehnt, dem Unternehmen Infobail die Genehmigung zum Einsatz von zwei Verarbeitungen zur Information professioneller Vermieter über die Verwaltung von Außenständen bzw. zur Erfassung der Mieter, die ihren Verpflichtungen nachkommen, zu erteilen, dies mit der Begründung, dass diese Dateien gegen das vom Gesetzgeber garantierte Recht auf Unterkunft verstoßen. Des Weiteren führte sie aus, es sei Sache des Gesetzgebers, sich zur Schaffung sowohl „negativer“ als auch „positiver“ Dateien im Wohnungssektor zu äußern.

Kontrollen im Rahmen der Erprobung der persönlichen Krankenakte (Dossier Médical Personnalisé/DMP)

Die CNIL hat bei den wichtigsten Akteuren der Erprobung der DMP – Hosting-Firmen, Krankenhauszentren, Gesundheitsnetzwerke, freie Ärzte und Anrufzentralen – 18 Kontrollen vor Ort vorgenommen. Nach Abschluss der Kontrollen hat sie folgende Feststellung getroffen:

Die CNIL hat festgestellt, dass gewisse Hosting-Anbieter den Pflegeeinrichtungen die Kennnummern von Patienten ohne besondere Schutzmaßnahmen auf elektronischem Weg übermittelt haben. Manche Anrufzentralen haben – im Falle des Verlusts der Kennnummern, anhand deren die DMP konsultiert oder ergänzt werden können – dem Patienten per unverschlüsselter E-Mail ein Passwort zugeschickt oder ihm dieses Passwort per Telefon mitgeteilt. Diese Praktiken können die Vertraulichkeit dieser Informationen gefährden.

Die CNIL hat außerdem vermerkt, dass die Patienten nicht alle ausreichend darüber informiert waren, dass der Zugang zu den in ihrer DMP enthaltenen medizinischen Daten einen Internet-Anschluss erforderte. Überdies wurde ihnen manchmal gesagt, der Zugang zu diesen Daten sei durch Vermittlung der Anrufzentrale des Hosting-Anbieters möglich, obwohl dieser letztere ausschließlich dazu da ist, die Patienten technisch zu unterstützen oder ihnen zu ermöglichen, die sie betreffenden Verwaltungsdaten, ihr Passwort oder die Zusammensetzung ihres Vertrauenskreises zu ändern.

Es wurde festgestellt, dass in den Anrufzentralen nur unzureichende Maßnahmen zur Identifizierung/Erkennung angewendet wurden, da die Erkennung der Patienten nicht systematisch auf Basis gezielter Fragen (zum Beispiel: „Vorname Ihrer Schwiegermutter? Marke Ihres ersten Autos?“) erfolgte, die mit den Patienten bei ihrer Einschreibung vereinbart wurden.

Außerdem stellen manche Hosting-Anbieter denjenigen Pflegeeinrichtungen, die ihr medizinisches Personal nicht mit einer CPS (professionelle Gesundheitskarte) ausgerüstet haben, einen Zugang zu den

DMP von ihrer Internet-Site aus zur Verfügung, und dies auf Basis einer einfachen Kennnummer und eines Passworts. Diese Lösung ist inakzeptabel und steht eindeutig im Widerspruch zu den Entscheidungen der CNIL vom 21. März und vom 30. Mai 2006.

Es wurde jedoch geprüft, dass das Verwaltungspersonal und die technischen Mitarbeiter sowohl des Hosting-Anbieters als auch der Anrufzentralen keinen Zugang zu den in den DMP enthaltenen Gesundheitsdaten haben.



Deutschland

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

Die Richtlinie 2004/82/EG vom 29. April 2004 (APIS Richtlinie) ist durch das Dritte Gesetz zur Änderung des Bundespolizeigesetzes vom 22.12.2007 in innerstaatliches Recht umgesetzt worden. Es wird am 1. April 2008 in Kraft treten.

Nach dieser Richtlinie ist ein bestimmter Datensatz von den Fluggesellschaften als Mindestanforderung zu übermitteln. Deutschland ging bei der Umsetzung in innerstaatliches Recht über diesen Datensatz zwar hinaus. Im Laufe des Gesetzgebungsverfahrens konnte jedoch erreicht werden, dass von den ursprünglichen Plänen abgesehen wurde und nunmehr nur noch das „Geschlecht“ sowie die „Nummer des Visums“ von den Beförderungsunternehmen an die deutschen Bundespolizeibehörden als zusätzliche Daten übermittelt werden müssen. Positiv hervorzuheben ist, dass die Daten sowohl bei den Beförderungsunternehmen als auch bei der Bundespolizei binnen 24 Stunden nach Erhebung bzw. Übermittlung gelöscht werden müssen.

Das im Juni 2007 geschlossene PNR-Abkommen mit den USA einschließlich des begleitenden Briefwechsels zwischen dem US-Heimatschutzministerium und der EU wurde durch Gesetz vom 20. Dezember 2007 ohne Änderungen umgesetzt. Es trat am 30. Dezember 2007 in Kraft.

Am 31. Dezember 2007 trat das Gesetz zur Neuordnung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BGBI. I, Nr. 70 vom 31.12.2007, S. 3198 ff.) in Kraft.

Das Gesetz sieht die Speicherung von Telefon-, E-Mail- und Internet-Verkehrsdaten für ein halbes Jahr vor, wobei die Speicherungspflicht für die Verkehrsdaten im Bereich des Internets erst zum 1. Januar 2009 gelten wird. Damit wird das gesamte Telekommunikationsverhalten aller Bürgerinnen und Bürger der Bundesrepublik Deutschland erfasst, obwohl voraussichtlich nur ein

verschwindend kleiner Teil der gigantischen Datenmenge von den Strafverfolgungsbehörden abgerufen werden soll.

Mit Blick auf die Rechtsprechung des Bundesverfassungsgerichts bestehen Zweifel an der Verfassungsmäßigkeit dieser Vorratsdatenspeicherung für nicht hinreichend bestimmbar Zwecke.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mehrfach mit Nachdruck gegen die gesetzliche Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter strafprozessualer Ermittlungsmaßnahmen, die durch das Gesetz ebenfalls vorgenommen werden, gewandt.

Gegen das Gesetz sind beim Bundesverfassungsgericht zahlreiche Verfassungsbeschwerden eingelegt worden.

Durch das Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften vom 20. Juli 2007 (BGBI. I, Nr. 35 vom 27.7.2007, S. 1566 ff.) wurde mit Wirkung zum 1. November 2007 in der Bundesrepublik Deutschland der elektronische Reisepass (E-Pass) der II. Generation, in dessen Biometriechip neben dem Passbild auch die Daten der beiden Zeigefinger gespeichert sind, eingeführt. Damit folgt die Bundesrepublik der „Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“. Die Einrichtung einer bundesweiten Datenbank hat der Gesetzgeber ausgeschlossen (§ 4 Abs. 3 Satz 3 PaßG).

Zuvor wurde in Deutschland seit dem 1.11.2005 auf den Reisepässen der ersten Generation in einem integrierten Chip das digitalisierte Gesichtsbild gespeichert.

Am 1. März 2007 trat das Telemediengesetz (TMG) in Kraft, das die Anforderungen für Tele- und Mediendienste aus verschiedenen Rechtsgrundlagen in einem einzigen Gesetz zusammenführt. Dabei handelt es sich einerseits um die wirtschaftlich orientierten Regelungen zur Umsetzung der E-Commerce-Richtlinie, die bis dahin im Teledienstegesetz (TDG) und im Mediendienst-

Staatsvertrag der Länder (MDStV) enthalten waren, und andererseits um die Datenschutzbestimmungen des vorher geltenden Teledienstedatenschutzgesetzes (TDDSG) und des genannten Staatsvertrags. Die Tele- und Mediendienste wurden unter dem Begriff „Telemedien“ zusammengefasst.

Inhaltlich wurden die alten Regelungen weitgehend unverändert übernommen. Dies gilt vor allem im Hinblick auf diejenigen Vorschriften, die die Anforderungen der E-Commerce-Richtlinie in deutsches Recht umsetzen. Im Datenschutz-Bereich wurde durch die Klarstellung, dass für Internet-Zugangsprovider, Anbieter von Internet-Telefonie und E-Mail-Diensten ausschließlich das Telekommunikationsdatenschutzrecht gilt, eine länger bestehende Rechtsunsicherheit beseitigt. Zum Schutz der Empfänger von elektronischer Werbung wurden im Sinne einer größeren Transparenz Regelungen aufgenommen, die das Verschleiern oder Verheimlichen des Absenders und des kommerziellen Charakters einer Werbe-E-Mail verbieten und ein Zuwiderhandeln mit einem Bußgeld belegen.

B. Bedeutende Rechtsprechung

Das Bundesverfassungsgericht hat am 13. Februar 2007 entschieden, dass die Gerichte die Verwertung heimlich eingeholter genetischer Abstammungsgutachten wegen Verletzung des Rechts des betroffenen Kindes auf informationelle Selbstbestimmung als Beweismittel ablehnen müssen. Der Gesetzgeber habe zur Verwirklichung des Rechts des rechtlichen Vaters auf Kenntnis der Abstammung seines Kindes von ihm (neben dem Vaterschaftsanfechtungsverfahren) ein geeignetes Verfahren allein zur Feststellung der Vaterschaft bereitzustellen. Dieses Urteil stärkt das Recht auf informationelle Selbstbestimmung. Die vom Gericht getroffene Abwägung zwischen dem Recht des Kindes, seine Daten nicht preiszugeben, und dem verfassungsrechtlich geschützten Recht des Vaters auf Kenntnis, ob das Kind von ihm abstammt, entspricht dem verfassungsrechtlichen Grundsatz der Verhältnismäßigkeit. Mit der Entscheidung des Bundesverfassungsgerichts wird auch einem drohenden Dambruch, heimliche Gentests in anderen Lebensbereichen (z. B. Versicherungen und Arbeitsverhältnisse) durchzuführen, ein Riegel vorgeschoben.

C. Wichtige spezifische Themen

Ein Schwerpunkt der datenschutzpolitischen Diskussion im Jahr 2007 war die Frage, inwieweit den Polizeien und Nachrichtendiensten zur Bekämpfung des internationalen Terrorismus die Befugnis zu heimlichen Online-Durchsuchungen von PCs und sonstigen informationstechnischen Systemen eingeräumt und entsprechende gesetzliche Befugnisnormen geschaffen werden sollen.

Der zunehmende Einsatz des Internets bei der Planung und Durchführung terroristischer Aktivitäten stellt die Sicherheitsbehörden vor neue Herausforderungen. Es werden daher Überlegungen angestellt, das Internet und private PCs mit dem Ziel zu durchsuchen, terroristische oder kriminelle Aktivitäten bereits in einem frühen Stadium aufzudecken. Das nordrhein-westfälische Verfassungsschutzgesetz enthält bereits eine entsprechende Befugnis zur Online-Durchsuchung für den dortigen Nachrichtendienst.

Um was es sich bei der Online-Durchsuchung genau handeln soll, deuten die Befürworter nur an. Klar ist nur, dass die Sicherheitsbehörden unter Verwendung des Internetanschlusses in Rechner bzw. Systeme eindringen sollen, um sich Zugriff auf die gespeicherten Daten zu verschaffen.

Die Online-Durchsuchung wirft schwerwiegende technische und verfassungsrechtliche Fragen auf. Denn nahezu jedermann verfügt über einen PC, auf dem ganz persönliche Informationen wie z. B. Tagebuchaufzeichnungen enthalten sind. Bisher ist insbesondere ungeklärt, wie Informationen, die dem grundgesetzlich garantierten Kernbereich der privaten Lebensgestaltung zuzurechnen sind, vor dem Online-Zugriff durch Sicherheitsbehörden wirksam geschützt werden können. Das Bundesverfassungsgericht wird sich im Laufe des Jahres 2008 mit der Zulässigkeit der heimlichen Online-Durchsuchung befassen, denn die Bestimmungen zur Online-Durchsuchung aus Nordrhein-Westfalen sind Gegenstand einer entsprechenden Verfassungsbeschwerde.



Griechenland

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

Richtlinie 95/46/EG

Die Richtlinie 95/46/EG wurde durch das Gesetz Nr. 2472/97 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in nationales Recht umgesetzt. Im Jahr 2007 änderte das Gesetz Nr. 3625/07 das Gesetz Nr. 2472/97 in folgenden Punkten ab:

Artikel 2 des Gesetzes Nr. 2472/97 wurde geändert, um die Veröffentlichung von Fällen strafrechtlicher Anklagen oder Verurteilungen zu erlauben. Insbesondere kann die Veröffentlichung im Anschluss an eine Weisung des zuständigen Staatsanwalts des erstinstanzlichen Gerichts oder des Leitenden Staatsanwalts zulässig sein, wenn der Fall vor dem Berufungsgericht anhängig ist, wenn es sich um Straftaten handelt, die als Kapitalverbrechen oder vorsätzliche Vergehen bestraft werden, und vor allem in Fällen von Verbrechen gegen das Leben, gegen die sexuelle Selbstbestimmung, Verbrechen in Verbindung mit sexueller Ausbeutung, Verbrechen gegen die persönliche Freiheit, gegen Eigentum, gegen das Recht auf Eigentum, Verstößen gegen die Drogengesetzgebung, Verschwörung gegen die öffentliche Ordnung sowie Verbrechen gegen Minderjährige. Die Veröffentlichung strafrechtlicher Anklagen oder Verurteilungen zielt darauf ab, die Gemeinschaft, Minderjährige und gefährdete oder benachteiligte Gruppen zu schützen und die Ahndung solcher Straftaten durch den Staat zu vereinfachen.

Gemäß der Änderung von Artikel 3 des Gesetzes Nr. 2472/97 ist es zulässig, Ton- oder Bildaufnahmegeräte oder andere spezielle technische Mittel einzusetzen, während Bürger ihr Recht auf Versammlungsfreiheit gemäß Artikel 11 der Verfassung ausüben, wenn die Staatsanwaltsbehörde eine entsprechende Weisung erlassen hat und die öffentliche Ordnung und Sicherheit ernsthaft gefährdet ist. Das einzige Ziel der oben erwähnten Aufzeichnungen ist ihre Verwendung als Beweis für die Begehung von Straftaten vor einer Ermittlungsbehörde, einer Staatsanwaltsbehörde oder einem Gericht. Die Verwendung jedes anderen Materials, das zur Verwirklichung des oben genannten Ziels der Überprüfung begangener Straftaten nicht notwendig ist, ist

verboten, und das betreffende Material wird auf Weisung des zuständigen Staatsanwalts vernichtet werden.

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

Richtlinie 2002/58/EG

Die Richtlinie 2002/58/EG wurde durch das Gesetz Nr. 3471/2006 (über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und Änderung des Gesetzes Nr. 2472/97) in nationales Recht umgesetzt. Das neue Gesetz wurde als neuer Gesetzestext eingeführt und nicht als Änderung des Gesetzes Nr. 2774/1999 (über den Schutz personenbezogener Daten im Telekommunikationssektor), das aus Gründen der Klarheit und um Verwirrung zu vermeiden, in seiner Gesamtheit aufgehoben wurde.

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

Richtlinie 2006/24/EG

Der Ständige Ausschuss des Justizministeriums arbeitet gegenwärtig an dem Entwurf eines Gesetzes, mit dem die Richtlinie 2006/24/EG in nationales Recht umgesetzt werden soll.

Die wichtigsten Entwicklungen

Ende 2007 hat die griechische Datenschutzbehörde (GDSB) begonnen, das neue Informationssystem in Betrieb zu nehmen, das nicht nur Back-office-Funktionen für die internen Benutzer verbessern, sondern auch ein neues Portal, das den Bürgern elektronische Regierungsdienstleistungen anbietet, verfügbar machen wird.

B. Bedeutende Rechtsprechung

Entscheidung 3/2007

Die GDSB hat entschieden, dass die Vorschriften des Gesetzes Nr. 2472/97 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten für die Sammlung und Verarbeitung personenbezogener Daten gelten, die mithilfe eines CCTV-Systems gesammelt werden, das in einem privaten Wohnhaus eingesetzt wird und darauf abzielt, Arbeiter, die dem Haushalt ihre professionellen Dienste angeboten haben, zu überwachen, oder das in eine solche Überwachung resultiert. Die Anbringung und

der Betrieb eines CCTV-Systems ohne die Einhaltung der festgelegten Bedingungen und, insbesondere, ohne die Meldung eines solchen Betriebs an die GDSB und ohne Information des Datensubjekts ist illegal, und der Kontrolleur kann entsprechend bestraft werden.

Entscheidung 6/2007

Die Veröffentlichung (durch das Ministerium für nationale Verteidigung) der Namen von Personen, die a) aus Gesundheitsgründen legal vom Militärdienst befreit wurden, b) nach der zweiten Überprüfung der Beweisunterlagen als vom Militärdienst befreit betrachtet wurden oder c) illegal aus Gesundheitsgründen vom Militärdienst befreit wurden, verstößt gegen die Bestimmungen des Gesetzes Nr. 2472/97, da die oben erwähnten Daten unter keine der gesetzlich vorgesehenen Ausnahmen fallen, nach denen die Verarbeitung zulässig wäre.

Entscheidung 62/07

Die griechische Datenschutzbehörde erließ die Entscheidung 62/2007, mit der sie die Betreibung eines biometrischen Systems zur Kontrolle der Anwesenheit der Arbeitnehmer und den Einsatz eines CCTV-Systems in Arbeitsbereichen für illegal erklärte. Sie verhängte anschließend eine Geldstrafe von 8000 Euro für die Betreibung des biometrischen Systems und von 6000 Euro für die Betreibung des CCTV-Systems. Ferner wies die GDSB den Datenkontrolleur an, das biometrische System zu entfernen und das in der Richtlinie 1122/2000 in Bezug auf den Einsatz eines CCTV-Systems vorgesehene Verfahren einzuhalten.

Entscheidung 64/07

Die GDSB richtete eine Empfehlung an die TEIRESIAS Bank Information Systems SA und an griechische Banken, ein Verfahren einzuführen, durch das Banken TEIRESIAS nach der Tilgung von Schulden aufgrund der Beendigung eines Personen- oder Verbrauchercredits, der natürlichen Personen von Banken oder Finanzeinrichtungen gewährt wurde, innerhalb von 15 Tagen nach der Tilgung eine entsprechende Meldung zukommen lassen. TEIRESIAS wird seine Aufzeichnungen umgehend, spätestens 15 Tage nach Erhalt der Meldung über die Tilgung, ändern, und zwar ohne irgendeine weitere Aktion seitens des Datensubjekts.

C. Wichtige spezifische Themen

Am 19. November 2007 reichten der Vorsitzende, der stellvertretende Vorsitzende und sieben Mitglieder der griechischen DSB im Anschluss an den unten beschriebenen Vorfall aus Protest ihren Rücktritt ein.

Die Datenschutzbehörde hatte die Entscheidung Nr. 58/2005 erlassen, mit der sie den Einsatz des C41-CCVT-Systems (239 Kameras) und von 49 bereits bestehenden Kameras ausschließlich zu Zwecken des Verkehrsmanagements unter bestimmten Umständen und aus Gründen, auf die in der Entscheidung detailliert Bezug genommen wird, gestattete.

Insbesondere hatte sie betont, dass der Betrieb des Systems und die Verwendung der mithilfe des Systems gesammelten und darin aufgezeichneten Daten für alle anderen Zwecke außer der Kontrolle von Straftaten gemäß dem rechtmäßigen Einsatz des Systems und den in der Entscheidung dargelegten Umständen verboten ist. Der Einsatz von Kameras, die an Straßenkreuzungen oder Verkehrsachsen angebracht sind, ist verboten, wenn der Fahrzeugverkehr auf diesen Straßen unterbrochen ist, d. h. während Kundgebungen, Demonstrationen usw.

Der Minister für öffentliche Ordnung hatte beim Staatsrat einen Aufhebungsantrag gegen die oben erwähnte Entscheidung gestellt; am 12.01.2007 fand dazu eine Anhörung statt, und seither ist die Sache vor der Plenarsitzung des Staatsrats anhängig. Bemerkenswert ist, dass der Vorschlag des Berichtstatters sich gegen den Aufhebungsantrag aussprach. Darüber hinaus hatte der Aufhebungsausschuss des Staatsrates den betreffenden Aufhebungsantrag bezüglich des Verbots des Betriebs von Kameras bereits zurückgewiesen. Im November 2007, während diese Sache anhängig war, und im Anschluss an eine vom griechischen Polizeipräsidium vorgelegte Frage erließ der Generalstaatsanwalt des Obersten Gerichtshofs Griechenlands für Zivilsachen (Areios Pagos) die Stellungnahme Nr. 14/2007, nach der der Betrieb des oben erwähnten CCTV-Systems unter der Aufsicht eines Staatsanwalts in allen Fällen erlaubt ist, auch wenn keine Fahrzeuge auf den Straßen sind oder wenn der Fahrzeugverkehr verboten ist, d. h. während Kundgebungen, Demonstrationen usw., wobei jedoch die Aufzeichnung der erhaltenen Bilder

in allen Fällen, ausgenommen wenn Straftaten verübt werden, untersucht ist. Die griechische Datenschutzbehörde, die einzige Behörde, die laut Verfassung befugt ist, diese Frage gemäß den Bestimmungen zum Schutz personenbezogener Daten zu prüfen, veröffentlichte eine Pressemitteilung zu diesem Thema und erklärte, ihre Entscheidung sei, da sie vom Staatsrat nicht aufgehoben wurde, rechtmäßig und daher nach wie vor anwendbar und verbindlich. Darüber hinaus würde ein Verstoß gegen ihre Vorschriften die durch das Gesetz Nr. 2472/97 vorgesehenen Verwaltungsstrafen nach sich ziehen. Aus diesem Grund sei bereits zwei Mal eine Verwaltungsstrafe gegen das Ministerium für öffentliche Ordnung verhängt worden. Trotz der klaren, kategorischen und rechtmäßigen Behandlung dieser Angelegenheit auf der Grundlage der Verfassung wird das erwähnte CCTV-System auf Weisung des Staatsanwalts noch immer betrieben. Daher wurden unter der Aufsicht des Staatsanwalts Bilder von der Kundgebung und dem Demonstrationszug erhalten, die am 17.11.2007 stattfanden, d. h. anlässlich der Gedenkfeier an den Aufstand vor dem Athener Polytechnikum, während der der Fahrzeugverkehr in dem Bereich verboten war. Dies wurde durch den Bericht der Prüfer der Datenschutzbehörde bestätigt, die nach Erhalt einer schriftlichen Anweisung die Polizeidirektion von Attika aufsuchten, um eine Prüfung vorzunehmen, wie durch die Bestimmungen von Artikel 19, Absatz 1 des Gesetzes Nr. 2472/97 vorgesehen. Auf diese Weise wurden die Vorschriften der oben erwähnten Entscheidung der griechischen Datenschutzbehörde eklatant verletzt, und die von der Verfassung geschützte Unabhängigkeit der Behörde wurde erheblich beeinträchtigt, während ihr Status gemindert wurde.



Ungarn

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

Letztes Jahr wurde versucht, die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die in Verbindung mit der Erbringung elektronischer Kommunikationsdienstleistungen verarbeitet werden, mit der die Richtlinie 2002/58/EG geändert wird, umzusetzen. Der Datenschutzkommissar erhielt im Rahmen des administrativen Koordinierungsverfahrens mehrere Entwürfe und gab Kommentare zu dem Recht auf Privatsphäre, der Vertraulichkeit der Kommunikationen und dem Schutz personenbezogener Daten ab. Er erklärte, dass die massenhafte Vorratsspeicherung von Daten den vom Europäischen Gerichtshof für Menschenrechte festgelegten Prinzipien bezüglich der Beschränkung der Menschenrechte nicht entspricht, es sei denn, die Beschränkung ist notwendig, angemessen und verhältnismäßig gegenüber dem Schutz der öffentlichen Ordnung, der nationalen und der öffentlichen Sicherheit und dient dazu, die Vorbeugung, Untersuchung und Bekämpfung von Straftaten und der illegalen Verwendung des elektronischen Kommunikationssystems zu gewährleisten. Der Kampf gegen Terrorismus und das organisierte Verbrechen kann auch nicht als Rechtfertigung für jedes Vorgehen dienen. Der Kommissar betonte, dass, selbst wenn das EU-Recht Raum für Gesetze der Mitgliedstaaten vorsieht, die automatische Umsetzung der niedrigsten oder höchsten Anforderungen (im Fall Ungarn: die längstmögliche Speicherfrist) inakzeptabel ist und die Prinzipien des Datenschutzes zu bedenken sind. Der Entwurf wurde dem Parlament nicht vorgelegt.

B. Bedeutende Rechtsprechung

Die Öffentlichkeit zeigte sich sehr besorgt über die Gesundheitsreform, die auch die Schließung und Integration von Einrichtungen mit sich brachte. Der Kommissar leitete eine Untersuchung von Amts wegen über den Aufbewahrungsort von Unterlagen ein, die ursprünglich im Besitz der geschlossenen Gesundheitseinrichtungen waren, da Kontrollen der Unterlagen beträchtliche Auswirkungen auf die Durchsetzung der

Patientenrechte auf informative Selbstbestimmung hatten. Die umfassende Untersuchung, an der die betroffenen Entscheidungsträger und die Leiter der geschlossenen Einrichtungen mitwirkten, ergab, dass die institutionelle Reform die Rechte der Patienten auf informative Selbstbestimmung erheblich gefährdet, da sie keine Lösung für die Kontrolle von Unterlagen vorsieht, die im Besitz von Einrichtungen sind, die geschlossen werden sollen. Es ist anzunehmen, dass Datensubjekte keinerlei Möglichkeit haben werden, die Übersicht über ihre medizinischen Daten und Unterlagen zu behalten, was bedeutet, dass man ihnen nicht nur ihr Recht auf Zugang zu Unterlagen versagt, sondern auch die Rechte, die ihnen das Gesetz über Gesundheitsversorgung einräumt, und dass Einrichtungen (Ärzte), die Versorgung anbieten, nicht in der Lage sein werden, Informationen über die Anamnese der Patienten zu erhalten, wodurch die Fähigkeit der Patienten, ihre eigene Gesundheit zu schützen, sich behandeln zu lassen und gesund zu werden, gefährdet wird. Der Datenschutzkommissar forderte den Gesundheitsminister auf, sich aufmerksam mit der Frage medizinischer Unterlagen zu befassen und die notwendigen Schritte zu ergreifen, um sicherzustellen, dass alle geschlossenen Einrichtungen den Patientenrechten bei Entscheidungen über die Handhabung medizinischer Unterlagen Rechnung tragen.

Um eine angemessene Patientenversorgung aufrechtzuerhalten, sollte das System der Übermittlung medizinischer Unterlagen derart konzipiert werden, dass ein ständiger Zugriff auf Informationen über Patientenversorgung möglich ist, wobei auch nicht papiergebundenen Unterlagen besondere Aufmerksamkeit gewidmet werden sollte.

Eine der wichtigsten Empfehlungen, die der Kommissar 2007 erließ, betraf datenschutzrechtliche Identifizierungsauflagen in der elektronischen Verwaltung. Die Empfehlung ging nur auf die Mindestkriterien ein; sie war nicht darauf ausgerichtet, die einzig mögliche praktische Lösung zur Identifizierung zu liefern. Der Zweck des Dokuments bestand darin, die Rahmenbedingungen zu schaffen, die es Kunden erlauben, sich effizient um ihre Angelegenheiten zu kümmern, und gleichzeitig gewährleisten, dass ihre Privatsphäre genauso geschützt ist wie in der traditionellen

Verwaltung. Die Umsetzungsprinzipien und -ideen erwiesen sich als nützliche Orientierungshilfen für elektronische Regierung, Behörden und nicht zuletzt Bürger.

Nachrichten, die in elektronischen Kommunikationen übermittelt und später in strafrechtlichen Verfahren verwendet werden, stellten 2007 ein immer wiederkehrendes Problem dar. Die anwendbaren Gesetze betreffen den traditionellen Versand im Allgemeinen sowie elektronischen Versand als außergewöhnliches Kommunikationsmittel, obwohl letzterer in der Praxis immer gebräuchlicher geworden ist. Für ausgelieferte traditionelle Briefe und Briefe, die „noch unterwegs“ sind, gelten verschiedene Vorschriften, und die Daten-subjekte werden durch angemessene Sicherungen vor der Ausforschung von Geheimnissen geschützt. Der Kern des Problems ist die Schwierigkeit, diese Vorschriften auf elektronische Mails anzuwenden.

Die „traditionelle“ Form des elektronischen Versands ist insofern mit dem Postversand vergleichbar, als es sich auch um eine Kommunikation zwischen zwei bestimmten Personen handelt, deren Inhalt nur dem Sender und dem Empfänger bekannt ist, und die Mails in ihrem Computer (System) ankommen. In vielen Fällen wird der Versand jedoch über einen Inhalt-Provider ausgeführt. Die Daten werden in diesen Fällen nicht im Computer des Senders oder Empfängers gespeichert, sondern im Computer des Providers, so dass der Sender und der Empfänger übers Internet darauf zugreifen können. Zu dieser Kategorie gehören kostenlose E-Mail-Systeme, da sie keine tatsächlichen Datenübermittlungen vornehmen.

Dies führt häufig zu Unsicherheit, beispielsweise wenn die Polizei zu entscheiden versucht, wer als Telekommunikationsanbieter zu betrachten ist, und daher die anwendbare Rechtsgrundlage nicht korrekt bestimmt. Die Beschlagnahmen von auf dem Server des Service-Anbieters gespeicherten Zugriffsdaten durch die Polizei geben ebenfalls Anlass zur Sorge. Die Anwendung traditioneller Begriffe wie „Auslieferung“ auf eine neue Technologie oder Methode dürfte zu Problemen führen. Während Auslieferung im Zusammenhang mit per Post verschickten Briefen ein eindeutiger Begriff ist, ist er zweideutig, wenn es

um E-Mails geht. Es lässt sich einfach bestimmen, ob der Empfänger seine Mailingliste oder eine spezielle E-Mail angesehen hat, aber nach der Interpretation des Staatsanwalts ist dies bedeutungslos: E-Mails sind als ausgeliefert zu betrachten, sobald sie verschickt wurden. Der Datenschutzkommissar informierte den Leitenden Staatsanwalt darüber, dass er dieser Interpretation nicht zustimme, und wies darauf hin, dass in der elektronischen Kommunikation die Merkmale und der Zweck des Datenflusses und nicht seine Methode die Anwendbarkeit von Vorschriften über das Briefgeheimnis bestimmen sollten.

C. Wichtige spezifische Themen

Die Vorschriften über Datenverarbeitung durch Strafverfolgungsbehörden wurden 2007 in mehreren Punkten erheblich geändert, zum Teil in Reaktion auf die Probleme, die während der politischen Unruhen 2006 aufgetreten sind. Die geänderten Vorschriften über Polizeikontrollen in dem Entwurf zur Änderung des Polizeigesetzes sind willkommen, ebenso wie die Verkürzung der übermäßig langen Vorratsspeicherfrist für Daten, die bei Kontrollen gesammelt werden. Aber die Ermächtigung der Polizei, jeden jederzeit und überall im öffentlichen Raum zu überwachen, ist zu allgemein gefasst.

Einer der fragwürdigen Punkte der Gesetzesvorlage zur Änderung bestimmter Gesetze im Bereich des Strafrechts ist der Einsatz elektronischer Überwachungsanlagen zum Zweck der Strafverfolgung durch Strafvollzugsanstalten. Der Entwurf würde die Installation derartiger Anlagen auch außerhalb von Strafvollzugsanstalten erlauben.

An dieser Stelle ist die Vorbereitung des neuen Bürgerlichen Gesetzbuches zu erwähnen, die seit mehreren Jahren läuft und 2007 noch immer nicht abgeschlossen war. Die Recodierung der Vorschriften über Geschäftsgeheimnisse durch den neuen Entwurf des Bürgerlichen Gesetzbuches weckt Bedenken. Unter dem Gesichtspunkt des Datenschutzes sollte auch dem Vorschriftenentwurf zum neuen Immobilienregister Aufmerksamkeit gewidmet werden.

2007 haben wir die Vorbereitungen für den Beitritt Ungarns zum Schengen-Gebiet fortgesetzt und die Datenschutzmethoden ungarischer Konsulate geprüft, die Visa ausstellen, wie etwa das Konsulat in St. Petersburg, Schanghai, Hongkong und Chisnau. Die Kontrollen konzentrierten sich auf die Notwendigkeit der gesammelten personenbezogenen Daten für die Beurteilung der Visaanträge und die Übereinstimmung der Datenverarbeitungsmethoden der Konsulate mit den Datenschutzvorschriften.



Irland

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

Beide Richtlinien wurden vollständig in irisches Recht umgesetzt. Die gesetzlichen Entwicklungen, die sich 2007 erheblich auf den Datenschutz in Irland ausgewirkt haben, umfassten neue Vorschriften zur Änderung der Bestellung von für die Datenverarbeitung Verantwortlichen und Datenverarbeitern, die sich künftig bei der Behörde registrieren lassen müssen. Weitere im Laufe des Jahres eingeführte Vorschriften sahen vor, dass die Verarbeitung genetischer Daten in Verbindung mit der Beschäftigung einer Person als Verarbeitung betrachtet wird, die nur mit vorheriger Zustimmung des Datenschutzkommissars stattfinden darf. Seit dem 24. Oktober 2007 werden sämtliche Bestimmungen des Datenschutzgesetzes auf alle manuellen Daten angewendet.

Was die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die in Verbindung mit der Erbringung öffentlich verfügbarer elektronischer Kommunikationsdienste verarbeitet werden (mit der die Richtlinie 2002/58/EG geändert wird), anbelangt, hat Irland die Rechtsgrundlage dieser Richtlinie vor dem Europäischen Gerichtshof angefochten. Derzeit läuft das Verfahren im Zusammenhang mit dieser Angelegenheit noch. Dennoch, und unbeschadet dieses Verfahrens, wird diese Richtlinie (die noch nicht umgesetzt wurde) voraussichtlich Anfang 2008 umgesetzt.

B. Bedeutende Rechtsprechung

In den meisten Fällen werden die dem Kommissar vorgelegten Beschwerden gemäß Abschnitt 10 des irischen Datenschutzgesetzes 1988 und 2003 gütlich beigelegt, ohne dass auf eine formelle Entscheidung zurückgegriffen wird. Derartige gütliche Einigungen können beinhalten, dass der betreffende Datenkontrolleur einer geeigneten Wohlfahrtsorganisation eine Spende zukommen lässt, oder Ähnliches. Andere Strategien beinhalten einen energischeren Einsatz der Vollzugsmacht, wenn für die Datenverarbeitung Verantwortliche die Zugangsrechte von Datensubjekten

nicht beachten, und die Benennung gewisser für die Datenverarbeitung Verantwortlicher in Fallstudien, die im Jahresbericht des Kommissars enthalten sind. Allerdings hat der Kommissar eine Reihe von Einzelentscheidungen über Beschwerden getroffen, die aufgrund der Bestimmungen der Datenschutzgesetze eingereicht wurden. Diese umfassten:

- a) Eine Entscheidung, ein Unternehmen anzuweisen, ihr „Cold call“-Marketing (Initiativanrufe) zu beenden. Im Anschluss an Beschwerden über unerbetene Direktmarketing-Anrufe seitens einer bestimmten Firma stellte die Behörde fest, dass die Marketingverfahren der Firma nicht solide genug waren, um die Datenschutzrechte der Abonnenten zu gewährleisten. Die irische Datenschutzbehörde hat sie daher angewiesen, alle Initiativanrufe einzustellen, bis die Firma das Problem behoben hat, da sie anderenfalls eine rechtsverbindliche Vollstreckungsankündigung zu diesem Zweck erhalten würde. Die Firma ist der Aufforderung der Datenschutzbehörde nachgekommen und hat ihre Initiativanrufe zwanzig Tage lang ausgesetzt, bis entsprechende Abhilfemaßnahmen ergriffen wurden.
- b) Eine Entscheidung, in Reaktion auf die Berufung auf das Anwaltsgeheimnis eine Informationsverfügung zu erlassen. Die Behörde erhielt eine Beschwerde über einen für die Datenverarbeitung Verantwortlichen, der sich mit der Begründung, die fraglichen Dokumente unterlägen dem Anwaltsgeheimnis, geweigert hatte, einem Zugangsantrag Folge zu leisten. Die Untersuchung der Datenschutzbehörde bestätigte, dass das Anwaltsgeheimnis für ein bestimmtes, von dem Datensubjekt angefordertes Dokument nicht geltend gemacht werden konnte. Dennoch berief sich der für die Datenverarbeitung Verantwortliche weiterhin auf das Anwaltsgeheimnis. Die Behörde hatte keine andere Möglichkeit, als eine Informationsverfügung zu erlassen, mit der die Anweisung erteilt wurde, ihr eine Kopie des betreffenden Dokuments zukommen zu lassen. Bei seiner Überprüfung stellte die Behörde zu ihrer Zufriedenheit fest, dass das Dokument personenbezogene Daten in Bezug auf das Datensubjekt enthielt, und die Datenbehörde erachtete es ebenfalls als zufriedenstellend, dass die in den Datenschutzgesetzen vorgesehenen beschränkten Ausnahmen vom

Zugangsrecht in diesem Fall nicht anwendbar waren.
Das Dokument wurde daraufhin freigegeben.

C. Wichtige spezifische Themen

Im Sommer 2007 führte die Behörde „Razzien“ bei einer Reihe von Unternehmen durch, die im Bereich des SMS-Marketings tätig sind. Diese Verdachtskontrollen erfolgten in Reaktion auf zahlreiche Beschwerden, die die Datenschutzbehörde über diese Unternehmen erhielten, und im Rahmen einer Strategie, die vollen Befugnisse der Behörde einzusetzen, um gegen unerbetene Textnachrichten vorzugehen. Im Anschluss an diese Razzien leitet die Datenschutzbehörde gegenwärtig Strafverfahren gegen diese Unternehmen ein, die unerbetene Nachrichten an Abonnenten geschickt bzw. ihren Versand zugelassen haben oder auf andere Weise ihren Verpflichtungen, die Privatsphäre natürlicher Personen zu achten, nicht nachgekommen sind.



Italien

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

Die Richtlinie 95/46/EG wurde per Gesetz vom 31. Dezember 1996 (Gesetz Nr. 675), das ein halbes Jahr später in Kraft trat, in nationales Recht umgesetzt. Im Juni 2003 wurde ein neues Gesetz (Datenschutzgesetzbuch) verabschiedet, das die bestehenden Gesetze zusammenfasste und vollständig ersetzte. Dieses Gesetz trat am 1. Januar 2004 in Kraft.

Die Richtlinie 2002/58/EG wurde mit dem genannten Datenschutzgesetzbuch in nationales Recht übernommen. Titel X des Gesetzbuches trägt die Überschrift „Elektronische Mitteilungen“ (Paragrafen 121 bis 132).

Parlamentarische Anhörungen

Im Jahr 2007 wurde die Datenschutzbehörde mehrmals von den zuständigen parlamentarischen Ausschüssen zu grundlegenden Themen befragt. Den Schwerpunkt bildeten Fragen, die der parlamentarische Ausschuss behandelt, der die Umsetzung des Schengener Abkommens, die Tätigkeiten von Europol und Zuwanderungsbelange überwacht und der an den Beratungen zum Gesetz über das so genannte „biologische Testament“ beteiligt ist. Weitere Anhörungen betrafen Gesetzesvorlagen zur systematischen Vermeidung von Betrugsfällen bei Verbraucherkrediten und zur Regulierung des Fernsehsektors während der Umstellung auf die Digitaltechnik. Darüber hinaus wirkte die Behörde an einer Studie über den Zusammenhang zwischen der Pressefreiheit und dem Schutz von Persönlichkeitsrechten sowie an einer Studie über Verwaltung und Gebrauch der bei den Finanzbehörden gespeicherten Daten mit. Ebenfalls zu nennen ist eine Anhörung über die Nutzung der satellitengestützten Navigationssysteme Galileo und GPS in Anbetracht der Errichtung eines weltweiten Satellitensystems für zivile Zwecke.

Sensibilisierungsmaßnahmen für Parlament und Regierung

Basierend auf dem Datenschutzgesetzbuch gehört es unter anderem zu den Aufgaben der italienischen Datenschutzbehörde, das Parlament und die Regierung

darauf hinzuweisen, dass die Regulierung bestimmter Wirtschaftszweige ratsam ist. In diesem Zusammenhang schlug die italienische Regierung dem Parlament vor, aus Sicherheitsgründen eine bei der Polizei geführte DNS-Datenbank zu errichten. Die Datenschutzbehörde hatte Gelegenheit, Parlament und Regierung darauf hinzuweisen, dass bei der Errichtung dieser landesweiten Datenbank grundlegende Schutzvorkehrungen notwendig seien. Insbesondere dürfe die Datenbank nur zur Identifizierung einzelner Personen dienen. Folglich darf keine obligatorische Sammlung von DNS-Proben angestrebt werden. Falls eine solche Sammlung für bestimmte Personengruppen wie beispielsweise Verhaftete, Verdächtige, Angeklagte und Verurteilte vorgesehen ist, so müssen verhältnismäßige Schutzvorkehrungen vorgeschrieben werden. Überdies soll die Frist für die Vorratsspeicherung von Identifizierungsdaten im Verhältnis zu den vorgesehenen Zwecken stehen. Weitere Schutzvorkehrungen wurden für den Zugriff (empfohlen wurde ein Anmeldeverfahren) und die Ausübung der Rechte von registrierten Personen bestimmt. Ähnliches galt für die parlamentarische Beratung über den Entwurf eines Gesetzes, demgemäß KMU und Freiberufler keine Mindestanforderungen an den Datenschutz hätten erfüllen brauchen. Dadurch wären bei einem Großteil der italienischen Unternehmen wesentlich geringere Schutzvorkehrungen für die Bearbeitung von Beschäftigtendaten notwendig gewesen. Die Datenschutzbehörde wies darauf hin, dass nach Maßgabe europäischen und internationalen Rechts weder die gruppenweite Befreiung von der Anwendung wesentlicher Bestimmungen zum Schutz personenbezogener Daten noch die Verursachung von Abweichungen gegenüber den Datenverarbeitungsprozessen der öffentlichen Hand zulässig sind. Des Weiteren forderte die Datenschutzbehörde das italienische Parlament auf, das Datenschutzgesetzbuch so abzuändern, dass weitere Mittel (insbesondere verbindliche Unternehmensregelungen) in Betracht gezogen werden können, damit ein angemessener Datenschutz im Sinne der europäischen Richtlinie (Artikel 26(2)) geleistet werden kann.

Stellungnahmen

Nach Maßgabe des Datenschutzgesetzbuches soll die italienische Datenschutzbehörde vom Ministerpräsidenten und jedem Ministerium immer dann hinzugezogen

werden, wenn Regelungen und Verwaltungsinstrumente beschlossen werden sollen, die Datenschutzbelange berühren dürften. Im Jahr 2007 war dies gleich mehrfach der Fall. Insbesondere handelte es sich dabei um Stellungnahmen zur computergestützten Erfassung von Kfz-Steuern, die Zusammensetzung und Aufgaben des Ausschusses für die Adoption ausländischer Kinder (in diesem Fall gestattete die Datenschutzbehörde die Verarbeitung personenbezogener Daten von ausländischen Kindern, die von italienischen Eltern adoptiert oder deren Vormundschaft unterstellt werden, ausschließlich in Bezug auf unverzichtbare Daten und im Einklang mit den Schutzbestimmungen des Datenschutzgesetzbuches), der Missbrauch des Finanzsystems zur Geldwäsche und zur Terrorismusfinanzierung, die technischen Regelungen für Personalausweise und elektronische Erkennungsmerkmale, die Koordinierung der Maßnahmen der öffentlichen Hand zum Schutz von Minderjährigen vor sexueller Ausbeutung und sexuellem Missbrauch, die Bestimmungen zu den Zahlungen der öffentlichen Hand, die freiwilligen Verhaltensregeln für Medien und Sport sowie die Beteiligung der lokalen Behörden an Steuerprüfungen und anderen Regelungen zur Bekämpfung von Steuerhinterziehung.

B. Bedeutende Rechtssprechung

Der italienische Kassationshof als oberster italienischer Gerichtshof hat im Jahr 2007 mehrere Entscheidungen zum Datenschutz erlassen.

Räumliche gerichtliche Zuständigkeit für den Datenschutz

Die räumliche Zuständigkeit für Streitigkeiten im Zusammenhang mit der Anwendung der Bestimmungen des Datenschutzgesetzbuches liegt bei den Gerichten des Ortes, an dem die datenverantwortliche Stelle ihren Sitz hat. Dabei handelt es sich um eine ausschließliche Zuständigkeit.

Zugriff auf E-Mails von Beschäftigten

Der Zugriff auf fremde Korrespondenz ist strafbar, wenn die Korrespondenz „versiegelt“ ist. Über Computernetze versandte Korrespondenz wird gegenüber jedem Unternehmen „versiegelt“, das nicht zum Zugriff auf jene IT-Systeme befugt ist, die für Versand bzw. Empfang der einzelnen Mitteilungen genutzt werden. Im konkreten

Fall entschied das Gericht, dass ein rechtmäßiger Zugriff auf die im IT-System eines Unternehmens gespeicherte Korrespondenz durch jede Einheit (einschließlich des Arbeitgebers) erfolgen könne, das rechtmäßig im Besitz der entsprechenden Zugriffsschlüssel (Nutzerkennung und Passwort) sei; die entsprechenden Weisungen und Informationen waren von dem Unternehmen an alle Beschäftigten zu dem Zweck ausgegeben worden, bei Abwesenheit eines einzelnen Nutzers den Zugriff zu ermöglichen. Das entspricht der Richtlinie, die von der italienischen Datenschutzbehörde in einer Entscheidung vom 1. März 2007 ausgesprochen wurde (siehe unten). Nach Maßgabe dieser Richtlinie dürfen leitende Angestellte des Unternehmens rechtmäßig auf die den Beschäftigten zur Verfügung gestellten Computer bzw. IT-Geräte zugreifen, falls die den Zugriff rechtfertigenden Umstände den betroffenen Beschäftigten vollständig mitgeteilt worden sind. Dagegen hieß es in einer anderen Gerichtsentscheidung, der Systemverwalter eines Unternehmens dürfe nicht mit Hilfe der ihm gewährten Vorrechte (im IT-Sinne) – beispielsweise die Möglichkeit zur Vergabe von Passwörtern an die Inhaber von E-Mail-Konten – auf die E-Mails von Beschäftigten zugreifen. Die Inhaber von E-Mail-Konten seien unzweifelhaft berechtigt, die vom Systemverwalter zugewiesenen Passwörter durch andere Passwörter ihrer Wahl zu ersetzen, um Geheimhaltung und Privatsphäre zu wahren, und danach sei der Verwalter nicht mehr zum Zugriff auf die einzelnen Konten berechtigt. Das Gericht hob hervor, dass die Betrugsabsicht beim Abfangen von Mitteilungen nicht darin bestehe, mit Hilfe des Abfangens das Aufspüren des abfangenden Unternehmens unmöglich oder extrem schwierig zu machen, sondern darin, jene Schutzmechanismen außer Kraft zu setzen oder zu umgehen, mit denen der Zugriff Dritter auf die betreffenden Mitteilungen verhindert werden soll.

Pressefreiheit und Quellenschutz

Die von einer Justizbehörde in Rom angeordnete Beschlagnahmung des Computers eines Journalisten wurde vom zuständigen Gericht unter anderem deshalb aufgehoben, weil das Berufsgeheimnis und die Vorrechte von Journalisten nicht berücksichtigt worden waren. Dem Gericht zufolge ist bei Maßnahmen gegen Journalisten wie beispielsweise Durchsuchungen oder Beschlagnahmungen besondere Sorgfalt anzuwenden, weil die Möglichkeit bestehe, dass derlei Maßnahmen

Einschränkungen der Pressefreiheit mit sich brächten. Das journalistische Berufsgeheimnis solle die Freiheit und Unparteilichkeit der Presse schützen und stelle kein Privileg des einzelnen Journalisten dar, so das Gericht.

Bildtelefone und Kinderpornographie

Die Verbreitung eines pornographischen Videos (auf dem der Geschlechtsverkehr zwischen einem jungen Mädchen und mehreren Jungen zu sehen ist) über Mobiltelefone fällt unter den gesetzlich bestimmten Begriff der Kinderpornographie. Nach Ansicht des Gerichts wird im Rahmen des entsprechenden Straftatbestands des italienischen Rechts nicht nur die gewerbliche Verwertung von Kinderpornographie, sondern jede Verhaltensweise geahndet, mittels derer pornographisches Material unter Einbindung von Minderjährigen erzeugt werden kann. Der Angeklagte hatte ein Video aufgenommen und (über sein Mobiltelefon) verbreitet, in dem ein junges Mädchen Geschlechtsverkehr mit mehreren Jungen hatte. Dabei handelte es sich nach Auffassung des Gerichts um Kinderpornographie, weil man leicht habe absehen können, dass die Erstempfänger das fragliche Material zwangsläufig weiterverbreiten würden, so dass sich dessen schädliche Wirkung insbesondere auf Lebensqualität und Persönlichkeitsentwicklung des Opfers noch verstärke.

