Achter Jahresbericht der Art. 29 Datenschutzgruppe

EUROPÄISCHE
KOMMISSION

Achter Jahresbericht

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

Berichtsjahr 2004

Angenommen im November 2005

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

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

INHALT

VORWORT DES VORSITZENDEN DER ART. 29 DATENSCHUTZGRUPPE

Für die Datenschutzgruppe war das Jahr 2004 durch den anhaltenden dramatischen Konflikt zwischen den zahlreichen Versuchen europäischer und anderer Regierungen, neue Instrumente im Kampf gegen den Terrorismus einzuführen, einerseits und der notwendigen Verteidigung des Datenschutzes als wesentlichem Bestandteil von Freiheit und Demokratie andererseits gekennzeichnet. Die vom Rat, den Mitgliedsstaaten und der Europäischen Kommission vorgeschlagenen Maßnahmen siedeln sich sowohl in der dritten Säule als auch in der ersten Säule an. Europaparlament, Rat und Europäische Kommission sind sich in der Rechtsgrundlage und somit in der weiteren Vorgehensweise uneinig. Die Datenschutzgruppe ist formal Teil der ersten Säule, die dritte Säule verfügt über kein äquivalentes beratendes Gremium. Es besteht die Gefahr, dass die Belange des Datenschutzes nicht vollständig berücksichtigt werden. Die Datenschutzgruppe hofft, dass Kommission und Rat bald auf den in der Breslauer Resolution vom September 2004 an sie gerichteten Appell der Europäischen Datenschutzkonferenz reagieren und den Weg für eine umfassende und effiziente Organisation bereiten werden.

Die Übermittlung von Fluggastdatensätzen (so genannten PNR-Daten) über die Buchungssysteme der Fluggesellschaften an das United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten, CBP), die von den Vereinigten Staaten verlangt wurde, wurde nach langwierigen Verhandlungen mit der amerikanischen Seite von der Kommission trotz einiger verbleibender, kritischer Anmerkungen der Datenschutzgruppe genehmigt. Diese Kritik bezog sich auf den Umfang der Datensätze und das Fehlen klarer, verbindlicher Richtlinien für die Verwendung der Passagierdaten und deren Aufbewahrungszeitraum, das heißt auf die Unverhältnismäßigkeit dieser Maßnahme (WP 87, 95 und 97). Die Datenschutzgruppe nahm mit Genugtuung zur Kenntnis, dass das Europäische Parlament ihre kritische Auffassung teilt. Das Parlament verklagte die Kommission sogar vor dem Europäischen Gerichtshof, mit dem Argument, dass das Abkommen eine Beschneidung der durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates geschützten Passagierrechte beinhalte und deshalb nicht ohne vorherige Zustimmung hätte unterzeichnet werden dürfen. Das Beispiel Kanadas und Australiens, wo alternative PNR-Lösungen gefunden wurden, zeigt, dass die Datenschutzgruppe der Erhebung neuer Datenströme zu Sicherheitszwecken durchaus zustimmen kann, sofern diese Datenströme angemessen sind, mit anderen Worten, sofern sie Sicherheitserfordernisse unter möglichst geringer Beeinträchtigung der Privatsphäre befriedigen (WP 85 und 88).

Bei der Erörterung der Pläne zur Einführung einer europaweiten präventiven Aufbewahrung aller Fernübertragungsdaten einschließlich der Daten über die Internetnutzung stehen wir vor dem gleichen grundsätzlichen Konflikt zwischen Freiheit und Sicherheit. Diese Maßnahme hätte nicht nur Folgen für Personen, die von Europa in Drittländer fliegen, sondern würde sehr stark in das Leben praktisch jedes europäischen Bürgers eingreifen, der ein Telefon oder elektronische Kommunikationsmittel benutzt. Es würde eine riesige Fülle an Informationen über fast alle unsere Kontakte, unsere Interessen, unseren Lebenswandel, unsere Aufenthaltsorte, unser Tun, Denken und Fühlen – mit anderen Worten über unsere Persönlichkeit - verfügbar. Es ist bekannt, dass sogar Daten, die von Banken und anderen Finanzinstituten mit höchsten Sicherheitsmaßstäben übertragen werden, auf unerlaubte Weise gelesen und missbraucht werden. Eine solche allgemeine Verpflichtung zur langfristigen Aufbewahrung von Daten im Datenverkehr würde nicht nur unsere Privatsphäre einschränken, sondern auch neue Risiken für den Datenschutz und die Vertraulichkeit von Daten mit sich bringen, denn Hacker und andere Unbefugte wären sehr an einem

Zugang zu solchen riesigen Mengen vertraulicher Daten interessiert. Sollen wir solche hohen Risiken eingehen? Die Datenschutzgruppe hat mit Hinweis auf die Europäische Menschenrechtskonvention ihre Vorbehalte zum Ausdruck gebracht (WP 99). Sie ist besorgt, dass sich die schwierige politische Lage, in der sich Europa zurzeit befindet, noch verschlimmern könnte, wenn Beschlüsse, die alle Europäer betreffen, ohne eine angemessene öffentliche Debatte und ohne ein klares demokratisches Verfahren in den Mitgliedsstaaten und auf europäischer Ebene getroffen würden. Deshalb begrüßt die Datenschutzgruppe den Standpunkt des Europäischen Parlaments und der Europäischen Kommission, dass die Regelung der Verarbeitung und der Aufbewahrung von Kommunikationsdaten im Rahmen eines gemeinsamen Entscheidungsfindungsprozesses erarbeitet werden soll.

Die Aufnahme biometrischer Daten in persönliche Dokumente ist ein weiterer Schritt in der europäischen Reaktion auf die weltweite Bedrohung der Sicherheit. Die Datenschutzgruppe hat den Datenschutzbedarf bei Visa und anderen Aufenthaltstiteln klar umrissen. Dies ist jedoch nur ein erster Schritt in ein neues Zeitalter der Identifikationstechnik. Die Biometrie betrachtet den menschlichen Körper als maschinenlesbare Datenquelle. Die Datenschutzgruppe hat die diesbezüglichen Auswirkungen untersucht und die einzelnen Möglichkeiten auf verschiedenen Ebenen in Bezug auf die Auswahl