Zu nennen ist ferner die Entscheidung des obersten Verwaltungsgerichtshofs (letzte Instanz bei verwaltungsrechtlichen Streitigkeiten), dass es rechtmäßig sei, ein Gespräch ohne Unterrichtung der Gesprächspartner aufzuzeichnen, um die Aufzeichnung als Beweismittel in einem Gerichtsverfahren zu verwenden. Nach Auffassung des Gerichts darf keine Disziplinarstrafe gegen einen Universitätsprofessor verhängt werden, der seine Gespräche mit anderen Lehrkräften und Studenten aufgezeichnet hatte, um einen vor Gericht verwertbaren Nachweis darüber zu erhalten. Eine solche Strafe sei gleichbedeutend mit der Bestrafung einer Tätigkeit, die in der gesetzmäßigen Ausübung des Rechts auf Einreichung und Abwehr einer gerichtlichen Klage bestehe, so das Gericht.

C. Wichtige spezifische Themen

Datenbanken zur Durchsetzung rechtlicher Bestimmungen

Die Verwaltung großer Datenbanken, die der Durchsetzung rechtlicher Bestimmungen dienen, stellte auch im Jahr 2007 einen der wichtigsten Tätigkeitsschwerpunkte für die italienische Datenschutzbehörde dar. Unter anderem führte die Behörde eingehende Untersuchungen der Datenverarbeitung bei den Justizbehörden durch. Es wurde darauf hingewiesen, dass auf diesem Gebiet – insbesondere beim Austausch von Abhörprotokollen zwischen Telefongesellschaften und Justizbehörden – strengere Sicherheitsvorkehrungen notwendig seien. Das Fehlen angemessener Vorkehrungen für die Speicherung und Bearbeitung personenbezogener Daten bestätigte sich unter anderem im Verlauf einer Untersuchung am erstinstanzlichen Gericht der Stadt Rom, dem nach Anzahl der jährlich bearbeiteten Verfahren größten Gericht in Italien. Die Datenschutzbehörde setzte ihre Zusammenarbeit mit dem Justizministerium, dem nationalen Richterrat und den Justizbehörden zu dem Zweck fort, die Einhaltung gesetzlicher Vorschriften durchzusetzen und zu erleichtern. Als einer der Hauptgründe für die Schwierigkeiten der Justiz bei der Gewährleistung geeigneter Vorkehrungen zum Schutz personenbezogener Daten ist der Mangel an ausreichenden Finanzmitteln zu nennen.

Sicherheit bei Telefonaten und elektronischen Mitteilungen

Im Zuge einer eingehenden Untersuchung der Verarbeitung personenbezogener Daten durch die großen Telefongesellschaften Italiens stellte die Datenschutzbehörde Unregelmäßigkeiten bei der Sammlung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung des Internets fest. Insbesondere einige als „Internetzugangsanbieter“ tätige Gesellschaften bewahrten – angeblich, weil sie gesetzlich dazu verpflichtet seien – ausführliche Aufzeichnungen über die Internetbewegungen ihrer Nutzer bzw. Kunden auf. Unter anderem mit Hilfe von Hardware-Sonden, transparenten Proxy-Servern und Datenpaketkontrollen konnten sie die IP-Adresse von Absender und Empfänger, ausführliche Internetprotokolle, die von den Nutzern eingegebenen Abfrageketten für Suchmaschinen, über einfache Internetverbindungen übertragene Zugriffsdaten und alle

sonstigen missbrauchsgefährdeten Daten sammeln, die in einer URL-Adresse angegeben werden können. Diese Art der Datenerfassung ist jedoch im Rahmen der Aufgaben eines Internetzugangsanbieters technisch nicht gerechtfertigt. Aus diesem Grund hat die Datenschutzbehörde drei entsprechende Verbotsbestimmungen erlassen und die Anbieter angewiesen, die gesetzwidrig erhobenen Navigationsdaten der Nutzer bzw. Kunden innerhalb von sechzig Tagen zu löschen. Des Weiteren erließ die italienische Datenschutzbehörde eine allgemeine Vorschrift zur Speicherung und Verarbeitung der von Telefongesellschaften und Internetanbietern erzeugten Verkehrsdaten. Damit sollte der Schutz derjenigen Verkehrsdaten verbessert werden, deren Vorratsspeicherung den Anbietern (unter anderem zur Durchsetzung gesetzlicher Bestimmungen) gesetzlich vorgeschrieben ist. Die neue Vorschrift regelt eindeutig, wer welche Daten zu speichern hat, und gibt technische und organisatorische Maßnahmen zur Gewährleistung einer sicheren Speicherung der betroffenen Daten vor. Insbesondere bestimmt sie eindeutig, dass die strittigen Pflichten zur Vorratsspeicherung im Sinne der Universaldienstrichtlinie 2002/22/EG sowie der Richtlinien 2002/58/EG und 2002/24/EG nicht für Internet-Inhaltsanbieter, Suchmaschinenbetreiber, Internetcafés und ähnliche Einrichtungen sowie nicht für staatliche Stellen gelten, die ihren Beschäftigten Telefon- und Internetnetze zur Verfügung stellen und/oder von anderen Körperschaften bereitgestellte Server nutzen. Zum Schutz der Daten wurden mehrere technische Maßnahmen vorgeschrieben; dazu gehören beispielsweise strenge Verfahren zur Prüfung der Zugriffsberechtigung, strenge biometrische Verfahren, die eingehende Überprüfung von Datenbanken und Computersystemen, die Verschlüsselung von Datenbanken, die zentralisierte und gesicherte Sammlung von Protokollen sowie physische Vorkehrungen zum Schutz von Computerräumen und Datenzentren.

Formelle Beschwerden

Im Jahr 2007 gab es 316 Entscheidungen zu formellen Beschwerden. Die meisten davon betrafen – wie schon in den Vorjahren – Banken, Finanzdienstleister und Auskunftsteilen. Einige wenige Fälle betrafen die Verarbeitung kaufmännischer Daten (Aktiva und Passiva, Insolvenz-/Liquidationsverfahren usw.) durch die auf diesem Gebiet tätigen Unternehmen; sie hatten die Weisung an diese

Unternehmen zur Folge, allgemein zugängliche Informationen vor der Wiederverwendung eingehend zu kontrollieren, damit ihre Aktualität, Richtigkeit und Vollständigkeit gewährleistet ist.

Anhand mehrerer Fälle, in denen es um die Verarbeitung von Daten zu journalistischen Zwecken ging, konnte die Datenschutzbehörde die Auslegung des Begriffs „personenbezogene Daten“ genauer untersuchen. So wurden Daten mit Bezug auf Personen, die nicht ausdrücklich identifiziert wurden, aber anhand anderer von der datenverantwortlichen (oder einer sonstigen) Stelle gespeicherter Angaben erkennbar waren, als personenbezogene Daten betrachtet. Es wurde jedoch betont, dass alle Mittel zu berücksichtigen seien, die bei angemessener Betrachtungsweise von den für die Datenverarbeitung Verantwortlichen und/oder einer anderen Stelle zur Identifizierung der betroffenen Person eingesetzt werden könnten. Zu erwähnen ist auch ein Fall, bei dem die veröffentlichten Angaben über zwei andere Personen als die Beschwerdeführerin – deren Ehemann angeblich bei einem Autounfall „im Beisein seiner aktuellen Partnerin“ gestorben war – als personenbezogene Daten mit – wenn auch indirektem – Bezug auf die Beschwerdeführerin betrachtet wurden, weil ihre Auswirkungen auch die Beschwerdeführerin betrafen.

Interessanterweise entschied die Datenschutzbehörde, dass die Beschwerde gegen ein Krankenhaus unzulässig sei, weil die Zugriffsanfrage nicht die Abfrage von bei der Klinik aufbewahrten personenbezogenen genetischen Daten zum Ziel hatte, sondern die Lieferung einer Gewebeprobe vom verstorbenen Vater des Beschwerdeführers (konkret ein „Gewebestück in Paraffin“ bzw. eine Blutprobe).

Inspektionen

Die Inspektionsaktivitäten des Datenschutzbeauftragten wurden 2007 ausgeweitet, teilweise auf der Grundlage von der Behörde erstellter 6-Monatspläne. Bei ihren Inspektionen darf die Datenschutzaufsichtsbehörde sich auf die Dienste einer Sonderabteilung 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. Insgesamt wurden

452 Inspektionsverfahren durchgeführt. Sie betrafen vorrangig private Unternehmen und zielten auf die Überprüfung der Einhaltung der wesentlichen im Datenschutzgesetz niedergelegten Anforderungen ab. Die Inspektionsabteilung konzentrierte sich insbesondere auf die Verarbeitung personenbezogener medizinischer Daten durch pharmazeutische Unternehmen und Einrichtungen des Gesundheitswesens, auf die elektronische Verarbeitung von personenbezogenen Daten, auf die Datenverarbeitung für den Fernabsatz von Waren und Dienstleistungen (Callcenter-Anrufe inbegriffen), die Datenverarbeitung in Finanzämtern, die Speicherung der Daten von Nutzern bzw. Kunden durch Telefongesellschaften und elektronische Bankdienstleistungen.

Im Anschluss an die Inspektionen wurden 228 Verfahren zur Verhängung von Verwaltungsstrafen eingeleitet. In 15 strafrechtlich relevanten Fällen wurde die Staatsanwaltschaft eingeschaltet. 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 voraussichtlich Einnahmen von mindestens 725 000 Euro erbringen.

Zu erwähnen sind ferner die Einzelmaßnahmen der italienischen Datenschutzbehörde im Zusammenhang mit internationalen Abkommen und Übereinkommen und hier insbesondere jenen, die den Betrieb des Schengener Informationssystems und der Eurodac-Datenbanken betreffen.

Öffentlicher Dienst

Biometrie. Die Datenschutzbehörde erteilte einer staatlichen Stelle (Amt des Superintendanten für das archäologische Erbe) die Genehmigung, ihren Beschäftigten den Zugang zu einem Hochsicherheitsbereich nur nach einer Handkonturprüfung zu ermöglichen. Das dafür vorgesehene biometrische System prüft lediglich die geometrischen Merkmale der Hände der Beschäftigten und keine sonstigen biometrischen Daten. Der Handkontur wird ein Verschlüsselungsalgorithmus zugewiesen, der im internen Speicher des Systems hinterlegt wird. Der interne Speicher wiederum funktioniert nur örtlich mit Hilfe eines digitalen Kennworts, das der

betroffene Beschäftigte selbst auswählt und eingibt. Diese Vorgehensweise wurde von der Datenschutzbehörde als rechtmäßig und verhältnismäßig beurteilt. Die Handkonturdaten ermöglichen anders als beispielsweise Fingerabdrücke keine Einzelidentifizierung; sie sind aber so ausführlich, dass sie in konkreten Situationen zur Identitätskontrolle ausreichen.

Belegschaftsbelange. Die Datenschutzbehörde erließ Richtlinien für die Verarbeitung personenbezogener Daten von Beschäftigten im öffentlichen Dienst. Sie erstrecken sich auf die Verarbeitung von Gesundheitsdaten, die Abnahme von Fingerabdrücken als Kennung für den Zugang zum Arbeitsplatz und die Verbreitung von Daten im Internet.

Lokale Behörden. Die Datenschutzbehörde erließ Richtlinien für die Verarbeitung personenbezogener Daten mit Bezug auf die Veröffentlichung und Verbreitung von Dokumenten durch lokale Behörden. Für die Daten von beispielsweise in Bekanntmachungen am Schwarzen Brett, in allgemein zugänglichen Dokumenten und/oder in Dokumenten im Internet namhaft gemachten Personen wurden konkrete Schutzvorkehrungen vorgeschrieben, um dem Grundsatz der Transparenz Rechnung zu tragen.

Schulen. Die Datenschutzbehörde stellte klar, dass Eltern von ihren Kindern bei Schultheateraufführungen Film- und Fotoaufnahmen machen dürfen, da die Aufnahmen nicht zur öffentlichen Verbreitung vorgesehen seien und lediglich für private Zwecke zur Weitergabe an Familienangehörige und Freunde gemacht würden. Darüber hinaus verfasste die Datenschutzbehörde in Zusammenarbeit mit dem Bildungsministerium eine Leitlinie für die Nutzung von Bildtelefonen durch Schüler in Schulen.

Gesundheitswesen

- Die italienische Datenschutzbehörde wies die lokalen Gesundheitseinrichtungen an, keine ärztlichen Diagnosen in die Arbeitsunfähigkeitsbescheinigungen einzutragen, die sie für jene Personen ausstellen müssen, die einen Antrag auf Aufnahme in ein Arbeitslosenverzeichnis oder auf Befreiung von Schul- oder Studiengebühren stellen.

- Die Verbreitung der Namen von 4 500 Patienten und von Angaben über ihren jeweiligen Gesundheitszustand auf der Internetseite einer italienischen Region wurde von der Datenschutzbehörde untersagt.
- Die Datenschutzbehörde stellte klar, dass die lokalen Gemeindebehörden keine Namens- und sonstigen Anfragen an Ärzte richten dürfen, um jene Patienten zu identifizieren, bei denen die Ärzte Hausbesuche machen.
- Nach Medienberichten über das Auftauchen mehrerer hundert Krankenakten auf einer Mülldeponie ordnete die Datenschutzbehörde eine Untersuchung an, die mit Hilfe der Finanzpolizei durchgeführt wurde. Gegen die zuständigen Datenverwaltungsstellen wurde Anzeige erstattet, weil sie den Mindestvorschriften für die Ergreifung von Schutzvorkehrungen nicht genügt hatten.
- Die Datenschutzbehörde forderte eine öffentlich-rechtliche Körperschaft nachdrücklich auf, in ihren Zahlungsvordrucken keine konkreten Angaben über die Krankheit des jeweiligen Empfängers und insbesondere nicht über HIV-Infektionen zu machen. Stattdessen empfahl die Behörde eine allgemeine Formulierung und/oder einen Zifferncode.
- In einer Broschüre mit dem Titel „Patientenrechte beim Schutz personenbezogener Daten“ klärte die Datenschutzbehörde die Bevölkerung über die Bedeutung des Datenschutzes bei der Datenverarbeitung durch Ärzteschaft, Pflegepersonal, Gesundheitsbehörden und Labore auf. Die Broschüre informiert kurz und knapp über die Datenschutzrechte der Patienten und die Möglichkeiten für ihre Durchsetzung.

Verarbeitung genetischer Daten

Genetische Daten dürfen nur mit konkreter Genehmigung des Datenschutzbeauftragten (nach Rücksprache mit dem Gesundheitsministerium, das dafür die Meinung des Höheren Gesundheitsrates einholen soll) und schriftlicher Zustimmung des Betroffenen verarbeitet werden.

Die allgemeine Zustimmung des Datenschutzbeauftragten vom Februar 2007 zu dieser Art der Datenverarbeitung füllte eine größere Lücke im Regelwerk. Sie findet auf mehrere Gruppen der für Datenverarbeitung verantwortlichen Stellen vor allem in der Gesundheitsfürsorge und der wissenschaftliche Forschung Anwendung. Auch

das Problem der Nutzung genetischer Daten für die Familienzusammenführung wurde angegangen.

In der Genehmigung werden die wichtigsten Begriffe (genetische Daten, biologische Probe, Gentest) definiert und die Unternehmen und Institutionen aufgeführt, die genetische Daten zu den im Einzelfall bestimmten Zwecken verarbeiten dürfen (Ärzte, öffentliche und private Gesundheitseinrichtungen, Gentechniklabore, natürliche und juristische Personen für wissenschaftliche Forschungszwecke). Der Grundsatz, demzufolge genetische Daten nur dann zu diesen Zwecken verarbeitet werden dürfen, wenn sie tatsächlich unverzichtbar sind, wurde ebenso bestätigt wie die Notwendigkeit, die schriftliche Einwilligung des Betroffenen einzuholen; eine Abweichung von dieser Regelung ist nur zulässig, wenn genetische Daten zum Schutz der genetischen Identität eines Dritten (im Hinblick auf Fortpflanzung oder Behandlung) benötigt werden, welcher derselben Vererbungslinie wie der registrierte Betroffene angehört, und die Einwilligung aus individuellen Gründen (Geschäftsunfähigkeit, körperliche oder geistige Behinderung) nicht erteilt wird, oder wenn statistische Erhebungen strittig sind oder die Forschungstätigkeit gesetzlich geregelt ist.

Die für die Datenverarbeitung verantwortlichen Stellen haben individuelle Pflichten zu erfüllen, die in Bezug auf den Inhalt von Auskünften besonders streng sind. Werden Daten zu gesundheitlichen Zwecken oder zu Zwecken der Familienzusammenführung verarbeitet, ist eine genetische Beratung sowohl vor als auch während des Gentests obligatorisch. Es sind besondere Verarbeitungsvorschriften einzuhalten und strenge Sicherheitsvorkehrungen zu ergreifen; beispielsweise müssen genetische Daten von persönlichen Daten getrennt aufbewahrt und bei Speicherung und Übermittlung verschlüsselt werden. Die Vorratsspeicherungsfrist darf nicht länger sein als für den konkreten Zweck unbedingt notwendig. Die Weitergabe genetischer Daten ist unzulässig.

Privatwirtschaft

Die italienische Datenschutzbehörde ergriff im Jahr 2007 weitreichende Maßnahmen für eine einfachere Anwendung des Datenschutzrechts in der Privatwirtschaft.

Überweisung und Verbriefung von Großbeträgen

In einer (im italienischen Gesetzblatt veröffentlichten) Entscheidung regelte die Datenschutzbehörde den Umgang mit mehreren an sie gestellten Anträgen auf Befreiung der für die Datenverarbeitung verantwortlichen Stellen von der Pflicht zur Auskunftserteilung an die Betroffenen im Zusammenhang mit der Überweisung und/oder Verbriefung von Großbeträgen. Bei derlei Geschäften gibt der Überweisungsabsender personenbezogene Daten der Schuldner an den Überweisungsempfänger weiter. Nach Maßgabe des Datenschutzgesetzbuches kann die Datenschutzbehörde die für die Datenverarbeitung verantwortliche Stelle im Einzelfall von der Auskunftspflicht befreien, sofern die betroffene Verarbeitung auf die von der Datenschutzbehörde vorgeschriebene Art und Weise angemessen publik gemacht wird. Die italienische Datenschutzbehörde entschied, dass die Auskunftserteilung an die einzelnen Betroffenen (die Schuldner) in diesem Fall einen unverhältnismäßig hohen Aufwand darstelle, und befreite die datenverantwortlichen Stellen unter zwei Bedingungen von der Auskunftspflicht. Zum einen mussten sie spätestens bei Wirksamwerden der Überweisung eine umfassende Bekanntmachung im Gesetzblatt veröffentlichen, und zum anderen mussten die Schuldner bei der ersten zweckdienlichen Gelegenheit nach der Überweisung (beispielsweise bei Versand des Kontoauszugs oder bei einer Zahlungsaufforderung) einzeln davon in Kenntnis gesetzt werden, dass der Überweisungsempfänger bei Dritten ihre personenbezogenen Daten erhoben hatte.

Richtlinien für die Überwachung des E-Mail-Verkehrs und der Internetnutzung

Die Datenschutzbehörde veröffentlichte (mit Datum 1. März 2007) eine allgemeine Entscheidung mit Bezug auf die Überwachung des E-Mail-Verkehrs und der Internetnutzung durch öffentlich-rechtliche und private Arbeitgeber. Als Grundlage für die Entscheidung dienten das Gerichtsurteil im Fall Copland gegen Großbritannien und der Standpunkt der Arbeitsgruppe 29. Die italienischen Arbeitgeber müssen ihren Beschäftigten verfassungsgemäß ein angemessenes Maß an Privatsphäre gewähren, damit sie ihre Persönlichkeit frei und ohne Beschränkungen entfalten können. Unter diesen Voraussetzungen strebte die Datenschutzbehörde mit ihren Richtlinien einen Interessenausgleich an, indem

sie einerseits das Recht der Arbeitgeber zur Festlegung der Nutzungsbedingungen (angemessene Disziplinarmaßnahmen inbegriffen) für die den Beschäftigten überlassenen IT-Geräte bekräftigte und andererseits das Recht der Beschäftigten auf schrittweise und nach dem Grundsatz der Verhältnismäßigkeit ausgeführte Kontrollen sowie angemessene Auskunft über die – so gering wie möglich zu haltende – Verarbeitung ihrer Daten bestätigte. In diesem Zusammenhang wurden konkrete Empfehlungen und Verbote ausgesprochen. So soll der Arbeitgeber eine hausinterne und der Unternehmensgröße angepasste Richtlinie erlassen und seine Beschäftigten angemessen über die Bedingungen für den E-Mail-Verkehr sowie für die Nutzung des Internets und anderer elektronischer Einrichtungen informieren und dabei auch mitteilen, ob und in welchem Umfang Kontrollen stattfinden. Darüber hinaus soll der Arbeitgeber konkret festlegen, welche Art Internetseiten als wichtig für die Tätigkeit der Beschäftigten betrachtet wird, und Konfigurationsverfahren und/oder Filter zur Vermeidung bestimmter Vorgänge (beispielsweise Downloads) einsetzen. Für den E-Mail-Verkehr sollen zudem sowohl gemeinsame E-Mail-Konten als auch Einzeladressen für Privatkorrespondenz eingerichtet und jeder Beschäftigte aufgefordert werden, einen vertrauenswürdigen Dritten (beispielsweise einen anderen Beschäftigten) zu benennen, der im Fall seiner Abwesenheit auf seine elektronische Post zugreifen und wichtige Mitteilungen weiterleiten darf. Verboten wurde hingegen jede Arbeitgebermaßnahme, die eine Fernüberwachung der Beschäftigten zum Ziel hat; betreffen derartige Überwachungen die Produktion, die Organisation oder die Arbeitsplatzsicherheit, soll analog zu anderen gesetzlichen Regelungen die Zustimmung der Gewerkschaften eingeholt werden. Unter der Vorgabe des Interessenausgleichs beschloss die Datenschutzbehörde, dass vorbeugende Überwachungsmaßnahmen ohne Zustimmung des Beschäftigten auch schon frühzeitig, d.h. ohne bereits eingeleitete oder geplante Gerichtsverfahren, ergriffen werden dürfen, sofern die beschriebenen Sicherheitsvorkehrungen getroffen worden sind und die Überwachung in dem konkreten Zusammenhang (z. B. Sicherheitsrisiken) dem Grundsatz der Verhältnismäßigkeit genügt.

Vereinfachte Verfahren zur Gewährleistung des Datenschutzes im Versicherungssektor

Die italienische Datenschutzbehörde gestattete den Versicherungsgesellschaften ein neues, vereinfachtes Auskunftsverfahren zur Unterrichtung der Kunden über die Verarbeitung personenbezogener Daten. Dabei wurde den Erfahrungen der letzten Jahre innerhalb der „Versicherungskette“ Rechnung getragen, der unter anderem Mitversicherer und Rückversicherungsgesellschaften angehören. Die Auskunft muss jetzt zwingend dasjenige Versicherungsunternehmen erteilen, das den Versicherungsvertrag mit dem betroffenen Kunden geschlossen hat. Dieses Unternehmen ist für die Unterrichtung des Kunden über jede spätere oder weitergehende Verwendung seiner personenbezogenen Daten – was die Angabe des Verwendungszwecks und des Empfängers einschließt – auch im Namen anderer Firmen in der „Versicherungskette“ verantwortlich, die häufig gar keinen direkten Kontakt mit den Betroffenen haben, auch wenn sie persönliche Angaben von der Versicherungsgesellschaft erhalten und danach möglicherweise verarbeiten. Als Voraussetzung dafür, dass die Unternehmen von diesen vereinfachten Auskunftsverfahren Gebrauch machen können, erließ die Datenschutzbehörde konkrete Sicherheitsvorschriften. So muss die Versicherungsgesellschaft die Kunden darüber in Kenntnis setzen, welche Unternehmen ihre Daten im Zusammenhang mit den einzelnen Verträgen verarbeiten, und ein aktuelles Verzeichnis dieser Unternehmen auf ihrer Internetseite zur Verfügung stellen – zum Teil auch, damit die betroffenen Personen ihre Zugriffsrechte leichter ausüben können. Darüber hinaus muss die Versicherungsgesellschaft in ihrer Auskunft darlegen, zu welchen anderen Zwecken als dem Risikomanagement die Daten verarbeitet werden, und immer dann eine Zustimmung einholen, wenn diese vorgeschrieben und tatsächlich notwendig ist. Das ist allerdings nicht häufig der Fall, weil beispielsweise die Kundendaten für Abschluss oder Durchsetzung des Vertrages unverzichtbar sind. Es wurde jedoch daran erinnert, dass die Verarbeitung von Kundendaten für Werbezwecke einer konkreten Zustimmung bedarf, und dass missbrauchsgefährdete Daten (Krankendaten inbegriffen) von den Versicherungsgesellschaften nur mit schriftlicher Zustimmung der Kunden verarbeitet werden dürfen.

Praxisleitlinien für KMU

Den besonderen Datenschutzbelangen der KMU trug die Datenschutzbehörde in Leitlinien für die Unternehmenspraxis Rechnung. Von der Überlegung ausgehend, dass bestimmte Rechtsvorschriften über den Schutz personenbezogener Daten bisweilen und vor allem von KMU als Belastung betrachtet werden, und zur Stärkung der Ansicht, dass Datenschutz wegen seines stärkenden Einflusses auf das Nutzer- und Kundenvertrauen einen wichtigen Wettbewerbsvorteil darstellen kann, will die italienische Datenschutzbehörde den KMU ein Mittel an die Hand geben, das ihnen die Einhaltung der gesetzlichen Bestimmungen erleichtert und die gegenwärtig nutzbaren Vereinfachungsmaßnahmen darstellen kann. Die Leitlinien verdeutlichen nicht nur die wesentlichen Pflichten jedes Unternehmens, das Daten verarbeitet, und die grundlegenden Datenschutzbegriffe (datenverantwortliche Stelle, datenverarbeitende Stelle, Auskunft und Zustimmung sowie die Mechanismen zur Sicherstellung, dass die Zustimmung vor allem dann fundiert ist, wenn missbrauchsgefährdete Daten verarbeitet werden sollen), sondern sie regeln auch eindeutig, in welchen Fällen die Verarbeitung der italienischen Datenschutzbehörde zu melden ist und welche Schutzvorkehrungen ein Unternehmen im gewöhnlichen Geschäftsverkehr ergreifen muss. Darüber hinaus werden die gegenwärtig vorhandenen Wahlmöglichkeiten für den grenzüberschreitenden Datenverkehr einschließlich der Nutzung einheitlicher Vertragsklauseln beschrieben. Hinzu kommt eine Prüfliste, anhand deren ein Unternehmen feststellen kann, ob alle wesentlichen Maßnahmen zur Einhaltung gesetzlicher Bestimmungen ergriffen worden sind.

Nutzung von Kundendaten durch Callcenter und Telefongesellschaften (ankommende und abgehende Anrufe)

Nach umfassenden Untersuchungen (mit Hilfe der Finanzpolizei) bei den großen Telefongesellschaften und Callcenter-Betreibern in ganz Italien stand fest, dass personenbezogene Daten in mehreren Fällen rechtswidrig verarbeitet und unlautere Verarbeitungsmethoden angewandt worden waren. In fünf Entscheidungen im Jahr 2007 schrieb die Datenschutzbehörde einigen der größten Telefongesellschaften und Callcenter-Betreibern vor, mit welchen Maßnahmen sie für die Einhaltung der Persönlichkeits- und sonstigen Rechte ihrer Nutzer zu sorgen haben. So mussten Unternehmen, die abgehende Anrufe tätigen, sämtliche rechtswidrigen

Datenverarbeitungsschritte (insbesondere die Aktivierung nicht bestellter Leistungen wie beispielsweise Hochgeschwindigkeits-Internetverbindungen) einstellen und die Datenschutzbehörde über ihr Vorgehen zur Ergreifung der in den Entscheidungen bestimmten organisatorischen, technischen und Verfahrensmaßnahmen in Kenntnis setzen (Auskunftserteilung an Nutzer und Einholung ihrer konkreten Zustimmung zur Nutzung von Daten zu Werbezwecken, Aufklärung der Nutzer über die Herkunft und Verwendungsweise der Daten schon bei der ersten Kontaktaufnahme, Dokumentation des Kundenwiderspruchs gegen eine weitere Kontaktaufnahme und Kontrolle der Tätigkeiten von zur Datenverarbeitung eingesetzten Callcenter-Betreibern). Für den Fall von Verstößen gegen ihre Entscheidungen behielt sich die Datenschutzbehörde den Erlass strengerer Bestimmungen wie beispielsweise die Sperrung oder das Verbot der Datenverarbeitung vor.

Mit Bezug auf ankommende Anrufe wurden die Vorschriften im Dezember 2007 vereinfacht, was zum Teil auf die Ergebnisse der Untersuchungen über die Einhaltung der Entscheidungen zu abgehenden Anrufen zurückzuführen war. Die Datenschutzbehörde stellte klar, dass alle Callcenter-Betreiber, die ankommende Kundenanrufe bearbeiten, die Kunden nur dann über die Verarbeitung personenbezogener Daten zu informieren brauchen, wenn die Daten, die von der den Anruf entgegennehmenden Person erhoben werden, für andere Zwecke (z. B. Werbung) verwendet werden sollen. In diesem Fall ist die auf fundierten Informationen beruhende Zustimmung des Betroffenen einzuholen.

Medien

Im Mediensektor wurden im Jahr 2007 mehrere strittige Fragen über Datenschutz und journalistische Tätigkeit geklärt. So stellte die Datenschutzbehörde fest, dass die Veröffentlichung der Gerichtsprotokolle (Abhörprotokolle inbegriffen) laufender Verfahren durch einige Medien gegen geltendes Datenschutzrecht verstieß. Die Protokolle enthielten personenbezogene Daten (unter anderem über das Geschlechtsleben), und ihre Verbreitung verstieß gegen den Grundsatz, dass veröffentlichte Informationen „von wesentlichem öffentlichen Interesse“ zu sein haben. Dieser Grundsatz ist in den journalistischen Verhaltensregeln für den Umgang mit personenbezogenen Daten niedergelegt. In anderen

Fällen wurde festgestellt, dass personenbezogene Daten unter Verletzung von Anstandsregeln und des Grundsatzes der Rechtmäßigkeit erfasst worden waren. Beispielsweise waren unter Verletzung der Privatsphäre Fotos oder ohne Wissen der Betroffenen Filmaufnahmen gemacht worden; von Bedeutung ist, dass die strittigen Fälle auch eine Verletzung der Anstands- und Transparenzpflichten der oben genannten journalistischen Verhaltensregeln darstellten. Ein weiterer Fall betraf Nachrichtenbeiträge über eine Frau, die nach schwerer Krankheit verstorben war. Diese enthielten so viele Identifizierungsdaten, dass nach Auffassung der Datenschutzbehörde sowohl die Bestimmungen des Datenschutzgesetzbuches als auch die journalistischen Verhaltensregeln verletzt worden waren, weil sie auch auf die Verstorbene Anwendung finden. Zu erwähnen ist ferner, dass das Datenschutzgesetzbuch Kindern im Zusammenhang mit Medien und Journalismus einen besonderen Schutz gewährt. Diesem Ziel entsprechend hat der Verband italienischer Journalisten vor einigen Jahren einen Verhaltenskodex (Charta von Treviso) beschlossen, der von der Datenschutzbehörde gebilligt wurde. Trotzdem beanstandete die Behörde viele Fälle, in denen Daten veröffentlicht wurden, die unnötigerweise die Identifizierung von Kindern ermöglichten, die von Rechtsstreitigkeiten (Trennung, Scheidung) und/oder Strafverfahren im Zusammenhang mit sexuellem Missbrauch betroffen waren.



Lettland

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

Die Richtlinie 95/46/EG wurde mit dem Gesetz zum Schutz personenbezogener Daten in nationales Recht übernommen. Das Gesetz trat am 20. April 2000 in Kraft und wurde zuletzt im Jahr 2007 geändert. Die vollständige Unabhängigkeit der lettischen Datenschutzbehörde soll in einem Gesetz geregelt werden, dessen Entwurf der Regierung spätestens Mitte 2008 vorgelegt werden sollte.

Änderungen des Gesetzes zum Schutz personenbezogener Daten

Das Gesetz zum Schutz personenbezogener Daten wurde am 1. März 2007 geändert. Ziel war es, Ausnahmen der Meldepflicht zu bestimmen und das Meldeverfahren für die Verarbeitung personenbezogener Daten zu vereinfachen:

1. Die Ausnahmen sind festgelegt worden.
2. Die Meldung geht nicht an die Systeme für die Verarbeitung personenbezogener Daten, sondern an die für die Datenverarbeitung verantwortlichen Stellen.
3. Es wird ein Beauftragter für den Schutz personenbezogener Daten ernannt.
4. Die Verfahrensregeln über die Übermittlung personenbezogener Daten in Drittländer sind festgelegt worden, und das lettische Kabinett hat einen entsprechenden Verordnungsentwurf erarbeitet.

Kabinettsverordnungen

Mit Bezug auf die Änderungen des Gesetzes zum Schutz personenbezogener Daten hat die lettische Datenschutzbehörde dem Kabinett mehrere Verordnungsentwürfe vorgelegt. Diese betreffen:

- die Zulassung von Prüfern für personenbezogene Daten;
- die Änderung der obligatorischen organisatorischen und technischen Vorschriften für den Schutz personenbezogener Daten;
- die Schulung des Datenschutzbeauftragten;

- einheitliche Vorschriften für Verträge mit Bezug auf die Übermittlung personenbezogener Daten an Drittländer;

Änderungen des Strafrechts

Zur Vereinfachung des Schutzes personenbezogener Daten und zur Vermeidung ihrer rechtswidrigen Verarbeitung sollte ein strafrechtlicher Rahmen für Verstöße gegen die Bestimmungen zum Schutz personenbezogener Daten geschaffen werden. Der entsprechende Gesetzentwurf wurde dem Parlament im Jahr 2007 vorgelegt.

Der Gesetzentwurf sieht für den Fall einer rechtswidrigen Verarbeitung personenbezogener Daten dann eine strafrechtliche Verantwortlichkeit vor, wenn erheblicher Schaden entstanden ist und die Verarbeitung aus Rache oder in Erpressungs- oder anderer Absicht erfolgt ist, oder wenn die Verarbeitung mit Gewalt, Betrug oder Drohungen verbunden ist. Strafrechtlich relevant sollen auch Fälle sein, in denen die notwendigen technischen und organisatorischen Mittel zum Schutz personenbezogener Daten und zur Vermeidung ihrer rechtswidrigen Verarbeitung nicht zur Anwendung kommen und dies einen erheblichen Schaden zur Folge hat, sowie Fälle von rechtswidriger Verarbeitung personenbezogener Daten, die einen erheblichen Schaden zur Folge haben.

Gegenwärtig besteht für die rechtswidrige Verarbeitung personenbezogener Daten lediglich eine verwaltungsrechtliche Verantwortlichkeit mit Abmahnungen, Ordnungsgeldern, dem Verbot der Verarbeitung personenbezogener Daten und der Einziehung der eingesetzten technischen Mittel.

Vorschriften über die Vorratsspeicherung von Daten zur Durchsetzung von Gesetzen

Die Richtlinie 2002/58/EG wird mit dem Gesetz über elektronische Kommunikation in nationales Recht übernommen.

Das lettische Kabinett erließ am 4. Dezember 2007 die Verordnung Nr. 820 über Auskunftersuchen von außergerichtlichen Ermittlungsstellen, den Betroffenen der Ermittlungen, staatlichen Sicherheitsorganen, Staatsanwaltschaften und Gerichten und über die Bereitstellung auf Vorrat gespeicherter Daten durch

die Anbieter elektronischer Kommunikationsleistungen sowie über die Zusammenfassung der Statistiken über die gewünschten Vorratsdaten und ihre Bereitstellung. Seit 2007 ist die Datenaufsichtsbehörde für die Zusammenfassung der Statistiken über die Vorratsspeicherung jener Daten zuständig, die im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Grundlage dafür sind Paragraf 19 des Gesetzes über elektronische Kommunikation und Artikel 10 der 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*.

B. Bedeutende Rechtsprechung

Die meisten wichtigeren Beschwerden, die im Jahr 2007 wegen Verletzungen des Gesetzes zum Schutz personenbezogener Daten bei der Datenaufsichtsbehörde eingingen, betrafen Fälle rechtswidriger Verarbeitung personenbezogener Daten.

Am häufigsten wurden die folgenden Verstöße genannt:

1. falsche und häufig eindeutig rechtswidrige Verarbeitung personenbezogener Daten beim Inkasso von Darlehensforderungen und überfälligen Zahlungen (schwarze Listen) sowie Veröffentlichung personenbezogener Daten im Zusammenhang mit der Instandhaltung von Gebäuden;
2. Verletzung des Rechts auf Zugang zu Informationen – den Betroffenen wurden Informationen unter anderem über ihre Videoüberwachung vorenthalten oder verweigert;
3. Verletzung des Grundsatzes der Verhältnismäßigkeit bei der Verarbeitung personenbezogener Daten, Überschreitung und Ausweitung des ursprünglichen Zwecks der Datenverarbeitung sowie Vervielfältigung von Reisepässen.

C. Wichtige spezifische Themen

Im Jahr 2007 gingen bei der Datenaufsichtsbehörde 120 Beschwerden ein. Bei den Datenschutzinspektionen wurden 30 Verstöße gegen das Gesetz zum Schutz personenbezogener Daten festgestellt. Die Beschwerden betrafen größtenteils die Datenverarbeitung ohne rechtliche Grundlage (50 Prozent der Verstöße im Jahr 2007), Verletzungen der Rechte Betroffener (Artikel 10 und 11 der Richtlinie 95/46/EG) und die Verletzung des Verhältnismäßigkeitsgrundsatzes bei der Datenverarbeitung.

Keine der Entscheidungen der Datenaufsichtsbehörde ist gerichtlich für unwirksam erklärt worden. Sämtliche Einsprüche wurden abgewiesen.

Überwachung unerbetener Werbenachrichten

Nach Maßgabe des Gesetzes über Leistungen für die Informationsgesellschaft kontrolliert die Datenaufsichtsbehörde seit dem 1. Juni 2007 auch den Missbrauch personenbezogener Daten durch unerbetene Werbenachrichten (Spam).

Die Datenaufsichtsbehörde hat eine erste Entscheidung zum Verbot des Versands unerbetener Werbenachrichten (Artikel 13 der Richtlinie 2002/58/EG) gefällt.

Informationsfreiheit und Datenschutz

Ein Diskussionspunkt war die Vorlage von Zahlen und Fakten über Montage- und Renovierungsarbeiten einer staatlichen Stelle in einer Wohnung, die der lettischen Präsidentin nach dem Ende ihrer Amtszeit zur Verfügung stehen würde.

Da die Montage- und Renovierungsarbeiten aus Steuergeldern finanziert wurden, vertrat die Datenaufsichtsbehörde die Auffassung, dass die entsprechenden Ausgaben der staatlichen Stelle offen zu legen seien.

Ein weiterer Fall betraf eine Zeitschrift, die missbrauchsgefährdete Krankendaten (konkret: ein Röntgenbild) veröffentlichte. Die Datenaufsichtsbehörde entschied, dass eine Boulevardzeitschrift derlei medizinische Daten nicht ohne Zustimmung des Betroffenen veröffentlichen dürfe. Die Zeitschrift habe gegen das Gesetz zum Schutz personenbezogener Daten und gegen das Presse- und

Mediengesetz verstoßen, das die Veröffentlichung von Krankendaten in Medien verbietet.

Schengener Informationssystem (SIS)

Vor dem Beitritt Lettlands zum Schengener Abkommen im Dezember 2007 überprüfte die Datenaufsichtsbehörde Institutionen und Behörden, die Zugang zum Schengener Informationssystem (SIS) haben würden. Es wurde geprüft, ob diese Institutionen und Behörden darauf vorbereitet waren, und wie sich das Recht der betroffenen Bürger auf Zugang zum SIS gewährleisten lässt.

Im Jahr 2007 trat das Gesetz zum SIS in Kraft, in dem alle Anforderungen an den Schutz personenbezogener Daten geregelt sind. Darüber hinaus wirkte die Datenaufsichtsbehörde bei der Ausarbeitung der Kabinettsverordnungen über die Verarbeitung personenbezogener Daten und das Recht der Betroffenen mit, Auskunft über die über sie gesammelten Daten und die Ergänzung, Berichtigung oder Löschung dieser Daten aus dem SIS zu verlangen.

Die Datenaufsichtsbehörde gab eine Broschüre in lettischer Sprache mit dem Titel „Personenbezogene Daten im Schengener Informationssystem“ heraus. Eine ähnliche Broschüre in englischer und russischer Sprache wurde in Zusammenarbeit mit dem Büro des slowenischen Datenbeauftragten erstellt.

Untersuchung einzelner Gebiete mit Bezug auf den Datenschutz

Die Datenaufsichtsbehörde veranstaltete in Schulen sowohl für das Leitungs- als auch für das Lehrpersonal Seminare zum Thema Datenschutz. Aufgrund der dabei gesammelten Erfahrungen hat die Behörde den Datenschutz in Schulen zu ihrem Untersuchungsschwerpunkt für das Jahr 2008 erklärt.



Litauen

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

1. Am 19. Dezember 2006 verabschiedete das Parlament (Seimas) der Republik Litauen eine (zum 11. Januar 2007 wirksame) Änderung des Gesetzes über Dokumente und Archive, die eine uneingeschränkte Einsichtnahme in die Urkunden des Sonderteils des nationalen Dokumentenfonds gestattet. Der Sonderteil des Dokumentenfonds besteht aus den Unterlagen der Opposition bzw. der Widerstandsgruppen über ihre Einsätze gegen die Besatzer aus der UdSSR und Deutschland, das Volkskommissariat für interne Angelegenheiten der litauischen sozialistischen Sowjetrepublik (SSR) (von 1940 bis 1941 und von 1944 bis 1946), das Volkskommissariat für die staatliche Sicherheit der litauischen SSR (1941 und von 1944 bis 1946), das Ministerium für Staatssicherheit der litauischen SSR (von 1946 bis 1953), das Ministerium für innere Angelegenheiten der litauischen SSR (von 1946 bis 1954), das Komitee für Staatssicherheit der litauischen SSR (von 1954 bis 1991), das Volkskommissariat für Staatssicherheit der UdSSR (NKGB), das Ministerium für Staatssicherheit der UdSSR (MGB), die Unterabteilungen des Ausschusses für Staatssicherheit der UdSSR (KGB) (in Litauen tätig von 1940 bis 1991), die Unterabteilungen des Volkskommissariats für innere Angelegenheiten der UdSSR (NKVD) und des Ministeriums für innere Angelegenheiten der UdSSR (MVD) (in Litauen tätig von 1946 bis 1954), die Unterabteilungen des Volkskommissariats für Verteidigung der UdSSR (NKO) und des Volkskommissariats (Ministeriums) der Marine (NKVMF) (in Litauen tätig im Jahr 1941 und von 1943 bis 1946), die Unterabteilungen der Geheimdiensthauptdirektion des Generalstabs der Sowjetarmee (GRU) (in Litauen tätig von 1940 bis 1991), die Kommunistische Partei Litauens sowie diesen Organisationen untergeordnete Stellen. Wer sich mit den Unterlagen vertraut zu machen wünscht, muss unter Beifügung eines Identitätsnachweises einen schriftlichen Antrag an die Verwahrungsstelle richten. Der Grund für den Wunsch zur Einsichtnahme braucht nicht angegeben zu werden. Die Einsichtnahme ist nur in den Räumlichkeiten der Verwahrstelle gestattet. Die Gesetzesänderung fixiert ferner eine eingeschränkte Einsichtnahme in Urkunden mit Angaben über Personen,

die eine geheime Zusammenarbeit mit den Geheimdiensten der UdSSR zugegeben haben und in ein Verzeichnis der Geständigen eingetragen worden sind, sowie für jene Fälle, in denen ein Opfer der Geheimdienste der UdSSR ausdrücklich wünscht, die über das Opfer vorhandenen Angaben bis zu seinem Tod nur eingeschränkt verwenden zu lassen.

2. Am 3. April 2007 verabschiedete das Parlament (Seimas) der Republik Litauen eine Änderung des Gesetzes über das Einwohnerverzeichnis, in der geregelt ist, dass Daten über Verwandtschafts- und Verschwägerungsverhältnisse im Einzelfall und unter Angabe des Verwendungszwecks an Vollstreckungsbehörden zur Ausübung ihrer Pflichten und an die Parlamentsausschüsse zur Ausübung ihrer gesetzlichen Aufgaben weitergegeben werden dürfen. Darüber hinaus dürfen Verwandtschaftsdaten nach Maßgabe der Änderung an den Ethikhauptausschuss zur Ausübung der ihm unmittelbar zugewiesenen Aufgaben, an Notare zur Bearbeitung von Erbschaftsangelegenheiten und zur Überprüfung gesetzlicher Einschränkungen für den Abschluss von Verträgen zwischen engen Verwandten des bzw. der Verstorbenen und an Personen weitergegeben werden, die kraft des Gesetzes zur Prüfung von und Entscheidung in Fragen im Zusammenhang mit der litauischen Staatsangehörigkeit befugt sind.

3. Die Datenschutzbehörde erließ mit Verordnung Nr. 1T-45 vom 4. Juli 2007 Musterregeln für die Verarbeitung personenbezogener Daten an Schulen. Mit diesen Regeln sollte eine Verarbeitung personenbezogener Daten an Schulen gewährleistet werden, die dem litauischen Gesetz über den rechtlichen Schutz personenbezogener Daten sowie anderen Gesetzen und sonstigen Rechtsvorschriften über Verarbeitung und Schutz personenbezogener Daten genügen.

B. Bedeutende Rechtssprechung

Familienstammbaum

Bei der Bearbeitung einer persönlichen Beschwerde stellte die Datenschutzbehörde fest, dass Polizeibeamte nach der Verhaftung des Beschwerdeführers wegen eines Verstoßes gegen die Straßenverkehrsordnung zur Identitätsfeststellung die personenbezogenen Daten des Betroffenen überprüft und seine Abstammung

nachvollzogen hatten. Die Verwandtschaftsdaten des Beschwerdeführers wurden dem Ordnungswidrigkeitsformular in gedruckter Form als Nachweis darüber beigefügt, dass der Betroffene den Verstoß begangen hatte. Die Datenschutzbehörde wies die Polizei an, die softwaregestützte Zusammenfassung der im Einwohnerverzeichnis geführten personenbezogenen Daten und die Zusammensetzung der Abstammung des Betroffenen zurückzunehmen, weil die Online-Suchfunktionen rechtlich unbegründet seien und deshalb im Widerspruch zu Artikel 3 Teil 1 (2) des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten ständen.

Die Polizei legte gegen den Bescheid Widerspruch ein mit der Begründung, die Anwendung der Suchsoftware sei zur Ausübung ihrer Pflichten im Sinne des litauischen Polizeigesetzes und zur Erfüllung der Vorschriften des Gesetzes zur Bekämpfung der organisierten Kriminalität, des Gesetzes über Ermittlungsmaßnahmen sowie des Waffen- und Munitionskontrollgesetzes der Republik Litauen notwendig.

Das Verwaltungsgericht des Bezirks Wilna befand, dass die Nutzung der genannten Software den Kriterien einer gesetzmäßigen Verarbeitung personenbezogener Daten im Sinne von Artikel 5 Teil 1 (6) des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten entspreche. In diesem Fall sei die Software, die eine Zusammenfassung der Daten aus dem Einwohnerverzeichnis und die Zusammensetzung des Stammbaums ermögliche, im rechtmäßigen Interesse benötigt worden, nämlich damit die Polizei ihren gesetzlichen Auftrag habe erfüllen können. Das Gericht urteilte, dass die Interessen des Betroffenen in diesem Fall nicht übergeordnet gewesen seien, und forderte die Datenschutzbehörde zur Rücknahme ihrer Weisung auf.

Die Datenschutzbehörde legte gegen die Entscheidung des Verwaltungsgerichts des Bezirks Wilna Berufung vor dem Obersten Verwaltungsgericht Litauens ein.

Das Oberste Verwaltungsgericht Litauens befand, dass die Polizei nicht nur personenbezogene Daten erhoben und verarbeitet, sondern auch den Stammbaum von Einzelpersonen im Verkehrsregister gespeichert habe. Es seien nicht nur personenbezogene Daten von

Verkehrssündern und ihren Familienmitgliedern erhoben und verarbeitet worden, sondern auch Daten von Verwandten ihrer Großeltern, Onkel, Tanten, Geschwister, Cousins und Cousins und sogar von den Kindern der Cousins und Cousins. Eine Frist für die Vorratsspeicherung dieser Daten gebe es nicht. Es gebe ferner keinerlei gesetzliche Bestimmung darüber, dass der Stammbaum von Verkehrssündern im Verkehrsregister gespeichert werden solle oder dürfe. Den Betroffenen sei diese Art der Verarbeitung personenbezogener Daten nicht bekannt. Das Gericht befand, dass die Verarbeitung personenbezogener Daten bei der Zusammensetzung des Stammbaums von Einzelpersonen als Verkehrssünder die Verarbeitung von Daten anderer Personen beinhalte, die weder mit dem begangenen Verkehrsverstoß noch mit den Bestimmungen von Artikel 5 (1) des Polizeigesetzes, Artikel 7 Teil 1 (11) des Gesetzes über Ermittlungsmaßnahmen oder Artikel 17 Teil 1 (9) des Waffen- und Munitionskontrollgesetzes der Republik Litauen zusammenhingen. Diese Daten dürften nach der Zusammensetzung des Stammbaums einer Einzelperson nur für Personen verarbeitet werden, gegen die ermittelt werde, aber nicht für Personen, die einen Verkehrsverstoß begangen hätten. Das Gericht bestätigte die Anordnung der Datenschutzbehörde als wirksam.

Bankunterlagen in Müllsäcken

Die Datenschutzbehörde wurde per E-Mail davon in Kenntnis gesetzt, dass man in der Nähe eines Bankinstituts Müllsäcke voller Bankunterlagen mit personenbezogenen Daten und Kopien von Identitätsnachweisen gefunden habe.

Bei einer Untersuchung, ob die Verarbeitung personenbezogener Daten durch das Bankinstitut rechtmäßig erfolgte, stellte sich heraus, dass die in den Müllsäcken gefundenen Unterlagen und Kopien nicht ordnungsgemäß entsorgt worden waren. Die vorhandenen Reste an Dokumenten und Kopien ermöglichten das Erkennen personenbezogener Daten und sogar die Identifizierung einer natürlichen Person. Im Einzelnen wurde festgestellt, dass die Bank im Einklang mit den Bestimmungen von Artikel 24 (1) des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten geeignete organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder rechtswidriger Vernichtung, Veränderung und

Weitergabe sowie sonstiger rechtswidriger Verarbeitung ergriffen hatte. Allerdings erfolgte die Vernichtung der für eine weitere Bearbeitung verzichtbaren Unterlagen und Kopien nicht ordnungsgemäß, so dass die darin enthaltenen personenbezogenen Daten erkennbar blieben und in den Müllsäcken für Dritte zugänglich waren und sich anhand der nur teilweise zerstörten Dokumente und Kopien personenbezogene Daten erkennen und zugehörige natürliche Personen identifizieren ließen. Folglich hatten die mit der Vernichtung beauftragten Beschäftigten der Bank die personenbezogenen Daten nicht vertraulich behandelt und gegen Artikel 24 (5) des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten verstoßen. Gegen sie wurde ein Ordnungswidrigkeitsverfahren eingeleitet. Das angerufene erstinstanzliche Gericht bestätigte in seiner Entscheidung, dass die beschuldigten Beschäftigten die Ordnungswidrigkeit begangen hatten.

C. Wichtige spezifische Themen

Verarbeitung personenbezogener Daten zu Wahlkampfwzwecken

Während des Kommunalwahlkampfes 2007 beklagten sich zahlreiche aufgebrachte Wähler bei der Datenschutzbehörde darüber, dass eine Partei oder ein Kandidat sie postalisch aufgefordert habe, ihr bzw. ihm ihre Stimme zu geben. In Reaktion auf diese Beschwerden überprüfte die Datenschutzbehörde die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zu Wahlkampfwzwecken und von Daten in allgemeinen Wählerverzeichnissen durch Parteien, Gewerkschaften und politische Organisationen.

Nach Maßgabe des litauischen Kommunalwahlgesetzes dürfen sich diejenigen Parteien, die im staatlichen Register der für Datenverarbeitung verantwortlichen Stellen eingetragen sind, allgemeine Wählerverzeichnisse (in elektronischer oder gedruckter Form) beschaffen, aus denen Vorname, Zuname, Adresse und Geburtsdatum der Wähler hervorgehen. Hat ein Wähler auf die gesetzlich vorgeschriebene Art und Weise zum Ausdruck gebracht, dass er mit der Veröffentlichung seiner Adresse oder seines Geburtsdatums in allgemeinen Wählerverzeichnissen nicht einverstanden ist, so dürfen nur sein Vor- und Zuname darin erfasst werden. Darüber hinaus dürfen politische Parteien Wählerverzeichnisse

weder an Dritte weitergeben noch sie zu anderen als Wahlkampfwzwecken verwenden. Die erhaltenen Daten haben sie binnen 30 Tagen nach Bekanntgabe des amtlichen Endergebnisses der Wahl zu vernichten.

Im staatlichen Register der für Datenverarbeitung verantwortlichen Stellen waren acht Parteien erfasst, die personenbezogene Wählerdaten zu Wahlkampfwzwecken verarbeiten wollten. Im Verlauf der Untersuchungen stellte sich heraus, dass zwei der acht eingetragenen Parteien von der Möglichkeit zur Beschaffung allgemeiner Wählerverzeichnisse keinen Gebrauch gemacht hatten. Sechs Parteien hatten Verzeichnisse erhalten, aber nur vier hatten persönliche Wahlkampfbriefe verschickt.

Schwere Verstöße gegen das litauische Gesetz über den rechtlichen Schutz personenbezogener Daten wurden lediglich bei einer der sechs Parteien festgestellt. Bei den übrigen fünf lagen unterschiedliche Übertretungen des Gesetzes vor: Regelungen für organisatorische und technische Maßnahmen zum Schutz personenbezogener Daten vor versehentlicher oder rechtswidriger Vernichtung, Veränderung und Weitergabe sowie sonstiger gesetzwidriger Verarbeitung waren nicht dokumentiert; es war nicht gewährleistet, dass personenbezogene Daten ausschließlich von Befugten verarbeitet wurden und diese Befugten schriftlich zur vertraulichen Behandlung personenbezogener Daten verpflichtet wurden; der Datenschutzbehörde wurden keine genauen Angaben über die Verarbeitung personenbezogener Daten gemacht; die als Datenverarbeitungspersonal ausgewählten Personen waren dafür nicht geeignet und zudem nicht ordnungsgemäß zur Verarbeitung personenbezogener Daten befugt; die Sicherheit personenbezogener Daten, geeignete technische Datenschutzmaßnahmen und die angemessene Vernichtung der den Datenverarbeitern übergebenen personenbezogenen Daten waren nicht gewährleistet. Die Parteien wurden von den festgestellten Verletzungen des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten in Kenntnis gesetzt und erhielten entsprechende Weisungen.

Verarbeitung von Videoüberwachungsdaten in Einkaufszentren

Die Datenschutzbehörde überprüfte aus eigener Initiative vier Einkaufszentren auf Umfang und Rechtmäßigkeit der

Verarbeitung von Videoüberwachungsdaten. An allen vier Standorten wurden Verstöße gegen das litauische Gesetz über den rechtlichen Schutz personenbezogener Daten festgestellt. So war der Datenschutzbehörde die Videoüberwachung von Besuchern der Einkaufszentren in keinem Fall gemeldet worden. An drei der vier Standorte erstreckte sich die Videoüberwachung auch auf Bereiche außerhalb des Einkaufszentrums (beispielsweise Straßenkreuzungen, Wohnhäuser, Tankstellen, Bargeldautomaten, Grundstücke anderer Unternehmen). Folglich wurden übermäßig viele personenbezogene Daten verarbeitet.

In drei Einkaufszentren wurde überhaupt nicht auf die Videoüberwachung aufmerksam gemacht. Im vierten gab es zwar entsprechende Aushänge an den Eingängen, aber man befand sich schon im Überwachungsbereich (z. B. auf dem Parkplatz), bevor man sie lesen konnte. Über die Verarbeitung der mittels Videoüberwachung beschafften personenbezogenen Daten, die eingebauten Sicherheitseinrichtungen und die Standorte der Überwachungskameras gab es keinerlei Unterlagen.

In einem der Einkaufszentren wurden in der Nähe einer Überwachungskamera Fotos von Ladendieben mit Namen, Kopien von Identitätsnachweisen und Unterlagen mit personenbezogenen Daten gefunden. Sie stammten von der Polizei. In der Nähe einer anderen Überwachungskamera wurden Fotos von verhafteten Ladendieben und ihren Kindern gefunden. Die Betreiber der zwei Zentren machten geltend, die Daten seien zur Personenidentifizierung und Diebstahlsvermeidung in ihren Zentren notwendig. Eine Veröffentlichung oder Weitergabe an Dritte sei nicht vorgesehen, und außerdem könne nur das Sicherheitspersonal auf die Daten zugreifen. Die Datenschutzbehörde stellte fest, dass für eine Diebstahlsvermeidung übermäßig viele personenbezogene Daten (Personalausweisnummern, Vorstrafen, Familienstand, für die Diebstahlsvermeidung unerhebliche Fotos von Kindern usw.) erhoben wurden. Die Betreiber der Einkaufszentren wurden von den festgestellten Verletzungen des litauischen Gesetzes über den rechtlichen Schutz personenbezogener Daten in Kenntnis gesetzt und erhielten entsprechende Weisungen.

Aufklärung der Öffentlichkeit

1. Am 26. Januar 2007 organisierten die litauische Datenschutzbehörde und das europäische Informationszentrum des litauischen Parlaments im Informationszentrum des litauischen Parlamentsausschusses für europäische Angelegenheiten mehrere Veranstaltungen aus Anlass des Europäischen Datenschutztages. Dazu gehörten eine Pressekonferenz zum Thema „Der Schutz personenbezogener Daten in Litauen“, eine Konferenz mit dem Titel „Probleme und Zukunft des Schutzes personenbezogener Daten“ sowie Gespräche mit Experten der Datenschutzbehörde. Schwerpunktthemen der Pressekonferenz und der Vorträge waren Videoüberwachung, der Gebrauch biometrischer Daten und der Datenschutz in der elektronischen Kommunikation. Über ihre Diskussionsbeiträge hinaus leisteten die Experten der Datenschutzbehörde auch Beratung in Fragen des Schutzes personenbezogener Daten.

2. Im Jahr 2007 beging die litauische Datenschutzbehörde den zehnten Jahrestag ihres Bestehens. Am 15. November 2007 stellte sie ihre Arbeit den öffentlichen Einrichtungen des Landes vor, und vom 13. bis 14. November 2007 fand die internationale Konferenz „Datenschutz Tendenzen in der Informationsgesellschaft“ statt. Im Mittelpunkt der Konferenz standen die raschen Fortschritte in der Informationstechnologie, ihre schnelle Verbreitung in Litauen und ihre positiven Aspekte, aber auch Maßnahmen zum Schutz der Privatsphäre vor der wachsenden Bedrohung durch die Erfassung und Verarbeitung von immer mehr personenbezogenen Daten. Diese Gefährdung der Privatsphäre hat ein größeres Interesse an entsprechenden Datenschutzmaßnahmen zur Folge. Die Konferenzbeiträge befassten sich daher mit dem Problem der Identifizierung von Personen im elektronischen Geschäfts- und Behördenverkehr sowie mit der Erbringung staatlicher Leistungen auf elektronischem Wege, mit der Vorratsspeicherung von Daten gemäß Richtlinie 2006/24/EG und der Umsetzung dieser Richtlinie, mit dem Schutz der Persönlichkeitsrechte bei Veröffentlichung von Gerichtsurteilen und Entscheidungen staatlicher Stellen sowie mit der Verarbeitung von Videoüberwachungsdaten und den personenbezogenen Daten von Beschäftigten. Auf der Konferenz fand nicht nur ein Erfahrungsaustausch zwischen den Mediatoren staatlicher und privater Institutionen aus Litauen statt, sondern auch Datenschutzbeauftragte und Vertreter von Datenschutzinstitutionen aus dem Ausland kamen zu Wort.



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)

Am 1. September 2007 trat das Gesetz vom 27. Juli 2007 zur Änderung von Bestimmungen des Gesetzes vom 2. August 2002 in Kraft. Mit diesem neuen Gesetz sollten mehrere der alten, als unnötige bürokratische Belastung empfundenen Bestimmungen erheblich vereinfacht werden. Ein merklich höherer Schutz der Datensubjekte war nicht beabsichtigt. Als wichtigste Änderungen sind zu nennen:

- eine erhebliche Ausweitung der an Bedingungen geknüpften Befreiungen von der Pflicht zur Meldung aktueller Datenverarbeitungsumstände;
- eine Ausweitung der Befreiungen von der Meldepflicht für bestimmte Berufe;
- die Vereinfachung der Ernennung eines Datenschutzbeauftragten, der jetzt auch ein Beschäftigter der für die Datenverarbeitung verantwortlichen Stelle sein kann;
- die Herausnahme juristischer Personen aus dem Geltungsbereich des Gesetzes;
- die Änderung wichtiger Begriffsbestimmungen (Zustimmung, personenbezogene Daten, Überwachung usw.);
- die Änderung der Bestimmungen über die Verarbeitung besonderer Datenkategorien;
- die Einführung zusätzlicher Gründe für die Legitimation der Datenverarbeitung zu Überwachungszwecken;
- die Videoüberwachung Dritter ohne Aufzeichnung der erzeugten Bilder, die künftig von der obligatorischen Vorabprüfung (Genehmigung durch die nationale luxemburgische Datenschutzkommission/Commission nationale pour la protection des données/CNPD) ausgenommen ist.

Gesetz vom 30. Mai 2005 über Sonderregelungen zum Schutz der Privatsphäre im Bereich elektronische Kommunikation (Umsetzung der Richtlinie 2002/58/EG)

Das Änderungsgesetz vom 27. Juli 2007 enthält auch Änderungen des Gesetzes vom 30. Mai 2005. Der

luxemburgische Gesetzgeber wollte mit Hilfe einer eindeutigeren Formulierung einiger Bestimmungen des ursprünglichen Gesetzestextes für eine genauere Umsetzung der Bestimmungen von Richtlinie 2002/58/EG sorgen. Darüber hinaus wurde die Frist für die Vorratsspeicherung von Verkehrsdaten ausdrücklich von 12 auf 6 Monate verkürzt.

Verordnungen und abgeleitetes Recht

In der luxemburgischen Verordnung vom 12. Juni 2007 sind die Modalitäten für die Errichtung des bei der luxemburgischen Handelskammer geführten Registers für Dienstleistungen erbringende juristische Personen geregelt. Unter anderem schreibt die Verordnung genau vor, welche Datenkategorien in einem solchen Register zu erfassen sind.

Die luxemburgische Verordnung vom 1. August 2007 genehmigt Errichtung und Gebrauch eines Videoüberwachungssystems in öffentlichen „Sicherheitsbereichen“ durch die Polizei. Sie sieht aber auch zahlreiche Vorkehrungen zum Schutz personenbezogener Daten vor, unter anderem wird der Zugriff auf die Überwachungsdaten streng kontrolliert und die Speicherung der Daten auf zwei Monate befristet. In der Verordnung vom 27. September 2007 ist ausdrücklich bestimmt, welche Bereiche als „Sicherheitsbereiche“ zu erachten sind und in welchen die Videoüberwachung stattfinden darf.

In der luxemburgischen Verordnung vom 21. Dezember 2007 sind die Höhe der Gebühr, die von der CNPD für eine Genehmigung oder eine Genehmigungsänderung einzuziehen ist, und die Zahlungsweise geregelt.

Weitere Entwicklungen in der Gesetzgebung

Die luxemburgische Regierung hat die CNPD um ihre Meinung zum Gesetzentwurf über die Verwaltungs- und die juristische Zusammenarbeit zwischen staatlichen Stellen gebeten. Die CNPD hat sowohl in ihrer Erstempfehlung als auch in ihren Folgeempfehlungen darauf hingewiesen, dass der Begriff „Datenzusammenfassung“ in dem Gesetzentwurf nicht den Bedingungen des Gesetzes von 2002 für eine rechtmäßige Verarbeitung entspreche. Folglich empfahl die CNPD dem Gesetzgeber, die Begriffsbestimmungen im Gesetzentwurf zu überprüfen, für Garantien mit Bezug auf bestimmte Datenkategorien zu sorgen, die unterschiedlichen Arten

der verwaltungsstellenübergreifenden Zusammenarbeit zu bestimmen und Garantien für die Geheimhaltung von Daten festzulegen. Die luxemburgische Regierung nahm die Empfehlungen der CNPD an.

Die CNPD beriet die Regierung ferner zu aktuellen Themen wie beispielsweise die Entwürfe von Gesetzen über katasteramtliche Mietrecherchen, über Errichtung und Gebrauch des allgemeinen Polizei-Informationssystems und über das neue Kindergeld sowie die Verordnung über die Bestimmung der zehn bei öffentlich-rechtlichen Körperschaften geführten Datenbanken, auf die Verwaltungs- und Polizeibeamte unmittelbaren Zugriff haben werden.

B. Bedeutende Rechtssprechung

Zivil- und Strafverfahren

Entscheidung des Bezirksgerichts Luxemburg, Berufungsgericht, 10. Strafkammer, über die Wirksamkeit von unter Verletzung des Datenschutzgesetzes von 2002 gesammelten Beweisen (Videoüberwachungsbilder)

Das Urteil der 9. Strafkammer vom 13. Juli 2006, dass ein unter Verletzung des Datenschutzgesetzes von 2002 beschaffter Beweis unzulässig sei und im Gerichtsverfahren nicht berücksichtigt werden dürfe, wurde am 28. Februar 2007 von der 10. Strafkammer des Berufungsgerichts bestätigt.

Das Urteil des Berufungsgerichts wurde vor dem Obersten Berufungsgericht (Cour de Cassation) angefochten und von diesem aufgehoben. Dabei berief sich das Oberste Berufungsgericht auf Artikel 6 der Europäischen Menschenrechtskonvention und das Recht auf eine faire Verhandlung. Nach Aufzählung der unterschiedlichen Hypothesen, aufgrund deren ein Richter rechtswidrig beschaffte Beweise ablehnen kann, urteilte das Gericht, dass ein Richter einen rechtswidrig beschafften Beweis trotzdem zulassen könne, wenn er die Elemente des Verfahrens insgesamt und dabei unter anderem die Art und Weise der Beweisbeschaffung und die Umstände berücksichtige, unter denen die rechtswidrige Handlung begangen worden sei. Nach Auffassung des Obersten Berufungsgerichts hatte das Berufungsgericht von vornherein nicht alle Elemente des Falles berücksichtigt und damit gegen Artikel 6 der Europäischen

Menschenrechtskonvention verstoßen. Folglich hob das Oberste Berufungsgericht die Entscheidung auf und verwies den Fall zur Neuverhandlung zurück an das Berufungsgericht.

Das neu zusammengesetzte Berufungsgericht entschied am 26. Februar 2008, dass die Vorlage eines gesetzwidrig beschafften Beweises in einem Gerichtsverfahren (*d. h. ohne Einwilligung der CNPD*) in Kombination mit einem Verfahren, das selber nicht den Bestimmungen über die Ausübung von Strafverfahren und gerichtlichen Untersuchungen entspreche, eine Verletzung des Rechts auf eine faire Verhandlung zur Folge habe.

Bezirksgericht Luxemburg, 12. Strafkammer, über die Verletzung von Artikel 5 und 6 des Datenschutzgesetzes von 2002

Am 11. Oktober 2007 erließ die 12. Strafkammer des Bezirksgerichts Luxemburg unter Berufung auf das Datenschutzgesetz von 2002 ein erstes Urteil gegen eine Einzelperson. Ein luxemburgischer Journalist hatte über seine Wochenzeitung und seine Internetseite eine Liste mit den Namen der Mitglieder der französischen Freimaurerloge „Grande Loge de France“ öffentlich preisgegeben, in Umlauf gebracht und verkauft. Die Veröffentlichung solcher Listen war zuvor von der französischen „Commission Nationale de l'Informatique et des Libertés“ (CNIL) verboten worden. Die CNIL war es auch, die der luxemburgischen Datenschutzbehörde das Vergehen anzeigte. Die CNIL untersuchte den Fall. Sie entschied, dass ein Verstoß gegen das Datenschutzgesetz von 2002 vorliege, und erstattete Anzeige bei der Staatsanwaltschaft. Das Bezirksgericht Luxemburg trat in seinem Urteil die Auffassung, dass der Journalist gegen Artikel 6 (5) (Weitergabe bestimmter Datenkategorien an Dritte) und 5 (2) (die Datenverarbeitung durch den Journalisten erfüllte keine der Rechtmäßigkeitsbedingungen des Gesetzes) des Datenschutzgesetzes von 2002 verstoßen habe.

Verwaltungsverfahren

Am 21. Mai 2007 wies das Verwaltungsgericht den Antrag auf Aufhebung einer Entscheidung der CNIL ab, in der die CNIL die Videoüberwachung in einem Einkaufszentrum insgesamt gestattete, aber die dauerhafte Videoüberwachung von zwei Befragungszimmern untersagte.

Das Argument der CNIL, das Datenschutzgesetz von 2002 räume dem Eigentümer des Einkaufszentrums keinerlei Befugnis ein, die Befragung mutmaßlicher Ladendiebe aufzuzeichnen, wurde vom Verwaltungsgericht bestätigt. Die genannte Entscheidung wurde am 13. Dezember 2007 vom Verwaltungsberufungsgericht bestätigt.

C. Wichtige spezifische Themen

Im Verlauf des Jahres 2007 führte die CNPD eine umfassende Überprüfung der größten luxemburgischen Telefongesellschaften durch, um sich einen Überblick darüber zu verschaffen, wie die Unternehmen die Bestimmungen des Gesetzes vom 30. Mai 2005 zur Umsetzung der Richtlinie 2002/58/EG erfüllten.

Im Jahr 2007 überprüfte die CNPD aufgrund der ihr mit dem Gesetz von 2002 übertragenen Ermittlungsbefugnisse die Einhaltung eines Gerichtsurteils, mit dem ein Antrag auf Videoüberwachung abgelehnt worden war. Die Überprüfung ergab, dass in keinem der kontrollierten Geschäfte eine Videoüberwachung in Betrieb war und somit kein Verstoß gegen das Urteil vorlag.

Die CNPD setzte ihre Aufklärungskampagne unter anderem dadurch fort, dass sie sich am ersten Europäischen Datenschutztag des Europarates beteiligte. Im Zuge dieser Beteiligung informierte die CNPD auf ihrer Internetseite und in Interviews mit den luxemburgischen Medien über die neuen gesetzlichen Bestimmungen.



Malta

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

Die Richtlinie 95/46/EG wurde mit Kapitel 440 des maltesischen Datenschutzgesetzes in inländisches Recht umgesetzt. Das vollständige Datenschutzgesetz trat im Juli 2003 in Kraft und sah für die Meldung automatischer Datenverarbeitungsprozesse eine Übergangsphase bis Juli 2004 vor. Bestimmte Vorschriften über manuelle Ablagesysteme treten spätestens im Oktober 2007 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 Kommunikation 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. Bedeutende Rechtssprechung

Keine nennenswerte.

C. Wichtige spezifische Themen

Im Berichtsjahr gingen beim maltesischen Datenschutzkommissar 37 Beschwerden ein, die überwiegend den ordnungswidrigen Einsatz von Überwachungskameras betrafen. Im Verlauf seiner Ermittlungen führte der Datenschutzkommissar 7 Prüfungen aus, drei davon nach einer Beschwerde und die übrigen als regelmäßige Kontrolle aufgrund der EU-Vorschriften.

Im Jahr 2007 traf sich der Datenschutzkommissar regelmäßig mit Vertretern von Staat und Wirtschaft aus den Bereichen Finanzen, Journalismus, Versicherungen, Sozialfürsorge, Bildung, Sicherheit, Glücksspiele und Polizei zu Gesprächen über den Datenschutz und die Ausarbeitung von Branchenrichtlinien für die Datenverarbeitung. Mit den Anbietern elektronischer Kommunikationsleistungen führte der Datenschutzkommissar konkrete

Gespräche über die Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden. Darüber hinaus setzte der Datenschutzkommissar seine enge Zusammenarbeit mit anderen Aufsichtsbehörden, Verbänden und Vereinigungen fort.

Des Weiteren beteiligte sich der Datenschutzkommissar an den europäischen und internationalen Foren durch Teilnahme an den Sitzungen der Art. 29 Arbeitsgruppe Datenschutz, an der Europäischen Konferenz der Datenschutzbehörden, an der Internationalen Konferenz zum Schutz der Persönlichkeitsrechte und personenbezogener Daten, an den Sitzungen der gemeinsamen Aufsichtsbehörden von Schengen, Zoll, Europol und Eurodac, am Seminar Fallbearbeitung, an den Sitzungen des Europarates und von Eurojust sowie an den Sitzungen des beratenden Ausschusses für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

In Informationsschreiben an Organisationen und verfassungsmäßige Behörden versuchte der Datenschutzbeauftragte, das Bewusstsein der wichtigsten Beteiligten für den Datenschutz weiter zu schärfen und sie in die Entwicklung einer Datenschutzkultur einzubeziehen. In der lokalen Presse sowie in Rundfunk und Fernsehen wurden Artikel und Beiträge zu verschiedenen Aspekten des Datenschutzes abgedruckt bzw. ausgestrahlt. Daraufhin gingen beim Datenschutzkommissar per Telefon und E-Mail zahlreiche Anfragen ein.

Am 28. Januar feierte der Datenschutzkommissar zusammen mit den anderen europäischen Datenschutzbehörden erstmals den Europäischen Datenschutztag. Dieser Tag fällt mit dem Tag der Unterzeichnung der Konvention 108 des Europarats mit dem Titel „Übereinkommen zum Schutz des Menschen bei der automatischen Datenverarbeitung personenbezogener Daten“ im Jahr 1981 in Straßburg zusammen. Der Datenschutztag stellte eine gute Gelegenheit dar, den europäischen Bürgern ihr Recht auf Privatsphäre im datenschutzrechtlichen Sinne näher zu erläutern.

Die Art. 29 Datenschutzgruppe, das Forum für die europäischen Datenschutzbehörden, erläuterte in einem anlässlich des Datenschutztages gefassten Beschluss, dass diese Initiative in einer Zeit der allumfassenden Datenverarbeitung hervorragend verdeutliche und verstehen lasse, wie notwendig der Schutz der Privatsphäre in einer demokratischen Gesellschaft sei. Zwischen den Behörden bestand Einvernehmen darüber, dass die Zusammenarbeit mit dem Europarat gestärkt werden müsse, damit dieser Datenschutztage ein Erfolg und deutlich gemacht werde, dass man den Schutz der Grundrechte am besten den Datenschutzbehörden überlasse.

Der Datenschutzkommissar gab im Vorfeld des Datenschutztages über das Informationsministeriums eine Pressemitteilung heraus, nahm an einer Sendung im Bildungsfernsehen teil und verteilte Informationsmaterial einschließlich Plakate und Lineale an Schulkinder. Des Weiteren nahm er mit Unterstützung des Ministerpräsidentenbüros Kontakt mit allen Datenschutzbeauftragten des öffentlichen Dienstes auf.



Niederlande

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

Die Richtlinie 95/46/EG wurde per *Wet bescherming persoonsgegevens (Wbp)* [niederländisches Datenschutzgesetz] in nationales Recht umgesetzt. Das Gesetz vom 6. Juli 2000⁹ trat am 1. September 2001 in Kraft und ersetzte damit das alte Datenschutzgesetz *Wet persoonsregistraties (Wpr)* vom 28. Dezember 1988.

Die Richtlinie 2002/58/EG wurde insbesondere durch das geänderte Telekommunikationsgesetz (*Telecommunicatiewet*), das am 19. Mai 2004¹⁰ in Kraft trat, in niederländisches Recht umgesetzt. 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 Einhaltung des niederländischen Datenschutzgesetzes liegt nicht nur im Interesse der einzelnen Bürger. Die Achtung der Privatsphäre dient auch dem kollektiven Interesse: In einer Gesellschaft, in der wir davon ausgehen können, dass unsere personenbezogenen Daten nicht missbraucht werden, kann man Regierung, Unternehmen, Institutionen und den Mitbürgern untereinander Vertrauen entgegen bringen.

2007 änderte die niederländische Datenschutzbehörde *College Bescherming Persoonsgegevens* (CBP) ihre strategische Ausrichtung und kümmerte sich vermehrt um die Durchführung von Untersuchungen und Durchsetzungsmaßnahmen – Kernaufgaben jeder unabhängigen Aufsichtsbehörde –, um ein größeres

Bewusstsein für Normen zu schaffen und eine stärkere, wirksamere Durchsetzung hinsichtlich der Einhaltung von Rechtsvorschriften sicherzustellen. Natürlich erfordern derartige Maßnahmen vorab eine entsprechende Klarheit hinsichtlich der Normen, die den Handlungen der Datenaufsichtsbehörde zugrunde liegen. Damit dieser Kurswechsel hin zu Normierung, Untersuchung und Durchsetzung gelingt, kümmert sich die Datenaufsichtsbehörde bei den Anträgen auf Hilfe und Unterstützung angesichts des ihr zugewiesenen Budgets vorrangig um schwere Verstöße struktureller Art und um Verstöße, die erste Folgen für eine beträchtliche Anzahl von Bürgern oder für Gruppen von Bürgern mit sich bringen. Die Zunahme und Erweiterung allgemeiner Informationen auf der Website der niederländischen Datenschutzbehörde unterstützt die Bürger dabei, ihre Probleme selbst anzugehen und zu lösen und gegebenenfalls auch eigene Maßnahmen zu ergreifen.

Mit anderen Worten: Die niederländische Aufsichtsbehörde, deren Aufgabe es ist, größtmöglichen Einfluss auszuüben, um die Einhaltung der gesetzlichen Bestimmungen sicherzustellen, die ihrer Kontrolle unterliegen, hat im vergangenen Jahr verstärkt damit begonnen, eine allgemeine Informationspolitik zu betreiben. Ziel ist es dabei, Bürger, Selbstständige und Organisationen verstärkt in die Lage zu versetzen, ihre Rechte und Pflichten genau zu kennen und diese einzuhalten (oder für deren Einhaltung Sorge zu tragen). Die Datenaufsichtsbehörde hat ferner damit begonnen, die Aufgaben vorrangig zu behandeln, die einer leistungsfähigen und effektiv arbeitenden Aufsichtsbehörde obliegen: Überprüfung der Verfahren zur Einhaltung der einschlägigen gesetzlichen Bestimmungen und Ergreifung von Durchsetzungsmaßnahmen bei Feststellung von Verstößen.

Genau wie in den vergangenen Jahren stand 2007 eine groß angelegte Datenerhebung und -verarbeitung wieder ganz oben auf der Tagesordnung der niederländischen Datenschutzbehörde. Auf nationaler Ebene stellt der Schutz der Privatsphäre in Bezug auf die *OV-chipkaart* (digitale Nahverkehrsfahrkarte) und die *Elektronisch Patiëntendossier* (elektronische Patientenakte) ein Kernthema dar. Diese und andere Themen werden in der nachfolgenden Auswahl der 2007 ergriffenen Maßnahmen kurz erläutert.

⁹ 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.cbppweb.nl.

¹⁰ 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.

Gesundheitswesen

Die niederländische Datenschutzbehörde äußerte ihre Bedenken hinsichtlich des Entwurfs für eine Rechtsvorschrift, welche die Einführung einer elektronischen Patientenakte vorsieht. Nach Meinung der niederländischen Datenschutzbehörde birgt der uneingeschränkte Zugriff aller Leistungserbringer auf die Patientenakten zu viele Risiken, zum Teil im Hinblick auf den Schutz besonders sensibler personenbezogener Daten. Mit Ausnahme von Notfällen sollte nur Leistungserbringern, die mit einem Patienten in einer Behandlungsbeziehung stehen, Zugriff auf die entsprechenden Akten gewährt werden. Anderenfalls besteht die Gefahr von missbräuchlicher oder rechtswidriger Verwendung medizinischer Daten durch unbefugte Dritte.

2007 riet die niederländische Datenschutzbehörde außerdem davon ab, die Anlegung eines *elektronisch kinddossier jeugdgezondheidszorg* (elektronische Akte jedes Neugeborenen für die Jugendgesundheitsfürsorge) im Rahmen der Gesetzesvorlage über Jugendgesundheitsfürsorge und Infektionskrankheiten zwingend vorzuschreiben. Die Notwendigkeit einer zentralen elektronischen Datenspeicherung war nicht ausreichend begründet. Inzwischen hat das Kabinett verlauten lassen, dass es nicht mehr an der Anlegung einer zentralen elektronischen Akte für jedes Neugeborene interessiert ist, sondern nach anderen Wegen sucht, um Informationen im Bereich der Jugendgesundheitsfürsorge auszutauschen.

Öffentliche Verwaltung

Ende November 2007 wurde die BSN [Bürgerservicenummer] eingeführt. Sie markiert den Beginn einer neuen Phase für die niederländische Datenschutzbehörde. Innerhalb der BSN-Verwaltungseinheit wird eine personenbezogene öffentliche Servicestelle eingerichtet, an die sich lokale Behörden und Bürger mit ihren Fragen wenden können. Die niederländische Datenschutzbehörde verfügt für die Kontrolle des sorgfältigen Umgangs mit personenbezogenen Daten über die erforderlichen Amtsbefugnisse, um im Falle von tatsächlichen Problemen bei der Umsetzung des Gesetzes einzugreifen.

Des Weiteren äußerte die niederländische Datenschutzbehörde Kritik an dem vorgeschlagenen *verwijsindex risicojongeren (VIR)* (nationales Register gefährdeter

Jugendlicher). Die niederländische Datenschutzbehörde unterstützt die Bemühungen um eine bessere und raschere Hilfe für Kinder und Jugendliche in Problemsituationen voll und ganz; es ist jedoch noch nicht eindeutig, ob dieses Register einzig und allein der Bereitstellung von Unterstützungsmaßnahmen oder auch der Aufrechterhaltung der öffentlichen Ordnung dienen soll. Vollkommene Klarheit hinsichtlich der Schlüsselbegriffe und Kriterien ist an dieser Stelle unabdingbar.

Polizei und Justizbehörden

Sowohl Sicherheit als auch Privatsphäre sind für die Bürger von entscheidender Bedeutung. Allerdings wird in öffentlichen Debatten viel zu häufig vereinfacht, indem man diese beiden Begriffe als gegensätzlich darstellt. Um die Diskussion wieder auf den rechten Kurs zu bringen, hat die niederländische Datenschutzbehörde in Zusammenarbeit mit dem niederländischen Justizministerium und dem niederländischen Innenministerium (*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*) eine Untersuchung in Auftrag gegeben, um das bestmögliche Gleichgewicht zwischen den Bemühungen um eine sichere Gesellschaft und den Bemühungen zur Wahrung des Rechts auf Privatsphäre zu ermitteln. Der daraus resultierende externe Untersuchungsbericht einschließlich Leitlinien für einen effizienteren Dialog wurde auf einem Symposium am 1. November 2007 vorgestellt.

Wenn die Polizei Telefongespräche im Rahmen von strafrechtlichen Ermittlungen abhört, kommt es oftmals auch zur Aufzeichnung von Gesprächen zwischen Anwälten und ihren Mandanten. Derartige Gespräche mit Inhabern von vertraulichen Informationen, die Anspruch auf Begünstigung haben, müssen schnellstmöglich gelöscht werden. Eine Untersuchung der niederländischen Telefonüberwachungsbüros seitens der niederländischen Datenschutzbehörde hat gezeigt, dass dies bei weitem nicht in allen Fällen ordnungsgemäß oder rechtzeitig erfolgt. Die niederländische Staatsanwaltschaft hat daher Maßnahmen zur Verbesserung dieser Situation angekündigt.

In Empfehlungen zur vorgeschlagenen neuen Gesetzgebung oder sonstigen Rechtsvorschriften im Bereich des Strafrechts äußert die niederländische Datenschutzbehörde regelmäßig folgende Frage: Ist es erwiesen, dass

die fraglichen Rechtsvorschriften tatsächlich erforderlich sind? Ist deutlich geworden, dass bestehende oder zuvor vorgeschlagene gesetzliche Möglichkeiten nicht ausreichen? Die vom niederländischen Justizminister vorgeschlagene zentrale Datenbank zur Speicherung der Identität aller Verdächtigen und verurteilten Straftäter ist vor dem Hintergrund der kommenden verbesserten Identifizierungsmöglichkeiten nach Meinung der niederländischen Datenschutzbehörde zum Beispiel unzureichend motiviert. Und trägt das geplante Vorhaben von Polizei, Staatsanwaltschaft und *Koninklijke Marechaussee (KMar)* [Königlich-Niederländische Gendarmerie], die Kennzeichen aller Autofahrer zu speichern, die nach Amsterdam über die Brücke „*Utrechtse Brug*“ einfahren – ungeachtet der Tatsache, ob sie sich straffällig gemacht haben oder nicht – tatsächlich zu einer sichereren Gesellschaft bei?

Ende 2007 veröffentlichte die niederländische Datenschutzbehörde auf Antrag des Senats ihre Empfehlung hinsichtlich einer Gesetzesvorlage, die die Befugnisse der Nachrichten- und Sicherheitsdienste im Rahmen der Terrorismusbekämpfung ausweiten würde, wenn es darum geht, Informationen über das Reiseverhalten, den Zahlungsverkehr und die Internetnutzung der Bürger zu erhalten. Die niederländische Datenschutzbehörde hält den Bedarf an diesen Maßnahmen zusätzlich zu den bereits bestehenden Vorkehrungen nicht für gegeben und ist der Ansicht, dass die Folgen der Auswertung dieser Daten für einzelne Bürger, aber auch für Verantwortungsträger und beteiligte Behörden bisher nicht (oder nicht hinreichend) ausgelotet worden sind.

Handel und Dienstleistungen

Im Anschluss an die Ankündigung der niederländischen Datenschutzbehörde, dass sie Durchsetzungsmaßnahmen gegen die rechtswidrige kombinierte Speicherung von Namen und Adressdaten von Reisenden sowie deren Reisedaten ergreifen wird, haben die öffentlichen Verkehrsunternehmen anscheinend schließlich anerkannt, dass die *OV-chipkaart* mit Konsequenzen verbunden ist, die im Widerspruch zum niederländischen Datenschutzgesetz stehen. 2007 wurden in einem Pilotprojekt im Amsterdamer U-Bahn-Netz Untersuchungen über die Auswirkungen der Karte durchgeführt, die eine rechtswidrige Verwendung der *OV-chipkaart* offen legten. Das städtische

Verkehrsunternehmen *Gemeentevervoerbedrijf (GVB)* sowie andere öffentliche Verkehrsunternehmen haben sich inzwischen verpflichtet, ihre Vorgehensweise an die Erfordernisse des niederländischen Datenschutzgesetzes *Wbp* anzupassen. Der technische Entwurf zur Datenspeicherung sieht eine Unterscheidung zwischen Namen und Adressdaten einerseits und Reisedaten andererseits vor. Die Gefahr der rechtswidrigen Überwachung des individuellen Reiseverhaltens wird somit erheblich eingeschränkt.

Das Internet

Personenbezogene Daten werden im Internet auf viele verschiedene Arten veröffentlicht und sind in der Regel einem umfangreichen und vielfältigen Publikum weltweit rund um die Uhr zugänglich. Dies kann unerwartet schwerwiegende Folgen für Internet-Nutzer – viele sind Kinder – haben, deren persönliche Daten im Internet stehen. 2007 hat die niederländische Datenschutzbehörde Leitlinien erarbeitet und herausgegeben, um zu verdeutlichen, was hinsichtlich der Veröffentlichung von personenbezogenen Daten im Internet erlaubt ist und was nicht. Auf der Grundlage dieser Leitlinien können verantwortliche Einzelpersonen beurteilen, ob die Veröffentlichung personenbezogener Daten im Internet zulässig ist. Umfangreiches Informationsmaterial wurde außerdem auf der Website der niederländischen Datenschutzbehörde veröffentlicht. Im Bereich des Jugendschutzes nimmt die niederländische Datenschutzbehörde eine proaktive Haltung ein und stellt Regeln für soziale Netzwerke und Online-Marketing auf.

Auch die Regierung bedient sich des Internets. 2007 führte die niederländische Datenschutzbehörde eine Untersuchung durch, um festzustellen, auf welche Weise die Stadtverwaltung von Nimwegen Daten über Baugenehmigungen veröffentlicht. Vollständige eingescannte Kopien der Antragsformulare wurden im Netz veröffentlicht und enthielten nicht nur Daten über das jeweilige Eigentum und die geplanten Renovierungsmaßnahmen, sondern auch die persönliche Daten des Antragstellers, einschließlich seiner Unterschrift. Nach Meinung der niederländischen Datenschutzbehörde darf die Gemeinde nur zwingend vorgeschriebene Daten bezüglich des jeweiligen Eigentums und der geplanten Renovierungsmaßnahmen im Internet veröffentlichen.

Die ordnungsgemäße Erfüllung einer öffentlich-rechtlichen Aufgabe rechtfertigt keinesfalls, dass ein Verwaltungsorgan automatisch alle Daten über das Internet veröffentlicht. Die niederländische Datenschutzbehörde wird 2008 auch Leitlinien über Aspekte der Privatsphäre bei der aktiven Veröffentlichung im Rahmen des *Wet openbaarheid van bestuur (WOB)* [Gesetz über die Öffentlichkeit der Verwaltung] herausgeben.

Arbeit und soziale Sicherheit

Bürger werden nicht automatisch zu Verdächtigen, nur weil sie Sozialleistungen oder Wohngeld erhalten. Im Waterproof-Projekt wurden alle Altersrentner und Sozialhilfeempfänger in 65 Gemeinden in Friesland, Groningen und Drenthe anhand der Daten über ihren Wasserverbrauch und der Wasserverschmutzungsabgabe auf Anhaltspunkte für Betrug untersucht. Anschließend wurden die Angaben verwendet, um Leistungsmissbrauch beim Wohngeldbezug aufzudecken. Die niederländische Datenschutzbehörde überprüfte diese Verknüpfung von Dateien und entschied, dass sie rechtswidrig ist. Der Kampf gegen den Leistungsmissbrauch ist wichtig, aber eine Überwachung anhand von Dateiverknüpfungen ist nur auf der Grundlage einer ordnungsgemäßen Risikoanalyse zulässig; denn hiermit kann aufgezeigt werden, dass eine weitere Überprüfung einer Gruppe von Bürgern erforderlich ist, die sehr stark Gefahr läuft, in den Bereich des Betrugs abzugleiten. Infolge der Entscheidung der niederländischen Datenschutzbehörde arbeitet der *Sociale Inlichtingen en Opsporingsdienst (SIOD)* [Sozialer Nachrichten- und Untersuchungsdienst] derzeit an der Entwicklung von Risikoanalysen mithilfe der *Privacy Enhancing Technology (PET)*. Auf diese Weise gehen Betrugsbekämpfung und Schutz personenbezogener Daten anscheinend Hand in Hand.

Eine weitere Möglichkeit zur Aufdeckung von Leistungsmissbrauch ist die verdeckte Observierung durch Ermittler der Sozialversicherungsbehörde. Die Methode zur Verarbeitung von personenbezogenen Daten im Zusammenhang mit diesen Aktivitäten wurde in einer von der niederländischen Datenschutzbehörde genehmigten Verfahrensbeschreibung niedergelegt. Untersuchungen im Jahr 2006 ergaben, dass der Pflicht zur Unterrichtung der Bürger über die Tatsache, dass sie beobachtet worden waren, nur ungenügend nachge-

kommen wurde. Die Verfahrensbeschreibung wurde daraufhin 2007 verschärft.

Kann im Falle eines Wechsels des Anbieters von arbeitsmedizinischen Diensten der ehemalige Anbieter die Aufzeichnungen über den Arbeitnehmer ohne ausdrückliche gesetzliche Grundlage an den neuen Anbieter weiterleiten? Die niederländische Datenschutzbehörde entschied 2006 dagegen. Als Reaktion auf Signale aus der Praxis, dass diese Auffassung Probleme bereitet, hat die niederländische Datenschutzbehörde 2007 Untersuchungen durchgeführt, um herauszufinden, ob innerhalb des bestehenden gesetzlichen Rahmens noch ein anderer Ansatz möglich ist. Dies führte zu dem Ergebnis, dass bei der Übertragung unterschieden werden muss zwischen Daten, die nicht unter die ärztliche Schweigepflicht fallen, und Daten, bei denen dies der Fall ist. Im ersten Fall dürfen die Daten weitergeleitet werden. Im zweiten Fall dürfen die Daten nur unter bestimmten Bedingungen übertragen werden.



Polen

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

Telekommunikationsgesetz

Im Berichtszeitraum wurde an den Änderungen des Gesetzes vom 16. Juli 2004 – Telekommunikationsgesetz gearbeitet, das die Bestimmungen der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG in die Rechtsordnung Polens umsetzt. Es wurde ein Vorschlag unterbreitet, den Speicherzeitraum von Sendedaten in Bezug auf Teilnehmer und Endverbraucher, die den für die nationale Verteidigung und Sicherheit und die öffentliche Sicherheit zuständigen Behörden offengelegt werden können, von 2 auf 5 Jahre zu verlängern. Es wurde argumentiert, dass die Verlängerung um den oben genannten Zeitraum zu einer Erhöhung der Effizienz der von den Strafverfolgungsbehörden im Verlauf von Strafverfahren und Untersuchungen durchgeführten Maßnahmen führen würde, wobei zu berücksichtigen ist, dass Rechnungsunterlagen und andere Telekommunikationsdaten überzeugende Beweise sind. Letztendlich wurden die Änderungsentwürfe des Telekommunikationsgesetzes jedoch nicht angenommen.

Bankengesetz

Im Jahr 2007 traten die Änderungen des Bankgesetzes vom 29. August 1997 in Kraft (vereinheitlichter Text: Gesetzesblatt 2002 Nr. 72 Ziffer 665). Unter anderem wurde Artikel 105 a des oben genannten Gesetzes geändert. Der Gesetzgeber ermöglichte es Banken und anderen zur Vergabe von Krediten berechtigten Institutionen, Daten natürlicher Personen, die durch das Bankgeheimnis geschützt sind, nach Ablauf der Verpflichtungen aus einem zwischen einer Bank oder einer anderen per Gesetz zur Vergabe von Krediten berechtigten Institution bestehenden Vertrag ohne Zustimmung der betroffenen Person für statistische Zwecke über einen Zeitraum von 12 Jahren nach Ablauf der Verpflichtung zu verarbeiten. Bisher dürfen Banken und die oben genannten Institutionen Daten natürlicher Personen, die durch das Bankgeheimnis

geschützt sind, nicht länger als 5 Jahre nach Ablauf der Verpflichtung verarbeiten.

Schengen-Gebiet

Am 24. August 2007 wurde das Gesetz über die Beteiligung der Republik Polen am Schengener Informationssystem und dem Visainformationssystem, das den Schengen-Besitzstand umsetzt, angenommen. Es legt unter anderem die Verpflichtungen von Behörden fest, die innerbetriebliche Maßnahmen festlegen und den Zugang zu den Daten im Schengener Informationssystem und im Visainformationssystem über das Nationale Informationssystem gewähren können. Polen ist dem Schengen-Gebiet am 21. Dezember 2007 beigetreten.

Genossenschaftsrecht

Die Anordnungsverfügung bezüglich der Veröffentlichung von Dokumentationen der Wohnungsbaugenossenschaften einschließlich personenbezogener Daten (durch Bekanntgabe der Daten im Internet) wurde mit dem Gesetz vom 14. Juni 2007 in Änderung des Gesetzes über Wohnungsbaugenossenschaften und andere Gesetze eingeführt. Eine derartige Dokumentation kann Personen bekannt gegeben werden, die weder Mitglied der betroffenen Wohnungsbaugenossenschaft noch mit Tätigkeiten der Genossenschaft beauftragt sind. Vom Augenblick der Veröffentlichung derartiger Informationen an können personenbezogene Daten (manchmal sogar vertrauliche Daten) online abgerufen und von Dritten verwendet werden.

Sozialfürsorge

Das Gesetz vom 16. September 2007 bezüglich der Unterstützung unterhaltsberechtigter Personen enthält keinerlei Richtlinien, die vom Minister für Sozialfürsorge bei der Vorbereitung der abgeleiteten Gesetzgebung in Bezug auf den Datenumfang zu berücksichtigen sind, der im Zentralregister der Unterhaltsverpflichteten zu erfassen ist. Die entschiedenen Einwände des Generalinspektors für den Schutz personenbezogener Daten wurden jedoch vom Gesetzgeber bei der Ausarbeitung des Entwurfs zum oben genannten Gesetz nicht berücksichtigt. Infolgedessen sieht ein Verordnungsentwurf des Ministers für Arbeit und Sozialpolitik hinsichtlich des Umfangs der im Zentralregister der Unterhaltsverpflichteten zu erfassenden Daten einen besonders großzügigen Datenkatalog einschließlich hier erfasster sensibler Daten vor.

B. Bedeutende Rechtsprechung

Zentraldatenbank mit Prepaid-Mobilfunknummern

Der Generalinspektor für den Schutz personenbezogener Daten nahm an der Diskussion über den Vorschlag zur Einrichtung einer Zentraldatenbank mit sämtlichen Teilnehmern und registrierten Nutzern von Prepaid-Mobilfunktelefonen teil, die von der Leiterin der Telekommunikationsbehörde verwaltet wird. Die Autoren des Vorschlags unterstrichen, dass eine solche Datenbank im Wesentlichen für Notfälle zur Verfügung stehen sollte, wenn Informationen über einen Anrufer und seinen Standort eingeholt werden müssten. Der Generalinspektor wies darauf hin, dass derartige Informationen auch über das in Artikel 78 des Telekommunikationsgesetzes vorgesehene Verfahren eingeholt werden könnten. Gemäß dieser Bestimmung müssen Betreiber öffentlicher Telefonnetze Informationen über den Standort der Netzabschlusseinheit zur Verfügung stellen, von der aus die Verbindung zum Notruf 112 und anderen Notrufnummern hergestellt wurde, wann immer die angerufenen Notrufdienste eine entsprechende Anfrage stellen, damit sie unverzüglich gemäß ihrem gesetzlichen Auftrag Hilfe leisten können.

Social-Networking-Website „Nasza-klasa“ – geprüft.

Der Generalinspektor für den Schutz personenbezogener Daten hat die Social-Networking-Website „Nasza-klasa“ (wo mehr als 6 Millionen User ihre Profile eingestellt haben) im Hinblick auf die Einhaltung der Anforderungen des Datenschutzgesetzes überprüft. Die Ergebnisse der ausführlichen Überprüfung zeigten, dass das Portal praktisch alle Anforderungen des Datenschutzgesetzes einhält (die Einführung weiterer Sicherheitsmaßnahmen beim Einloggen in das Portal wurden empfohlen) und dass es personenbezogene Daten gemäß ihrer eigenen Datenschutzpolitik verarbeitet. Die Eigentümer des Portals, die vorab ihr Ablagesystem für personenbezogene Daten zur Registrierung übermittelt hatten, kündigten an, dass sie ihre Datenverarbeitung gemäß allen Hinweisen und Empfehlungen des Generalinspektors nach entsprechender Überprüfung verbessern werden.

C. Weitere Entwicklungen und Ereignisse

Datenschutztag

Am 28. Januar 2007 wurde der erste Datenschutztag begangen, der auf eine Initiative des Europarates zurückgeht. Es fanden zahlreiche Veranstaltungen statt, an denen sich der Generalinspektor aktiv beteiligte. Zu den wichtigsten Ereignissen gehörte die vom Generalinspektor für den Schutz personenbezogener Daten, Herrn Michał Serzycki, und dem Kanzler der Kozminski Business School in Warschau unter der Schirmherrschaft des Sejm-Marschalls (oberster Repräsentant einer der beiden Kammern des polnischen Parlaments) organisierte Konferenz „Schutz personenbezogener Daten – eine Garantie oder eine Bedrohung für die Privatsphäre?“, deren Bedeutung durch die Anwesenheit zahlreicher Vertreter der Wissenschaftskreise, die sich auf den Schutz personenbezogener Daten spezialisiert haben, sowie Mitglieder des Parlaments und Vertreter der Regierungsbehörden unterstrichen wurde. Der Generalinspektor für den Schutz personenbezogener Daten kündigte eine Reihe von Bildungsinitiativen an, die auf ein gesteigertes öffentliches Bewusstsein auf dem Gebiet des Schutzes personenbezogener Daten und des Rechts auf Privatsphäre abzielen und somit auf eine Verbesserung des Schutzes solcher Daten in Polen. Am 31. Januar fanden die Feiern in den Räumlichkeiten der Ständigen Vertretung Polens bei der Europäischen Union in Brüssel statt. Zu diesem Anlass wurden zahlreiche Personen, die mit den Problemen des Daten- und Privatsphärenschutzes in den Institutionen der Europäischen Union und des Europarates zu tun haben, wie auch polnische Mitglieder des Europäischen Parlaments, Vertreter der diplomatischen Dienststellen Polens in Belgien sowie polnische und ausländische Journalisten eingeladen.

Darüber hinaus gab der Generalinspektor der Presse und verschiedenen Fernsehkanälen zahlreiche Interviews.

Bildungskampagne

Im Jahr 2007 hat der Generalinspektor eine weitreichende Bildungskampagne ins Leben gerufen, die auf eine Steigerung des gesellschaftlichen Bewusstseins im Bereich des Datenschutzes abzielte. Zu den Bildungsmaßnahmen gehörten Zeichenwettbewerbe für Kinder unter dem Titel „Mein Privatbereich“ und ein Wettbewerb für die beste Diplomarbeit zum Thema Datenschutz. Ferner unterzeichnete der Generalinspektor einen Vertrag mit einer

Wirtschaftshochschule in Warschau über die Einrichtung eines Aufbaustudiums zum Datenschutz.

Die Mitarbeiter des Büros des Generalinspektors für den Schutz personenbezogener Daten führten eine Reihe von Workshops für die Mitarbeiter anderer Institutionen durch, darunter wichtige Regierungsbehörden wie das Kanzleramt des Sejm und der Senat (ebenfalls eine Kammer des polnischen Parlaments), das Außenministerium, die Zollbehörden und die Nationalbank Polens. Sie beteiligten sich ebenfalls aktiv an den von anderen Regierungsstellen organisierten Veranstaltungen. Um der breiten Öffentlichkeit das Problem des Datenschutzes näher zu bringen, nahmen sie auch an der „Customs Service Conference“ in Allenstein und an der wissenschaftlichen Konferenz der Universität von Thorn „10 Jahre polnisches Datenschutzgesetz“ teil. Des Weiteren fand eine Reihe von Bildungstagungen mit Studierenden der verschiedenen polnischen Universitäten statt.

Das Büro des Generalinspektors für den Schutz personenbezogener Daten arbeitete auch mit den polnischen Mitgliedern des Europäischen Parlaments zusammen und organisierte Workshops zum Thema Schutz personenbezogener Daten. Im Rahmen der im Jahr 2007 geplanten Bildungsmaßnahmen lag ebenfalls die Konferenz „Das Recht auf Privatsphäre im Überwachungsstaat“, die am 22. und 23. Oktober in Warschau stattfand.

Konferenz „Das Recht auf Privatsphäre im Überwachungsstaat“

Die Konferenz anlässlich des 10. Jahrestages des Erlasses des polnischen Datenschutzgesetzes fand am 22. und 23. Oktober 2007 im Säulensaal des Sejm (polnisches Parlament) statt.

Sie wurde begleitet von Workshops unter dem Namen „Privatsphäre und Medien“, die in Zusammenarbeit mit der Europäischen Kommission organisiert wurden und in denen die Fragen zu Privatsphäre und Datenschutz im journalistischen Kontext diskutiert wurden.

Viele namhafte Redner aus dem In- und Ausland stellten den Konferenzteilnehmern die wichtigsten Probleme beim Schutz personenbezogener Daten und Privatsphäre vor.

Ziel der Konferenz war es, die wichtigen Aspekte des Datenschutzgesetzes zu erörtern, die in der heutigen Zeit rasanter Entwicklung neuer Technologien, insbesondere von Datentechnologien, von besonderer Bedeutung sind.

Die drei für den 22. Oktober 2007 geplanten Sitzungen befassten sich mit Themen „neue Technologien – neue Möglichkeiten der Überwachung“ den Europäischen Informationssystemen und der Rolle der Datenschutzbeauftragten im Überwachungsstaat. Die erste Sitzung konzentrierte sich auf die verschiedenen Aspekte der neuen Technologien und die Überwachungsmöglichkeiten, die sie schaffen. Die zweite Sitzung behandelte die Europäischen Informationssysteme. Die ständig an Bedeutung gewinnende Rolle der Datenschutzbeauftragten, die das Recht auf den Schutz personenbezogener Daten und den Schutz der Privatsphäre in den europäischen Ländern wahren, war Thema der dritten Sitzung.

Am zweiten Tag der Konferenz konnten in den Workshops „Privatsphäre und Medien“ die derzeitigen Fragen im Hinblick auf die Privatsphäre und den Datenschutz im Kontext journalistischer Aktivitäten diskutiert werden; die Leiter der jeweiligen Sitzungen – Vertreter der Europäischen Kommission und der Europäischen Datenschutzbehörden – gaben den Teilnehmern die Gelegenheit, über den Schutz der Privatsphäre öffentlicher Personen und Internetnutzer nachzudenken.



Portugal

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

Die Richtlinie 95/46/EG wurde per Gesetz 67/98 vom 26. Oktober 1998 – Datenschutzgesetz – in nationales Recht 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 Hinblick auf die Umsetzung der oben genannten Richtlinien wurden keine weiteren rechtlichen Verfügungen erlassen. Allerdings sind mehrere Gesetze zu Fragen des Datenschutzes in Kraft getreten wie beispielsweise das Gesetz 7/2007, das einen neuen Personalausweis für alle Bürger über sechs Jahren vorsieht. Diese Karte enthält die Bürger-Identifikationsnummer, die Steuer-Identifikationsnummer, die Sozialversicherungsnummer und die Krankenversicherungsnummer auf der Gesundheitskarte. Sie weist außerdem einen Fingerabdruck und ein digitales Foto auf. Die neue Bürgerkarte soll – entsprechend ihrer Bezeichnung – sowohl die physische als auch elektronische Identifizierung ermöglichen. Sie hat viele wichtige Fragen zum Datenschutz aufgeworfen, die die portugiesische Datenschutzbehörde in ihren Stellungnahmen im Laufe von 2006 aufgegriffen hat.

Das Gesetz 33/2007 über Videoüberwachung in Taxis ist ebenfalls in Kraft getreten und erlaubt somit Taxifahrern, in ihren Fahrzeugen Videokameras zu installieren. Das System sieht vor, dass der Taxifahrer die Kamera nur bei drohender Gefahr einschaltet. In diesem Fall werden die Bilder an eine private Zentrale übertragen, mit der das Taxi verbunden ist; dort werden sie aufgezeichnet und im Falle möglicher Sicherheitsprobleme zur Untersuchung an Strafverfolgungsbehörden weitergeleitet; anderenfalls werden die Bilder gelöscht.

Das Gesetz besagt, dass die Zentralen verantwortlich für die Datenverarbeitung sind und somit ihre Datenverarbeitungsweise der portugiesischen Datenschutzbehörde melden müssen, die auch die eingerichteten Sicherheitsmaßnahmen und die Zuverlässigkeit der verwendeten Geräte und Maschinen überwacht.

B. Bedeutende Rechtsprechung

Im Laufe des Jahres 2007 erging eine wichtige Entscheidung seitens eines zentralen Verwaltungsgerichtshofs infolge eines Rechtsmittelverfahrens gegen den Beschluss der portugiesischen Datenschutzbehörde über den Einsatz von Videoüberwachung in einer Eigentumswohnung. Es wurde zugunsten der Datenschutzbehörde entschieden.

Im Rahmen ihrer Befugnis, den Einsatz von Videoüberwachungssystemen zum Schutz von Menschen und Vermögenswerten zu genehmigen, billigt die Datenschutzbehörde die Installation derartiger Systeme innerhalb von Wohneigentum nur dann, wenn Bewohner und Besitzer ihre Zustimmung einstimmig erteilen. In der Annahme, dass eine einstimmige Zustimmung vonseiten der Bewohner und Besitzer erfolgt war, hatte die Datenschutzbehörde den Einsatz von Videoüberwachungssystemen in diesem konkreten Fall nach Erhalt der Informationen von dem Verantwortlichen für die Datenverarbeitung genehmigt. Es stellte sich jedoch heraus, dass die Zustimmung aller Einwohner noch gar nicht vorlag, sodass die Datenschutzbehörde ihre Genehmigung zurückzog, da diese auf einer falschen Grundlage erteilt worden war. Der für die Datenverarbeitung Verantwortliche focht diesen letzten Beschluss mit der Begründung an, die Forderung der Einstimmigkeit als Bedingung für die Genehmigung seitens der Datenschutzbehörde sei übertrieben und die Genehmigung könne nicht zurückgenommen werden. Das Gericht entschied, dass die Entscheidung über die Genehmigung revidiert werden könnte (da sie auf falschen Tatsachen beruhte) und dass es durchaus angemessen und verhältnismäßig sei, den Einsatz solcher Systeme in Wohneigentum nur bei einstimmiger Zustimmung der Bewohner zu genehmigen, da Videoüberwachung einen Eingriff in das Privatleben darstelle.

C. Wichtige spezifische Themen

Stellungnahmen zu Gesetzesentwürfen

Gemäß dem Datenschutzgesetz müssen Gesetzesentwürfe, die Fragen zum Datenschutz enthalten, auf nationaler wie auch internationaler Ebene der portugie-

sischen Datenschutzbehörde CNPD zur Stellungnahme unterbreitet werden.

2007 erarbeitete die portugiesische Datenschutzbehörde 62 Stellungnahmen, von denen sich einige auf bilaterale Vereinbarungen zwischen Portugal und Drittländern im Bereich der Polizeikooperation bezogen und andere Fragen zu Datenschutzverordnungen betrafen; es ging dabei insbesondere um folgende Themen: Entwicklung von E-Government-Maßnahmen (Vereinfachung von Verfahren, Austausch von Ausdrucken gegen digitale Dokumente, Online-Zugänge, Daten-Verbindungen), Regulierung des portugiesischen Statistiksystems, zentrale Datenbank mit Begünstigten von Lebensversicherungen, Hotel-Formulare für Ausländer, zentrale Datenbank zur Bewertung des Kreditrisikos.

Die Datenschutzbehörde erarbeitete auch eine Stellungnahme bezüglich der Umsetzung der Richtlinie 2006/24/EG zur Speicherung von Verkehrsdaten und machte entscheidende Vorschläge, insbesondere im Hinblick auf die verschiedenen Erfordernisse: eindeutige Zweckbestimmung, konkrete Definition von „schweren Straftaten“ nach portugiesischem Recht und Verkürzung des offiziell vorgeschlagenen Zeitraums von 2 Jahren für die Vorratsspeicherung von Daten. Die Meinung der Datenschutzbehörde wurde letztendlich weitestgehend berücksichtigt und die Vorratsspeicherung auf 12 Monate begrenzt.

2007 ließ die Datenschutzbehörde zwei maßgebliche Stellungnahmen über die Schaffung von DNA-Datenbanken im Hinblick auf strafrechtliche Ermittlungen und zivile Identifizierung ergehen – Letzteres auf freiwilliger Basis. Die Datenschutzbehörde äußerte angesichts dieses Vorschlags zahlreiche Bedenken. Manche Vorschläge wurden in einen neuen Entwurf aufgenommen, aber eine der wichtigsten Angelegenheiten – die DNA-Datenbank für zivile Zwecke der Identifikation – wurde trotzdem beschlossen.

Leitlinien für klinische Studien

2007 gab die portugiesische Datenschutzbehörde wichtige Leitlinien für Verantwortliche der Datenverarbeitung bezüglich ihrer Aufgaben bei der Durchführung von Studien im Gesundheitssektor sowie bei klinischen Versuchen experimenteller Medizin bei Menschen heraus.

Diese Leitlinien haben die Zeit für Zulassungsverfahren verkürzt und beschreiben die Anforderungen, die Verantwortliche für Datenverarbeitung erfüllen sollen. Gleichzeitig werden sich die betroffenen Personen der Rahmenbedingungen für die Verarbeitung ihrer Daten sowie ihrer Rechte bewusst.

Videoüberwachung in öffentlichen Räumen

Die portugiesische Datenschutzbehörde gab ihre erste Stellungnahme zum Einsatz von Videoüberwachungssystemen in Straßen ab. Die Möglichkeit dazu ergibt sich aus dem Gesetz 1/2005, das den Einsatz der Videoüberwachung vonseiten der Strafverfolgungsbehörden regelt. Gemäß diesem Gesetz können Stadtverwaltungen die Installation solcher Systeme in Straßen im Anschluss an eine positive Stellungnahme der örtlichen Polizei sogar anfordern. Äußert sich die Polizei abschlägig, so wird eine entsprechende Stellungnahme von der Datenschutzbehörde herausgegeben, die dann verbindlich gilt. Im Falle einer positiven Verlautbarung seitens der Datenschutzbehörde obliegt die endgültige Entscheidung dem Innenministerium.

Deshalb beantragte die Verwaltung der Stadt Porto aus Sicherheitsgründen die Genehmigung zur Montage von Videokameras in einigen sehr belebten Straßen der Innenstadt mit Restaurants, Bars und Promenaden. Das System sah die Aussparung bestimmter Bereiche für Wohngebäude vor, wobei alle Bilder direkt an eine Polizeistation übertragen werden sollten. Die Datenschutzbehörde äußerte sich dazu positiv – mit Ausnahme der Nutzung des Systems während der Tagstunden, während denen es abgeschaltet werden musste (da das Problem der Kriminalität hauptsächlich nachts bestand) und seines Einsatzes für Audioaufnahmen, die der Datenschutzbehörde unverhältnismäßig und durchaus indiskret erschienen, besonders weil es sich um einen Bereich handelte, in dem die Menschen ihre Freizeit verbrachten, und ihre Gespräche auf den Promenaden mitgehört und aufgezeichnet werden konnten.

Das portugiesische Innenministerium erteilte daraufhin die endgültige Genehmigung für den Einsatz des Videoüberwachungssystems, allerdings innerhalb der von der Datenschutzbehörde festgelegten Rahmenbedingungen. Laut Gesetz gilt diese Genehmigung nur

für ein Jahr, danach muss ihr Fortbestand durch eine Überprüfung dahingehend abgewogen werden, ob die Voraussetzungen, die zur Installation des Systems geführt haben, weiterhin gegeben sind und ob das System seinen Zweck (Verbrechensverhütung und Strafverfolgung) erfüllt hat.

Vereinbarung mit dem Bildungsministerium

Bei den Feierlichkeiten anlässlich des ersten Europäischen Datenschutztages unterzeichnete die portugiesische Datenschutzbehörde eine Vereinbarung mit dem Bildungsministerium, damit Datenschutzangelegenheiten in die Lehrpläne aller Jahrgangsstufen (1-12) aufgenommen und an öffentlichen Schulen behandelt werden.

Diese Vereinbarung ist von großer Bedeutung, da sie die langfristige und systematische Integration des Datenschutzprogramms in das Unterrichtswesen an Schulen ermöglicht. Dabei geht es darum, das Bewusstsein im Hinblick auf Datenschutzbelange weiter zu steigern, den angemessenen Einsatz der neuen Technologien zu unterstützen und dafür zu sorgen, dass junge Menschen ein Gefühl für Privatsphäre entwickeln und verinnerlichen, damit sie ihr Bürgerrecht auf informationelle Selbstbestimmung voll ausschöpfen können.

Mit dieser Vereinbarung fördert das Bildungsministerium das Kräftespiel zur Übernahme dieses pädagogischen Projekts in das Schulnetzwerk. Mit der Unterstützung des Ministeriums erarbeitet die portugiesische Datenschutzbehörde alle notwendigen und auf Schüler ausgerichteten Unterlagen im Hinblick auf deren Verbreitung an den Schulen.

Im Anschluss an die Unterzeichnung der Vereinbarung verteilte die Datenschutzbehörde Poster zum Thema Internet an Jugendliche im Alter von 10 bis 15 Jahren und begann in einer ersten Phase damit, an einem speziellen Strukturprogramm für Kinder in diesem Alter zu arbeiten, das dem Ministerium im Oktober 2007 vorgestellt wurde. Dieses Projekt wurde im Januar 2008 an den Schulen gestartet.

Preis für den besten Datenschutz-Aufsatz

Vergangenes Jahr rief die Datenschutzbehörde einen Preis für den besten Datenschutz-Aufsatz ins Leben, der einmal pro Jahr für eine schriftliche rechtlich,

soziologisch oder technisch orientierte Abhandlung zum Thema Datenschutz vergeben wird.

Damit soll verstärkt zur Analyse, Reflektierung und Ausarbeitung eigener Arbeiten im Bereich des Datenschutzes ermutigt werden. Der Preis besteht in der Veröffentlichung des Gewinner-Werks. Die offizielle Preisverleihung findet jedes Jahr am 28. Januar als Teil der Feierlichkeiten anlässlich des Europäischen Datenschutztages statt.

Im ersten Jahr war der Preis im Dezember 2007 mit dem Vermerk „hervorragend“ vergeben worden.

V. Ibero-Amerikanische Konferenz zum Thema Datenschutz

Im November veranstaltete die portugiesische Datenschutzbehörde die V. Ibero-Amerikanische Datenschutz-Konferenz, an der afrikanische Länder mit Portugiesisch als Landessprache als Beobachter teilnahmen. Die Konferenz verabschiedete Richtlinien zur Harmonisierung des Datenschutzes in der ibero-amerikanischen Gemeinschaft sowie die Lissabon-Erklärung, welche die jüngsten Entwicklungen in einigen Ländern in Bezug auf den Erlass von Datenschutzgesetzen hervorhebt und betont, wie wichtig in einer globalisierten Wirtschaft die Förderung einfacherer Mechanismen für den internationalen grenzüberschreitenden Datenverkehr unter gleichzeitiger Wahrung des Grundrechts auf Datenschutz ist.

Die Ibero-Amerikanische Konferenz unterstrich auch den Anreiz für diese Gemeinschaft, das Übereinkommen Nr. 108 zu unterzeichnen.



Rumänien

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 in Rumänien am 12. Dezember 2001 durch die Annahme des Gesetzes Nr. 677/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umgesetzt.

Das Gesetz Nr. 677/2001 gewährt der Aufsichtsbehörde eine vollständige Unabhängigkeit und hat sie mit Befugnissen zum Untersuchen, Kontrollieren und Intervenieren, Konsultieren, Regulieren und Informieren der Öffentlichkeit ausgestattet, indem es die in der Richtlinie 95/46/EG verankerten Grundsätze übernommen hat.

Mit den Befugnissen der Aufsichtsbehörde wurde zunächst das Büro des Bürgerbeauftragten (Ombudsmann) betraut. Gemäß der Forderung der Europäischen Kommission, eine unabhängige, autonome Kontrollinstanz mit spezifischen Überwachungs- und Kontrollbefugnissen im Bereich des Schutzes personenbezogener Daten gemäß der Richtlinie 95/46/EG einzurichten, nahm das rumänische Parlament jedoch das Gesetz Nr. 102/2005 über die Einrichtung, Organisation und Arbeitsweise der nationalen Kontrollinstanz für die Verarbeitung von personenbezogenen Daten an, das im rumänischen Amtsblatt Nr. 391 vom 9. Mai 2005 veröffentlicht wurde. Gemäß diesem Gesetz ist die nationale Kontrollinstanz für die Verarbeitung von personenbezogenen Daten eine Behörde mit eigener Rechtspersönlichkeit; sie ist autonom und von jeder anderen Behörde sowie jeder anderen natürlichen oder juristischen Person öffentlichen und privaten Rechts unabhängig.

Eine wichtige Änderung, die das Gesetz Nr. 102/2005 zu den Bestimmungen des Gesetzes Nr. 677/2001 hinzugefügt hat, bestand in der Abschaffung des Artikels 27 Absatz (5) dieses Gesetzes, demzufolge die Kontrollinstanz erst die Zustimmung der Strafverfolgungsbehörde oder des zuständigen Gerichtes erhalten musste, bevor sie mit einer im strafrechtlichen Bereich durchgeführten

Untersuchung im Zusammenhang mit der Verarbeitung von personenbezogenen Daten beginnen konnte.

Eine weitere Änderung gegenüber dem Gesetz Nr. 677/2001 erfolgte durch das Gesetz Nr. 278/2007, mit dem die Mitteilungsgebühr für die Verarbeitung von personenbezogenen Daten abgeschafft wurde, die unter den Geltungsbereich von Gesetz Nr. 677/2001 fällt.

Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation wurde durch das Gesetz Nr. 506/2004 über die Verarbeitung personenbezogener Daten und den Schutz des Privatlebens im Bereich der elektronischen Kommunikation in nationales Recht umgesetzt.

Das Gesetz Nr. 506/2004 garantiert den Schutz personenbezogener Daten, die vom öffentlichen elektronischen Kommunikationsnetz und den Dienstleistungsanbietern sowie von Anbietern von Abonnentenregistern verarbeitet werden. Dieses Gesetz ergänzt und spezifiziert den vom Gesetz 677/2001 über die besonderen Anforderungen des Sektors der elektronischen Kommunikation festgelegten gesetzlichen Rahmen.

Angesichts der Tatsache, dass die Verarbeitung von bestimmten Daten häufig nicht im Interesse des Gesetzes bzw. der erfassten Person erfolgt und dazu neigt, die Rechte der erfassten Person zu verletzen, gab der Präsident der Kontrollinstanz zwei im Amtsblatt von Rumänien veröffentlichte Entscheidungen aus (Entscheidung Nr. 90/2006 und Entscheidung Nr. 100/2007), in denen die Fälle bestimmt werden, in denen eine Mitteilung über die Verarbeitung von personenbezogenen Daten nicht erfolgen muss.

Die Kontrollinstanz wird immer dann hinzugezogen, wenn Gesetzgebungsakte entworfen werden und diese auf den Schutz der Rechte und der Freiheiten des Einzelnen in Bezug auf die Verarbeitung personenbezogener Daten gemäß den Bestimmungen des Gesetzes Nr. 677/2001, wie geändert, verweisen. Deshalb hat die Kontrollinstanz auch zu mehreren Gesetzgebungsakten eine Mitteilung abgegeben. Zu diesen gehören: der Entscheidungsentwurf der rumänischen Regierung über die Billigung der methodischen Normen für die einheitliche

Durchführung von Gesetzesbestimmungen zum Nachweis, zum Wohnsitz und zu Ausweisdokumenten für rumänische Staatsbürger; der Entscheidungsentwurf der rumänischen Regierung über Form und Inhalt von Ausweisdokumenten für selbstklebende Etikette, auf denen ein neuer Wohnsitz oder neue Gebäude eingetragen sind; der Gesetzesentwurf über die Verpflichtung für Luftfahrtunternehmen zur Mitteilung von Passagierdaten; der Gesetzesentwurf der rumänischen Regierung über den freien Personenverkehr für Bürger aus EU- und EWR-Staaten auf rumänischem Staatsgebiet und zur Bestimmung von Form und Inhalt der Ausweisdokumente für EU-Bürger und ihre Familienangehörigen; der Gesetzesentwurf über die Festlegung und Organisation des nationalen Systems für genetisches Datenmaterial.

Darüber hinaus hat die Aufsichtsbehörde mehrere Mitteilungen über Verhaltenskodizes verschiedener Berufsverbände ausgegeben wie etwa der Vereinigung der rumänischen Börsenmakler, des rumänischen Verbands privater Stomatologie-Praxen und des rumänischen Bankenverbands, die angemessene Normen für den Schutz des Einzelnen enthalten, deren personenbezogene Daten verarbeitet werden.

Angesichts der Notwendigkeit der Gewährleistung eines wirksamen Schutzes für die Rechte von Einzelnen, deren personenbezogene Daten innerhalb von Systemen in der Art von Kreditauskunfteien verarbeitet werden, und insbesondere angesichts der mit dieser Art der automatisierten Verarbeitung aufgrund der Art der verarbeiteten Daten und des Zwecks der Verarbeitung verbundenen Risiken für Privatsphäre, Familie und das Privatleben des Einzelnen, hat der Präsident der Aufsichtsbehörde in Jahr 2007 seine Entscheidung Nr. 105/2007 über die Verarbeitung personenbezogener Daten innerhalb des Systems von Kreditauskunfteien ausgegeben.

Festgelegt werden in dieser Entscheidung die Kategorien von Teilnehmern bei Ablagesystemen dieser Art, die Daten, die darin verarbeitet werden können, sowie die Bedingungen, zu denen diese Daten übertragen werden können, die Speicherfrist, die Verpflichtungen der Teilnehmer einschließlich der Gewährleistung der Vertraulichkeit und Sicherheit der in diesen Systemen enthaltenen personenbezogenen Daten.

B. Bedeutende Rechtsprechung

Es wurde festgestellt, dass die Gerichte im Jahre 2007 in den Fällen, die im Zusammenhang mit dem Schutz von personenbezogenen Daten standen, eine einheitliche Praxis verfolgt haben, obwohl es zunächst bei den vorinstanzlichen Gerichten unterschiedliche Herangehensweisen gab.

1. Nach einer Ermittlung beim Generalinspektorat der rumänischen Polizei konnte die Aufsichtsbehörde einen Verstoß feststellen. Hierbei handelte es sich um die nicht erfolgte Meldung über die Verarbeitung von personenbezogenen Daten durch Einrichtung von Überwachungskameras auf einer der wichtigsten Verbindungsstraßen des Landes, mit denen die Identifizierung der Kennzeichen von Fahrzeugen möglich ist. Die von der Aufsichtsbehörde verhängte Geldbuße wurde vom Generalinspektorat der rumänischen Polizei gerichtlich angefochten. Dieser Fall erreichte das rumänische Kassationsgericht. Als oberstes Gericht Rumäniens unterstützte dieses schließlich die Entscheidung der Aufsichtsbehörde.

2. In einer weiteren Gerichtsentscheidung ging es darum, dass die Aufsichtsbehörde einem Kindergarten eine Strafe verhängte, weil dieser personenbezogene Daten ohne jede Mitteilung an die Behörde verarbeitet hatte. Die personenbezogenen Daten wurden innerhalb eines betriebsfähigen Videoüberwachungssystems verarbeitet, das Bilder aller Kinder im Kindergarten aufzeichnete. Angesichts der Tatsache, dass die personenbezogenen Daten sowohl von Kindern als auch vom Personal auf diese Weise ohne eine vorherige Mitteilung an die Aufsichtsbehörde verarbeitet wurden, entschied das Gericht über ein Beibehalten der Entscheidung der Aufsichtsbehörde für eine Sanktionierung, da dieser Tatbestand (die nicht erfolgte Meldung) nur einen geringfügigen Verstoß darstellte.

3. In einem weiteren Fall aus dem Jahr 2007 ging es um ein Reisebüro, das die E-Mail-Adressen seiner Kunden automatisch verarbeitete und ebenfalls von der Aufsichtsbehörde bestraft wurde, weil es diese Art der Verarbeitung nicht gemeldet hat. Die Entscheidung der Behörde wurde als rechtmäßig und begründet vom

obersten Gericht erachtet, das somit die von der Behörde auferlegte Geldbuße unterstützte.

4. Ein besonderer Fall begann mit der Beschwerde einer Person, die angab, von einem privaten Unternehmen unerbetene elektronische Werbenachrichten (Spam) erhalten zu haben, die gegen die Bestimmungen des Gesetzes Nr. 506/2004 über die Verarbeitung personenbezogener Daten und den Schutz des Privatlebens in Bereich der elektronischen Kommunikation verstoßen. In diesem Gesetz verbot der Gesetzgeber das Versenden von elektronischen Werbenachrichten durch automatisierte Systeme, die kein Mitwirken eines menschlichen Betreibers erfordern, über Fax, E-Mail oder sonstige Methoden, bei der öffentlich verfügbare elektronische Informationsdienste beteiligt sind, mit Ausnahme von den Fällen, in denen die erfasste Person eindeutig ihre Zustimmung ausgedrückt hat. Darüber hinaus schreibt das Gesetz vor, dass das Versenden von Werbenachrichten durch die elektronische Post dann grundsätzlich verboten ist, wenn die Identität des Absenders (bzw. der Person, in deren Auftrag die elektronischen Werbenachrichten gesendet werden) verborgen bleibt, oder wenn nicht erwähnt wird, wie das Datensubjekt die Einstellung solcher Nachrichten verlangen kann.

Im Hinblick auf Werbe- und Marketingaktivitäten hat sich bei der Untersuchung herausgestellt, dass die Werbenachrichten tatsächlich einen Befehl für die Streichung aus der Verteilerliste enthielten. Der Kläger hatte diese Option zwar verwendet, er erhielt jedoch weiterhin an seine Adresse gerichtete Werbenachrichten. Letztendlich wurde der für die Datenverarbeitung Verantwortliche bestraft, weil er gegen die gesetzlichen Bestimmungen über unerbetene Werbenachrichten verstoßen und so das Recht seiner Kunden auf den Schutz der Privatsphäre verletzt hat. Über diesen Fall soll ein rumänisches Gericht noch befinden.

Trotz der Vielfalt von Themen, über die gerichtlich gestritten wird, wurde der gesetzliche Rahmen zum Schutz von personenbezogenen Daten von den Gerichten jeweils ähnlich interpretiert wie von der Aufsichtsbehörde.

C. Wichtige spezifische Themen

Eine besondere Aufmerksamkeit widmete die Aufsichtsbehörde der korrekten Umsetzung des gesetzlichen Rahmens zum Schutz personenbezogener Daten, was bedeutet, dass die Kontrollaktivitäten bei der Tätigkeit der Behörde im Jahr 2007 eine wichtige Rolle spielten. Im Jahre 2007 wurden 280 Untersuchungen durchgeführt, davon 235 von Amts wegen und 45 aufgrund von Beschwerden (21) bzw. Meldungen (24) aus der Öffentlichkeit.

Die meisten der von Amts wegen erfolgten Ermittlungen waren vorgesehen im Jahresplan der Behörde über spezifische Fragen, die anhand von früheren Erfahrungen ausgewählt wurden. Bei diesen hatte sich herausgestellt, dass die Bestimmungen des Gesetzes Nr. 677/2001 nur unzulänglich bekannt waren, dass insgesamt weniger Meldungen von den für die Datenverarbeitung Verantwortlichen aus verschiedenen Bereichen vorgenommen wurden, und dass sich aus diesen Datenverarbeitungsvorgängen ein potenzielles Risiko für die Rechte und Freiheiten von Einzelnen ergeben kann. Die vier wichtigsten Bereiche waren in jedem Quartal:

1. **Telemarketing** – die Verarbeitung von personenbezogenen Daten durch Verschicken von Werbenachrichten;
2. **Schuldeneinzahlung** – die Verarbeitung von personenbezogenen Daten zur Schuldeneintreibung;
3. **Auswahl und Entsendung von Beschäftigten** – die Verarbeitung von personenbezogenen Daten von Bewerbern für Arbeitsplätze im In- und Ausland;
4. **Reiseagenturen** – Verarbeitung von personenbezogenen Daten während der Buchung oder der Erbringung sonstiger Dienstleistungen für Touristen.

Den gemäß diesem Jahresplan durchgeführten Untersuchungen zufolge konnte gegenüber den früheren Zeiträumen eine deutliche Zunahme bei der Anzahl der Meldungen beobachtet werden. Diese Untersuchungen führten daneben auch zu einer besseren Einhaltung der Grundrechte und Freiheiten des Einzelnen, insbesondere im Hinblick auf den Schutz ihrer personenbezogenen Daten sowie der Privatsphäre.

Abgesehen von den gemäß dem Jahresplan im Jahr 2007 durchgeführten Untersuchungen, erfolgten mehrere Ermittlungen im Rahmen der Zusammenarbeit mit anderen europäischen Behörden innerhalb der Art. 29 Datenschutzgruppe. Als Beispiel kann hier die Verarbeitung personenbezogener Daten innerhalb des internationalen Finanztransaktionssystems SWIFT erwähnt werden.

Eine erhebliche Anzahl der Meldungen, die jedes Jahr der Aufsichtsbehörde vorgelegt werden, steht im Zusammenhang mit Marketing- und Werbeaktivitäten.

Was die Operationen im Bereich **Direktmarketing** angeht, so setzte die Aufsichtsbehörde die Maßnahmen fort, mit denen 2006 auf der Ebene des rumänischen Direktmarketingverbands begonnen wurde, um die Schritte durchzuführen, die erforderlich waren, um das Recht der Einzelnen auf Widerspruch gegen den Empfang von Werbematerial zu gewährleisten.

Eine besondere Form von Direktmarketing, die offensichtlich in letzter Zeit immer häufiger zum Einsatz kommt, ist die des **Telemarketing**. Im Laufe des Jahres 2007 wurden zehn Untersuchungen durchgeführt, bei denen überprüft werden sollte, unter welchen Bedingungen bei dieser Tätigkeit personenbezogene Daten verarbeitet werden. Dort, wo ein Verstoß gegen die einschlägigen gesetzlichen Bestimmungen festgestellt wurde, wurden Sanktionen verhängt. Im Rahmen dieser Untersuchungen konnten insbesondere folgenden Tatsachen beobachtet werden:

- Im Allgemeinen lassen die größten Unternehmen in Rumänien Tätigkeiten dieser Art jeweils durch ihre eigenen Abteilungen („Inbound-Telemarketing“) oder durch spezialisierte Unternehmen (auf Vertragsbasis) durchführen. Die Untersuchungen zeigten, dass die für die Datenverarbeitung Verantwortlichen in diesem Bereich ihre Datenverarbeitungsvorgänge üblicherweise durch andere, auf Telemarketing spezialisierte, Unternehmen melden ließen. In einigen Fällen, bei denen die Meldepflicht nicht eingehalten worden war, wurden gegen die für die Datenverarbeitung Verantwortlichen gemäß Artikel 31 des Gesetzes Nr. 677/2001 Sanktionen verhängt.

Die bei auf Schuldeneintreibung spezialisierten Firmen durchgeführten Untersuchungen, ergaben, dass personenbezogene Daten von Schuldnern auch dann noch gespeichert waren, nachdem die Schulden bezahlt waren. Deshalb ordnete die Aufsichtsbehörde die Löschung der Daten an, die für die Erfüllung des spezifischen Verarbeitungszwecks (Schuldeneintreibung/Wiederauffinden von Schuldnern) nicht mehr erforderlich waren. In anderen Situationen wurde festgestellt, dass die für die Datenverarbeitung Verantwortlichen die Daten der Schuldner weiterhin speicherten, um „schwarze Listen“ zu erstellen, die dann in einigen Fällen sogar im Internet auf der Website des für die Datenverarbeitung Verantwortlichen veröffentlicht wurden. Da in diesen Fällen die Grundsätze der Zulässigkeit und nicht-unverhältnismäßigen Verarbeitung missachtet wurden, ordnete die Aufsichtsbehörde die Einstellung dieser Verarbeitungsoperationen sowie die Löschung der bis zum Zeitpunkt der Untersuchung gespeicherten und veröffentlichten Daten an. Weitere Verpflichtungen von für die Datenverarbeitung Verantwortlichen auf diesem Gebiet, denen im Rahmen dieser Untersuchungen besondere Aufmerksamkeit gewidmet wurde, bezogen sich auf den Zeitraum, in dem die Daten gespeichert werden, sowie auf die Aneignung schriftlicher Sicherheitsverfahren.

Im Jahr 2007 wurden bei den für die Datenverarbeitung Verantwortlichen, die im Bereich der Personalauswahl und Entsendung tätig sind, 46 Untersuchungen durchgeführt, um zu überprüfen, wie die Bestimmungen des Gesetzes Nr. 677/2001 eingehalten wurden. Diesen Untersuchungen zufolge haben die für die Datenverarbeitung Verantwortlichen die Empfehlungen der Aufsichtsbehörde erfüllt. Die häufigsten Verstöße auf diesem Gebiet standen im Zusammenhang mit Fällen, in denen der für die Datenverarbeitung Verantwortliche die erfassten Personen nicht ordnungsgemäß informiert und die Mindestanforderungen hinsichtlich der Vertraulichkeit und Sicherheit der verarbeiteten Daten nicht eingehalten hat.

Bei Reiseagenturen wurden im Jahre 2007 insgesamt 35 Untersuchungen durchgeführt. Dabei wurden folgende Verstöße gegen die Bestimmungen über den Schutz von personenbezogenen Daten festgestellt:

- nur in wenigen Fällen wurden Meldungen von Reiseagenturen getätigt;

- die erfassten Personen wurden nicht vorschriftsmäßig über ihre Rechte informiert;
- in diesem Bereich erfolgte keine Meldung über die Weitergabe von personenbezogenen Daten ins Ausland. Aufgrund all dieser Verstöße wurden gegen die für die Datenverarbeitung Verantwortlichen Strafen verhängt.

Ein weiteres wichtiges Thema im Jahr 2007 war das Engagement der Aufsichtsbehörde im Hochschulbereich als Teil ihrer Kampagne, mit der die Öffentlichkeit für die besonderen Probleme im Zusammenhang mit dem Schutz personenbezogener Daten sensibilisiert werden sollte. Nach den Veranstaltungen zum Europäischen Datenschutztag 2007 haben die juristische Simion-Bărnuțiu-Fakultät in Sibiu und die Aufsichtsbehörde ein Zusammenarbeitsprotokoll unterzeichnet. Im Rahmen dieser Zusammenarbeit ist ein neues Fachgebiet, der „Schutz personenbezogener Daten“, als Kurs für Postgraduierte in den Lehrplan aufgenommen worden; die Vorlesungen werden vom Präsidenten der Aufsichtsbehörde gehalten.

Nach zahlreichen Sitzungen mit den Mitgliedern von Hochschulinstitutionen und dem Präsidenten der Aufsichtsbehörde konnte ein verstärktes Interesse unter Studierenden im Bereich Privatsphäre und Schutz von personenbezogenen Daten festgestellt werden. Ein weiteres Ergebnis ist auch, dass man derzeit vorsichtig darüber nachdenkt, Kurse über den Schutz von personenbezogenen Daten und die Tätigkeit der Polizei einzuführen. Außerdem laufen Verhandlungen über die Einführung eines Kurses über den „Schutz personenbezogener Daten“ an der privaten Universität Hyperion.



Slowakei

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

Umsetzung der Richtlinie 95/46/EG

Die slowakische Behörde zum Schutz personenbezogener Daten hat durch eine eigene Initiative versucht, die bestmögliche Harmonisierung des Gesetzes Nr. 428/2002 Coll. über den Schutz personenbezogener Daten in seiner durch spätere Bestimmungen ergänzten Fassung (im Weiteren „Datenschutzgesetz“ genannt) mit der Richtlinie 95/46/EG zu erreichen, und hat sich diesbezüglich mit der Generaldirektion Justiz, Freiheit und Sicherheit der Europäischen Kommission beraten. Im Januar 2007 hat die Europäische Kommission auf der Grundlage dieser Beratungen festgestellt, dass die Lage in der Slowakei hinsichtlich des Schutzes personenbezogener Daten zufriedenstellend ist. Trotzdem wird im Jahr 2008 das Datenschutzgesetz unter Berücksichtigung der neuesten rechtlichen und technologischen Entwicklungen in der Europäischen Union und aufgrund der Erfahrung mit der Durchsetzung des Datenschutzes ergänzt.

Weitere Entwicklungen in der Gesetzgebung

Die Datenschutzbehörde gab Stellungnahmen zu 223 Gesetzentwürfen, Vorschriften und Erlassen der slowakischen Regierung ab. Bei den meisten Entwürfen handelte es sich um Vorschläge des Innen-, des Gesundheits- und des Landwirtschaftsministeriums der slowakischen Republik. Hier kam es zu einer erheblichen Steigerung, nicht nur zahlenmäßig, sondern auch im Hinblick auf das allgemeine Bewusstsein der staatlichen Verwaltungsbehörden, die am nationalen Gesetzgebungsverfahren beteiligt sind, insbesondere im Bezug auf die erforderliche engere Zusammenarbeit mit der nationalen Datenschutzbehörde.

Bis Ende 2007 wurde die Richtlinie 2006/24/EG (Vorratsspeicherung von Daten) in slowakisches Recht umgesetzt, und zwar durch Ergänzung des Gesetzes über elektronische Kommunikation. Der Speicherzeitraum für operative Daten, Standortdaten und Daten über die kommunizierenden Parteien wurde auf 6 Monate für Internet-Kommunikationsdaten und auf 12 Monate für andere Kommunikationsarten festgelegt.

Im Rahmen der Gesetzgebungsaktivitäten hinsichtlich der Vorbereitung des Beitritts zum Schengen-Abkommen wurden teilweise Ergänzungen zu einem Sondergesetz und einem staatlichen Erlass vorgesehen und angenommen; dabei handelte es sich um die Ergänzung zum Polizeikorps-Gesetz und einen Erlass des Innenministeriums. Der Vorschlag der Datenschutzbehörde, den Innenminister zum Beauftragten für das Schengen-Informationssystem und auch für alle anderen Polizeinformationssysteme zu ernennen, wurde angenommen. Die Annahme dieses Gesetzes war ein letzter Schritt für den erfolgreichen Beitritt der Slowakei zum Schengener Abkommen.

B. Bedeutende Rechtsprechung

Im Jahr 2007 wurden zwei Fälle aus den letzten Jahren wieder aufgenommen – in einem der Fälle klagte das Justizministerium der Slowakei gegen die Entscheidung der Datenschutzbehörde aus dem Jahr 2006 bezüglich der rechtswidrigen Veröffentlichung der nationalen Identifikationsnummern (die sogenannte Geburtsnummer) auf den Internetseiten des Wirtschaftsbuletins. Die Datenschutzbehörde ordnete in Übereinstimmung mit dem Wortlaut des Datenschutzgesetzes an, dass alle veröffentlichten Geburtsnummern aus dem Internet entfernt werden oder unleserlich gemacht werden sollten. Das Ministerium legt Einspruch gegen die Entscheidung ein und forderte die Datenschutzbehörde auf, ihre Entscheidung aufzuheben. Die Datenschutzbehörde wies den Einspruch des Ministeriums zurück. Das Ministerium machte von seinem Recht auf Rechtsschutz Gebrauch und brachte den Fall vor das Landgericht. Das Gericht lehnte die Forderung des Ministeriums in allen Punkten ab und bestätigte Ende Januar 2008 die Entscheidung der Datenschutzbehörde.

Im zweiten Fall klagte eine betroffene Person gegen die Datenschutzbehörde, weil diese keine Rechtsvorschrift gegen einen Zeitungsverlag erlassen hat, der auf seiner Website personenbezogene Daten einer Person veröffentlichen konnte, ohne dass die betroffene Person davon in Kenntnis gesetzt wurde. Gleichzeitig ermöglichte die Website es jedem, diverse Meinungen zu veröffentlichen. Der Kläger reklamierte, dass eine unbekannte Person seine persönlichen Daten einschließlich Namen, Vornamen und Anschrift auf der Website

veröffentlicht hatte. Der Kläger forderte das Landgericht auf, anzuerkennen, dass seine Rechte, wie sie im Datenschutzgesetz vereinbart sind, verletzt wurden; es war jedoch bekannt, dass besagte Person selbst früher wiederholt ihre persönlichen Daten auf anderen Websites veröffentlicht hatte. Im November 2004 entschied das Landgericht, dass das Vorgehen der Datenschutzbehörde dem Datenschutzgesetz entsprach. Der Kläger legte Einspruch gegen das Urteil ein. Im Mai 2007 bestätigte der Oberste Gerichtshof den Urteilsspruch des Landgerichts in allen Punkten und kam ebenfalls zu dem Ergebnis, dass das Vorgehen der Datenschutzbehörde gerechtfertigt war.

C. Bedeutende spezifische Themen

Im Jahr 2007 gingen bei der Datenschutzbehörde 121 Beschwerden von Datensubjekten und anderen natürlichen Personen ein, die ihre im Datenschutzgesetz niedergelegten Rechte unmittelbar verletzt sahen. 27 Beschwerden wurden von anderen Personen wegen Verdachts auf Verletzung des Datenschutzgesetzes eingereicht. Der leitende Ermittler der Datenschutzbehörde ordnete die Durchführung von 125 Verfahren von Amts wegen an. Insgesamt bearbeitete die Datenschutzbehörde im Jahr 2007 rund 290 Meldungen. Die relativ hohe Zahl enthielt eine Reihe ungelöster Fälle von Ende 2006.

Es sollte darauf hingewiesen werden, dass die Ermittlungsabteilung im Jahr 2007 insgesamt 102 Überprüfungen von Beauftragten und Verarbeitern von Informationssystemen und 62 „Aufforderungen zur Erläuterung“ durchgeführt hat. Im Vergleich zum Jahr 2006 stellte dies eine Steigerung von 65 % dar. Im Jahr 2007 ergingen 104 verbindliche Anordnungen. Die Datenschutzbehörde kontrollierte vorhandene Kamerasysteme, insbesondere die der Stadtpolizei.

Die Datenschutzbehörde verhängte im Jahr 2007 sieben Geldstrafen, wobei die Sanktionen im unteren Bereich der Geldstrafenskala blieben.

Im Hinblick auf die Vorbereitungen für den Beitritt zum Schengener Abkommen und gemäß den Bestimmungen des Datenschutzgesetzes, wonach die Datenschutzbeauftragten den Datensubjekten detaillierte Auskunft

über die Verarbeitung ihrer personenbezogenen Daten geben müssen, führte die Datenschutzbehörde eine Inspektion der diplomatischen Vertretungen der Slowakei und ihrer Konsularabteilungen in Serbien (Belgrad), Kroatien (Zagreb), in der Ukraine (Uzhorod), in Weißrussland (Minsk), in der Russischen Föderation (St. Petersburg) und in der Türkei (Ankara, Istanbul) durch. Die Inspektionen fanden auch im Außenministerium und bei der Grenz- und Auslandspolizei der Slowakei, im Büro für Kriminaltechnik und Fachwissen, Abteilung EURODAC, und bei der Oberzolldirektion der Slowakei statt.

SWIFT

Die Generaldirektion Justiz, Freiheit und Sicherheit der Europäischen Kommission bat in einer E-Mail vom 20. April 2007 den Datenschutzbeauftragten um Zusammenarbeit bei der Ermittlung im SWIFT-Fall. Unter anderem bat sie um die offizielle Stellungnahme der Datenschutzbehörde zum gegenwärtigen Stand der von den Banken ergriffenen Maßnahmen, um ihrer gesetzlichen Verpflichtung zur Information ihrer Kunden (Datensubjekte) über die Verarbeitung ihrer personenbezogenen Daten nachzukommen, die zum Zwecke von Banküberweisungen via SWIFT erfasst worden waren.

In dieser Hinsicht hat der leitende Ermittler der Datenschutzbehörde in einem Schreiben 24 Bankinstitute aufgefordert, eine umfassende Überprüfung ihrer Pflichten in Bezug auf grenzüberschreitende Zahlungssysteme via SWIFT im Rahmen einer Überwachung gemäß Abschnitt 19 Absatz 4 des Gesetzes Nr. 428/2002 Coll. vorzunehmen und sich dabei auf die Beurteilung zu konzentrieren, ob die Verarbeitung personenbezogener Daten eine Verletzung der Rechte und Freiheiten der jeweiligen Kunden (Datensubjekte) verursacht oder nicht.

Auch die Nationalbank der Slowakei wurde angeschrieben. Bei der Erfassung, Verarbeitung und anschließenden grenzüberschreitenden Weiterleitung personenbezogener Daten ist jede Bank verpflichtet, die jeweiligen Betroffenen über die Bedingungen ihrer personenbezogenen Daten (Abschnitt 10 Absatz 1 bis 3 des Gesetzes Nr. 428/2002 Coll. und Artikel 10 und 11 der Richtlinie 95/46/EG) ausreichend zu informieren. Die Datenschutzbehörde forderte die Bankinstitute auf, eine umfassende und vollständige Stellungnahme zu ihren besonderen

Maßnahmen und Mechanismen vorzulegen, die zwecks Einhaltung ihrer in den Punkten 5 und 6 der Position Nr. 10 bei der SWIFT-Datenverarbeitung vereinbarten Pflichten erfolgt sind oder erfolgen würden, und sich dabei auf die Punkte 5.3.2, 5.5, 6.1, 6.2, 6.5 und 6.6 zu konzentrieren. Wenn ein Bankinstitut keine entsprechenden Maßnahmen ergriffen hat, war es verpflichtet anzugeben, welche Mechanismen und besondere Maßnahmen vom Verarbeiter der personenbezogenen Daten bis spätestens 31. Mai 2007 ausgeführt werden. Unter Berücksichtigung dieser Ergebnisse hat die Inspektionsabteilung der Datenschutzbehörde Informationen für die Europäische Kommission zusammengestellt, die am 14. Mai 2007 an den Vorsitzenden der EU-Datenschutzbehörde gesandt wurden. Bis Ende August 2007 wurde der Fragebogen über die Erfüllung der Pflichten bezüglich der Information der jeweiligen Bankkunden über internationale Zahlungsanweisungen durch die SWIFT an die EU gesandt.

Die Verarbeitung personenbezogener Daten von Kunden von Bestattungsunternehmen

Die Datenschutzbehörde führte Inspektionen der Informationssysteme verschiedener Bestattungsunternehmen durch. Ziel war zu überprüfen, ob alle Dienstleistungen in Übereinstimmung mit dem Datenschutzgesetz erbracht und die Kundendaten entsprechend verarbeitet worden sind. In einigen Fällen konnte nachgewiesen werden, dass die jeweiligen Beauftragten für die Informationssysteme verschiedene Aspekte des slowakischen Datenschutzgesetzes nicht eingehalten haben.

Besondere Registrierung personenbezogener biometrischer Daten

Bei der Durchführung einer Inspektion in einem Unternehmen, einem bekannten Hersteller von Markenelektronik, wurde festgestellt, dass der für die Datenverarbeitung Verantwortliche sein mit biometrischen Daten gefülltes Informationssystem nicht hat registrieren lassen. Gemäß dem Datenschutzgesetz ist der für die Datenverarbeitung Verantwortliche verpflichtet, das Informationssystem einer besonderen Registrierung zu unterziehen, wenn er die Absicht hat, biometrische Daten zu verarbeiten, oder dies bereits tut, mit Ausnahme der DNA-Analyse und des DNA-Profiles natürlicher Personen zum Zwecke der Registrierung oder

Erkennung beim Zutritt zu sensiblen und besonders geschützten Anlagen, Werksgelände mit Zugangsbeschränkung oder Zugriff auf technische Geräte oder Einrichtungen mit hohem Gefahrenpotenzial und im Falle rein interner Anforderungen des für die Datenverarbeitung Verantwortlichen. In diesem bestimmten Fall verhängte die Datenschutzbehörde eine erhebliche Geldstrafe in Höhe von 30 000,00 SKK.

Rechtswidrige Veröffentlichung personenbezogener Daten durch ein Kredit vergebendes Nichtbankeninstitut

Eine Gesellschaft, deren Zweck die Kreditschuldeneintreibung ist, hat ihren Schuldnern üblicherweise eine offene Mahnung in Form einer Briefkarte mit dem ausdrücklichen, farblich markierten Hinweis zugesandt, dass der Empfänger ein „SCHLECHTER ZAHLER“ ist, und auf der Karte den offenstehenden Betrag angegeben. Auf diese Art und Weise wurde die wirtschaftliche Situation der betroffenen Person Dritten bekannt gegeben, was allerdings für die Erfüllung der Datenverarbeitungszwecke nicht erforderlich war. Die Datenschutzbehörde wies den für die Datenverarbeitung Verantwortlichen an, eine derartige Verarbeitung personenbezogener Daten einzustellen. Dieser widersprach der Anordnung der Datenschutzbehörde, da das Unternehmen sonst sein Instrument des psychologischen Drucks auf seine Schuldner verloren hätte. Da der für die Datenverarbeitung Verantwortliche nicht innerhalb der gesetzlich vorgesehenen Frist Einspruch gegen die Anordnung eingereicht hatte, verlor das Unternehmen die Möglichkeit, einen effizienten Schutz durch das Gericht zu erhalten. Infolgedessen stellte der für die Datenverarbeitung Verantwortliche einen Prüfungsantrag bei der Generalstaatsanwaltschaft der Slowakei bezüglich der Rechtmäßigkeit der erteilten Anordnung und verlangte die Aufhebung der Anordnung. Als Grund gab der für die Datenverarbeitung Verantwortliche eine Verletzung seines verfassungsmäßigen Rechts auf freie Berufsausübung an. Der Staatsanwalt bestätigte die sachliche Ordnungsmäßigkeit der Anordnung und ihre Rechtmäßigkeit im vorliegenden Fall. Daher stellte der für die Datenverarbeitung Verantwortliche einen zweiten Antrag an den obersten Staatsanwalt und bat um erneute Überprüfung der Anordnung. Der oberste Staatsanwalt bestätigte ebenfalls die Ordnungsmäßigkeit des Vorgehens der Datenschutzbehörde und erklärte dem für die

Datenverarbeitung Verantwortlichen, dass er weitere Anträge in diesem Fall nicht bearbeiten würde.

Gesetzeswidrige Bekanntgabe nationaler Identifikationsnummern (Geburtsnummern)

Im Jahr 2007 stellte die Datenschutzbehörde weitere Untersuchungen in Bezug auf den Schutz personenbezogener Daten an und konzentrierte sich insbesondere auf die Veröffentlichung nationaler Identifikationsnummern, der so genannten „Geburtsnummern“, im Internet. Anordnungen hinsichtlich der Behebung erkannter Mängel wurden seitens der Datenschutzbehörde an verschiedene Stellen, wie beispielsweise das Finanzamt der Slowakei, einen Fußballverband, die slowakische Kartellbehörde und andere, erlassen.

Scannen und Kopieren von Dokumenten ohne die Zustimmung der betroffenen Person

Dokumente dürfen ohne eine ordnungsgemäße rechtliche Grundlage weder kopiert noch gescannt werden; diese Grundlage ergibt sich in der Slowakei durch ein Sondergesetz bzw. durch die schriftliche Zustimmung der betroffenen Person. Überprüfungen verschiedener öffentlicher juristischer und natürlicher Personen durch die Datenschutzbehörde ergaben, dass diese Vorschrift in den meisten Fällen von den für die Datenverarbeitung Verantwortlichen missachtet wurde. Die Datenverarbeitung erfolgte üblicherweise weit über das für den Zweck der Verarbeitung personenbezogener Daten notwendige Maß hinaus und ohne die Zustimmung der betroffenen Personen. Die Datenschutzbehörde erließ diesbezüglich verbindliche Anordnungen.

Grenzüberschreitender Datenverkehr

Im Jahr 2007 veröffentlichte die Datenschutzbehörde über 30 offizielle Stellungnahmen (Erklärungen, Gesetzesauslegungen) zum grenzüberschreitenden Datenverkehr innerhalb und außerhalb der Europäischen Union. Die willkürliche Festlegung des Status des für die Datenverarbeitung Verantwortlichen oder des Datenverarbeiters in den verschiedenen Vertragsbeziehungen oder das Fehlen ihrer vertraglichen Festlegung zwingt die Datenschutzbehörde zu eingehenden Erläuterungen. Beschäftigungsdaten gehören zu den am häufigsten gewünschten Kategorien personenbezogener Daten, die an Dritte im Ausland weitergeleitet werden. Aber auch die Banken verlangen einige sensible

personenbezogene Daten, wie die nationale Identifikationsnummer, was angesichts ihrer Serviceleistungen übertrieben scheint. Sie rechtfertigten dies mit ihrem weltweit vernetzten und gespiegelten Informationssystem. Die Datenschutzbehörde wurde hauptsächlich von betroffenen Personen im Finanz- und Banksektor um Genehmigung gebeten, und derartige Übertragungen wurden (in insgesamt neun Fällen) ebenfalls genehmigt. In anderen Fällen führten zumeist weitgehend unvollständige Begründungen seitens der für die Datenverarbeitung Verantwortlichen, die die Datenschutzbehörde um Genehmigung für bestimmte Datenübertragungen weltweit baten, zu Ablehnungen. Eine Genehmigung wurde einem weltweit tätigen Mobilfunkanbieter Anfang Januar 2008 erteilt.

Auf der Website der Datenschutzbehörde wurden Richtlinien für die für die Datenverarbeitung Verantwortlichen veröffentlicht, die von der Datenschutzbehörde Genehmigungen für die internationale Weiterleitung personenbezogener Daten beantragen, damit die jeweiligen Abschnitte des Datenschutzgesetzes im grenzüberschreitenden Datenverkehr genau angewendet werden.

Öffentliche Umfrage

Eine öffentliche Umfrage zum Bekanntheitsgrad von Fragen des Schutzes personenbezogener Daten wurde vom Meinungsforschungsinstitut des slowakischen Amtes für Statistik durchgeführt. Die Umfrage zeigte, dass über die Hälfte der Befragten sich ihrer Rechte in Bezug auf den Schutz personenbezogener Daten bewusst waren. Dies war das erste Mal seit 1999, dass eine erhebliche Gruppe der Befragten (51 %) sich ihrer Rechte in Bezug auf den Datenschutz bewusst waren, d. h. dass das Bewusstsein um 31 % gestiegen ist. Im Vergleich zum Jahr 2005 ergab sich eine Steigerung von 6 %. Am bekanntesten ist das Thema Bürgern mit Hochschulabschluss (78 %), Unternehmern (70 %), Angestellten (65 %), Absolventen einer höheren Schule (59 %), Bürgern in Städten mit mehr als 50 000 und weniger als 100 000 Einwohnern (59 %). Das geringste Bewusstsein hatten Bürger mit einem niedrigen Bildungsabschluss (30 %). Ein relativ hohes Bewusstsein zwischen 57 % und 59 % zeigte sich in weiten Teilen der Bevölkerung zwischen 35 und 49 Jahren.

Die Studie zur öffentlichen Meinungsumfrage ist ein umfangreiches Dokument, das sich auf verschiedene Aspekte der Rechte und Pflichten konzentriert, die im Datenschutzgesetz vereinbart sind, beispielsweise die Sensibilität personenbezogener Daten im Hinblick auf einen möglichen Missbrauch, das Fotokopieren von Originalausweisen, das Vertrauen der Bürger in verschiedene Gruppen von Datenschutzbeauftragten, die Übertragung personenbezogener Daten in Drittländer, drohender Missbrauch von über das Internet mitgeteilten personenbezogenen Daten, Zustimmung der Bürger zu Telefonüberwachung und Internetkommunikationsüberwachung als Teil der Terrorismusbekämpfung. Einzelheiten zur Analyse finden sich im Jahresbericht 2007 der Datenschutzbehörde, die auf der Website www.dataprotection.gov.sk veröffentlicht ist.

Internationale Zusammenarbeit

Am 21. März 2007 besuchte die zweite Schengen-Expertengruppe Sch-Eval der Europäischen Kommission die Slowakei. Zusammen mit anderen relevanten Behörden wurde die Datenschutzbehörde überprüft.

Die Schengen-Expertengruppe hatte die Aufgabe festzustellen, ob die Empfehlungen der ersten Expertengruppe vom Februar 2006 umgesetzt worden sind. Folgende Bereiche wurden bewertet:

1. Rechtsgrundlage für die Umsetzung des SIS (Schengener Informationssystem), insbesondere SIS one 4 all;
2. Kompetenzen, Kapazität und Funktionalität der Datenschutzbehörde;
3. Visa-Ausstellungsverfahren im Rahmen des Schengener Abkommens;
4. Information der breiten Öffentlichkeit über die Durchsetzung der Rechte von Datensubjekten im Hinblick auf die Verarbeitung ihrer persönlichen Daten im Rahmen des Schengener Informationssystems sowie über Änderungen bezüglich des Beitritts der Slowakei zum Schengen-Gebiet.

Die Datenschutzbehörde hat ihre Fähigkeit nachgewiesen, ihre Kompetenzen bei der Inspektion der Polizei-Datenbanken voll und ganz auszuüben. Die Slowakei trat dem Schengen-Gebiet eine Minute nach Mitternacht am 21. Dezember 2007 bei.

Im Rahmen des Aufbaus von Partnerschaften mit Datenschutzbehörden in Mittel- und Osteuropa fanden neben der jährlichen Konferenz der mittel- und osteuropäischen Datenschutzbeauftragten, die 2007 im kroatischen Zadar abgehalten wurde, im April 2007 zwei Tage lang Verhandlungen mit den Vertretern der rumänischen Datenschutzbehörde in Bratislava statt, in deren Verlauf die Hauptprobleme beim Schutz personenbezogener Daten, die eingehaltenen Bedingungen und die noch zu ergreifenden Schritte bis zum vollen Beitritt der Slowakei zum Schengen-Gebiet behandelt wurden. Beide Datenschutzbehörden vereinbarten eine Zusammenarbeit.

Im Rahmen des internationalen Vorhabens zur Schaffung und Förderung der Effizienz der Tätigkeiten des Direktorats für den Schutz personenbezogener Daten und der Durchsetzung des Datenschutzes in der ehemaligen jugoslawischen Republik Mazedonien nahm ein Mitarbeiter aus der Abteilung der Datenschutzbehörde für ausländische Beziehungen als Kurzzeit-Experte für Informationstechnologie und Sicherheit an dem Projekt teil. Im Juni 2007 wurde dieser Vertreter der Datenschutzbehörde zum Vorsitzenden der Gemeinsamen Zollaufsichtsbehörde für das Zollinformationssystem gewählt.



Slowenien

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

Das Gesetz zum Schutz personenbezogener Daten (im Folgenden: Datenschutzgesetz)¹¹, das am 15. Juli 2004 von der Nationalversammlung der Republik Slowenien angenommen wurde, wurde 2007 geändert. Mit der Verabschiedung des Gesetzes zum Schutz personenbezogener Daten, des Gesetzes über den Datenschutzbeauftragten und der Einrichtung der Stelle des Datenschutzbeauftragten, wurde gewährleistet, dass die Richtlinie 95/46/EG vollständig in slowenisches Recht umgesetzt wurde.

Das Datenschutzgesetz wurde 2007 durch das Gesetz über Änderungen und Ergänzungen des Gesetzes zum Schutz personenbezogener Daten, das vom Parlament der Republik Slowenien am 12. Juli 2007¹² angenommen wurde, geändert. Gemäß den Ergänzungen sind alle für die Datenverarbeitung zuständigen Stellen mit weniger als 50 Beschäftigten (früher 20 Beschäftigte) von den Auflagen in Artikel 25, Absatz 2 des Datenschutzgesetzes (Pflicht, in den internen Regularien die Vorgehensweisen und Maßnahmen zum Schutz personenbezogener Daten vorzuschreiben und die Personen festzulegen, die für einzelne Ablagesysteme verantwortlich sind, sowie Personen, die aufgrund der Art ihrer Tätigkeit personenbezogene Daten von Einzelpersonen verarbeiten) befreit sowie von den Auflagen in den Artikeln 26 und 27 des Datenschutzgesetzes (Erstellen eines Ablagesystemkatalogs für jedes Ablagesystem und Pflicht, die nationale Aufsichtsbehörde – die Datenschutzbeauftragte über das Erstellen eines Ablagesystems oder vor dem Eintragen einer neuen Art von personenbezogenen Daten in ein Ablagesystem zu benachrichtigen). Diese Ausnahmen gelten allerdings nicht für Ablagesysteme, die von Daten verarbeitenden Stellen im öffentlichen Sektor, Notaren, Rechtsanwälten, Detektiven, Gerichtsvollziehern, privaten Sicherheitsfirmen, privatem Pflegepersonal oder privaten Gesundheitsdienstleistern verwendet werden, und auch nicht für die für die Daten-

verarbeitung Verantwortlichen, die Ablagesysteme mit vertraulichen personenbezogenen Daten verwenden und für die das Verarbeiten vertraulicher personenbezogener Daten Teil ihrer registrierten Tätigkeit ist.

Außerdem wurde der Zeitraum für die Häufigkeit, mit der man Zugang zu Informationen beantragen kann, geändert (Artikel 31 des Datenschutzgesetzes). Gemäß den Ergänzungen können solche Anträge auf ähnliche Weise wie vor der Ergänzung gestellt werden: alle drei Monate einmal, und in Bezug auf vertrauliche personenbezogene Daten und personenbezogene Daten im Rahmen der Regelungen von Kapitel 2, Teil VI dieses Gesetzes (Datenverarbeitung im Zusammenhang mit Videoüberwachung) einmal pro Monat. Durch die Ergänzung wurde die Regelung aber wie folgt erweitert: Wenn eine faire, gesetzeskonforme oder im Umfang angemessene Verarbeitung von personenbezogenen Daten sichergestellt werden muss, besonders wenn die personenbezogenen Daten einer Person in einem Ablagesystem häufig aktualisiert oder versendet werden oder häufig aktualisiert oder an Datenempfänger versendet werden könnten, muss der für die Datenverarbeitung Verantwortliche der Person erlauben, den Antrag binnen eines angemessen kürzeren Zeitraums zu stellen, der nicht weniger als fünf Tage ab Bekanntwerden der personenbezogenen Daten, die sich auf ihn beziehen, oder der Ablehnung dieses Bekanntwerdens betragen darf.

In der Ergänzung wurde überdies vorgeschrieben, dass die für die Datenverarbeitung Verantwortlichen der betroffenen Person ermöglichen müssen, eine Bescheinigung gemäß Artikel 30, Absatz 1, Unterabsätze 1 und 2 dieses Gesetzes einzusehen, abzuschreiben, zu kopieren und zu erhalten, und zwar am gleichen Tag, an dem die Anfrage eingeht (zuvor musste dies binnen 15 Tagen nach Eingang des Antrags geschehen), oder binnen maximal 15 Tagen der betroffenen Person schriftlich mitteilen müssen, warum keine Bescheinigung eingesehen, abgeschrieben, kopiert oder ausgestellt werden kann.

Darüber hinaus sind Vorschriften enthalten zu den mit der Informationsanfrage verbundenen Materialkosten, die der für die Datenverarbeitung Verantwortliche der Person für die Abschrift, Kopie, schriftliche Bescheinigung, den Auszug, die Liste oder die Informationen

¹¹ Staatliches Amtsblatt der Republik Slowenien, Nr. 86/2004.

¹² Staatliches Amtsblatt der Republik Slowenien, Nr. 67/2007.

aus den Punkten 5 und 6 und die Erklärung aus Punkt 7, Absatz 1, Artikel 30 dieses Gesetzes in Rechnung stellen darf. Der für die Datenverarbeitung Verantwortliche darf der Person nur die Materialkosten gemäß einem vorgegebenen Tarif (der vom Justizminister auf Vorschlag der Datenschutzbeauftragten festgelegt wird) berechnen; mündliche Bestätigungen, mündlich erteilte Auskünfte und mündliche Erklärungen sind kostenfrei. Wenn eine Person eine schriftliche Bestätigung, Information oder Erklärung wünscht, obwohl sie bereits eine mündliche Bestätigung, Information oder Erklärung erhalten hat, muss sie der für die Datenverarbeitung Verantwortliche trotzdem ausstellen.

Im Zuge der Ergänzung wurden außerdem alle Strafgebühren für Verstöße gegen das Datenschutzgesetz auf Euro umgestellt.

Die Datenschutzbeauftragte nahm 2007 regelmäßig an fünf EU-Arbeitsgruppen teil, die sich mit dem Schutz personenbezogener Daten befassen, und ist den Datenschutzinstitutionen der Mitgliedsstaaten beigetreten (Art. 29 Datenschutzgruppe, Gemeinsame Kontrollinstanz von Europol, Gemeinsame Kontrollinstanz von Schengen, Gemeinsame Kontrollinstanz Zoll und Koordinierungsgruppe für die Aufsicht über EURODAC, die aus den nationalen Datenschutzbehörden und der Datenschutzbeauftragten besteht und sich mit der Verarbeitung personenbezogener Daten in verschiedenen Kontexten innerhalb der EU befasst). Innerhalb der Art. 29 Datenschutzgruppe hat die Datenschutzbeauftragte im Unterausschuss ITF einen Vertreter.

Die Richtlinie 2002/58/EG wurde durch Änderungen am Gesetz über elektronische Kommunikation in slowenisches Recht umgesetzt¹³, das am 9. April 2004 angenommen wurde und am 1. Mai 2004 in Kraft trat. Kapitel 10 des Gesetzes regelt 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 Kommu-

nikation¹⁴ 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 traten am 15. September 2007 in Kraft, während die Regelungen über die Datenspeicherung bei Internetzugang, E-Mail und Internettelefonie (VoIP) am 15. März 2009 rechtswirksam werden sollen.

Die Datenschutzbeauftragte nahm 2007 als Mitglied des Inspektionsteams der Gemeinsamen Kontrollinstanz von Europol an der Jahresinspektion von Europol teil. Die Datenschutzbeauftragte führte eine Inspektion der nationalen Europol-Einheit durch.

Die 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 definiert auch Bedingungen, unter denen biometrische Maßnahmen zu genehmigen sind. Solche Maßnahmen dürfen nur mit vorheriger Genehmigung der Aufsichtsbehörde durchgeführt werden.

Bezeichnenderweise war 2007 bei der Zahl entsprechender Anträge ein steigender Trend zu verzeichnen. Die Datenschutzbeauftragte erhielt 2007 40 Anträge, von denen 31 aus dem privaten Sektor und 9 aus dem staatlichen Sektor stammten (2006 waren insgesamt nur 15 Anträge zu verzeichnen).

¹³ Staatliches Amtsblatt der Republik Slowenien, Nr. 43/2004 und 86/2004.

¹⁴ Staatliches Amtsblatt der Republik Slowenien, Nr. 129/2006.

Insgesamt hat die Datenschutzbeauftragte vergangenes Jahr 35 Entscheidungen zur Durchführung **biometrischer Maßnahmen** getroffen; in 24 Fällen hat sie die Durchführung der Maßnahmen genehmigt. Anträge auf Durchführung biometrischer Maßnahmen wurden in zwei Fällen verworfen, in einem Fall teilweise genehmigt und in weiteren zehn Fällen abgelehnt. Die Datenschutzbeauftragte genehmigte den Einsatz biometrischer Maßnahmen für den Zugang zu Räumlichkeiten, in denen geschützte Programmierausrüstung gelagert wird, und zu Bereichen, in denen Dokumente über Handelsgeheimnisse eines Unternehmens oder andere geschützte Daten aufbewahrt werden. Die Datenschutzbeauftragte lehnte einen Antrag ab, bei dem biometrische Maßnahmen an Beschäftigten durchgeführt werden sollten, nur um die Anwesenheit am Arbeitsplatz festzustellen.

Es war außerdem eine Zunahme von Genehmigungen für das **Verbinden von Ablagesystemen** zu verzeichnen. Die Datenschutzbeauftragte erhielt 2007 12 Anträge (7 im Jahr 2006) für das Verbinden von Ablagesystemen. Insgesamt fällte die Datenschutzbeauftragte sieben Entscheidungen zum Verbinden von Ablagesystemen.

Im Allgemeinen braucht jemand, der Daten verarbeitet, laut Datenschutzgesetz eine angemessene Rechtsgrundlage oder die persönliche Zustimmung der Person, auf die sich die personenbezogenen Daten beziehen, um diese Daten in irgendeiner Art und Weise verarbeiten oder in den Medien veröffentlichen zu dürfen. Wenn jedoch gemäß dem Grundsatz der Verhältnismäßigkeit das verfassungsmäßig garantierte Recht auf Information schwerer wiegt als das Recht auf Schutz der personenbezogenen Daten des Einzelnen, könnte die Veröffentlichung solcher Daten unter Umständen legal sein. Da das Datenschutzgesetz keine gesonderten Ausnahmen für die Medien enthält, muss die Umsetzung des Datenschutzes und somit der Vorschriften des Datenschutzgesetzes in Bezug auf das verfassungsmäßig garantierte Recht auf freie Meinungsäußerung (das in der Praxis durch das öffentliche Mediengesetz¹⁵ geregelt wird) so interpretiert werden, dass sich die Medien an das Datenschutzgesetz halten müssen und somit an den Grundsatz der Verhältnismäßigkeit, wie

er in Artikel 3 des Datenschutzgesetzes festgelegt ist. 2007 hat die Datenschutzbeauftragte mehrere Verfahren gegen die Medien eingeleitet, die gegen die Vorschriften des Gesetzes zum Schutz personenbezogener Daten verstoßen haben.

1. Ein Journalist von einem der großen Fernsehsender veröffentlichte in einer täglichen abendlichen Nachrichtensendung den Inhalt einer Strafanzeige, ohne die Daten zu anonymisieren; dabei veröffentlichte er folgende personenbezogene Daten der beschuldigten Personen: Name, Geburtsdatum, Adresse und Personenkennzahl. Der Zuwiderhandelnde hatte weder eine rechtliche Grundlage noch die persönliche Zustimmung der betroffenen Personen für die Veröffentlichung dieser Daten, noch hatte in diesem Fall das Informationsrecht der Öffentlichkeit Vorrang. Die veröffentlichten Daten waren in ihrem Ausmaß nicht dem Zweck angemessen, zu dem sie veröffentlicht worden waren, und dies stellt einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit dar. Der Verstoß bestand darin, dass personenbezogene Daten, insbesondere Geburtsdaten, Adressen und Personenkennzahlen von drei Personen unrechtmäßig veröffentlicht wurden. Der Journalist entfernte die umstrittene Nachricht umgehend von der Website und verhinderte weitere Verstöße.

2. Die Datenschutzbeauftragte deckte bei ihrer Inspektion einen Verstoß gegen das Datenschutzgesetz auf, im Zuge dessen ein Personalausweis mit folgenden personenbezogenen Daten veröffentlicht wurde: Foto, Name, Geburtsdatum, Geburtsort, Personenkennzahl, Geschlecht, Personalausweisnummer, Ausstellungsort sowie Gültigkeitszeitraum des Ausweises und Unterschrift der Person. Da die betroffene Person nicht eindeutig eine Person des öffentlichen Lebens war, hatten die Medien kein Recht, uneingeschränkt in die Privatsphäre dieser Person einzudringen. Die genauen Daten des Personalausweises sind eindeutig unerheblich für die öffentliche Debatte über Themen von allgemeinem oder öffentlichem Interesse. Die Datenschutzbeauftragte legte in einem bestimmten Fall außerdem fest, dass aus Sicht des öffentlichen Interesses, über aktuelle Angelegenheiten informiert zu sein, und für das Ausstellen eines Such- oder Haftbefehls für die Ergreifung einer Person nur bestimmte personenbezogene Daten erforderlich sind (Foto und Name),

¹⁵ Staatliches Amtsblatt der Republik Slowenien, Nr. 110/2006.

nicht aber alle Daten. Auch wenn personenbezogene Daten nur in begrenztem Umfang veröffentlicht werden, würde die Öffentlichkeit alle Informationen erhalten, die sie braucht, um ausreichend informiert zu sein. Alle übrigen personenbezogenen Daten der betroffenen Person sind mit Blick auf das öffentliche Interesse und die freie Meinungsäußerung nicht von Bedeutung, da Personen anhand eines Fotos und des vollständigen Namens identifiziert werden können.

Nach dem Grundsatz der Verhältnismäßigkeit gab es keine angemessene rechtliche Grundlage, die die Veröffentlichung der oben genannten personenbezogenen Daten der betreffenden Person gerechtfertigt hätte; daher stellte die Veröffentlichung der Daten auf der Website einen Verstoß gegen Artikel 3 des Datenschutzgesetzes dar. Der Umfang der veröffentlichten personenbezogenen Daten war dem Zweck der Veröffentlichung nicht angemessen.

Nachdem das Medienunternehmen die Entscheidung der Datenschutzbeauftragten erhalten hatte, beseitigte es innerhalb einer gesetzten Frist die festgestellten Unregelmäßigkeiten und verhinderte weitere Verstöße.

3. Ähnlich wie im oben genannten Fall veröffentlichte ein anderes Medienunternehmen für dieselbe Person folgende personenbezogenen Daten auf ihrer Website: Foto, Name, Geburtsdatum, Geburtsort, Personenkennzahl (EMŠO), Geschlecht, Personalausweisnummer, Ausstellungsort sowie Gültigkeitszeitraum des Ausweises und die Unterschrift der Person. Aus den in Punkt 2 genannten Gründen und nach der aufsichtsrechtlichen Entscheidung der Datenschutzbeauftragten entfernte das Medienunternehmen die unnötigerweise veröffentlichten personenbezogenen Daten von der Website.

4. In einem anderen Fall im Rahmen der Inspektion stellte die Datenschutzbeauftragte folgenden Verstoß gegen das Datenschutzgesetz fest: In der Druckausgabe einer Tageszeitung wurde das Foto eines Reisepasses abgedruckt, und somit wurden folgende personenbezogenen Daten des Passinhabers veröffentlicht: Foto, Name, Nationalität, Geburtsdatum, Geschlecht, Geburtsort, Ausstellungsdatum, Gültigkeitszeitraum des Passes, Passnummer, Personenkennzahl (EMŠO), ausstellende Behörde und Unterschrift. Der für die Datenverarbeitung

Verantwortliche hatte keine rechtliche Grundlage für diese Verwendung der Daten, das heißt für die Veröffentlichung der personenbezogenen Daten (weder per Gesetz noch durch die persönliche Zustimmung der betreffenden Person), und es handelte sich auch nicht um einen Fall, in dem das Informationsrecht der Öffentlichkeit die Veröffentlichung aller offengelegten personenbezogenen Daten gerechtfertigt hätte. Ähnlich wie in den oben genannten Fällen war der Umfang der veröffentlichten personenbezogenen Daten auch in diesem Fall nicht dem Zweck der Veröffentlichung angemessen.

5. Die Tageszeitung druckte eine Strafanzeige, die die Polizei gegen eine Privatperson erstattet hatte, und nutzte damit auf rechtswidrige Weise die folgenden personenbezogenen Daten: Name, Geburtsdatum, Geburtsort, Adresse, Nationalität und Personenkennzahl (EMŠO). Die Datenschutzbeauftragte stellte auch in diesem Fall einen Verstoß gegen das Datenschutzgesetz fest, der darin bestand, dass die oben genannten personenbezogenen Daten ohne angemessene Rechtsgrundlage oder die persönliche Zustimmung der betreffenden Person veröffentlicht wurden.

Die Datenschutzbeauftragte erließ 2007 **eine Reihe von Beschlüssen, die von den nationalen Medien veröffentlicht wurden**; dabei sind vor allem zwei zu nennen:

1. Die Datenschutzbeauftragte leitete Inspektionen aller slowenischen Apotheken und Versicherungen, die freiwillige Krankenversicherungen anbieten, ein. Auslöser dafür war die öffentliche Debatte über den Streit zwischen verschiedenen Apotheken und der Krankenversicherung Vzajemna. In ihrer Entscheidung interpretierte die Datenschutzbeauftragte die Mittel, mit denen die personenbezogenen Daten im Zusammenhang mit freiwilligen Krankenversicherungen übertragen werden sollten, da die Übertragung von personenbezogenen Daten eines der Streitthemen zwischen Apotheken und Versicherungen war. Im Zuge der Inspektion wurde festgestellt, dass die folgenden personenbezogenen Daten der Versicherten zwischen Versicherungen und Apotheken ausgetauscht werden: Krankenversicherungsnummer, Nummer der Krankenversicherungskarte, Geburtsdatum, Geschlecht, Name oder Kennnummer

sowie die Menge des betreffenden Arzneimittels oder der betreffenden medizinischen Geräte und das Datum, an dem das Medikament oder Gerät verabreicht bzw. ausgeliefert wurde.

Krankenversicherungen sind auf Grundlage bestehender Gesetze berechtigt, personenbezogene Daten zu erhalten. Die Datenschutzbeauftragte wies insbesondere darauf hin, dass die Versicherungen (sowie alle Verantwortlichen für Datenablatesysteme, einschließlich der Apotheken in diesem Fall) die Daten in Übereinstimmung mit dem Zweck behandeln müssen, zu dem die Daten erhoben wurden (In diesem Fall durften personenbezogene Daten für Ausgleichsregelungen sowie für Verrechnungszwecke und die Behandlung von Verlusten benutzt werden; die Apotheken durften die Daten nur für die Übertragung an die Versicherungen, die Überprüfung von Abrechnungen, und möglicherweise für von anderen Gesetzen festgelegte Zwecke verwenden.). Besonders bei Versicherungen ist es nicht gestattet, diese Daten in irgendein anderes Datenablatesystem einzuspeisen, das mit anderen Versicherungstransaktionen verbunden ist.

Nach Artikel 22, Absatz 1 des Datenschutzgesetzes besteht eine Verpflichtung zur Weitergabe personenbezogener Daten. Daher müssen die für die Datenverarbeitung Verantwortlichen (die Apotheken) diese Daten weiterleiten und haben nicht das Recht, sich anders zu entscheiden. Apotheken und Versicherungen dürfen keine potenziell unangemessenen (zu geringe) Entgelte für die Übertragung verwenden, die zulasten des öffentlichen Interesses der Republik Slowenien und der versicherten Personen gehen. Insbesondere dürfen sie nicht ihre Verpflichtung zum Schutz der personenbezogenen Daten vernachlässigen, zum Beispiel indem sie die Daten in nicht gesicherter elektronischer Form versenden, oder entgegen der gesetzlichen Vorschriften das Einfordern der Erstattung für die bezahlten Medikamente und das Übertragen der personenbezogenen Daten auf die Versicherten abwälzen (indem sie die Versicherten bitten, der Versicherung die Quittungen vorzulegen). Das Gesetz schreibt weiterhin eindeutig vor, dass die Daten ausschließlich von Apotheken an Versicherungen übertragen werden dürfen.

Die strittigen Kosten dieser Dienstleistung, die die Apotheken für die Versicherungen erbringen, können

natürlich unter Umständen Gegenstand separater gerichtlicher Auseinandersetzungen sein; doch da das Gesetz eindeutig vorschreibt, wer für die Datenübertragung verantwortlich ist, darf die Datenübertragung auch während solcher gerichtlicher Auseinandersetzungen nicht unterbrochen werden. Da die übertragenen Daten vertrauliche personenbezogene Daten enthalten (über den Gesundheitszustand einer Person), hat die Datenschutzbeauftragte beschlossen, dass die Daten verschlüsselt mit einer elektronischen Signatur übertragen werden müssen, um sicherzustellen, dass sie unlesbar und unkenntlich sind.

Eine der verantwortlichen Parteien hat Berufung gegen die Entscheidung der Datenschutzbeauftragten eingelegt. Das Gericht hat in einem Verwaltungsstreit angeordnet, dass die Entscheidung der Datenschutzbeauftragten annulliert wird.

2. Die Datenschutzbeauftragte hat eine Reihe von Beschwerden von Personen erhalten, die sich darüber beklagten, dass sie offene, bereits ausgefüllte Steuererklärungen oder Formulare, die schlecht versiegelt waren, erhalten haben, sodass jeder die darin enthaltenen steuerrelevanten Informationen einsehen konnte. Die Datenschutzbeauftragte leitete eine Inspektion gegen die Steuerbehörden der Republik Slowenien ein sowie gegen die Personen, die in den Behörden dafür verantwortlich sind, beim Versand ausgefüllter Steuererklärungen einen angemessenen Schutz personenbezogener Daten zu gewährleisten. Darüber hinaus wurde ein Verfahren wegen Datenschutzverstößen gegen den externen Datenverarbeitungsanbieter der Behörde eingeleitet.

Sowohl die Behörde als auch ihr externer Datenverarbeitungsanbieter haben den Verstoß begangen, nicht in ausreichendem Maße für den Schutz personenbezogener Daten beim Zustellen von Steuerbescheiden zu sorgen, sodass nicht autorisierte Personen die betroffenen personenbezogenen Daten einsehen und verarbeiten konnten. Die Behörde muss gemäß Artikel 24 und 25 des Datenschutzgesetzes als Verantwortlicher für die Datenverarbeitung den Schutz der personenbezogenen Daten aus ihren Datenablatesystemen gewährleisten – auch während der Übertragung an andere Nutzer und während des Transports der Steuerunterlagen an die

jeweilige steuerpflichtige Person. Dies beinhaltet für die Behörde auch die Pflicht, sicherzustellen, dass jegliche Unterlagen mit vertraulichen personenbezogenen Daten über steuerpflichtige Personen (Steuergeheimnis) in Umschlägen versandt werden, die erstens verhindern, dass Dritte die darin enthaltenen Daten ohne sichtbare Schäden am Umschlag einsehen können, und zweitens so beschaffen sind, dass Dritte bei normalem Licht den Inhalt der Umschläge (einschließlich personenbezogener Daten) nicht sehen können.

Die Steuerverwaltung der Republik Slowenien hat den Fehler behoben und sofort nach Eingang der Beschwerden der Einzelpersonen das Zustellen der ausgefüllten Steuerunterlagen eingestellt. Danach wurden alle weiteren Sendungen zusätzlich durch eine Plastikfolie gesichert und zusätzlich versiegelt, um einen angemessenen Schutz der ausgefüllten Steuererklärungen zu gewährleisten.

Die Datenschutzbeauftragte hat 2007 **zwei Anträge auf richterliche Überprüfung gestellt**:

In ihrer Amtszeit hat die Datenschutzbeauftragte zwei Anträge auf eine verfassungsrechtliche Überprüfung bestimmter Vorschriften aus vier Gesetzen (Statute Laws) beantragt (2 im Jahr 2007) und zur Vorbereitung vieler nationaler Gesetze in Bezug auf den Schutz personenbezogener Daten beigetragen.

1. 2007 entschied¹⁶ das Verfassungsgericht über den im Dezember 2006 von der Datenschutzbeauftragten gestellten Antrag auf eine verfassungsrechtliche Überprüfung von Artikel 96, Absatz 1; Artikel 98, Absatz 2; Artikel 100; Artikel 103, Absätze 5 und 6; sowie Artikel 114, Absatz 1 des Grundbuchgesetzes¹⁷. Das Gericht bewilligte den Antrag der Datenschutzbeauftragten, der sich zum Teil auf den öffentlichen Charakter des Grundbuchs und auf physische Personen bezog (Daten zu Eigentümern, Nutzern, Mietern und Verwaltern von Immobilien – deren Namen und Personenkennzahl (EMŠO)); dies war die Hauptbeschwerde, die die Datenschutzbeauftragte gegen den Gesetzgeber vorgebracht hatte. Der öffentliche Charakter des Grundbuchs ermögliche, dass im

Zusammenhang mit einer Immobilie der Name und die Personenkennzahl einer Person veröffentlicht werden. Diese Informationen seien dann im Internet verfügbar, und damit könnten die personenbezogenen Daten für jeden beliebigen Zweck verwendet werden; und dies, so befand das Verfassungsgericht, ist verfassungswidrig. Das Gericht bestätigte mit der Entscheidung, dass durch die Veröffentlichung des Grundbuchs dem Einzelnen ein irreparabler Schaden zugefügt wird.

2. Eine richterliche Überprüfung von Artikel 62, Absatz 2, Punkt 7 sowie Artikel 62d, Absatz 2, des Gesetzes über Gesundheitsversorgung und Krankenversicherung (Health Care and Health Insurance Act)¹⁸, die die Nutzung und Übertragung von Daten regeln, die für die Umsetzung anfechtbarer Regelungen notwendig sind, sowie Artikel 2 der Regeln für die Umsetzung von Krankenzusatzversicherungen, die die Anbieter von Gesundheitsdienstleistungen befolgen sollen¹⁹. Die Datenschutzbeauftragte argumentierte, in Bezug auf die geforderte Spezifizierung der Art der zu verarbeitenden personenbezogenen Daten widersprächen die fraglichen Regelungen Artikel 38 der slowenischen Verfassung. Die fraglichen Regelungen des Gesetzes enthalten eine allgemeine Regel und schreiben vor, alle notwendigen Daten oder alle Daten, die für die Umsetzung der anfechtbaren Regelungen notwendig sind, zu übertragen. Die bestehende Gesetzgebung spezifiziert nicht die Art der zu verarbeitenden personenbezogenen Daten; dies führt zu unterschiedlichen Auslegungen und somit unter Umständen zu einer unverhältnismäßigen Nutzung personenbezogener Daten. Dies widerspricht dem verfassungsmäßigen Grundsatz der Verhältnismäßigkeit, der besagt, dass jeglicher Eingriff in verfassungsmäßig geschützte Rechte den Zielen angemessen sein muss, die durch einen solchen vom Gesetz festgelegten Eingriff erreicht werden sollen. Ebenso ist es verfassungswidrig, den Umfang und die Art der erhobenen personenbezogenen Daten durch eine Regelung festzulegen, die nicht den Status eines Gesetzes erfüllt (anstatt durch ein Gesetz, das von einem zur Gesetzgebung befugten Organ erlassen wurde). Die rechtliche Definition, die vorschreibt, dass „alle notwendigen Daten“ übertragen werden sollen, ist

¹⁶ Staatliches Amtsblatt der Republik Slowenien, Nr. 65/2007.

¹⁷ Staatliches Amtsblatt der Republik Slowenien, Nr. 47/2006.

¹⁸ Staatliches Amtsblatt der Republik Slowenien, Nr. 72/2006 und 91/2007.

¹⁹ Staatliches Amtsblatt der Republik Slowenien, Nr. 7/2007.

nicht festgelegt und definiert nicht hinreichend genau die Verarbeitung der personenbezogenen Daten, wie es Artikel 38 der Verfassung vorschreibt; sie überlässt die Regulierung der Verarbeitung personenbezogener Daten in zu großem Umfang Verordnungen, die keinen Gesetzescharakter haben.

3. Richterliche Überprüfung von Artikel 47, Absatz 4; Artikel 58, Absatz 2, Punkt 1, Unterabsatz 1; Artikel 123, Absatz 1, Punkt 5; Artikel 165, Punkte 3 und 4; Artikel 247, Absatz 2, Punkt 2; Artikel 334, Absatz 1, Punkt 3; Artikel 432, Absatz 1, Punkt 3; sowie Artikel 543, Absatz 1, Punkt 1 des Finanzmarktgesetzes (Market in Financial Instruments Act)²⁰ Diese rechtlichen Vorgaben widersprechen nach Meinung der Datenschutzbeauftragten Artikel 38 der slowenischen Verfassung, weil sie die Art der zu verarbeitenden personenbezogenen Daten nicht hinreichend spezifizieren.

Die strittige Gesetzgebung spezifiziert weder den Zweck noch den Umfang der personenbezogenen Daten, die erhoben oder verarbeitet werden sollen. Die strittigen gesetzlichen Vorschriften schreiben lediglich das Verarbeiten personenbezogener Daten vor, spezifizieren aber nicht, welche personenbezogenen Daten verarbeitet werden sollen. Dies lässt die Frage nach dem Umfang der zu verarbeitenden und zu erhebenden personenbezogenen Daten offen und überlässt diese Frage der unter Umständen willkürlichen Entscheidung der Finanzmarktaufsicht. Die bestehende Rechtsvorschrift überlässt die Definition dieses Bereichs Regelungen ohne Gesetzescharakter, und dies ist verfassungswidrig. Umfang und Art der personenbezogenen Daten sollten vollständig durch ein Gesetz geregelt werden.

Dass die bestehende Rechtsgrundlage, die das Verarbeiten personenbezogener Daten definiert, offen und nicht hinreichend spezifisch ist, könnte zu unterschiedlichen Auslegungen führen und somit zu einer unverhältnismäßigen Nutzung personenbezogener Daten. Dies widerspricht dem Grundsatz, dass jede Maßnahme, das heißt der Umfang der Verletzung des geschützten Wertes oder Gutes, dem Wert des vom Gesetz definierten Ziels angemessen sein sollte. Daher sollte der rechtmäßige Eingriff in bestimmte Rechte

auf das Minimum reduziert werden, das gerade noch gewährleistet, dass die definierten Ziele erreicht werden. So wird ein angemessener Kompromiss erzielt zwischen dem Wert dieser Ziele und der Schwere des Verletzens der Rechte einer Person.

C. Wichtige spezifische Themen

Das Gesetz zum Schutz personenbezogener Daten legt detailliert fest, unter welchen Bedingungen eine Videoüberwachung von Eingängen zu Geschäfts- und Wohngebäuden sowie Arbeitsbereichen erlaubt sein kann. Sind diese Regelungen erfüllt, müssen die Personen, die solch eine Videoüberwachung durchführen, für die Einrichtung der Videoüberwachung keine Erlaubnis der Aufsichtsbehörde einholen. Die Personen, die die Videoüberwachung durchführen, müssen sich lediglich bei der Umsetzung der Videoüberwachung an die gesetzlichen Bestimmungen halten, das heißt, einen förmlichen Beschluss über die Durchführung der Videoüberwachung fassen, eine angemessene Bekanntmachung veröffentlichen, die Beschäftigten schriftlich informieren, im Falle eines Wohngebäudes die Zustimmung der anderen Eigentümer einholen, die Gewerkschaft konsultieren usw. Viele der für die Videoüberwachung Verantwortlichen versäumten es indes, ihre Videoüberwachungspraxis an die gesetzlichen Bestimmungen anzupassen, was zu zahlreichen Beschwerden bei der Aufsichtsbehörde führte.

Die Gründe für Vermutungen eines Verstoßes gegen das Datenschutzgesetz hatten in vielen Fällen mit einer illegalen Erhebung personenbezogener Daten zu tun, zum Beispiel: Das Erheben von personenbezogenen Daten im Zusammenhang mit der Teilnahme an verschiedenen Glücksspielwettbewerben, in Bezug auf Verträge mit Telekommunikationsbetreibern oder in Bezug auf die Überwachung von Beschäftigten durch den Arbeitgeber. Andere Bereiche, in denen Verstöße gegen das Datenschutzgesetz vermutet wurden, waren unter anderem: Direktmarketing, die illegale Veröffentlichung personenbezogener Daten (auf verschiedenen Informationstafeln in Wohngebäuden und am Arbeitsplatz), ein unangemessener Schutz personenbezogener Daten und die Übertragung personenbezogener Daten an unbefugte Nutzer. Wichtige Bereiche, in denen die Inspektionen erhebliche Versäumnisse aufdeckten, sind:

²⁰ Staatliches Amtsblatt der Republik Slowenien, Nr. 67/2007 und 100/2007.

Das Fehlen einer Rechtsgrundlage für die Datennutzung (entweder per Gesetz oder durch die persönliche Zustimmung der Person, auf die sich die Daten beziehen); unzureichender Schutz personenbezogener Daten; fehlendes Eintragen des Datenablatesystems in das Register der Datenschutzbehörde; Verarbeiten vertraulicher personenbezogener Daten.

Ende 2007 hatten rund 10 000 Personen, die personenbezogene Daten verarbeiten, ihre Ablagesysteme für personenbezogene Daten gemeldet (nach der Ergänzung des Datenschutzgesetzes im Jahr 2007 sank die Zahl der für die Datenverarbeitung Verantwortlichen, die Daten der von ihnen verwalteten Ablagesysteme für personenbezogenen Daten melden müssen, deutlich). Das Register der Ablagesysteme für personenbezogene Daten ist auf der Website der Datenschutzbeauftragten veröffentlicht und ermöglicht es jedermann, Informationen zu den Dateisystemen der für die Datenverarbeitung Verantwortlichen in Slowenien, Informationen über die von den einzelnen für die Datenverarbeitung Verantwortlichen verwalteten Dateisysteme, die Art der in den einzelnen Dateisystemen enthaltenen personenbezogenen Daten, den Verarbeitungszweck usw. einzusehen.

Inspektionen (per 1. Dezember 2007 beschäftigt die Datenschutzbeauftragte elf Inspektoren): Die Datenschutzbeauftragte erhielt 2007 **406** Anträge und Beschwerden (179 im öffentlichen und 227 im privaten Sektor) bezüglich möglicher Verstößen gegen die Bestimmungen des Datenschutzgesetzes; im Vorjahr waren es **231** Fälle (88 im öffentlichen und 143 im privaten Sektor). Dies entspricht einem Zuwachs von 76 %. Bei den meisten Beschwerden ging es um die Offenlegung personenbezogener Daten gegenüber unbefugten Nutzern, um das unrechtmäßige oder übermäßige Erheben personenbezogener Daten, um illegale Videoüberwachungen, unzureichenden Schutz personenbezogener Daten, unrechtmäßige Veröffentlichung personenbezogener Daten usw. Dementsprechend war ein deutlicher Anstieg der eingeleiteten Verfahren wegen Ordnungswidrigkeiten zu verzeichnen: 133 Fälle im Jahr 2007 im Vergleich zu 41 Fällen im Vorjahr.

Die Zahl der Anträge auf **schriftliche Stellungnahme und Klärung**, die die Datenschutzbeauftragte erhalten

hat, ist ebenfalls deutlich gestiegen: von 616 im Jahr 2006 auf 1 144 im Jahr 2007 (im Jahr 2005 waren es sogar nur 34 Fälle!). Dies spiegelt zweifellos das wachsende Bewusstsein der Öffentlichkeit für das Recht auf Schutz der Privatsphäre wider, das das moderne Gesetz zum Schutz personenbezogener Daten verbietet, und hängt hoffentlich auch mit der transparenten Arbeit und der intensiven Öffentlichkeitsarbeit der Datenschutzbeauftragten zusammen.



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 die Annahme des Organgesetzes 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. Der Königliche Erlass 1720/2007 vom 21. Dezember 2007, durch den die Verordnung bestätigt wird, die zur Umsetzung des Organgesetzes über den Schutz personenbezogener Daten geführt hat

Die Bestätigung dieser Verordnung stellt einen Meilenstein für die spanische Gesetzgebung im Bereich des Datenschutzes dar. Damit sollen in einem für die Grundrechte sehr heiklen Bereich wie dem Datenschutz die erforderliche Rechtssicherheit garantiert und die von der spanischen Datenschutzbehörde (*Agencia Española de Protección de Datos* – AEPD) erarbeiteten Präzedenzfälle konsolidiert werden. Darüber hinaus sollen damit die am häufigsten gestellten Fragen beantwortet und die möglicherweise noch vorhandenen Probleme bei der Deutung beseitigt werden, wobei besonderes Augenmerk auf Probleme von potenziell größerer Bedeutung gelegt wird. Dabei wurden Kommentare und Feststellungen der zuständigen Behörden der Autonomen Gemeinschaften sowie von Personen aus den über sechzig Organisationen und Verbänden berücksichtigt, die die von dieser Verordnung betroffenen Rechte und Interessen repräsentieren.

Die Verordnung bezieht in ihren Anwendungsbereich ausdrücklich nicht automatisierte Dateien und Datenverarbeitung (auf Papier) mit ein und legt bestimmte Kriterien hinsichtlich der Sicherheitsmaßnahmen fest. Sie regelt auch den räumlichen Geltungsbereich und legt fest, dass Datenverarbeitung grundsätzlich dieser Verordnung unterliegt, sofern nach den Regeln des internationalen öffentlichen Rechts spanisches Recht anwendbar ist, oder wenn Mittel eingesetzt werden, die sich auf spanischem Hoheitsgebiet befinden, es sei denn, sie werden ausschließlich zum Transit genutzt.

Von besonderer Bedeutung ist die Einbeziehung der Genehmigung zur Datenverarbeitung als Vorbedingung für die von dem für die Datenverarbeitung Verantwortlichen verfolgten berechtigten Interessen.

Die Verordnung legt außerdem ein Verfahren fest, das gewährleistet, dass jede Person genaue Kenntnis über die Verwendung der Daten hat, bevor sie deren Erfassung und Verarbeitung zustimmt. Des Weiteren ist die Schaffung besonderer Vorschriften im Hinblick auf die Einholung der Zustimmung von Minderjährigen von besonderer Bedeutung, da hierfür bei Kindern unter 14 Jahren die Mitwirkung der Eltern oder Erziehungsberechtigten erforderlich ist.

Im Streben nach einer besseren Gewährleistung des Bürgerrechts auf Überwachung der Richtigkeit und Nutzung der persönlichen Daten ist der für die Datenverarbeitung Verantwortliche ausdrücklich verpflichtet, den betroffenen Personen kostenfreie und einfache Mittel zur Verfügung zu stellen, die es ihnen ermöglichen, ihr Recht auf Zugriff, Berichtigung, Löschung und Einspruch auszuüben. Es ist gleichermaßen verboten, die betroffene Person aufzufordern, Einschreiben oder dergleichen zu versenden bzw. Telekommunikationsmittel zu benutzen, die zusätzliche Gebühren verursachen. Und obwohl die Verordnung nicht für verstorbene Personen gilt, sieht sie letztlich vor, dass Bürger den für die Datenverarbeitung Verantwortlichen über den Tod eines Angehörigen informieren und die Löschung seiner Daten beantragen können, um die Angehörigen somit vor schmerzhaften Situationen zu bewahren.

Die für die Datenverarbeitung Verantwortlichen geltenden Vorschriften werden ebenfalls im Einzelnen geregelt. Eine weitere Neuheit ist die Einrichtung eines detailreichen Verarbeitungssystems in Bezug auf Zahlungsfähigkeit und Kreditwürdigkeit einerseits und Werbung und Marktforschung andererseits, mit dem die im Organgesetz 15/1999 enthaltenen besonderen Vorschriften umgesetzt werden.

Im Bereich des internationalen Datentransfers räumt die Verordnung dem Direktor der spanischen Datenschutzbehörde systematisch die Möglichkeit ein, das Vorhandensein eines angemessenen Datenschutzniveaus in einem Land festzustellen, in dem es eine solche Erklärung seitens der Europäischen Union nicht gibt; sie trägt damit zur Klärung von Situationen bei, in denen Garantien erteilt werden können, die eine Datenübertragung durch den Direktor erlauben, und

schließt die sogenannten „verbindlichen Unternehmensvorschriften“ oder firmeninternen Kodizes von multinationalen Konzernen oder Gruppen ein. Schließlich legt die Verordnung die Verfahren fest, die die spanische Datenschutzbehörde zur Erfüllung ihrer Aufgaben anwenden sollte, und dehnt die Aufgaben der spanischen Datenschutzbehörde auf die Zusammenarbeit mit den Datenschutzbehörden der Autonomen Gemeinschaften aus.

https://www.agpd.es/upload/English_Resources/reglamentolopd_en.pdf

2. Organgesetz 10/2007 vom 8. Oktober 2007 zur Vereinheitlichung polizeilicher Datenbanken mit DNA-Merkmalen

Nach der Unterzeichnung des Vertrags von Prüm im Mai 2005 war es notwendig, die polizeilichen Datenbanken zusammenzulegen, welche zum damaligen Zeitpunkt in Spanien rechtmäßig Geninformationen enthielten. Ziel dieses Organgesetzes war die Vereinheitlichung der polizeilichen Datenbanken, in denen DNA-Merkmale gespeichert waren, welche man aus bei strafrechtlichen Ermittlungen entnommenen Proben gewonnen hatte. Diese Merkmale liefern jedoch nur genetische Informationen über die Identität der Person und ihr Geschlecht (nichtkodierende DNA). Ebenso vereinheitlicht die Verordnung die Gewährleistung für die Weitergabe derartiger Informationen an dazu befugte Sicherheitskräfte sowie die Speicherdauer. Derartige Informationen dürfen nur von zugelassenen Einrichtungen und allein im Rahmen von strafrechtlichen Ermittlungen verwendet werden. Die Daten werden bis zur Verjährung des jeweiligen Vergehens aufbewahrt.

3. Gesetz 37/2007 vom 16. November über die Weiterverwendung von Informationen des öffentlichen Dienstes

Dieses Gesetz setzt die Richtlinie 2003/98/EG in spanisches Recht um. Es betrifft Dokumente, die der öffentliche Dienst Bürgern oder Unternehmen zur Weiterverwendung zugänglich machen könnte, um das Potenzial derartiger Informationen im Hinblick auf wirtschaftliches Wachstum und die Schaffung von Arbeitsplätzen voll auszuschöpfen und um die Leistungen des öffentlichen Dienstes transparenter zu machen. Gemäß den Bestimmungen der Richtlinie ändert dieses Gesetz die im spanischen Datenschutzgesetz festgeschriebenen Pflichten und Rechte in keiner Weise.

http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/19814 (auf Spanisch)

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 staatliche Telekommunikationsgesetz 32/2003 vom 3. November 2003 in spanisches Recht umgesetzt und per Königlichem Dekret 424/2005 vom 15. April 2005 verabschiedet, das die Bedingungen für die Bereitstellung von elektronischen Kommunikationsdiensten und des Universaldienstes sowie den Schutz der Benutzer festlegt.

1. Gesetz 25/1807 vom 18. Oktober 2007 über die Vorratsspeicherung von Daten in Bezug auf elektronische Kommunikation und öffentliche Kommunikationsnetze

Dieses Gesetz, eine Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, begrenzt die Speicherung von Daten über elektronische Kommunikation aus Gründen der öffentlichen Sicherheit auf 12 Monate. Informationen über vergebliche Anrufe und Prepaid-Karten werden ebenfalls gespeichert. Die Übertragung dieser Informationen an Sicherheitskräfte erfolgt nach einer gerichtlichen Anordnung und nur an dazu befugte Agenten.

http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (auf Spanisch)

2. Gesetz 11/2007 vom 22. Juni 2007 über den elektronischen Zugang von Bürgern zu öffentlichen Diensten

Mit diesem Gesetz soll der Einsatz von elektronischen Medien in den Beziehungen zwischen Regierung und Bürgern verstärkt und damit der universelle Zugang zu den Informationen und Dienstleistungen der öffentlichen Verwaltungen sowie die Kommunikationsfähigkeit zwischen den einzelnen Verwaltungsstellen verbessert werden. Das Gesetz legt fest, dass die zugängliche Nutzung dieser Art von Mitteln in sicherer und umfassender Form ein Bürgerrecht und infolgedessen eine Pflicht der Verwaltungsbehörden darstellt. Bei der Datenverarbeitung müssen daher die im spanischen Datenschutzgesetz festgelegten Rechte und Pflichten eingehalten werden, um zu gewährleisten, dass Daten, die auf elektronischem Wege erfasst wurden, auch nur zu dem Zweck verwendet werden, zu dem sie an eine bestimmte Behörde übermittelt wurden.

Infolge dieses Gesetzes werden das offizielle spanische Amtsblatt und andere offizielle Amtsblätter in elektronischer Form veröffentlicht. Da es sich hier ja um ein grundlegendes Gesetz

handelt, wird es von den Autonomen Gemeinschaften entsprechend umgesetzt (z.B. Dekret 232/2007 der Autonomen Gemeinschaft des Baskenlandes vom 18. Dezember 2007). http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/12352 (auf Spanisch)

3. Gesetz 56/2007 vom 28. Dezember 2007 über die Maßnahmen zur Förderung der Informationsgesellschaft

Dieses Gesetz legt einige Neuerungen in Bezug auf elektronische Verfahren zur Rechnungsstellung und Auftragsvergabe im elektronischen Handel fest, um die Beziehungen zwischen den Nutzern und Verbrauchern und den Anbietern elektronischer Dienste, die die Einhaltung der spanischen Rechtsvorschriften im Bereich des Datenschutzes für ihre eigene Datenverarbeitung gewährleisten müssen, abzusichern.

Außerdem sollten Unternehmen, die gewisse Dienstleistungen von besonderer wirtschaftlicher Bedeutung anbieten, den betroffenen Personen die Ausübung ihrer Rechte auf Auskunft, Berichtigung, Löschung und Einspruch auf elektronischem Wege ermöglichen. http://www.boe.es/g/es/bases_datos/doc.php?coleccion=iberlex&id=2007/22440 (auf Spanisch)

B. Bedeutende Rechtsprechung

Anlässlich einer Analyse des Grads der Rechtssicherheit bei der Anwendung des spanischen Datenschutzgesetzes muss geprüft werden, inwieweit die Entscheidungen der Datenschutzbehörde AEPD ratifiziert oder vor Gericht widerrufen werden. Das Berufungsgericht beim spanischen Gerichtshof (*Audiencia Nacional*) hat 158 Urteile und der Oberste Gerichtshof Spaniens 13 Urteile und zwei Annahmeverweigerungen erlassen. Nachfolgend werden die wichtigsten Urteile zusammengefasst:

1. Oberster Gerichtshof

- Massenzusendung von Spam-Mails.
- Das Urteil vom 25. Oktober 2007 bestätigt, dass die Veröffentlichung personenbezogener Daten eines Bürgers in dem Informationssystem eines Unternehmens ohne seine Zustimmung sein Recht auf Datenschutz verletzt.
- Im Urteil vom 14. November 2007 heißt es, dass die datenschutzrechtlichen Bestimmungen und die

Regulierungsbehörde für Patientenautonomie nicht zwingend vorschreiben, medizinische Untersuchungsergebnisse zurückzugeben.

- Im Urteil vom 19. Dezember 2007 wird der Konflikt zwischen zwei Grundrechten, dem Recht auf Vereinigungsfreiheit und dem Recht auf Schutz personenbezogener Daten, analysiert und Ersterem Vorrang eingeräumt.
- Urteil des Obersten Gerichtshof Spaniens über Apostasie. Gegen den Beschluss der Datenschutzbehörde AEPD in Bezug auf das Bürgerrecht, nicht im Taufregister verzeichnet zu sein, und auf das Recht auf Löschung dieser Dateien wurde vom Erzbischof von Valencia vor dem Obersten Gerichtshof Spaniens Berufung eingelegt. Der Beschluss des Obersten Gerichtshofs bestätigte das Urteil der spanischen Datenschutzbehörde. Folgende Aspekte dieser Entscheidung müssen hervorgehoben werden: Bei Taufverzeichnissen handelt es sich um Dateien mit personenbezogenen Daten im Sinne des Datenschutzgesetzes; wird einem Wunsch auf Löschung dieser Daten nicht entsprochen, so kann es sich hierbei um einen Verstoß gegen das Datenqualitätsprinzip handeln.

2. Oberster Spanischer Gerichtshof

Es muss betont werden, dass die Kriterien der spanischen Datenschutzbehörde AEPD bei 11 von 13 Gelegenheiten, bei denen dieses Thema dem Obersten Spanischen Gerichtshof zur Prüfung vorgelegt wurde, durch Letzteren ratifiziert wurde.

Insbesondere muss auf die folgenden Urteile des Obersten Gerichtshofs Spaniens hingewiesen werden:

- Mit dem Urteil vom 16. Februar 2007 wird die Berufung zurückgewiesen, welche gegen das Urteil des spanischen Gerichtshofes eingelegt worden war, mit dem wiederum das Rechtsmittelverfahren zurückgewiesen worden war, das zur Annullierung der von dieser Behörde erlassenen Anweisung 1/1995 angestrengt worden war. Das Urteil des Obersten Gerichtshofes geht davon aus, dass die Behörde Anweisungen erlassen darf, um die Maßnahmen der Datenverarbeiter im Hinblick auf die automatisierte Verarbeitung zu organisieren, damit diese die gesetzlich verankerten Grundsätze verpflichtend und nach außen hin sichtbar erfüllen, und zwar zu ähnlichen

Bedingungen wie die, die eben dieses Gericht anderen Regulierungsbehörden zugestanden hat.

- Das Urteil vom 27. März 2007 bestätigt die Entscheidung der Behörde, laut der die Überlassung von Kundendaten eines [Telekommunikations-]Betzreibers an einen Drittanbieter den Bestimmungen des Datenschutzgesetzes widerspricht, da diesem Letztgenannten die Überprüfung der Zahlungsfähigkeit dieser Personen ermöglicht wird.
- Mit dem Urteil vom 17. April 2007 wird bestätigt, dass die Sanktionen, die die Datenschutzbehörde AEPD einer Reihe von Einrichtungen auferlegt hat, die Bestimmungen des Gesetzes erfüllt, weil diese Einrichtungen während ihrer Beteiligung an einem Auswahlverfahren für Teilnehmer eines bestimmten TV-Programms Dritten gewisse Daten überlassen haben, die sich zum Teil auf den Gesundheitszustand der Teilnehmer bezogen, und weil die seitens der Datenschutzvorschriften geforderten Sicherheitsmaßnahmen nicht erfüllt wurden.
- Mit dem Urteil vom 12. April 2007 wird bestätigt, dass die Behörde bei ihrer Entscheidung hinsichtlich der ungesetzlichen Datenverarbeitung eines Unternehmers die Bestimmungen des Gesetzes erfüllt hat; dieser hatte eine Einrichtung beauftragt, die Ursachen von Fehlzeiten seiner Mitarbeiter zu ermitteln und der Einrichtung zwecks dessen Informationen über den Gesundheitszustand seiner Mitarbeiter zukommen lassen.

3. Beschlüsse der spanischen Datenschutzbehörde

Im Laufe des Jahres 2007 ist die Anzahl der bei der spanischen Datenschutzbehörde AEPD eingereichten Beschwerden von Bürgern um rund 7 % auf insgesamt 1 624 gestiegen. Die Anzahl der Untersuchungen, die die Datenschutzbehörde AEPD aufgrund von Beschwerden oder von Amts wegen auf Initiative des Leiters der Behörde eingeleitet hat, belief sich auf 1 263. Auf der anderen Seite entschied die Datenschutzbehörde 2007 in insgesamt 399 Strafverfahren, was einem Anstieg von 32,5 % gegenüber dem Vorjahr entspricht. Für die Fälle, die als Straftat betrachtet wurden, hat die spanische Datenschutzbehörde AEPD Geldstrafen in Höhe von insgesamt 19,6 Millionen Euro verhängt.

Es gab eine sehr starke Zunahme der Anträge auf Rechtsschutz, wobei die Zahl der Anträge, die bewilligt wurden

(879 insgesamt) um 54 % stieg. Diese Anwendungsgebiete des Schutzes der Menschenrechte zeugen von den gleichen Überlegungen wie die oben beschriebenen Fälle, wobei die Rechte auf Löschung (62 %) und auf Zugriff (32 %) insgesamt am häufigsten gewahrt werden mussten.

Das Recht auf Löschung der Daten aus dem Jahr 2007 wurde wegen der Besonderheit im Zusammenhang mit der Löschung von Daten aus den Taufregistern der katholischen Kirche stark beeinflusst: Von den 896 eingeleiteten Verfahren auf Wahrung der Menschenrechte wurden insgesamt 34 % (304) aus eben diesem Grunde angestrengt.

Die von den Bürgerinnen und Bürger eingereichten Anträge auf Löschung betrafen außerdem folgende Angelegenheiten:

- Unrechtmäßige Speicherung von personenbezogenen Daten durch Finanzinstitute in Informationsdateien über Zahlungsfähigkeit und Kreditwürdigkeit sowie die entsprechende Löschung der Daten bei Beendigung der rechtlichen Beziehung zu den besagten Instituten.
- Löschung von personenbezogenen Daten aus den Dateien von Telekommunikationsbetreibern bei Wechsel des Telekommunikationsanbieters ohne Zustimmung des Teilnehmers.
- Löschung von Daten im Internet (Foren oder Messageboards, YouTube).
- Zugang zu Patientenakten.

Was die Sanktionen pro Wirtschaftssektor betrifft, lag der Telekommunikationsbereich mit 112 rechtskräftig entschiedenen Strafverfahren an erster Stelle, gefolgt von den Finanzinstituten mit 80 Fällen und dem Bereich Marketing-Kommunikation und Spams mit 37 Fällen. Nachfolgend finden Sie einige der wichtigsten Beschlüsse.

- **Videoüberwachung:** Die Datenschutzbehörde AEPD hat von Amts wegen Ermittlungen wegen der Erfassung und Verbreitung von Bildern einer Straße in Madrid über YouTube eingeleitet, um zu klären, ob es sich bei der Erfassung durch Videokameras und der darauf folgenden Verbreitung über YouTube um eine Verletzung des Datenschutzgesetzes handelt, da hierbei möglicherweise schwere oder sehr schwere Verstöße gegen die Datenschutzvorschriften begangen wurden, welche mit Strafen von bis zu 600 000 EUR geahndet werden können.

- **Emule:** Die spanische Datenschutzbehörde AEPD verhängte eine Strafe, weil personenbezogene Daten über das File-Sharing-System Emule in das Internet gelangt waren. Es handelt sich hierbei um die erste Strafe, die die Datenschutzbehörde für den Einsatz von Systemen verhängt, die u. a. den Austausch und das Herunterladen von Text-, Video- oder Musik-Dateien ermöglichen, die auf den Computern anderer Benutzer gespeichert sind. Die spanische Datenschutzbehörde AEPD fordert die Einführung von Sicherheitsmaßnahmen wie z. B. Firewalls und die sorgfältige Auswahl des Verzeichnisses, in dem mehrfach genutzte Informationen gespeichert werden.
- **YouTube:** Die Datenschutzbehörde AEPD hat von Amts wegen Ermittlungen wegen der Erfassung und Verbreitung von Bildern eines behinderten Menschen eingeleitet und das Recht des Vertreters der betroffenen Person auf Löschung geschützt, da es sich hierbei möglicherweise um einen sehr schweren Verstoß gegen das Datenschutzgesetz handelt, bei dem Bilder über den Gesundheitszustand eines Menschen verarbeitet und im Anschluss verbreitet wurden.
- **Internetforen:** Die spanische Datenschutzbehörde hat entschieden, dass das Recht auf Löschung auch für personenbezogene Daten gilt, die in einem Internetforum veröffentlicht wurden, sofern es sich bei der betroffenen Person weder um eine berühmte Persönlichkeit handelt noch um jemanden, der in einen bedeutenden Umstand verwickelt ist. Die Veröffentlichung personenbezogener Daten im Internet unterliegt nicht immer dem Schutz durch das Recht auf Meinungsfreiheit.

C. Wichtige spezifische Themen

1. Transparenz:

Vor dem Parlament

Erscheinen des Leiters der spanischen Datenschutzbehörde vor dem Unterhaus des spanischen Parlaments

In seiner jährlichen Rede wies der Leiter der spanischen Datenschutzbehörde AEPD auf die neuerdings zunehmende Verbreitung von Videoüberwachungsgeräten nicht nur durch die öffentliche Hand, sondern vor allem auch im privaten Sektor durch die allgemeine Zunahme von Initiativen zur Anbringung von Kameras beispielsweise in Wohnungseigentumsanlagen, Geschäftsräumen oder öffentlichen Verkehrsmitteln hin.

Er verwies auch auf Plattformen wie beispielsweise „YouTube“, die die weltweite Verbreitung von Filmen oder Bildern für alle Internetnutzer ermöglichen.

In seiner Rede wies er auch auf die Notwendigkeit hin, angesichts der neuen Risiken, die sich aus Internetdiensten wie „Suchmaschinen und E-Mail-Anbietern“ ergeben, Gewährleistungen anzubieten, und erinnerte daran, dass Suchmaschinen die wirksame Ausübung der Rechte auf Zugriff, Berichtigung, Löschung und Widerspruch gewährleisten müssen.

2. Zusammenarbeit mit den Datenschutzbehörden der autonomen Gemeinschaften

Die inzwischen gewonnenen Erfahrungen haben zusammen mit dem Prozess der erneuten Unterzeichnung einiger Gesetze durch die autonomen Regierungen zum Nachdenken darüber angeregt, ob es nicht sinnvoll wäre, zwischen den bestehenden Datenschutzbehörden ein neues Kooperationsmodell einzuführen. Zwecks dessen wurden fünf Arbeitsgruppen eingerichtet (Registrierung; Prüfung; rechtliche und behördliche Analyse; Organisation, Kommunikation und Modernisierung; sowie Internationales). Die Maßnahmen, die in vollständiger Länge zitiert wurden, verstärken die Grundlagen zur Gewährleistung der Gleichheit aller Bürger in Bezug auf das Grundrecht auf Schutz personenbezogener Daten. Es vereinfacht die Pflichten der für die Dateienverwaltung Verantwortlichen und steigert die Effizienz der Aktivitäten seitens der Datenschutzbehörden.

3. Empfehlungen an die Regierung

Im Laufe des Jahres 2007 hat die spanische Datenschutzbehörde AEPD eine Reihe von Empfehlungen ausgesprochen, die sich speziell an Behörden richten. Die Erweiterung des gesetzlichen Rahmens wurde unter anderem für folgende Bereiche vorgeschlagen:

- Durchführung von Verfahren zum Schutz des Urheberrechts in Übereinstimmung mit dem Grundrecht auf Datenschutz;
- Schaffung eines rechtlichen Rahmens für die anonyme Veröffentlichung von Urteilen durch gerichtliche Stellen;
- Regulierung von internen, den Arbeitnehmern in Unternehmen zur Verfügung stehenden Berichterstattungssystemen sowie Beschreibung der Aktivitäten, in denen sich die Einrichtung derartiger Systeme als notwendig erweisen könnte, wobei sowohl der Bericht erstattenden Partei Vertraulichkeit gewährleistet als

auch den Berichtsempfängern der Schutz ihrer Rechte zugestanden werden muss.

Außerdem hat die spanische Datenschutzbehörde eine Reihe von maßgeblichen Empfehlungen erarbeitet, in denen die Notwendigkeit zur Durchführung der folgenden Maßnahmen seitens der zuständigen Behörden hervorgehoben wird:

- Plan zum Schutz der Daten von Minderjährigen im Internet: Behörden müssen verpflichtet werden, besondere Pläne für den Schutz von Minderjährigen im Internet zu formulieren.
- Förderung von Vorsichtsmaßnahmen zur Verhinderung des unerwünschten Austauschs von sensiblen personenbezogenen Daten über P2P-Netze im Internet.
- Förderung der Selbstkontrolle in den Medien, um den Schutz der Privatsphäre und den Schutz personenbezogener Daten zu gewährleisten; Förderung von Praktiken, die die datenschutzrechtlichen Bestimmungen eingehender berücksichtigen.
- Erstellung von Orientierungshilfen hinsichtlich der Verwendung von Vertraulichkeitsgarantien gegenüber den Empfängern bei der Übersendung von E-Mails.
- Plan zur Förderung von bewährten Verfahren bei der Gewährleistung der Privatsphäre in nationalen und europäischen Amtsblättern mithilfe von Maßnahmen, die sich nicht negativ auf das eigentliche Ziel von Amtsblättern auswirken und dennoch geeignet sind, die Erfassung personenbezogener Daten durch Suchmaschinen im Internet zu begrenzen.
- Eine lokale Strategie zur Anpassung der Anbringung von Verkehrskameras an die Datenschutzvorschriften.

4. Mehr Information, mehr Bewusstsein, mehr Anfragen

Information ist ein zentrales Element, wenn es gilt, das Bewusstsein der Bürgerinnen und Bürger für den Schutz personenbezogener Daten zu fördern und zu stärken. Vor diesem Hintergrund hat die Datenschutzbehörde ihre Beziehungen zu den Medien intensiviert, die Belegschaft verstärkt und die materiellen Publikationsmittel aufgestockt, um den wachsenden Anforderungen im Bereich der Information gerecht zu werden und vermehrt öffentliche Informationskampagnen durchführen zu können. Dieses größere Bewusstsein hat zu einem beträchtlichen Zuwachs der beim Bürger-Service (*Servicio de Atención al Ciudadano*)

eingereichten Anfragen geführt, die während des letzten Kalenderjahres um 30 % (auf eine Gesamtzahl von 47 741 Anfragen) gestiegen sind.

5. Umsetzung

Das gestiegene Bewusstsein der betroffenen Personen bezüglich der datenschutzrechtlichen Bestimmungen hat zu einem Anstieg der Zahl der eingereichten Beschwerden wegen angeblicher Verletzung des Datenschutzgesetzes geführt. Der Gesetzgeber hat der spanischen Datenschutzbehörde AEPD eine Reihe von Befugnissen verliehen, die es ihr erlauben, bei der Untersuchung von Verstößen und der Verhängung von Strafen eigenverantwortlich zu handeln, um somit die wirksame Anwendung der geltenden Verordnungen zu gewährleisten. Die durchgeführten Untersuchungen betrafen zumeist Telekommunikationsfirmen und Finanzinstitute, gefolgt von der Videoüberwachung, die einen Anstieg von über 400 % verzeichnete und sich jetzt an dritter Stelle befindet.

5.1. Ausweitung präventiver Maßnahmen

a) Plan zum Schutz personenbezogener Daten von Minderjährigen im Internet

Die Durchführungsbestimmung des spanischen Datenschutzgesetzes hat die grundlegenden Regeln für die Verarbeitung personenbezogener Daten von Minderjährigen festgelegt. Allerdings reicht die Verabschiedung eines rechtlichen Rahmens allein nicht aus. Die Schaffung von Programmen zur Inhaltskontrolle, die Unterstützung der Eltern und der Inhaber von Internetunternehmungen sowie die Förderung der Sicherheit im Internet erfordern ein entschlossenes Vorgehen seitens der öffentlichen Behörden, das sich in speziellen Plänen zum Schutz von Minderjährigen ausdrückt.

b) Erklärung über Internet-Suchmaschinen

2007 veröffentlichte die spanische Datenschutzbehörde AEPD eine Erklärung mit ihren wichtigsten Beobachtungen hinsichtlich der Anpassung der Methoden zur Erfassung, Aufbewahrung und Nutzung personenbezogener Daten durch Internet-Suchmaschinen an die spanischen Datenschutzvorschriften. Dieser Bericht umfasst die wichtigsten Schlussfolgerungen aus den Analysen über potenzielle Auswirkungen dieser Praktiken auf die Privatsphäre der Nutzer von Suchmaschinen und

anderen Diensten, die diese Unternehmen anbieten, und ist auf der Website der spanischen Datenschutzbehörde einsehbar.

Schlussfolgerungen:

- Suchmaschinen müssen die Aufbewahrungsfristen vereinheitlichen und gleichzeitig die Gefährdung der Privatsphäre der Nutzer minimieren.
- Die den Nutzern zur Verfügung gestellten Informationen sind komplex und ineffizient.
- Bürger haben das Recht, ihre Daten zu löschen bzw. der Veröffentlichung ihrer Daten zu widersprechen, wenn diese bei Durchführung einer Suche erscheinen.

Der vollständige Bericht kann hier eingesehen werden:
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/declaracion_aepd_buscadores_en.pdf

c. *Branchenbezogene Überprüfung von Amts wegen in Kolumbien*

Diese Überprüfung wurde bei Unternehmen durchgeführt, die internationalen Kunden personenbezogene Daten zur Erbringung von Dienstleistungen im Zusammenhang mit Telemarketingdiensten oder Kunden-Service-Centern übermitteln. Zentrale Themen sind dabei die Entwicklung und der Anstieg der Nachfrage nach internationalem Datentransfer, die die spanische Datenschutzbehörde AEPD in den letzten paar Jahren verzeichnen konnte, sowie die Zielländer und die Hauptzwecke, für die sie beantragt werden.

Den Bericht und die entsprechenden Schlussfolgerungen finden Sie unter folgendem Link:
https://www.agpd.es/upload/Canal_Documentacion/Recomendaciones/report_Inter_data_transfers_colombia_en.pdf

6. Aktivitäten Spaniens innerhalb des Ibero-Amerikanischen Datenschutzzetzes

2007 war ein besonders aktionsreiches Jahr im Wirkungsbereich des Ibero-Amerikanischen Datenschutzzetzwerks, das 2003 infolge der Initiative der spanischen Datenschutzbehörde zur Förderung der Regulierung des Datenschutzes in Ibero-Amerika ins Leben gerufen worden war. Die V. Ibero-Amerikanische Konferenz [zum Thema Datenschutz] fand

2007 in Lissabon (Portugal) statt. 2007 wurde außerdem ein Seminar zur Schaffung eines Informationsdiskussions- und Austauschforums in Cartagena de Indias (Kolumbien) abgehalten. Es wurden Leitlinien zur Förderung von Initiativen erarbeitet, die es in den Ländern der Ibero-Amerikanischen Gemeinschaft ermöglichen, ein angemessenes Datenschutzniveau zu erreichen, und somit den freien Verkehr personenbezogener Daten in diesen Ländern unterbinden. Im Rahmen ihres Engagements für diese Länder begrüßte die spanische Datenschutzbehörde AEPD Vertreter Mexikos, Chiles und Uruguays an ihrem Verwaltungssitz und beriet sie hinsichtlich ihrer Datenschutzgesetzgebung.



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 Gesetz zum Schutz personenbezogener Daten (Personal Data Act, PDA, 1998:204) umgesetzt, das am 24. Oktober 1998 in Kraft trat. Das Gesetz zum Schutz personenbezogener Daten wird durch die Datenschutzverordnung ergänzt (1998:1191), die am gleichen Tag in Kraft trat. Das Gesetz findet wie die Richtlinie auf die automatisierte ebenso wie auf die manuelle Datenverarbeitung Anwendung. Dieses 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 Gesetzes zum Schutz personenbezogener Daten oder ergänzend zu diesem. Auch beim Entwurf dieser speziellen Gesetze und Beschlüsse wurde der Richtlinie Rechnung getragen.

In den vorhergehenden Jahresberichten der Art. 29 Datenschutzgruppe war das vorgeschlagene sogenannte *Missbrauchsmodell* beschrieben worden, das der Änderung des PDA entspricht, die am 1. Januar 2007 in Kraft trat. Zweck der Änderung ist die Vereinfachung der täglichen Verarbeitung personenbezogener Daten im Rahmen der Richtlinie. Dies betrifft Datenverarbeitungsmethoden, die üblicherweise nicht die Gefahr von Verstößen gegen die Privatsphäre der betroffenen Person vergrößern. Die Handhabungsvorschriften – die Melde- und Informationsvorschriften, die Sicherheitsvorschriften im Bereich der Verarbeitung sensibler Daten sowie die Forderung nach Einwilligung in bestimmten Fällen – müssen bei der Verarbeitung derjenigen personenbezogenen Daten nicht eingehalten werden, die keinem Satz von personenbezogenen Daten, der in eine bestimmte Struktur gebracht worden ist, um die Datensuche bzw. die Datenzusammenstellung wesentlich zu erleichtern, angehören (bzw. dafür bestimmt sind). Somit sind Verantwortliche für Datenverarbeitung bei unstrukturierter Verarbeitung, zum Beispiel hinsichtlich einer E-Mail oder Fließtext auf einer Internetseite, nicht mehr verpflichtet, alle Handhabungsvorschriften zu

beachten. Stattdessen greift die *Missbrauchsregel*, die besagt, dass die Verarbeitung nicht durchgeführt werden darf, wenn dies zur Verletzung der Privatsphäre der betroffenen Person führen würde. Wird die Missbrauchsregel verletzt, so gelten die Haftpflichtregelungen und in manchen Fällen kommt es sogar zur Verhängung von Strafmaßnahmen. Die Unterscheidung zwischen dem, was als strukturierte, und dem, was als unstrukturierte Verarbeitung gilt, kann natürlich zu Problemen bei der Anwendung führen. Die Datenschutzbehörde ist jedoch der Auffassung, mit der Abänderung der Wirklichkeit etwas näher gekommen zu sein.

Die EU-Richtlinie 2002/58/EG wurde mit Inkrafttreten des Gesetzes über die elektronische Kommunikation ECA (2003:389) im Juli 2003 in schwedisches Recht umgesetzt. Das Kapitel 6 dieses Gesetzes enthält Datenschutzregeln für den elektronischen Kommunikationssektor. Die Einhaltung der Datenschutzbestimmungen des ECA-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 Änderungen 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.

Im April 2004 hat die Regierung die Einsetzung eines Ausschusses (*Integritetsskyddskommittén* – Ausschuss für den Schutz der Privatsphäre) beschlossen, der sich aus Experten und Mitgliedern des *Riksdag* (des schwedischen Parlaments) zusammensetzt und dessen Aufgabe in der Durchführung einer Umfrage zur schwedischen Gesetzgebung in Bezug auf die Privatsphäre und in ihrer Analyse besteht. Der Ausschuss wurde später auch damit beauftragt zu beurteilen, ob zusätzlich zu den bestehenden Rechtsvorschriften auch allgemein gültige Vorschriften zum Schutz der Privatsphäre aufgestellt werden sollten. Im Frühjahr 2007 legte der Ausschuss einen umfangreichen Bericht – das Ergebnis seiner ursprünglichen Aufgabe – vor, der die Umfrage und die Analyse enthielt. Der Ausschuss beschrieb relativ eingehend, wie sich Rechtsvorschriften in den verschiedenen Bereichen der Gesellschaft entwickelt haben, auf welcher Art von Informationen Regierung und *Riksdag* ihre Entscheidungen gestützt haben, und auch,

inwieweit das Gleichgewicht zwischen dem Interesse für den Schutz der Privatsphäre und anderen Interessen gelitten hat. Gegenstand besonderer Analyse war das Prinzip der Verhältnismäßigkeit. Der Ausschuss äußerte mehrere Kritikpunkte systematischer und methodischer Art und zeigte, wie diesbezügliche Mängel zu einem geringeren Schutz der Privatsphäre als nötig geführt haben. Der Ausschuss beantwortete die direkte Frage, ob der Schutz der Privatsphäre als zufrieden stellend geregelt betrachtet werden kann, eindeutig abschlägig. Der zweite und letzte Bericht des Ausschusses wurde im Januar 2008 vorgelegt, und in diesem Bericht analysierte der Ausschuss, auf welche Art und Weise der verfassungsrechtliche Schutz der Privatsphäre geregelt werden sollte und welche weiteren Maßnahmen erforderlich sind.

Der Untersuchungsausschuss, der seitens des schwedischen Justizministers im Mai 2006 mit der Überprüfung der innerstaatlichen Rechtsvorschriften auf diesem Gebiet betraut worden war und Änderungen vorschlagen sollte, die in Bezug auf die Annahme der *EG-Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden*, legte im November 2007 seinen Bericht vor. Die Datenschutzbehörde war in der Untersuchung vertreten und im Laufe der Untersuchung waren auch Dienstleister befragt worden. Das Justizministerium hat den Bericht zur Prüfung vorgelegt und die Datenschutzbehörde ist derzeit damit beschäftigt, die Vorschläge der Untersuchung zu analysieren. Die Regierung wird dem *Riksdag* im Laufe dieses Jahres noch einen Gesetzentwurf vorlegen. Die Umsetzung der Richtlinie in schwedisches Recht vor 2009 ist unwahrscheinlich.

Der Jahresbericht vom vergangenen Jahr enthielt Vorschläge zur Neuregelung von Patientenakten und Gesundheitswesen. Ein völlig neues Gesetz, das Patientendatengesetz, in dem der Umgang mit personenbezogenen Daten im Gesundheitswesen einheitlich geregelt wird, war von einer entsprechend beauftragten Untersuchungskommission vorgeschlagen worden. Ein Vertreter der Datenschutzbehörde war an der Arbeit an dem neuen Gesetzesvorschlag beteiligt. Der Vorschlag wurde zur Beratung vorgelegt und wird derzeit seitens

der Regierung aufbereitet. Das neue Gesetz soll zum 1. Juli 2008 in Kraft treten. Die Untersuchungskommission legte ihren letzten Bericht über Patientendaten und Medikamente im Sommer 2007 vor.

Im November 2007 legte das Justizministerium einen Bericht mit einem Vorschlag für ein neues Gesetz zur Verarbeitung personenbezogener Daten durch die Polizei bei der Verbrechensbekämpfung vor. Der neue Gesetzesvorschlag soll das Polizeidatengesetz von 1992 ablösen. Der neue Gesetzesvorschlag regelt – mit einigen wenigen Ausnahmen – jegliche Verarbeitung personenbezogener Daten bei der Verbrechensbekämpfung durch die Polizei. Es wird für den schwedischen Polizeiausschuss, die Polizeibehörden und die schwedische Behörde für Wirtschaftskriminalität gelten. Für die Datenverarbeitung innerhalb des schwedischen Sicherheitsdienstes werden besondere Regeln greifen. Der neue Gesetzesvorschlag schafft darüber hinaus Möglichkeiten zur Verbesserung der Zusammenarbeit zwischen Behörden der Verbrechensbekämpfung, indem es neue Vorschriften zur Offenlegung von Daten einführt. Der Bericht wurde zur Beratung vorgelegt, und die Datenschutzbehörde prüft derzeit die Vorschläge. Ein Inkrafttreten der Vorschläge zum 1. Januar 2009 ist angedacht.

B. Bedeutende Rechtsprechung

Im 9. Jahresbericht war ein Fall präsentiert worden, in dem biometrische Daten in Schulen verwendet worden waren. In diesem Fall ging es um einen Beschluss der schwedischen Datenschutzbehörde aus dem Jahr 2004 über die Erfassung und Verarbeitung der Fingerabdrücke von Schülern zwecks Zugangskontrolle zur Schulkantine. Ungeachtet der Tatsache, dass man dafür die Zustimmung der Schüler eingeholt hatte, ließ die Behörde verlautbaren, dass die Verarbeitung dieser Daten unangemessen oder fragwürdig gewesen wäre und dass derartige Kontrollen möglich seien, ohne gleich so tief in die Privatsphäre Dritter einzudringen. Diese Ansicht wurde in anderen ähnlichen Fällen ebenfalls vertreten. Gegen die Beschlüsse der Datenschutzbehörde wurde vor dem zuständigen kommunalen Verwaltungsgericht Berufung eingelegt, das die Beschlüsse der Behörde bestätigte. Daraufhin wurden diese Fälle vor das Verwaltungsberufungsgericht in Stockholm gebracht, das

feststellte, dass bei einer derartigen Datenerfassung und -verarbeitung die Grundsätze des Datenschutzes in qualitativer Hinsicht erfüllt werden und ohne Zustimmung rechtmäßig sind. Die Datenschutzbehörde hat nun vor dem obersten Verwaltungsgericht Schwedens Berufung eingelegt; derzeit sind dort Berufungsverfahren in drei Fällen anhängig.

Im Juni 2007 verkündete das Verwaltungsberufungsgericht in Stockholm das Urteil im Fall des Amts zur Bekämpfung von Urheberrechtspiraterie (*Svenska anti-piratbyrå, APB*), der im letzten Jahresbericht behandelt worden war. Dieser Fall befasst sich mit der Frage, ob es sich bei IP-Adressen um personenbezogene Daten handelt oder nicht. Das „Anti-Piraterie-Büro“ – eine Schutzgemeinschaft verschiedener privatwirtschaftlicher Unternehmen – hatte eine Vielzahl von Einzelnformationen, insbesondere IP-Adressen, in Verbindung mit der Verbreitung von urheberrechtlich geschütztem Material per Filesharing über das Internet gesammelt und erfasst. Die schwedische Datenschutzbehörde stellte in ihrem Beschluss fest, dass es sich bei IP-Adressen um personenbezogene Daten handelt und dass die vom „Anti-Piraterie-Büro“ vorgenommene Datenverarbeitung die Bestimmungen des Gesetzes zum Schutz personenbezogener Daten (PDA) verletzt, da dabei Informationen über Rechtsverletzungen im Sinne von Paragraph 21 des PDA verarbeitet werden. Es ist nämlich nur den zuständigen Behörden gestattet, personenbezogene Daten zu verarbeiten, die Rechtsverletzungen und strafbare Handlungen betreffen, es sei denn, die Datenschutzbehörde bewilligt eine entsprechende Ausnahmegenehmigung. In seinem Beschluss vom Juni 2005 ordnete die Datenschutzbehörde an, das „Anti-Piraterie-Büro“ solle die Verarbeitung dieser Daten einstellen. Das „Anti-Piraterie-Büro“ machte jedoch geltend, dass es sich bei den IP-Adressen nicht um personenbezogene Daten handeln würde, da das Büro keinen Zugriff auf die Daten hat, in denen den Abonnenten von Internetzugängen bestimmte IP-Adressen zugeordnet werden. Das Büro legte gegen das Urteil Berufung ein. Sowohl das kommunale Verwaltungsgericht als auch das Verwaltungsberufungsgericht bestätigten die Entscheidung der Datenschutzbehörde.

Nach der Entscheidung der Datenschutzbehörde vom Juni 2005 beantragte das „Anti-Piraterie-Büro“ für sich

eine Ausnahmegenehmigung zu den Bestimmungen aus Paragraph 21 Datenschutzgesetz im Hinblick auf die Verarbeitung der IP-Adressen, um beispielsweise bei der Polizei Anzeige zu erstatten und Internetdienstanbieter über die Urheberrechtsverletzungen ihrer Teilnehmer zu informieren. Die Datenschutzbehörde hat daraufhin eine Ausnahmegenehmigung erlassen, die inzwischen verlängert wurde, sodass das Büro noch bis Ende 2008 befugt ist, personenbezogene Daten über strafbare Handlungen zu verarbeiten.

C. Bedeutende 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 im Zusammenhang mit den Interessengebieten der Datenschutzbehörde. 2007 wurden vier Ausgaben veröffentlicht und die Anzahl der Abonnenten der gedruckten Ausgabe ist im Laufe von 2007 erheblich gestiegen.

Die Datenschutzbehörde hat von der Regierung den Auftrag erhalten, zur Entwicklung sicherer und effizienter E-Government-Dienste beizutragen. Im Rahmen dieser Arbeit hat die Datenschutzbehörde „*Leitlinien für die Gemeinden: personenbezogene Daten und E-Government*“ erarbeitet. Die Druckschrift wurde an alle Gemeinden in Schweden verteilt. Gemäß den Veranschlagungsanweisungen (*regleringsbrev*) soll die Datenschutzbehörde außerdem neue Phänomene beobachten und hat daher im Rahmen ihrer Arbeit folgende Berichte verfasst: „*Ubiquitäres Computing: eine Vision, die wahr werden kann*“, „*Das Visa-Informationssystem (VIS): die größte Fingerabdruck-Datenbank der Welt*“ und „*Der Prüm-Vertrag verleiht der Polizei innerhalb der EU das Recht auf Abfrage von DNA oder Fingerabdrücken Dritter und die Suche im Kraftfahrzeugregister*“.

Ein Marktforschungsunternehmen hat im Auftrag der Datenschutzbehörde die Einstellung junger Leute zum Internet untersucht und präsentiert die Ergebnisse im Bericht „*Junge Leute und Privatsphäre*“. Die Datenschutzbehörde hat des Weiteren ein Portrait der Behörde – sowohl auf Schwedisch als auch auf Englisch – herausgegeben: „*Was in aller Welt macht die Datenschutzbehörde?*“ In dieser

Publikation stellt die Datenschutzbehörde ihre Aktivitäten vor, indem sie zehn Mitarbeiter von ihrer Arbeit und sich selbst erzählen lässt. Und zu guter Letzt hat die Datenschutzbehörde noch eine Checkliste veröffentlicht: *„Elektronische Schlüssel in Wohnungsbauunternehmen und Wohnungsbaugenossenschaften“*.

Im Bereich der Selbstregulierung hat die Datenschutzbehörde eine Stellungnahme zum neuen System ID06 im Bausektor abgegeben. Das System hat zwei Ziele: den Einsatz illegaler Arbeitskräfte zu erschweren und die Anwesenheit der Personen am Arbeitsplatz – aus Sicherheitsgründen – zu kontrollieren. Die Datenschutzbehörde hat festgestellt, dass das System die Vorschriften des Datenschutzgesetzes erfüllt, wies jedoch ausdrücklich daraufhin, dass die betroffenen Personen darüber entsprechend und eindeutig in Kenntnis gesetzt werden müssen. Die personenbezogenen Daten, die dabei erfasst werden, dürfen maximal zwei Jahre gespeichert werden, da die Steuerbehörden diese Daten eventuell zu Kontrollzwecken benötigen.



Vereinigtes Königreich

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 Datenschutz und elektronische Kommunikation in britisches Recht umgesetzt und am 11. Dezember 2003 rechtswirksam.

Die endgültige Übergangszeit endete am 23. Oktober 2007, womit die vor 1998 manuell erstellten Aufzeichnungen nun den gesetzlichen Bestimmungen unterliegen.

B. Bedeutende Rechtsprechung

Das Berufungsgericht wies die Berufung von David Paul Johnson im Fall Johnson/The Medical Defense Union ([2007] EWCA Civ. 262) zurück. Zwei der drei Richter blieben in ihrem Urteil dabei, dass das Datenschutzgesetz nicht auch für die Auswahl persönlicher Informationen durch einen Menschen gilt, selbst wenn diese Informationen im Anschluss auf einem automatisierten System abgelegt werden. Es bleibt abzuwarten, ob diese Auslegung nachhaltige Folgen haben wird.

C. Wichtige spezifische Themen

Im November hatte die britische Zoll- und Steuerbehörde, *Her Majesty's Revenue and Customs (HMRC)*, eingeräumt, dass ihr zwei CD-ROMs mit der kompletten Kindergeld-Datenbank abhanden gekommen waren, welche die persönlichen Daten von fünfundzwanzig Millionen Menschen enthält. Dies hob die Bedeutung des Datenschutzes sowie die begrenzten Möglichkeiten des Datenschutzbeauftragten hervor, derartige Verstöße zu verhindern oder zu ahnden. Im Dezember forderte der Datenschutzbeauftragte die Regierung auf, ihm weitere reichende Befugnisse zu erteilen, um Verantwortliche für Datenverarbeitung ohne deren Einwilligung überprüfen zu können und um Sanktionen für vorsätzliche oder grob

fahrlässige Verstöße gegen die Datenschutzgrundsätze zu verhängen. Darüber hinaus wurde die Einführung einer Staffelung der Meldegebühren vorgeschlagen, welche eine erhebliche Steigerung der dem Datenschutzbeauftragten zur Verfügung stehenden Mittel hätte. Es wird erwartet, dass die Regierung sich 2008 über die vorgeschlagenen Änderungen berät.

Im Laufe des Jahres 2007 führte die nationale Datenschutzbehörde des Vereinigten Königreichs ICO eine Gruppenbefragung zur neuen Datenschutzstrategie durch. Diese Strategie wird sich u. a. auf die Einkünfte der Behörde konzentrieren, um festzustellen, in welchen Fällen eine tatsächliche Benachteiligung von Privatpersonen möglich ist. Ziel des Datenschutzbeauftragten ist es, der überwindenden Mehrheit der pflichtbewussten Verantwortlichen für Datenverarbeitung die Einhaltung ihrer Pflichten zu vereinfachen und gleichzeitig mehr Befugnisse gegenüber der Minderheit der Verantwortlichen zu erhalten, die ein tatsächliches Risiko für die Informationsrechte von Privatpersonen darstellen. Die Strategie wird im März 2008 anlaufen.

Im Oktober forderte der britische Premierminister Gordon Brown den Datenschutzbeauftragten Richard Thomas und Dr. Mark Walport vom Wellcome Trust auf, eine unabhängige Untersuchung zum Datenaustausch durchzuführen. Ihr Bericht wird Empfehlungen über mögliche Änderungen der Gesetzgebung und der Politik in diesem Bereich beinhalten.

Im Januar 2007 setzte der Datenschutzbeauftragte beim ersten Europäischen Datenschutntag ein Zeichen, indem er die öffentliche Aufmerksamkeit auf die Gefahr des Identitätsschwindels lenkte. Die Datenschutzbehörde ICO veröffentlichte Umfrageergebnisse, aus denen hervorging, dass die meisten Personen im Vereinigten Königreich entweder bereits Opfer eines Identitätsschwindels waren oder sich selbst diesbezüglich einem unnötigen Risiko aussetzen. Die Behörde ließ einen kurzen Informationsfilm („Der Mann im Spiegel“) anfertigen, um die Öffentlichkeit für diese Bedrohung zu sensibilisieren, und gab ein „*Personal Information Toolkit*“ heraus: einen kurzen Leitfaden über den Schutz der eigenen personenbezogenen Daten.

Nachdem in den Medien berichtet worden war, dass vertrauliche Bankdaten in herkömmlichen Abfalleimern und Plastikbeuteln weggeworfen worden waren, deckte die Datenschutzbehörde ICO im März auf, dass elf Banken und Finanzinstitute gegen das Datenschutzgesetz verstoßen hatten. Die Geschäftsführer der betroffenen Banken unterzeichneten schriftliche Zusagen zur Verbesserung ihrer Sicherheitsvorschriften.

Im August veröffentlichte die Datenschutzbehörde ICO ein Schriftstück bezüglich der Definition von personenbezogenen Daten unter Berücksichtigung der Meinung der Art. 29 Datenschutzgruppe.

Im Oktober veröffentlichte die Datenschutzbehörde ICO einen Verhaltenskodex als Rahmenwerk zur gemeinsamen Nutzung von Daten. Dieses soll Unternehmen dabei unterstützen, eigene Regeln für den Austausch personenbezogener Daten festzulegen. Die Datenschutzbehörde ICO startete außerdem eine Befragung bezüglich der überarbeiteten Fassung der Videoüberwachungsregeln des Datenschutzbeauftragten, die im Januar 2008 eingeführt worden waren.

Im November 2007 beauftragte der Datenschutzbeauftragte Polizeikräfte mit der Löschung von Daten über alte, geringfügige Verurteilungen aus dem nationalen Polizeicomputer. Das britische *Information Tribunal* wird diesen Fall im April 2008 anhören.

Am 11. Dezember leitete der Datenschutzbeauftragte eine Konferenz mit dem Namen „Überwachungsgesellschaft: Vom Verhandeln zum Handeln“ in der Bridgewater Hall in Manchester. Das Handbuch der ICO zu Beurteilung der Auswirkungen auf die Privatsphäre und Untersuchungen im Zusammenhang mit dem Datenschutz wurden bei dieser Veranstaltung erstmalig vorgestellt. Es handelt sich hierbei um das erste Handbuch zur Beurteilung der Auswirkungen auf die Privatsphäre, das von einer europäischen Datenschutzbehörde herausgegeben wird. Die Datenschutzbehörde ICO dankt dem finnischen Amt für Datenschutz sowie anderen Behörden für ihre Unterstützung bei diesem Projekt.

Im Laufe des Jahres 2007 legte der Datenschutzbeauftragte sieben parlamentarischen Sonderausschüssen

Beweismittel zu zehn Untersuchungen vor (eine signifikante Erhöhung gegenüber 2006):

- dem Sonderausschuss des britischen Oberhauses (House of Lords) für die Europäische Union, Unterausschuss F (Innere Angelegenheiten): Untersuchungen zu Schengen II, zu den Passagiernamensregistern (PNR) und zum Prüm-Vertrag;
- dem Sonderausschuss des britischen Oberhauses (House of Lords) für verfassungsrechtliche Belange: „Untersuchung der Auswirkungen von Überwachung und Datenerfassung auf die Privatsphäre der Bürger und ihre Beziehung zum Staat“;
- dem Gesundheitsausschuss des britischen Unterhauses (House of Commons): eine Untersuchung zur elektronischen Patientenakte;
- dem Sonderausschuss des Innenministeriums: eine Untersuchung zu „Die Überwachungsgesellschaft?“ sowie Beweismittel zu Justiz und Innerem auf Ebene der Europäischen Union.
- dem Sonderausschuss für Kultur, Medien und Sport: die Rolle des britischen Presseaufsichtsrats (Press Complaints Commission);
- dem Ausschuss für die Gesetzesvorlage über Strafrechtspflege und Einwanderung: Paragraph 55 des Datenschutzgesetzes (unerlaubte/r Zugang, Verarbeitung oder Verkauf von Daten als Straftat);
- dem Justizausschuss: der Schutz privater Daten.

Im Laufe des Jahres 2007 hat der Datenschutzbeauftragte 47 Anfragen beantwortet (ein erheblicher Anstieg gegenüber 2006).

Kapitel 3

Aktivitäten der Europäischen Union und der Gemeinschaft



3.1. DIE EUROPÄISCHE KOMMISSION

Mitteilung der Kommission an das Europäische Parlament und an den Rat über den Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie, Brüssel, 7.3.2007²¹

Der erste Bericht der Kommission bezüglich der Umsetzung dieser Richtlinie²² stellte fest, dass, obwohl keine Gesetzesänderungen notwendig waren, noch viele Aufgaben erledigt werden mussten und dass es einen erheblichen Bedarf an Verbesserungen bei der Umsetzung der Richtlinie gab. Der Bericht enthielt ein *Arbeitsprogramm zur besseren Umsetzung der Datenschutz-Richtlinie*.

Die Mitteilungen vom 7. März 2007 befassten sich mit den Arbeiten, die im Rahmen dieses Programmes durchgeführt wurden, beurteilten die gegenwärtige Situation und umrissen die Aussichten für die Zukunft als eine Bedingung für den Erfolg in einer Reihe von Politikbereichen angesichts des Artikels 8 der Charta der Grundrechte der Europäischen Union, in dem ein eigenständiges Recht auf den Schutz personenbezogener Daten anerkannt wird.

Die wichtigsten Schlussfolgerungen dieser Mitteilungen waren, dass die Kommission in naher Zukunft nicht beabsichtigt, einen Gesetzentwurf zur Ergänzung der Richtlinie vorzulegen, und die Mitgliedstaaten darauf drängt, eine ordnungsgemäße Umsetzung der Richtlinie in nationale Gesetze zu gewährleisten. Die im Arbeitsprogramm aufgeführten Aktivitäten werden fortgesetzt und die Beteiligung aller interessierten Parteien ist eine solide Basis, um eine bessere Umsetzung der Grundsätze der Richtlinie anzustreben; um sich sämtliche Vorteile dieses Auftrags zu sichern, sollten sich die Datenschutzbehörden ebenfalls bemühen, die jeweilige nationale Praxis dem europäischen

Leitfaden anzupassen, der von der Arbeitsgruppe verabschiedet wurde.

Mitteilung der Kommission an das Europäische Parlament und an den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, Brüssel, 2.5.2007²³

Zweck der Mitteilung über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre ist es, die Vorteile der datenschutzfreundlichen Technologien zu berücksichtigen, wie sie in den Zielen der Kommission auf dem Gebiet der Förderung dieser Technologien festgelegt sind, und deutliche Aktionen durchzuführen, um dieses Ziel durch Unterstützung der Entwicklung von Technologien zum Schutz der Privatsphäre und ihren Einsatz durch Datenschützer und Verbraucher zu erreichen.

Die Kommission geht davon aus, dass Technologien zum Schutz der Privatsphäre entwickelt und insbesondere dort stärker eingesetzt werden sollten, wo personenbezogene Daten durch IKT-Netzwerke verarbeitet werden. Die Kommission ist der Ansicht, dass ein stärkerer Einsatz von datenschutzfreundlichen Technologien den Schutz der Privatsphäre verbessern würde und auch hilfreich wäre, die Datenschutzvorschriften einzuhalten. Der Einsatz von datenschutzfreundlichen Technologien wäre eine Ergänzung zu dem vorhandenen Gesetzesrahmen und den Durchsetzungsmechanismen.

Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, 13.11.2007²⁴

²¹Mitteilung der Kommission an das Europäische Parlament und an den Rat über den Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie, Brüssel, http://ec.europa.eu/justice_home/fsj/privacy/docs/lawreport/com_2007_87_f_de.pdf, ABl. C 138 vom 22.6.2007, S. 17

²²Erster Bericht über die Umsetzung der Datenschutzrichtlinie (95/46/EC), KOM(2003) 265 endg., vom 15.5.2003, ABl. C 76 vom 25.3.2004, S. 18

²³Mitteilung der Kommission an das Europäische Parlament und an den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, ABl. C 181 vom 3.8.2007, S. 22; <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0228:FIN:DE:PDF>

²⁴KOM(2007) 698 endg., ABl. C 55 vom 28.2.2008, S. 4 <http://eur-lex.europa.eu/de/index.htm>

Am 13. November 2007 hat die Kommission den Vorschlag zur Änderung von Richtlinien angenommen, unter anderem der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Das zentrale Ziel dieses Vorschlags war die Verbesserung des Schutzes personenbezogener Daten und der Privatsphäre von Privatpersonen in der elektronischen Kommunikation, insbesondere durch Stärkung der sicherheitsbezogenen Vorschriften und Durchsetzungsmechanismen.

Erster Europäischer Datenschutztag: Brüssel, 28. Januar 2007²⁵

Die Kommission begrüßte und unterstützte die Initiative des Europarats, den Kern des Datenschutzes zur Sprache zu bringen und den 28. Januar 2007 zum „Datenschutztag“ zu erklären, da dies der Tag der Unterzeichnung der Europaratskonvention 108 zur Regelung der Verarbeitung personenbezogener Daten war.

Die Veranstaltungen fanden in allen Mitgliedstaaten statt und informierten die Menschen über ihre persönlichen Datenrechte.

Konferenz „Öffentliche Sicherheit, Privatsphäre und Technologie“, Brüssel, 20. November 2007²⁶

Am 20. November 2007 organisierte die Europäische Kommission eine Konferenz zur öffentlichen Sicherheit, Privatsphäre und Technologie. Technologie ermöglicht sowohl den Datentransfer als auch die bessere Kontrolle des Datenzugangs und die genaue Lokalisierung bestimmter Daten in Abstimmung der Bedürfnisse von Sicherheit und Privatsphäre. An dieser

Konferenz nahmen Vertreter der öffentlichen Hand sowie aus der Privatwirtschaft teil.

Die Konferenz bot eine Gelegenheit, verschiedene Bereiche umfassende Aktivitäten zu erörtern, wie die Entwicklung von Technologien, insbesondere solcher Technologien, die den Schutz der Privatsphäre verbessern, einen öffentlich-privaten Dialog über Sicherheitsforschung und –innovation zu führen, und zu erörtern, wie neue Technologien zur Verbesserung der Sicherheit genutzt werden könnten.

Schutz personenbezogener Daten im Vertrag von Lissabon

Eine abgeänderte Version der Charta der Grundrechte der Europäischen Union²⁷ wurde am 12. Dezember 2007 in Straßburg veröffentlicht. Am 13. Dezember 2007 wurde der Vertrag von Lissabon²⁸ von den Staats- und Regierungschefs der 27 Mitgliedstaaten in Lissabon unterzeichnet. Beide Verträge führten wichtige Bestimmungen zum Schutz personenbezogener Daten ein:

Artikel 8 der EG-Charta der Grundrechte gewährleistet rechtsverbindlich die Grundrechte einer jeden Person auf Schutz personenbezogener Daten.

Der (neue) Artikel 16 des Vertrages über die Arbeitsweise der Europäischen Union sorgt für eine einheitliche rechtliche Grundlage zur Annahme von Gesetzgebungsakten in Bezug auf den Schutz von Privatpersonen und den freien Verkehr personenbezogener Daten, die dem üblichen Gesetzgebungsverfahren folgen (Mitentscheidung). Dies gilt für die Verarbeitung personenbezogener Daten aus Institutionen, Körperschaften, Behörden und Agenturen sowie Mitgliedstaaten der Union bei der Ausführung von Aktivitäten im Rahmen der Rechtsvorschriften der Europäischen Union und auf den freien Verkehr personenbezogener Daten. Der neue Wortlaut betont insbesondere die Zusammenarbeit von Polizei und Justiz bei Strafsachen auf nationaler sowie auf

²⁵Im Namen der Europäischen Kommission abgegebene Erklärung von Vizepräsident Frattini zum Tag des Datenschutzes (28. Januar): <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/07/102&format=HTML&aged=1&language=DE&guiLanguage=en>
Resolution der Art. 29 Datenschutzgruppe für den 1. Europäischen Datenschutztag:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_de.htm

²⁶Weitere Informationen zur Konferenz „Öffentliche Sicherheit, Privatsphäre und Technologie“: http://ec.europa.eu/justice_home/news/events/events_2007_en.htm

²⁷ABl C 303 vom 14.12.2007, S. 1

²⁸ABl C 306 vom 17.12.2007, S. 1

EU-Ebene, wobei die besondere Natur dieser Bereiche spezielle Regeln erforderlich machen kann²⁹.

Der (neue) Artikel 39 des EU-Vertrags bietet für den Schutz personenbezogener Daten in der Europäischen Sicherheits- und Verteidigungspolitik (ESVP) eine besondere rechtliche Grundlage und Regeln für den freien Verkehr solcher Daten. Dies gilt für die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten bei der Ausführung von Aktivitäten im Rahmen von Kapitel 2 („Besondere Bestimmungen zur Europäischen Sicherheits- und Verteidigungspolitik“). Es entspricht dem Interesse der Mitgliedstaaten, Kernaktivitäten der Außen- und Verteidigungspolitik im zwischenstaatlichen Bereich zu belassen, und hierin liegt auch die Ausnahme von der Regel einer einheitlichen rechtlichen Basis, ganz in Übereinstimmung mit dem Grundsatz des Vorrangs der Europäischen Union bzw. den Rechtsvorschriften der EU³⁰.

PNR-Abkommen von 2007³¹

Am 23. Juli 2007 und am 26. Juli 2007 wurde in Brüssel bzw. in Washington ein Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Record – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (US-Ministerium für Heimatschutz) geschlossen. Dieses Abkommen soll weder die Gesetze der Vereinigten Staaten von Amerika noch die der Europäischen Union oder ihrer Mitgliedstaaten einschränken oder ergänzen. Sein Ziel ist vielmehr die wirksame Abwendung und Bekämpfung des Terrorismus und des grenzüberschreitenden Verbrechens zum Schutz der jeweiligen demokratischen Gesellschaften und der gemeinsamen Werte der Vertragsparteien.

Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken (KOM(2007) 654 endgültig)³²

Der am 6. November 2007 angenommene Vorschlag der Kommission für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken sieht vor, dass Fluggesellschaften den zuständigen Behörden in den Mitgliedstaaten die PNR-Daten der Fluggäste internationaler Flüge zur Verfügung stellen, um terroristische Angriffe und organisierte Kriminalität zu verhindern und zu bekämpfen. Er sieht ebenfalls das Erfassen und Speichern dieser Daten von den genannten Behörden sowie den Austausch der Daten zwischen ihnen vor.

SWIFT

Nach den Terroranschlägen vom 11. September 2001 entwickelte das US-Finanzministerium ein Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP, Terrorist Finance Tracking Program), mit dem Personen oder Organisationen, die terroristische Aktivitäten finanziell unterstützen, ermittelt, aufgespürt und strafrechtlich verfolgt werden sollen. Im Rahmen dieses Programms erließ das US-Finanzministerium eine Anordnung auf Herausgabe von Daten an die Society for Worldwide Interbank Financial Telecommunication (SWIFT). Aufgrund dieser Anordnungen muss SWIFT in den USA einen bestimmten Teil der persönlichen finanziellen Daten, die die Gesellschaft auf ihrem dortigen Server gespeichert hat, dem US-Finanzministerium übermitteln, wo diese im Zusammenhang mit verdächtigen Personen oder Organisationen zur Terrorismusbekämpfung verwendet werden können.

Als diese Fakten im Jahre 2006 bekannt wurden, gab die belgische Datenschutzbehörde eine Stellungnahme heraus, nach der die Datenverarbeitungstätigkeiten von SWIFT bei der Durchführung des

²⁹ Erklärungen 20 und 21

³⁰ Artikel 40 des EU-Vertrages in der im Vertrag von Lissabon geänderten Fassung

³¹ Beschluss 2007/551/GASP/JI des Rates vom 23. Juli 2007, ABl. L 204 vom 4.8.2007, S. 16
Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika, ABl. L 204 vom 4.8.2007, S. 18
http://eur-lex.europa.eu/LexUriServ/site/de/oj/2007/l_204/l_20420070804de00160017.pdf

³² Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken (KOM(2007) 654 endgültig), ABl. C 55/4:
<http://eur-lex.europa.eu/de/index.htm>

Zahlungsverkehr zwischen Banken eine Verletzung des belgischen Datenschutzgesetzes darstellten, mit dem die Richtlinie 95/46/EG zum Schutz personenbezogener Daten umgesetzt wird. Die Art. 29 Datenschutzgruppe gab im November 2006³³ ebenfalls eine Stellungnahme heraus, nach der die SWIFT und die Finanzinstitute, die die Dienstleistungen der SWIFT in Anspruch genommen haben, gegen das in der Richtlinie 95/46/EG enthaltene Datenschutzgesetz der EU verstoßen haben, u. a. aufgrund der Weitergabe von personenbezogenen Daten an die Vereinigten Staaten von Amerika ohne Gewährleistung eines angemessenen Schutzes und ohne die betroffenen Personen über die Art und Weise, wie ihre personenbezogenen Daten verarbeitet wurden, informiert zu haben. Im Verlauf des Jahres 2007 hat die Art. 29 Datenschutzgruppe diesen Fall weiter verfolgt, um den Fortschritt der verschiedenen Akteure im Hinblick auf die Ergebnisse ihrer Stellungnahme vom 22. November 2006 zu beurteilen. Die Art. 29 Datenschutzgruppe hat sich mehrere Male mit Vertretern von SWIFT und Bankenverbänden getroffen, um festzustellen, welche Schritte und Initiativen zur Einhaltung der Datenschutzgrundsätze unternommen und ergriffen werden können.

Parallel zur Arbeit der Art. 29 Datenschutzgruppe und der nationalen Datenschutzbehörden haben die Kommission und der Ratspräsident sich mit der Verletzung des EU-Datenschutzgesetzes durch die SWIFT und die Finanzinstitute befasst und arbeiten an einer Lösung der verschiedenen aufgetretenen Probleme.

Die Kommission hat stets unterstrichen, dass es zur Lösung der verschiedenen aufgetretenen Probleme zunächst notwendig ist, dass die SWIFT und die Finanzinstitute die Datenschutzrichtlinie einhalten und dass es insbesondere an der SWIFT liegt, die notwendigen Schritte zu unternehmen, um das belgische Datenschutzgesetz einzuhalten (ihre Verarbeitungstätigkeiten der belgischen Datenschutzbehörde zu melden) und die Kunden von Banken und anderen Finanzinstituten über die Art und Weise zu unterrichten, wie die SWIFT-Daten verarbeitet werden, dass sie

beispielsweise auf den US-SWIFT-Server weitergeleitet werden und dort von den US-Behörden für Zwecke der Terrorismusbekämpfung eingesehen werden könnten. Zweitens muss die SWIFT auch sicherstellen, dass Weiterleitungen der SWIFT-Daten für wirtschaftliche Zwecke auf ihren Spiegelserver in den Vereinigten Staaten gemäß der Datenschutzrichtlinie rechtmäßig sind. Zu diesem Zweck trat die SWIFT im Juni 2007 der US Safe Harbour bei.

Drittens haben die Kommission und der Ratspräsident mit dem US-Finanzministerium eine Reihe von „Zusicherungen“ besprochen, nach denen das US-Finanzministerium sich einseitig verpflichtet, personenbezogene Daten aus der EU in Übereinstimmung mit den Datenschutzgrundsätzen der EU zu verarbeiten. Das Parlament (der Ausschuss für bürgerliche Freiheiten, Justiz und innere Angelegenheiten) und der Rat (der Ausschuss der ständigen Vertreter der Mitgliedstaaten bei der EU) sowie auch die Art. 29 Datenschutzgruppe wurden über diese Gespräche regelmäßig auf dem Laufenden gehalten. Am 28. Juni 2008 informierte das US-Finanzministerium den Ratspräsidenten und die Kommission über die „Zusicherungen“ des US-Finanzministeriums in Bezug auf die Handhabung, Verwendung und Weitergabe von Daten aus dem Terrorist Financing Tracking Program (TFTP)³⁴.

3.2. DER EUROPÄISCHE GERICHTSHOF

*Urteil des erstinstanzlichen Gerichts vom 8. November 2007 – Bavarian Lager/Kommission (Rechtssache T-194/04)*³⁵

Die Dritte Kammer des erstinstanzlichen Gerichts der Europäischen Gemeinschaft hob eine Entscheidung der Kommission vom 18. März 2004 auf, die den Antrag auf Einsichtnahme in das vollständige Protokoll einer Versammlung ablehnte. Das erstinstanzliche Gericht hielt dagegen, dass eine Anfrage an die Kommission der Europäischen Gemeinschaft wegen einer Einsichtnahme personenbezogener Daten in einem Bericht der Kommission nur aus Gründen der Privatsphäre und

³³ Stellungnahme 10/2006 zur Verarbeitung personenbezogener Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP 128) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_de.pdf

³⁴ ABI C 166 vom 20.7.2007, S. 17.

³⁵ ABI C 315 vom 22.12.2007, S. 33.

Unversehrtheit von Personen abgelehnt werden darf, wenn besagte Privatsphäre und Unversehrtheit im Allgemeinen und im Besonderen durch die Bekanntgabe unterminiert würden; der Antragsteller muss nicht beweisen, dass die Bekanntgabe erforderlich ist. Die Kommission hat Einspruch eingelegt.

3.3. DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Einleitung

Die Hauptaktivitäten des Europäischen Datenschutzbeauftragten umfassen, wie in der Verordnung 45/2001³⁶ festgelegt, Folgendes:

- Überwachung der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der EU; Sicherstellung, dass die Rechte und Freiheiten von natürlichen Personen, deren Daten verarbeitet werden, nicht verletzt werden (Überwachung);
- Beratung bei Vorschlägen für neue EU-Regelungen mit Auswirkung auf den Datenschutz (Beratung);
- Zusammenarbeit mit anderen Datenschutzbehörden zwecks Gewährleistung eines hohen und einheitlichen Niveaus des Datenschutzes überall in Europa (Zusammenarbeit).

Im Jahr 2007 wurde ein wesentlicher Fortschritt im Bereich der Überwachung erzielt. Der auf dem Umfang der Ergebnisse liegende Schwerpunkt hat in den meisten Institutionen und Körperschaften der Gemeinschaft dazu geführt, dass in die Einhaltung der Datenschutzerfordernungen investiert wurde. Es gibt also Grund für eine gewisse Zufriedenheit, aber bis zur vollen Einhaltung sind weitere Anstrengungen erforderlich.

Im Bereich Beratung wurde viel Wert auf einen einheitlichen und effizienten Rahmen für den Datenschutz gelegt, und zwar sowohl für die erste und für die dritte Säule, aber nicht immer mit zufriedenstellenden Ergebnissen. Dennoch profitiert eine wachsende Vielzahl von Politikbereichen von den beratenden

Tätigkeiten der Europäischen Datenschutzbeauftragten (EPDS).

Der Vertrag von Lissabon ist ein wichtiger Höhepunkt in der Geschichte der Gemeinschaft, aber er sollte auch als Herausforderung angesehen werden. Die darin hervorgehobenen grundlegenden Sicherheitsvorkehrungen müssen nun in die Praxis umgesetzt werden. Dies gilt überall dort, wo Institutionen und Einrichtungen personenbezogene Daten verarbeiten, aber auch dort, wo Regeln und Strategien entwickelt werden, die Auswirkungen auf die Rechte und Freiheiten europäischer Bürger haben.

Überwachung

Die vom stellvertretenden Beauftragten übernommenen Überwachungsaufgaben reichen von der Beratung und Unterstützung der Datenschutzbeauftragten (DSB) über vorherige Überprüfung bedenklicher Verarbeitungsvorgänge bis zur Abwicklung von Anfragen und Bearbeitung von Beschwerden usw. Seine Arbeit besteht auch in der Ausarbeitung von Hintergrund- und Positionspapieren und in der Überwachung der Zentralstelle der Eurodac.

Im Jahr 2007 blieb das vorherige Überprüfen weiterhin eine der Haupttätigkeit der Überwachungsaufgaben des Europäischen Datenschutzbeauftragten. Die Meldefrist Frühjahr 2007 für den Eingang von Meldungen, die vorab vom Europäischen Datenschutzbeauftragten überprüft werden sollten – *Ex-Post-Fälle* –, wurde festgelegt, um die Institutionen und Einrichtungen der Gemeinschaft zu veranlassen, ihre Bemühungen hinsichtlich der vollständigen Erfüllung ihrer Meldepflichten zu steigern.

Insgesamt hat das Vorprüfungs-Programm des Europäischen Datenschutzbeauftragten im Jahr 2007 gezeigt, dass **die Meldefrist „Frühjahr 2007“** zu einem enormen Anstieg der Meldungen von vielen Datenschutzbeauftragten geführt hat, insbesondere im ersten Halbjahr des Jahres. Dennoch gibt es in Bezug auf den Zeitrahmen der Institutionen und Agenturen bei der Beantwortung von Informationsanforderungen seitens des Europäischen Datenschutzbeauftragten noch Vieles zu verbessern.

³⁶Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8, 12.1.2001, S. 1

Daher werden sich im Jahr 2008 die Bemühungen hauptsächlich auf folgende Punkte konzentrieren:

- Die Institutionen sollten ihr *Ex-post*-Mitteilungsverfahren endgültig festlegen und die Agenturen sollten im Jahr 2008 einen großen Sprung nach vorn in Richtung desselben Ziels machen;
- weitere Empfehlungen werden systematisch durch Informationen vom Datenschützer gegeben und mit Vor-Ort-Inspektionen kombiniert.

Im Jahr 2007 sind 65 **Beschwerden** eingegangen. Die Fälle wurden für zulässig befunden und bezogen sich insbesondere auf die Erfassung exzessiver Daten über Besucher, Zugriff auf Daten, Weiterleitung und Kopieren von E-Mails, Anforderungen von Kreditkartendaten, Verarbeitung sensibler Daten, Recht auf Berichtigung und Informationspflicht.

Eine Reihe von *Anfragen* wurde im Verlaufe des Jahres 2007 in verschiedenen Bereichen durchgeführt. Darunter waren zwei, die der besonderen Aufmerksamkeit des Europäischen Datenschutzbeauftragten bedurften, nämlich das OLAF-Sicherheitsaudit und die Rolle der Europäischen Zentralbank (ECB) im SWIFT³⁷-Fall.

Der Europäische Datenschutzbeauftragte beriet auch weiterhin im Falle von **Verwaltungsmaßnahmen**, die die Institutionen und Einrichtungen der Gemeinschaft in Bezug auf die Verarbeitung personenbezogener Daten in Betracht zogen. Es ergab sich eine Vielzahl von schwierigen Fragen, wie etwa die nach der Festlegung von Aufbewahrungsfristen für bestimmte Dateikategorien, Internetstrategiepapieren, Untersuchungsverfahren wegen Betrug und Korruption, Informationsaustausch, Einführung von Vorschriften zum Datenschutz und Anwendbarkeit nationaler Datenschutzgesetze.

Der Europäische Datenschutzbeauftragte arbeitete weiter an den **Videoüberwachungsrichtlinien** als praktischer Anleitung für Institutionen und Einrichtungen zur Einhaltung der Datenschutzvorschriften beim Einsatz von Videoüberwachungssystemen.

Die gemeinsam mit den Datenschutzbehörden der Mitgliedstaaten durchgeführte Überwachung von **Eurodac** wurde im Verlauf des Jahres 2007 fortgesetzt. Nach der Durchführung eines eingehenden Sicherheitsaudits im September 2006 wurde im November 2007 ein Abschlussbericht über das Audit vorgelegt. Die wesentliche Schlussfolgerung war, dass die ursprünglich im Hinblick auf die Eurodac umgesetzten Sicherheitsmaßnahmen und die Art und Weise, wie sie in den ersten vier Jahren ihrer Aktivität beibehalten wurden, bis jetzt einen angemessenen Schutz geboten haben. Dennoch weisen einige Teile der Systeme und die Organisationssicherheit gewisse Schwächen auf, auf die eingegangen werden muss.

Beratung

Im Jahr 2007 fanden die Aktivitäten des Europäischen Datenschutzbeauftragten im Kontext verschiedener Entwicklungen statt, deren gemeinsamer Nenner die Tatsache war, dass sie alle zur Ausbildung einer „**Überwachungsgesellschaft**“ beitrugen. Zu diesen Entwicklungen gehören neue Instrumente für die Strafverfolgung durch Erfassen und Verarbeiten personenbezogener Daten, die gestiegene Verwendung biometrischer Daten und RFID-Technologien sowie die wachsende Bedeutung weltweiter Datenströme.

Im Jahr 2007 gab der Europäische Datenschutzbeauftragte **12 Stellungnahmen** zu vorgeschlagenen EU-Regelungen ab. Im Bereich Freiheit, Sicherheit und Gerechtigkeit gab es erhebliche Bedenken in Bezug auf den Erlass neuer vorgeschlagener Regelungen zur Erleichterung der Speicherung von Daten durch die Strafverfolgungsbehörden und des Informationsaustauschs zwischen ihnen, ohne dass eine ordnungsgemäße Beurteilung der Wirksamkeit der vorhandenen Rechtsinstrumente erfolgt ist. Dieses Problem war von besonderer Relevanz in Verbindung mit der Umsetzung des Prüm-Vertrags auf EU-Ebene und dem Aufzeichnungssystem für Datensätze europäischer Fluggäste.

Ein weiteres Thema, das eine zentrale Rolle in den Stellungnahmen des Europäischen Datenschutzbeauftragten in Bezug auf die dritte Säule spielte, war

³⁷ Society for Worldwide Interbank Financial Telecommunication.

das Fehlen eines umfassenden rechtlichen Rahmens für den Datenschutz.

Ein drittes wesentliches Problem ist die Tatsache, dass die EU-Regelungen es einem Mitgliedstaat zur Pflicht machen, nationale Behörden für bestimmte Aufgaben bei der Verarbeitung personenbezogener Daten einzurichten, die Bedingungen der Arbeitsweise dieser Behörden aber dann weitestgehend dem alleinigen Ermessen des Mitgliedstaates überlassen. Das erschwert den Informationsaustausch zwischen den Mitgliedstaaten und beeinträchtigt die Rechtssicherheit der betroffenen Personen, deren Daten unter den Behörden der einzelnen Mitgliedstaaten ausgetauscht werden.

Der Informationsaustausch mit Drittländern für Strafverfolgungszwecke war ein weiteres Problem, das in den verschiedenen Stellungnahmen des Europäischen Datenschutzbeauftragten angesprochen wurde.

In einem allgemeineren Kontext wurden zwei Stellungnahmen bezüglich der Schlüsselmitteilung der Kommission zum **zukünftigen Rahmen des Datenschutzes** abgegeben. In seiner Stellungnahme zur Umsetzung der Datenschutzrichtlinie³⁸ hat der Europäische Datenschutzbeauftragte verschiedene Perspektiven eines sich verändernden Kontextes aufgezeigt, darunter einer in Bezug auf die Interaktion mit technischen Möglichkeiten. Neue Technologieentwicklungen haben eine eindeutige Auswirkung auf die Anforderungen an einen effizienten rechtlichen Rahmen für den Datenschutz. Ein entscheidendes Merkmal dieser technologischen Entwicklungen ist die **Radio Frequency Identification** (Funkerkennung), die Gegenstand einer separaten Stellungnahme des Europäischen Datenschutzbeauftragten war.

Im Dezember 2007 wurde die **Aufstellung 2008** (die zweite Jahresaufstellung) auf der Website des Europäischen Datenschutzbeauftragten veröffentlicht. Sie folgt den Hauptlinien, wie sie in der Aufstellung 2007 festgelegt wurden. Der Anhang der Aufstellung

beweist, dass der Tätigkeitsbereich des Europäischen Datenschutzbeauftragten nun eine breite Palette von Politikbereichen umfasst.

Fünf Perspektiven für den zukünftigen Wechsel, die als Agenda für die zukünftigen Aktivitäten des Europäischen Datenschutzbeauftragten dienen, ließen sich in seiner Stellungnahme zur Mitteilung über die Umsetzung der Datenschutzrichtlinie erkennen, und zwar:

- Interaktion mit technischen Möglichkeiten;
- Auswirkung des Vertrags von Lissabon;
- Strafverfolgung;
- globale Privatsphäre und Rechtsprechung; und
- vollständige Umsetzung der Richtlinie.

Zusammenarbeit

Das Hauptforum für die Zusammenarbeit zwischen den Datenschutzbehörden in Europa ist die **Art. 29 Datenschutzgruppe**. Der Europäische Datenschutzbeauftragte nimmt an den Aktivitäten der Datenschutzgruppe teil, die eine zentrale Rolle bei der einheitlichen Anwendung und Auslegung der allgemeinen Grundsätze der Richtlinie 95/46 spielt.

Der Europäische Datenschutzbeauftragte begrüßt die Stellungnahmen der Datenschutzgruppe, die mit seinen eigenen Stellungnahmen konform gehen und zu denen er aktiv beigetragen hat. Beispiele guter Synergien zwischen den Stellungnahmen der Datenschutzgruppe und des Europäischen Datenschutzbeauftragten im Jahr 2007 zeigten sich auf den Gebieten der gemeinsamen konsularischen Instruktionen an die diplomatischen Missionen und die konsularischen Vertretungen in Bezug auf die Einführung biometrischer Daten in Visa sowie die Übermittlung von Fluggastdaten an die USA und die Verwendung der Fluggastdaten für Strafverfolgungszwecke.

Der Europäische Datenschutzbeauftragte und die Datenschutzgruppe haben auch bei der Analyse zweier großer Systeme der ersten Säule eng zusammengearbeitet, und zwar des Systems der Zusammenarbeit der Verbraucherschutzbehörden und des Informationssystems für den Binnenmarkt.

³⁸Stellungnahme vom 25. Juli 2007 zu der Mitteilung der Kommission an das Europäische Parlament und an den Rat über den Stand des Arbeitsprogramms für eine bessere Durchführung der Datenschutzrichtlinie, Brüssel, ABl. C 255, vom 27.10.2007, S. 1.

Eine der wichtigsten Aufgaben des Europäischen Datenschutzbeauftragten in Bezug auf die Zusammenarbeit betraf **Eurodac**, für deren Verantwortung hinsichtlich der Überwachung des Datenschutzes die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte zeichnen. Im Juli 2007 hat der Koordinierungsausschuss zur Eurodac-Überwachung, der sich aus den Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten zusammensetzt, einen Bericht über seine erste koordinierte Überprüfung der Eurodac veröffentlicht. Der Ausschuss fand keine Hinweise auf einen Missbrauch des Eurodac-Systems. Einige Aspekte jedoch, wie beispielsweise Informationen an betroffene Personen, müssen verbessert werden.

Der Europäische Datenschutzbeauftragte bemüht sich, ein hohes und einheitliches Datenschutzniveau in den Arbeiten der Gemeinsamen Aufsichtsbehörden für die Informationssysteme Schengen, Europol, Eurojust und das Zollinformationssystem zu gewährleisten. Im Jahr 2007 konzentrierte sich das Augenmerk auf zwei Hauptthemen: den Vorschlag der Kommission für einen Rahmenbeschluss zum Datenschutz in der dritten Säule und den Austausch von Informationen für die Strafverfolgung gemäß dem Grundsatz der Verfügbarkeit.

Der Europäische Datenschutzbeauftragte nahm auch an den **europäischen und internationalen Konferenzen** zum Datenschutz und Schutz der Privatsphäre teil. Die letztere fand im September 2007 in Montreal statt und konzentrierte sich auf zahlreichen Fragen, mit denen sich die Beauftragten für Datenschutz und Privatsphäre befassen müssen, wie öffentliche Sicherheit, Globalisierung, Recht und Technologie, „Computereinsatz an beliebigen Orten“ und „menschlicher Körper als Ansammlung von Daten“. Der Europäische Datenschutzbeauftragte führte den Vorsitz einer nichtöffentlichen Sitzung für Kommissionsmitglieder zur Londoner Initiative und machte einen Beitrag zu einem Workshop über Globalisierung.

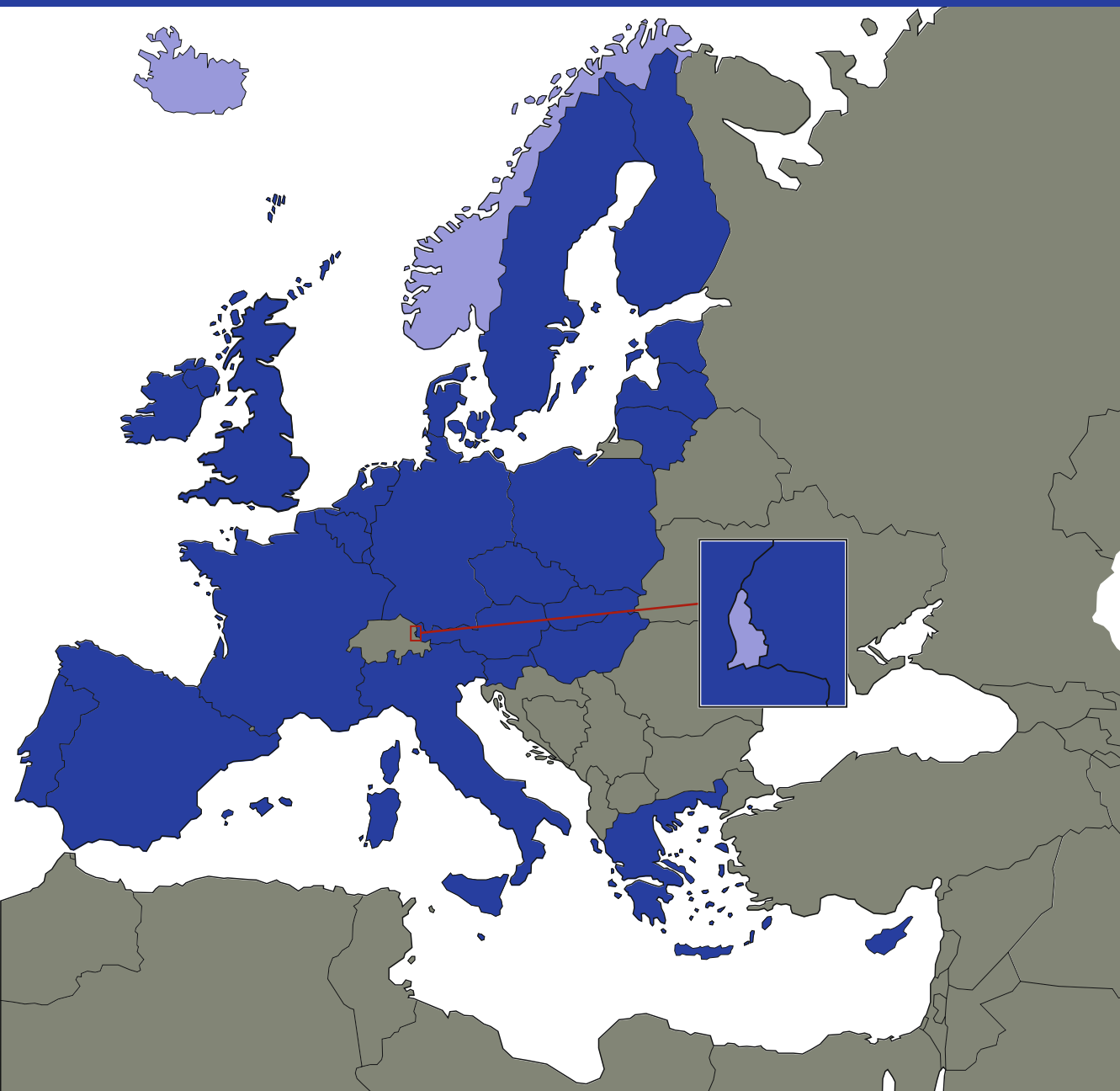
Mitteilung

Ein eindeutiger Schwerpunkt der Mitteilungsaktivitäten des Europäischen Datenschutzbeauftragten lag in seinen ersten Tätigkeitsjahren in der Erhöhung der **Sichtbarkeit** des europäischen Datenschutzbeauftragten auf der politischen Landkarte der EU. Drei Jahre nach Arbeitsaufnahme sind nun die positiven Ergebnisse seiner Kommunikationsbemühungen deutlich erkennbar. Ein Beispiel hierfür ist die Wahl des Beauftragten zu einem der 50 Nominierten von European Voice für den „European-of-the-Year-Award 2007“.

Als einer der Hauptarchitekten der „**Londoner Initiative**“, die die Kommunikation über Datenschutz und den Datenschutz an sich effizienter machen soll, verfolgte der Europäische Datenschutzbeauftragte dieses Ziel im Februar 2007 durch seine aktive Teilnahme am Kommunikationsworkshop der französischen Datenschutzbehörde (CNIL). Ein wichtiges Ergebnis war die Einrichtung eines Netzwerkes aus Kommunikationsbeauftragten, über das die Datenschutzbehörden sich über bewährte Verfahren austauschen und spezielle Projekte durchführen können.

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 Jahre 2007 wurde eine Reihe von Rechtsakten im Zusammenhang mit dem Datenschutz erlassen, die die Richtlinie 95/46/EG (jedoch nicht die Richtlinie 2002/58/EG) betrafen. Die wichtigsten davon waren die Folgenden:

1. Gesetz Nr. 36/2007 zur Änderung des Gesetzes Nr. 66/1985 über die National Archives. – Gemäß Gesetz Nr. 36/2007 soll eine Sonderabteilung innerhalb der National Archives alle Dokumente verwahren, die die nationale Sicherheit Islands in den Jahren 1945–1991 betreffen. Das Gesetz wurde in einer Zeit erlassen, in der es intensive Diskussionen über die telefonischen Abhörmaßnahmen während des Kalten Krieges gab. Diese telefonischen Abhörmaßnahmen richteten sich unter anderem gegen Personen, die in der Arbeiterbewegung und in der Sozialistischen Partei eine einflussreiche Rolle spielten. Mit diesem Gesetz sollten Dokumente über diese Ereignisse – z. B. Gerichtsurteile – und über die nationale Sicherheit in diesen Jahren im Allgemeinen der Öffentlichkeit und den betroffenen Personen, d. h. denjenigen, die in diesen Dokumenten erwähnt wurden, zugänglich gemacht werden. Dabei werden jedoch personenbezogene Daten sensibler Art über andere Personen als diejenigen, die eine Einsichtnahme wünschen, aus Kopien dieser Dokumente entfernt. Falls jedoch eine Person, über die solche Daten aufbewahrt werden, mit deren Veröffentlichung einverstanden ist, werden die Daten der Öffentlichkeit zugänglich gemacht.

2. Gesetz Nr. 40/2007 über das Gesundheitswesen. – Gemäß Art. 20 des Gesetzes muss das National Hospital unter anderem eine Blutbank betreiben. Es gibt jedoch keine weiteren Bestimmungen bezüglich dieser Blutbank, z. B. über den Schutz personenbezogener Daten. Im älteren Gesetz über das Gesundheitswesen 97/1990 gab es hierzu noch klare Bestimmungen, unter anderem diejenige, dass die Datenschutzbehörde die Aufgabe hatte, die Verarbeitung personenbezogener Daten in Blutbanken zu überwachen. Das Fehlen diesbezüglicher Bestimmungen wurde in der Stellungnahme der

Datenschutzbehörde zur Gesetzesvorlage bemängelt, die später als Gesetz Nr. 40/2007 gebilligt wurde. Änderungen am Gesetz im Sinne der Einwendungen wurden aber nicht vorgenommen.

3. Gesetz Nr. 41/2007 über die Nationale Gesundheitsbehörde. – Das Gesetz enthält Bestimmungen über die Verarbeitung personenbezogener Daten, deren wichtigste die Register betreffen, die die Nationale Gesundheitsbehörde führt. Gemäß Art. 8 des Gesetzes werden Patienten nicht um ihre Zustimmung gebeten, bevor ihre Daten in diese Register aufgenommen werden. Hierbei handelt es sich um Register über Geburten, Herz- und Gefäßkrankheiten, Erkrankungen des Nervensystems, Krebs, Unfälle, Aufnahme in Gesundheitseinrichtungen, Kommunikation zwischen Kliniken und Kommunikation zwischen im Gesundheitswesen Tätigen mit eigener Praxis.

Zuständig für diese Register ist der Leiter der Nationalen Gesundheitsbehörde. Diese Register werden aber nicht alle innerhalb der nationalen Gesundheitsbehörde geführt. So wird zum Beispiel das Krebsregister von der Icelandic Cancer Society geführt. Kennzeichnungen der persönlichen Identität müssen kodiert sein. Die Verarbeitung personenbezogener Daten muss gemäß dem Datenschutzgesetz Nr. 77/2000 erfolgen, und für die Datensicherheit gelten die Forderungen der Datenschutzbehörde. Eine Verwendung von Daten für die Zwecke wissenschaftlicher Forschung ist nur mit einer Genehmigung der Datenschutzbehörde möglich.

Weiterhin führt die Nationale Gesundheitsbehörde gemäß dem Medizinproduktegesetz Nr. 93/1994, vgl. Gesetz Nr. 89/2003, eine Arzneimitteldatenbank mit Daten über alle Rezeptverschreibungen der letzten drei Jahre (dies wird auch im Kapitel über Island im Jahresbericht für 2002 und 2003 erwähnt). Kennzeichnungen der persönlichen Identität sind codiert, können aber decodiert werden. Im Parlament wird derzeit eine Vorlage über eine Fristverlängerung der Vorratsspeicherung auf 30 Jahre behandelt. Die Datenschutzbehörde ist strikt gegen dieses Vorhaben und hat hierzu bereits mehrfach Stellungnahmen abgegeben.

4. Gesetz Nr. 163/2007 über das Statistische Amt Islands. Gemäß Art. 5-8 erhebt das Statistische Amt Daten – einschließlich personenbezogener Daten – für Statistische Untersuchungen. Das Statistische Amt hat gemäß Art. 9. des Gesetzes das Recht, seine eigenen Register mithilfe persönlicher Identifikationsnummern oder anderer Identifikationskennzeichnungen mit denjenigen anderer Parteien zu verknüpfen.

Weiterhin gibt es Bestimmungen über den Schutz personenbezogener Daten im Gesetz, z. B., dass Mitarbeiter des Statistischen Amtes zur Geheimhaltung verpflichtet sind (s. Art. 11) und dass vertrauliche Daten nach der Verwendung gelöscht werden müssen, sofern sie nicht für weitere statistische Untersuchungen nützlich sind, in welchem Fall Kennzeichnungen der persönlichen Identität unsichtbar gemacht oder gelöscht werden müssen (s. Art. 12). Weiterhin muss das Statistische Amt gemäß Art. 12 Bestimmungen bezüglich der Sicherheit und Aufbewahrung von vertraulichen Daten erlassen, z. B. über die Aufbewahrung und Vernichtung von Papierdokumenten, ob und wann rechnergestützte Daten gelöscht werden sollen und ob Kennzeichnungen der persönlichen Identität in solchen Daten unsichtbar gemacht oder codiert werden sollen.

Art. 13 enthält eine Bestimmung, dass das Statistische Amt Dritten zu Forschungszwecken Zugang zu sensiblen personenbezogenen Daten gewähren kann, sofern sie die Daten nach Abschluss des betreffenden Forschungsprojekts zurückgeben oder die Kennzeichnungen der persönlichen Identität löschen. In einer Stellungnahme zu der Vorlage, die später als Gesetz Nr. 163/2007 gebilligt wurde, schlug die Datenschutzbehörde vor, dass für die Aufbewahrung von Daten durch Dritte grundsätzlich eine bestimmte zeitliche Begrenzung gelten solle sowie dass, falls der Forscher die Daten über einen längeren Zeitraum aufbewahren möchte, er hierfür die Zustimmung des Statistischen Amtes einholen müsse. Dieser Vorschlag wurde angenommen.

Dagegen folgte das Parlament dem Vorschlag der Datenschutzbehörde nicht, in das Gesetz eine Bestimmung über die Codierung von Daten aufzunehmen, wenn gemäß der oben genannten Bestimmung von Art. 9 Register miteinander verknüpft werden.

B. Bedeutende Rechtsprechung

Am 6. Dezember 2007 fällte das Oberste Gericht von Island ein Urteil über die Entscheidung der Datenschutzbehörde vom 27. Februar 2006. Beim Kläger handelte es sich um einen Arzt, der laut der Entscheidung auf die Patientenakte einer Person zugegriffen hatte, um eine Gesundheitsbeurteilung für eine Versicherungsgesellschaft zu erstellen, ohne die Einwilligung dieser Person eingeholt zu haben. Die Datenschutzbehörde befand, dass es sich um einen gesetzwidrigen Zugriff handelte, da keine Einwilligung der betroffenen Person vorlag. Das Bezirksgericht Reykjavik schloss sich in einem Urteil vom 21. Dezember 2006 dieser Auffassung an (dieses Urteil ist im Kapitel über Island im Jahresbericht für 2006 erwähnt).

Das Gericht erklärte jedoch die Entscheidung der Datenschutzbehörde für nichtig. Das Gericht verwies diesbezüglich darauf, dass die betreffende Person ihrem Rechtsanwalt die schriftliche Erlaubnis für den Zugang zu ihrer Krankenakte erteilt habe. Der Rechtsanwalt habe dem Arzt eine Kopie der Erlaubnis übergeben. Aus diesem Grund befand das Gericht, dass der Arzt beim Zugriff auf die Krankenakte der betreffenden Person in gutem Glauben gehandelt habe. Das bedeutet mit anderen Worten, dass das Gericht der Auffassung war, dass der Arzt Grund zu der Annahme hatte, dass die betreffende Person ihre Zustimmung zu diesem Zugriff erteilt habe, auch wenn die betreffende Person die schriftliche Genehmigung nicht dem Arzt selbst erteilt hatte.

C. Wichtige spezifische Themen

Die wichtigsten von der Datenschutzbehörde im Jahre 2007 behandelten Fälle waren die Folgenden:

Am 19. Februar 2007 fällte die Datenschutzbehörde eine Entscheidung über die Rechtmäßigkeit und Sicherheit des Zugangs zu elektronischen Krankenakten im National Hospital. Die Klinik hatte bestimmten Mitarbeitern, u. a. allen Ärzten, sehr weitgehende Zugangsrechte gewährt, d. h. zu allen elektronischen Krankenakten aller Patienten mit Ausnahme bestimmter Datenkategorien wie zum Beispiel Daten über psychische Erkrankungen, die in einer speziellen Abteilung aufbewahrt wurden.

Der Klinik zufolge war dieser weitreichende Zugang notwendig, weil die fraglichen Mitarbeiter Patienten in allen Abteilungen der Klinik behandelten und in allen Abteilungen Beratung bezüglich der Behandlung erteilten. Die Datenschutzbehörde prüfte die Stichhaltigkeit dieser Einschätzung nicht weiter nach. Die Datenschutzbehörde entschied aber, dass strenge Sicherheitsmaßnahmen ergriffen werden müssten, z. B. dass Mitarbeiter einen Grund für ihren Zugriff auf eine Krankenakte angeben müssten (z. B. durch Ankreuzen eines Kästchens), dass alle Zugriffe protokolliert werden und dass die Protokolle regelmäßig überprüft werden müssten.

Am 26. Juni 2007 entschied die Datenschutzbehörde, dass die Nationale Gesundheitsbehörde nicht berechtigt sei, Forschern Zugang zu sensiblen Daten zu gewähren, darunter Daten über Abtreibungen. Die Forscher hatten Zugang zu Daten über Frauen beantragt, die an einem Forschungsprojekt über Empfängnisverhütung teilgenommen hatten. Die Frauen hatten die Auskunft erhalten, dass die über sie erhobenen Daten nach Abschluss des Projekts gelöscht werden würden. Lange nach Abschluss dieses vorangegangenen Projekts sollten nun jedoch weitere Daten über die Frauen erhoben werden, ohne ihre Zustimmung einzuholen. Die Datenschutzbehörde betrachtete dies als Verstoß gegen das Datenschutzgesetz Nr. 77/2000, weshalb die Behörde zu der oben erwähnten Entscheidung kam. Daraufhin löschte der Forscher alle personenbezogenen Daten, die beim vorangegangenen Projekt erfasst worden waren.

Am 6. Oktober 2007 fällte die Datenschutzbehörde eine Entscheidung über die Datenerfassung durch ein Aluminiumwerk in der Gemeinde Hafnarfjörður, das die Meinung der Einwohner der Gemeinde über eine beabsichtigte Erweiterung des Werks eingeholt hatte. Die Bewohner wurden telefonisch um ihre Meinung gebeten. Dann wurden die Daten über ihre Meinungen in einer elektronischen Datenbank gespeichert, ohne dass die Bewohner darüber informiert worden wären. Die Datenschutzbehörde kam zu der Entscheidung, dass dies ein Verstoß gegen das Datenschutzgesetz sei.

Am 26. November 2007 fällte die Datenschutzbehörde eine Entscheidung über die Verwendung von

Fingerabdrücken in der Mensa einer Grundschule. Die Fingerabdrücke wurden zur Identifizierung derjenigen verwendet, die Anspruch auf eine Schulmahlzeit hatten. Das Gerät verwendete Schablonen für den Vergleich mit den Fingerabdrücken der Schüler. Diese Schablonen konnten nicht für die Wiederherstellung von Fingerabdrücken verwendet werden. Die Eltern waren mit diesem Verfahren einverstanden, aber sie konnten sich stattdessen auch für so genannte Essensbons entscheiden, die an die Kinder ausgegeben wurden. Die Datenschutzbehörde entschied, dass dieses Verfahren nicht gegen das Datenschutzgesetz verstieße.

Am 26. November 2007 fällte die Datenschutzbehörde eine Entscheidung darüber, ob die Erlaubnis zur Verknüpfung genetischer Daten in verschiedenen Forschungsprojekten, die das Genforschungsunternehmen deCode durchführte, erteilt werden könne. Die Daten betrafen 85 000 Personen, die an 66 Projekten teilgenommen hatten. Diese Personen hatten die Einwilligung erteilt, dass ihre Daten für die Verwendung in einem bestimmten Projekt aufbewahrt werden dürften, aber auch für die Verwendung bei weiteren Projekten, da die Datenschutzbehörde und die nationale Bioethikkommission ihre Zustimmung erteilt hatten. Unter diesen Umständen wollte deCode davon absehen, die Einwilligung der betroffenen Personen zu einer Verknüpfung der Daten einzuholen. Falls sich herausstellen sollte, dass sie einen Genotyp besaßen, der auch bei Personen in einem anderen Projekt auftrat, sollten ihre Daten in dieses Projekt übernommen werden. Kennzeichnungen der persönlichen Identität sollten codiert werden, jedoch sollte es möglich sein, sie zu decodieren. Die Datenschutzbehörde war der Auffassung, dass diese Verarbeitung zu weitreichend sei, um von der Einwilligung der Betroffenen zur Verwendung der Daten bei weiteren Forschungen abgedeckt zu sein. Darüber hinaus war die Datenschutzbehörde der Meinung, dass sie nicht berechtigt sei, diese Verarbeitung zu genehmigen. Daher lehnte es die Datenschutzbehörde ab, eine Erlaubnis zu erteilen.

Am 10. Dezember 2007 fällte die Datenschutzbehörde eine Entscheidung über die Rechtmäßigkeit und Sicherheit der beiden Biobanken der Isländischen Krebsgesellschaft. Gemäß dem isländischen Gesetz über Biobanken Nr. 110/2000 müssen Bioproben in Biobanken

immer getrennt von Kennzeichnungen der persönlichen Identität gehalten werden. Dies war jedoch bei einer der Biobanken der Gesellschaft nicht der Fall, und die Datenschutzbehörde verlangte, dass dies spätestens bis zum 1. September 2008 geändert werden müsse. Diese Biobank wird zu Behandlungszwecken verwendet, und inzwischen wurde eine Gesetzesvorlage erarbeitet, in der es heißt, dass es in solchen Fällen nicht notwendig sei, Bioproben in einer Biobank von Kennzeichnungen der persönlichen Identität getrennt zu halten.



Liechtenstein

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

Eine der Aufgaben des Datenschutzbeauftragten (DSB) ist es, zu gesetzlichen Vorlagen und Erlassen, die für den Datenschutz erheblich sind, Stellung zu nehmen und die Übereinstimmung mit den Bestimmungen der Richtlinie 95/46/EG zu überprüfen. 2007 gab der DSB zu mehr als 20 Gesetzesvorhaben eine Stellungnahme ab. Im Folgenden sei eine Auswahl kurz dargestellt:

Anlässlich der Stellungnahmen zu den Vernehmlassungsberichten über die Änderung des *Gesetzes betreffend die Anerkennung von Hochschuldiplomen und beruflichen Befähigungsnachweisen*, des *Ärztegesetzes*, des *Gesetzes über das Veterinärwesen*, des *Gesetzes über die Rechtsanwälte, die Treuhänder und die Patentanwälte* sowie des *Gesetzes für die im Bauwesen tätigen Ingenieure und Architekten* war vor allem die Einführung des Internal Market Information System (IMI) von datenschutzrechtlicher Relevanz. In den Stellungnahmen wurde auf die Wichtigkeit einer einheitlichen Regelung für die verschiedenen Berufsgruppen hingewiesen. Es wurde im Wesentlichen angeregt, sich in den verschiedenen Gesetzestexten möglichst nahe am Text von Art. 56 Abs. 2 der Berufsqualifikationsrichtlinie zu halten und auf die umfangreiche Stellungnahme der Art. 29 Datenschutzgruppe zu den durch das IMI aufgeworfenen datenschutzrechtlichen Aspekten verwiesen (WP 140). Zum Ende des Berichtsjahres 2007 waren noch nicht alle der im Zusammenhang mit IMI stehenden Gesetzesrevisionen abgeschlossen.

Mit der Schaffung eines *Gesetzes über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz)* wird die Informationsweiterverwendungs-Richtlinie 2003/98/EG in nationales Recht umgesetzt. In seiner Stellungnahme hat der DSB zum einen auf die Stellungnahme 7/2003 der Art. 29 Datenschutzgruppe zur Weiterverwendung von Informationen des öffentlichen Sektors und Schutz personenbezogener Daten vom 12. Dezember 2003 (WP 83) Bezug genommen. Zum anderen wurde insbesondere eine gleichzeitige Abänderung des Datenschutzgesetzes in Art. 17 Abs. 2 Buchstabe f und Art. 23 Abs. 1

Buchstabe c angeregt. Im Unterschied zu manch anderen nationalen Datenschutzgesetzen innerhalb Europas dürfen nach dem liechtensteinischen Gesetzestext nur dann Personendaten bearbeitet werden, wenn die betroffene Person die Daten selbst allgemein zugänglich gemacht hatte. Der DSB strebt hier jedoch eine liberalere Handhabung an. Aus diesem Grund hat der DSB eine Änderung des Datenschutzgesetzes dahingehend vorgeschlagen, dass es als Rechtfertigungsgrund ausreiche, wenn die Personendaten allgemein öffentlich zugänglich sind (z. B. Telefonbuch). Dies würde eine grosszügigere Praxis erlauben, die auch im Lichte des neuen IWG sinnvoll und wünschenswert wäre. Das Widerspruchsrecht nach Art. 16 Abs. 3 DSG bleibt hiervon unberührt.

Im Berichtsjahr stand weiterhin die Abänderung des *Gesetzes über den unlauteren Wettbewerb (UWG)* an, um die Bestimmungen der europäischen Richtlinie 2005/29/EG über unlautere Geschäftspraktiken umzusetzen, die insbesondere die Vereinfachung des grenzüberschreitenden Handels zum Ziel hat. Neu in Liechtenstein eingeführt werden soll unter anderem demzufolge auch, dass neben Fax oder E-Mail auch hartnäckige und unerwünschte Werbung übers Telefon zu den aggressiven Geschäftspraktiken zählen, die bei Hartnäckigkeit als unlauter gilt. Dadurch ergäbe sich aber im Gegensatz zum liechtensteinischen Kommunikationsgesetz eine unterschiedliche rechtliche Beurteilung von unerwünschter Werbung, je nachdem welches Medium benutzt wird: Nach dem geltenden liechtensteinischen Kommunikationsgesetz ist Werbung, die ohne vorherige Einwilligung des Empfängers über Fax/E-Mail verschickt wird, grundsätzlich schon ab dem ersten Mal unzulässig.³⁹ Unerwünschte Werbung per Telefon wird vom Kommunikationsgesetz dagegen nicht erfasst. Die Revision des UWG hätte also zur Folge, dass nur unerwünschte Telefonwerbung nicht schon beim ersten Mal, sondern erst bei Vorliegen von „Hartnäckigkeit“ im Sinne des neuen UWG (straf-)rechtliche Konsequenzen nach sich ziehen würde. Demzufolge würde in Liechtenstein *de facto* eine rechtliche Unterscheidung zwischen unerwünschter Werbung per Telefon und der per Fax/E-Mail eingeführt. Dem DSB war es daher im Interesse der Verbraucher ein Anliegen, in seiner Stellungnahme zur Vorlage der Revision des UWG auf diese Diskrepanz

³⁹ Art. 50 Kommunikationsgesetz (KomG).

hinzuweisen und im Sinne eines durchgängigen Verbraucherschutzes eine Gleichstellung aller Medien zu fordern.

Von besonderer datenschutzrechtlicher Relevanz war ausserdem die Abänderung des *Polizeigesetzes*, die im Jahr 2007 bereits in Kraft trat. Im Rahmen der polizeilichen Ermittlungskompetenzen wurden etliche neue Rechtsgrundlagen geschaffen: So ist unter bestimmten Voraussetzungen die Erhebung und Bearbeitung biometrischer Daten zulässig; auch der Einsatz von Bild- und Tonträgern bei Massenveranstaltungen oder an allgemein öffentlich zugänglichen Orten ist nun bei Erfüllung bestimmter Bedingungen möglich. Die grundsätzliche Zulässigkeit einer Videoüberwachung durch die Landespolizei ist in Liechtenstein die bislang erste und einzige gesetzliche Regelung einer Videoüberwachung im öffentlichen Raum und ist allein schon aus diesem Grunde von entscheidender Bedeutung für den Datenschutz. Weiterhin wurden zahlreiche Regelungen für die (internationale) Amtshilfe sowie die Rechtsgrundlage für ein elektronisches Informationssystem geschaffen. Dieses Informationssystem ist aus datenschutzrechtlicher Sicht nicht ganz unproblematisch, da es die Verknüpfung verschiedener Datenbanken ermöglichen soll. Gänzlich neu eingeführt wurde zudem ein indirektes Auskunftsrecht. Soweit Staatsschutz oder Ermittlungen zur vorbeugenden Bekämpfung einer Straftat tangiert sind, kann die betroffene Person nicht selbst, sondern nur über den DSB Auskunft von der Landespolizei begehren, ob Daten über sie bearbeitet werden. Bis Ende 2007 wurde dieses indirekte Auskunftsrecht von niemandem in Anspruch genommen.

Von nationaler Bedeutung waren weiterhin die Abänderung des *Gesetzes über den Erwerb und Verlust des Landesbürgerrechts* sowie die *Schaffung einer rechtlichen Grundlage für die Zentrale Personenverwaltung der liechtensteinischen Landesverwaltung (ZPV)*; ein Gesetzesvorhaben, das aufgrund der datenschutzrechtlichen Problematik bereits seit mehreren Jahren aktuell ist und auch im Jahr 2007 noch nicht abgeschlossen werden konnte.⁴⁰

Im Rahmen der Abänderung des *Bankengesetzes* schlussendlich wurden Datenschutz relevante Pflichten in Bezug auf behördliche Zusammenarbeit oder in Zusammenhang mit Kunden, insbesondere eine allgemeine Informationspflicht gegenüber den Bankkunden, neu eingeführt. Erwähnenswert ist insofern, dass diese Informationspflicht nicht nur gegenüber dem bereits bestehenden Kundenkreis, sondern in Anlehnung an die Richtlinien 2004/39/EG und 2006/73/EG gleichwohl auch gegenüber potenziellen Kunden besteht.

Zu erwähnen ist in diesem Zusammenhang auch die *EU-Verordnung 1781/2006* (Übermittlung von Angaben zum Auftraggeber bei Geldtransfers), die zwar 2007 noch keine Gültigkeit in Liechtenstein hatte. Da sie aber 2007 bereits in der EU anwendbar war, hat die Verordnung bereits jetzt schon eine gewisse Wirkung für Liechtenstein, nämlich beim grenzüberschreitenden Zahlungsverkehr zwischen einer liechtensteinischen Bank mit einer Bank im EU-Raum. Einige liechtensteinische Banken sahen sich daher veranlasst, ihre Kunden schon im Berichtsjahr über die Auswirkungen besagter Verordnung zu informieren, obwohl sie noch nicht in das liechtensteinische Recht übernommen wurde.

B. Bedeutende Rechtsprechung

Der liechtensteinische Staatsgerichtshof hat als Verfassungsgerichtshof ein grundlegendes Urteil zur (internationalen) Amtshilfe und zum Bankkundengeheimnis gefällt.⁴¹ Danach kommt dem Bankkundengeheimnis materiell Verfassungsrang zu, auch wenn es nur auf Gesetzesstufe verankert ist. Es soll die finanziellen Aspekte der Geheim- und Privatsphäre eines Rechtssubjektes im Rahmen der gesetzlichen Schranken schützen. Dieser Schutz wird durch das in Art. 32 der liechtensteinischen Landesverfassung genannte verfassungsmässig gewährleistete Recht der persönlichen Freiheit geschützt.

Das Bankkundengeheimnis wird danach nicht verletzt, wenn die zuständige Aufsichtsbehörde bei einer Anfrage um internationale Amtshilfe die in Art. 36 Bankengesetz ausdrücklich verankerten Prinzipien der Spezialität, der

⁴⁰Vgl. 9th Annual Report of the Art. 29 Working Party on Data Protection, S. 128.

⁴¹Urteil des Staatsgerichtshofs vom 6. Februar 2006, StGH 2005/50, das aber erst im Jahr 2007 veröffentlicht wurde in: Liechtensteinische Juristenzeitung, 2007, LES 4/07, S. 396ff.

Vertraulichkeit, des Grundsatzes der «langen Hand» und der Verhältnismässigkeit befolgt. Amts- und Rechtshilfe sind nicht immer leicht auseinander zu halten. Das Amtshilfeverfahren kann dann nicht die Strafrechtshilfe umgehen, wenn die Amtshilfe unter Einhaltung dieser Prinzipien erfolgt. Da zusätzlich zum Anfangsverdacht weitere Elemente vorliegen müssen, die einen hinreichend begründeten Verdacht auf das Vorliegen einer strafrechtlich relevanten Verhaltensweise ergeben, sind so genannte «fishing expeditions», d. h. das Amtshilfeverfahren als solches als Vorwand für eine reine Beweisausforschung zu missbrauchen, nicht möglich und nicht zulässig.

C. Wichtige spezifische Themen

In Bezug auf den Zugriff von US-amerikanischen Behörden auf Daten internationaler Finanztransaktionen (Swift-Affäre) kamen die Banken der Forderung des DSB nach und änderten die Allgemeinen Geschäftsbedingungen. Nun wird darauf aufmerksam gemacht, dass im Falle der Abwicklung über internationale Kanäle die Auftragsdaten ins Ausland gelangen. In diesem Fall sind die Daten nicht mehr durch liechtensteinisches Recht geschützt und es ist nicht mehr sichergestellt, dass das Schutzniveau hinsichtlich dieser Daten demjenigen in Liechtenstein entspricht. Schliesslich wird auch darüber informiert, dass ausländische Gesetze und behördliche Anordnungen die involvierten Banken und Systembetreiber dazu verpflichten, diese Daten gegenüber Dritten offen zu legen.

Ausserdem wurde ein Projekt zum „Integrierten Case Management“ beratend begleitet.⁴² Hierbei ging es aus Sicht des DSB um die Verankerung von umfassenden Datenschutzerklärung, Geheimhaltungs- und Schweigepflichtvereinbarungen.

Der steigende Wunsch nach einer Videoüberwachung durch Behörden gab im Jahr 2007 Anlass zu teilweise

kontroversen Diskussionen. Ein Fall einer Videoüberwachung des öffentlichen Raums durch eine Behörde wurde der Datenschutzkommission zur Entscheidung vorgelegt. Der Fall war Ende 2007 noch nicht abgeschlossen.

Generell zu erwähnen ist ein leichter Anstieg der Anfragen⁴³ sowie der Zugriffe auf die Homepage⁴⁴. Dies spiegelt sicherlich das wachsende Datenschutz-Bewusstsein der Bevölkerung wider. Über die Internetseite sind neben aktuellen Themen auch Anleitungen für die Auslegung und Anwendbarkeit des Datenschutzgesetzes abzurufen, die so genannten Richtlinien. Neu im Jahr 2007 wurden die „Richtlinien zur Videoüberwachung durch Behörden“ sowie die „Richtlinien über den Umgang mit unerwünschter Werbung, insbesondere mit Spam“ veröffentlicht.

⁴² Beim Integrierten Case Management geht es darum, einem Arbeitnehmer, der länger als 6 Wochen arbeitsunfähig ist, die Wiedereingliederung ins Arbeitsleben zu erleichtern. Eine neue Gesetzesregelung sieht vor, dass u. a. der Arbeitgeber spätestens nach 6-wöchiger Abwesenheit eines Arbeitnehmers eine entsprechende Meldung an die Krankenkasse machen muss, die dann einen Case Manager einsetzen kann. Dieser Case Manager meldet sich sodann beim Arbeitnehmer und fragt nach, ob er etwas tun könne, damit eine Wiedereingliederung ins Arbeitsleben erleichtert wird. Der Arbeitnehmer kann dies ablehnen oder dem auch zustimmen.

⁴³ Im Berichtsjahr 2007 wurden insgesamt 338 Anfragen registriert und bearbeitet.

⁴⁴ Im Berichtsjahr 2007 betrug die Anzahl der Zugriffe auf die Internetseite der SDS 54679.



Norwegen

A. Umsetzung der Richtlinie 95/46/EG Bedeutende Änderungen in Datenschutzgesetzen bzw. Gesetzen zum Schutz der Privatsphäre

Anmerkung zum Bericht

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

Änderungen im Gesetz über die Umsetzung von Strafmaßnahmen und im Allgemeinen Bürgerlichen Strafgesetzbuch – Einführung der Informationspflicht, von Bestimmungen über bisherige gute Führung, die Benachrichtigung der geschädigten Partei usw.

Die Änderung betrifft eine erweiterte Informationspflicht gegenüber der geschädigten Partei bzw. den Hinterbliebenen der geschädigten Partei, was bedeutet, dass sie auch für den Ausgang vor dem voraussichtlichen Entlassungszeitpunkt und für eine Verbüßung der Strafe außerhalb des Gefängnisses gilt. Die Benachrichtigung soll *unter anderem* den Zeitpunkt und die Bedingungen der Strafverbüßung umfassen, wenn die Bedingungen unmittelbare Auswirkungen auf die geschädigte Partei beziehungsweise ihre Hinterbliebenen haben. Diese Bedingungen können sich auf den Wohnsitz beziehen oder darauf, ob es der verurteilten Personen untersagt ist, Kontakt mit bestimmten Personen aufzunehmen und wenn die verurteilte Person ihre Anschrift ändert.

Während der normalen Beratungsrunde der Änderungen erklärte die Datenschutzbehörde, dass die vorgeschlagenen Änderungen einseitig den Standpunkt der geschädigten Partei berücksichtigten und dass die Folgen für die verurteilte Person noch weiter untersucht werden müssten. Die Datenschutzbehörde verlangte weiterhin, dass nur ein Mindestmaß an Informationen zur Verfügung gestellt werden dürfe, und erklärte, dass nicht einzusehen sei, warum die geschädigte Partei jederzeit über den Wohnsitz der verurteilten Person informiert sein müsse, auch während der Bewährungsfrist. Es sollte ausreichen zu wissen, dass sich die verurteilte Person nicht mehr im Gefängnis befindet. Die Datenschutzbehörde wies weiterhin darauf hin, dass die Norwegische Strafvollzugsbehörde grundsätzlich verpflichtet ist, die

verurteilte Person über diese Informationspflicht zu informieren.

Gleichzeitig wurden neue und strengere Regelungen bezüglich der Nutzung elektronischer Kommunikationsmittel durch Gefangene innerhalb des Gefängnisses beschlossen. Die Datenschutzbehörde wies darauf hin, dass nicht klar sei, ob die vorgeschlagene Verschärfung in der Tat notwendig sei, und stellte sich auf den Standpunkt, dass das Recht auf elektronische Kommunikation in unserer heutigen technischen Gesellschaft nicht anders gehandhabt werden dürfe als dies hinsichtlich der herkömmlichen Post- und Telefondienste der Fall sei, soweit dies im Rahmen der Möglichkeiten der Strafvollzugsbehörden liege.

Änderungen an den Regeln über die Veröffentlichung von Listen von Steuerveranlagungen

Im Jahre 2004 wurden die Regeln verschärft, die für die Veröffentlichung von Listen von Steuerveranlagungen gelten, so dass die Listen jetzt nur noch in einem Zeitraum von drei Wochen nach der Veröffentlichung von Einzelpersonen durchsucht werden können. Die Listen der Steuerveranlagungen wurden seinerzeit elektronisch auf der Website der Steuerbehörden veröffentlicht und lagen als Ausdruck bei den Finanzämtern aus. 2007 erhielten die Medien durch eine Gesetzesänderung wieder Zugang zu vollständigen Listen der Steuerveranlagungen auf CD-ROM. Die Regierung begründete dies unter anderem mit dem Wunsch, die kritische Diskussion über das Steuersystem zu fördern.

Die Datenschutzbehörde hält die Gesetzesänderung für unglücklich. Die Frage der Veröffentlichung von Listen von Steuerveranlagungen wird von der Datenschutzbehörde schon seit Jahren kritisch gesehen. Die Datenschutzbehörde ist der Meinung, dass es fundamentalen Grundsätzen des Datenschutzes widerspricht, wenn Informationen, die norwegische Bürger vorlegen müssen, zu Unterhaltungszwecken genutzt werden, Gegenstand von Suchabfragen werden und über Mobiltelefone in Form von SMS-Diensten oder Ähnlichem verkauft werden können. Es sei weiterhin fragwürdig, dass die Listen der Steuerveranlagungen noch vor Ablauf der Einspruchsfrist gegen die steuerliche Veranlagung veröffentlicht werden.

Neue Regelungen bezüglich Kontaktaufnahme zum Zwecke sexuellen Missbrauchs

Es wurden neue Regelungen eingeführt, die die Kontaktaufnahme zu Missbrauchszwecken mit einem Kind unter Strafe stellen. Die Datenschutzbehörde erklärte, dass es wünschenswert sei, dass Politiker versuchen, Möglichkeiten der Vorbeugung gegen sexuellen Missbrauch von Kindern zu finden. Es wurde jedoch darauf hingewiesen, dass es unter dem Blickwinkel des Schutzes personenbezogener Daten eine interessante Frage sei, welche Maßnahmen mit der Strafvorschrift verbunden werden, das heißt welche Ermittlungsmethoden der Polizei zur Verfügung stehen sollen, damit das Ziel der Bestimmung erreicht wird.

B. Bedeutende Rechtsprechung

Keine nennenswerten.

C. Wichtige spezifische Themen

Inspektion des Gefängniswesens

Die Datenschutzbehörde hat nach einer Überprüfung des Umgangs mit sensiblen personenbezogenen Daten im Gefängniswesen heftige Kritik am Justizministerium geübt. Die schweren Rechtsverletzungen, die aufgedeckt wurden, zeigen, dass das Recht auf Datenschutz von über 30 000 ehemaligen Gefängnisinsassen und ihren Angehörigen missachtet wurde und wird.

Seit Jahren erhält die Datenschutzbehörde Beschwerden von Insassen norwegischer Gefängnisse bezüglich des Umgangs mit personenbezogenen Daten in den Gefängnissen. Die meisten Beschwerden betreffen den mangelnden Schutz von Informationen über die Häftlinge und ihre Angehörigen.

Nach der Inspektion kam die Datenschutzbehörde zu dem Ergebnis, dass es im norwegischen Gefängnis Ila ein inoffizielles und offenes Personenregister gibt („Insassen nach Nummer“). Dieses Register enthält sehr sensible personenbezogene Daten. Darüber hinaus fehlt für die Verwendung personenbezogener Daten im angewendeten professionellen System die rechtliche Grundlage. Die Grundrechte der erfassten Personen gemäß dem Datenschutzgesetz bezüglich des Rechts

auf Zugang, Berichtigung und Löschung werden nicht eingehalten.

Große Sicherheitslücken bei den Telekommunikationsgesellschaften – formelle Beschwerde

Im Zeitraum vom 28. Juli bis etwa 7. August 2007 wurden die Websites mehrerer Telekommunikationsgesellschaften für die Gewinnung personenbezogener Daten benutzt. Die Gewinnung personenbezogener Daten begann mit einer Liste möglicher persönlicher Kennnummern, die von einem Datenprogramm gespeichert wurden. Diese wurden anschließend mit einer offiziellen Website verglichen, um Nummern zu entfernen, die nicht verwendet wurden. Danach wurden die Nummern für die Suche nach Name und Anschrift einzelner Personen über die Website der Telekommunikationsbetreiber verwendet. Nur wenige der betroffenen Personen hatten eine Verbindung mit den Telekommunikationsgesellschaften, und sehr viele waren verärgert und überrascht, dass ausgerechnet sie betroffen waren.

Die Datenschutzbehörde ist der Auffassung, dass die schwerwiegendsten Verletzungen eindeutig mit dem unzulänglichen Schutz von Informationen, der Nicht-zurverfügungstellung weiterer Informationen und der Tatsache zu tun haben, dass es mehrere Gesellschaften nicht für nötig hielten, die Opfer über den Vorfall zu informieren. Die Tatsache, dass betroffene Personen nicht benachrichtigt wurden, beweist eine Missachtung des Rechts auf den Schutz der Privatsphäre.

Die Datenschutzbehörde beschloss, eine formelle Beschwerde wegen der Verletzung der Bestimmungen des Datenschutzgesetzes im Hinblick auf den Schutz von Informationen und auf die Bestimmung bezüglich der Verpflichtung, die Datenschutzbehörde zu informieren, einzureichen. Mehrere der registrierten Personen reichten ebenfalls formelle Beschwerden ein. Die formellen Beschwerden wurden zunächst von den Strafverfolgungsbehörden abgewiesen, werden jetzt jedoch erneut behandelt.

Neues Gesetz und neue Verordnungen zur Informationsfreiheit

Es wurde ein neues Informationsfreiheitsgesetz verabschiedet, das am 1. Juli 2008 in Kraft treten soll. Mit den vorgeschlagenen Verordnungen bezüglich des neuen

Informationsfreiheitsgesetzes, die in einer Beratungsrunde erörtert wurden, werden eine Reihe von Behörden und Ministerien angewiesen, ihre Aufzeichnungen über elektronische Post im Internet zur Verfügung zu stellen. Das Gesetz sieht weiterhin vor, dass die Dokumente so weit wie möglich veröffentlicht werden sollen. Eine solche Veröffentlichung großer Mengen von Informationen über Personen ist aus der Sicht der Datenschutzbehörde bedenklich. Bei einer übergroßen Menge an personenbezogenen Daten können umfassende Profile von Einzelpersonen erstellt werden. Diese Informationen können für Werbezwecke nützlich sein, können aber auch für den Identitätsdiebstahl verwendet werden. Wer eine Identität stehlen möchte, kann sich einen praktisch lückenlosen Überblick über die Handlungen und Vorlieben einer bestimmten Person verschaffen.

Der Datenschutzbehörde sind eine Reihe von Beispielen bekannt, dass Behörden personenbezogene Daten veröffentlicht haben, die nicht im Internet hätten verfügbar sein dürfen. Einige der Dokumente enthielten Informationen über das Geburtsdatum und Kennnummern, andere betreffen Personen in einer Krisensituation, die sich mit einem Hilfeersuchen an die Behörde wandten, und bei wieder anderen handelte es sich um Bewerbungen samt eingescannten Zeugnissen und Referenzen. Wenn hier Fehler gemacht werden, kann dies für die betreffende Person schwerwiegende Folgen haben. Wenn Ministerien und Behörden feststellen, dass vertrauliche personenbezogene Daten veröffentlicht wurden, berufen sie sich oft auf menschliche Irrtümer. Die Datenschutzbehörde ist der Meinung, dass wiederholte „Pannen“ auf ein Systemversagen bei der Behörde hinweisen.

Arbeitswelt – Zugang zu E-Mails von Mitarbeitern – formelle Beschwerden

2005 hat die Datenschutzbehörde zwei formelle Beschwerden gegen zwei Unternehmen wegen einer Verletzung der Bestimmungen des Datenschutzgesetzes im Hinblick auf die Auskunftspflicht im Zusammenhang mit dem Zugang zu E-Mails von Mitarbeitern eingereicht. 2006 hat die Strafverfolgungsbehörde beide Verfahren eingestellt. Die Datenschutzbehörde hat gegen beide Verfahrenseinstellungen Berufung eingelegt, jedoch wurden diese vom Generalstaatsanwalt bestätigt. Der Generalstaatsanwalt wies jedoch den Staatsanwalt

an, weitere Erkundigungen darüber einzuziehen, ob Mitarbeiter in einem der Unternehmen der Datenschutzbehörde Informationen vorenthalten haben. Im Oktober 2007 wurde auch dieses Verfahren eingestellt.

2006 reichte die Datenschutzbehörde eine formelle Beschwerde gegen einen Verleger wegen einer Verletzung des Datenschutzgesetzes ein. Hintergrund des Falles war, dass der Geschäftsführer des Verlages über einen „Überwachungsaccount“ automatisch Blindkopien der eingehenden E-Mail-Korrespondenz an den Leiter des Verlagsbüros in Schweden weiterleitete. Der persönliche E-Mail-Account des Mitarbeiters war mit einem Benutzernamen und einem persönlichen Passwort geschützt. Daraufhin griff der Verleger auf die Eingangs-E-Mails des Mitarbeiters über den „Überwachungsaccount“ zu. Der Mitarbeiter, der seine Eingangs-E-Mails herunterlud und öffnete, wurde nicht über das Herunterladen der E-Mails, den Zugriff auf diese, den Zweck der Maßnahme oder eine eventuelle Bekanntgabe der Informationen informiert.

Sowohl der Verlag als auch der Verleger wurden 2007 wegen einer Verletzung ihrer Informationspflicht angeklagt, und beide wurden mit einer Buße belegt, die sie akzeptierten.

Mautchips - AutoPASS

Im Frühjahr 2007 wurde die Datenschutzbehörde darüber informiert, dass alle Fahrzeuge, die die Mautstationen passierten, routinemäßig fotografiert wurden. Diese Informationen standen nicht im Einklang mit der offiziellen Spezifikation der Anforderungen bezüglich AutoPASS und den Informationen, die die Datenschutzbehörde bezüglich dieses Themas von der Direktion Straßenverkehr zuvor erhalten hatte. Daher wurde die Direktion Straßenverkehr aufgefordert zu bestätigen/zu widersprechen, dass alle Fahrzeuge, die die Mautstationen passierten, in Norwegen fotografiert werden. Auf der Grundlage der Antwort der Direktion Straßenverkehr kam die Datenschutzbehörde zu dem Ergebnis, dass alle Fahrzeuge, die die Mautstationen passieren, fotografiert werden. Allerdings werden die Aufnahmen nur in das System weitergeleitet, wenn die Durchfahrt ungültig ist oder wenn Zufallsprüfungen durchgeführt werden. Ein weiterer einschränkender Faktor ist die Tatsache, dass der interne Speicher der Kamera begrenzt ist und

dass Aufnahmen, die nicht weitergeleitet werden, daher relativ schnell wieder überschrieben werden. Die Datenschutzbehörde hält es für bedauerlich, dass weder die allgemeine Öffentlichkeit noch die Datenschutzbehörde bereits in einem früheren Stadium über den Sachverhalt informiert wurden. Es wird davon ausgegangen, dass das System verbessert wird.

Die 100 letzten Durchfahrten werden im AutoPASS-Chip gespeichert

Zu Beginn des Benachrichtigungsjahres stellte die Datenschutzbehörde fest, dass die 100 letzten Durchfahrten durch Mautstationen von AutoPASS-Benutzern in ihrem AutoPASS-Chip gespeichert wurden. Außerdem wurden auch andere Durchfahrtspunkte aufgezeichnet. Die Datenschutzbehörde reagierte auch auf die Tatsache, dass diese personenbezogenen Daten ohne jeglichen Vertraulichkeitsschutz auf fernablesbaren Chips gespeichert wurden. Der schwerwiegendste Verstoß liegt nichtsdestoweniger darin, dass die etwa eine Million Benutzer von AutoPASS nicht aktiv darüber informiert wurden, dass der Chip auf ihrer Windschutzscheibe auch eine Speicherkapazität für Informationen über Ort und Zeit der letzten 100 Durchfahrten besitzt.

Neues Gesundheitsforschungsgesetz

Im Sommer 2007 wurde dem Storting (norwegische Nationalversammlung) eine Vorlage für ein neues Gesetz über medizinische und gesundheitsbezogene Forschungen vorgelegt. Nach Auffassung der Datenschutzbehörde enthält die Vorlage eine Reihe unklarer Punkte, unter anderem bezüglich des Umfangs der Befugnisse der Datenschutzbehörde im Rahmen des Gesetzes. Formell lautet die grundsätzliche Regel der Vorlage, dass Forschungen über Gesundheitsinformationen nur mit Einwilligung der Person durchgeführt werden dürfen, auf die sich die Informationen beziehen.

Der Gesetzentwurf enthält jedoch eine so große Anzahl von Möglichkeiten, die Einwilligung außer Acht zu lassen, dass die *de facto* und in der Praxis geltende Grundregel der Notwendigkeit einer Einwilligung leicht lauten könnte, dass eine Einwilligung nicht erforderlich ist.

Der Gesetzentwurf führt auch eine neue Rechtskonzeption ein, nämlich die „generelle Einwilligung“. Diese Form der Einwilligung geht über dasjenige hinaus, was

gegenwärtig akzeptiert wird, und kommt dem Einverständnis mit einem Vertrag gleich, ohne dass man Gelegenheit hätte, die Vertragsbedingungen zu lesen. Die Tatsache, dass dies im Entwurf des Gesundheitsforschungsgesetzes als Einwilligung definiert wird, ist in den Augen der Datenschutzbehörde unglücklich gewählt. Wir laufen Gefahr, das Grundrecht des Einzelnen auf Information und Selbstbestimmung zu untergraben, was letztlich das Vertrauen belasten könnte, das zwischen der Gesellschaft und dem Arzt bestehen muss. Die Datenschutzbehörde hat das Storting aufgefordert, die positiven und negativen Auswirkungen des Gesetzes näher zu prüfen, bevor dieses verabschiedet wird.

Kapitel 5

Mitglieder und Beobachter der Art. 29 Datenschutzgruppe



MITGLIEDER DER ART. 29 DATENSCHUTZGRUPPE IM JAHR 2007

Österreich	Belgien
<p>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/</p>	<p>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 2 213 85 40 Fax: +32 2 213 85 65 E-Mail: commission@privacycommission.be Website: http://www.privacycommission.be/</p>
Bulgarien	Zypern
<p>Herr Krassimir Dimitrov Kommission für Schutz persönlicher Daten (Комисия за защита на личните данни) 1 Dondukov - BG - 1000 Sofia Tel: +359 2 940 2046; +359 2 915 3501 Fax: +359 2 940 3640 E-Mail: kzld@government.bg Website: http://www.cdpgd.bg</p>	<p>Frau Goulla Frangou Kommissionsmitglied 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</p>
Tschechische Republik	Dänemark
<p>Herr Igor Nemec Büro für Schutz persönlicher Daten (Úřad pro ochranu osobních údajů) 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/</p>	<p>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</p>

Estland	Finnland
<p>Herr Urmas Kukk Estrisches 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</p>	<p>Herr Reijo Aarnio Büro des Datenschutzombudsmannes (Tietosuoja valtuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tel: +358 10 36 166700 Fax: +358 10 36 166735 E-Mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi</p>
Frankreich	Deutschland
<p>Herr Alex Türk 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</p> <p>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: laoyere@cnil.fr Website: http://www.cnil.fr</p>	<p>Herr Peter Schaar Vorsitzender Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 - DE -53117 Bonn Tel: +49 1888 7799-0 Fax: +49 1888 7799-550 E-Mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de</p> <p>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</p>

Griechenland	Ungarn
<p>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</p>	<p>Herr Attila Peterfalvi Datenschutzbeauftragter 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://www.abiweb.obh.hu</p>
Irland	Italien
<p>Herr Billy Hawkes Kommissionsmitglied des Datenschutzes (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlinton, IE -Co.Laois Tel: +353 57 868 4800 Fax: +353 57 868 4757 E-Mail: info@dataprotection.ie Website: http://www.dataprotection.ie</p>	<p>Herr Francesco Pizzetti Italienische Datenschutzaufsichtsbehörde (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06 69 67 71 Fax: +39 06 69 67 77 85 E-Mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it</p>
Lettland	Litauen
<p>Frau Signe Plumina Staats Datenschutz Inspektorat (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</p>	<p>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</p>

Luxemburg	Malta
<p>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</p>	<p>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 2328 7198 E-Mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt</p>
Niederlande	Polen
<p>Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ Den Haag Tel: +31 70 888 85 00 Fax: +31 70 888 85 01 E-Mail: info@cbpweb.nl Website: http://www.cbpweb.nl http://www.mijnprivacy.nl</p>	<p>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: Sekretariat@giodo.gov.pl Website: http://www.giodo.gov.pl</p>
Portugal	Rumänien
<p>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</p>	<p>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</p>

Slowakei	Slowenien
<p>Herr Gyula Veszelei Büro für den persönlichen Datenschutz der Slowakische Republik (Úrad na ochranu osobných údajov Slovenskej republiky) 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</p>	<p>Frau Natasa Pirc Musar Kommissionsmitglied der Informationen (Informacijski pooblaščenec) 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</p>
Spanien	Schweden
<p>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 62 19/20 Fax: +34 91 445 56 99 E-Mail: director@agpd.es Website: http://www.agpd.es</p>	<p>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, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se</p>
Vereinigtes Königreich	European Data Protection Supervisor
<p>Herr Richard Thomas Büro des Kommissionsmitgliedes der Informationen (Information Commissioner's Office) Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-Mail: Fuellen Sie bitte das Online-Kontaktformular auf unserer Website aus Website: http://www.ico.gov.uk</p>	<p>Herr Peter Hustinx Europäischer Datenschutzbeauftragter (EDPS) (European Data Protection Supervisor – EDPS) Postanschrift: 60, rue Wiertz, BE - 1047 Bruxelles Büro: rue Montoyer, 63, BE - 1047 Bruxelles Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-Mail: edps@edps.europa.eu Website: http://www.edps.europa.eu</p>

BEOBACHTER DER ART. 29 DATENSCHUTZGRUPPE IM JAHR 2007

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	Republik Kroatien
Herr Philipp Mittelberger Datenschutzbeauftragter 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 Franjo Lacko Direktor Kroatische Datenschutzaufsichtsbehörde (Agencija za zaštitu osobnih podataka - AZOP) Republike Austrije 25, 10000 Zagreb Tel. +385 1 4609 000 Fax +385 1 4609 099 E-Mail: azop@azop.hr or info@azop.hr Website: http://www.azop.hr/default.asp
die ehemalige jugoslawische Republik Mazedonien	
Frau Marijana Marusic Datenschutzdirektion (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3244 760 Fax: +389 2 3244 766 Website: www.dzlp.mk , info@dzlp.gov.mk	

Sekretariat der Art. 29 Datenschutzgruppe

Herr Alain Brun
Referatsleiter
Referat Datenschutz
Generaldirektion Justiz, Freiheit und Sicherheit
Europäische Kommission
Büro: LX 46 01/182 - BE - 1049 Bruxelles
Tel: +32 2 296 53 81
Fax: +32 2 299 80 94
E-Mail: Alain.Brun@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm



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 978-92-79-10362-9



9 789279 103629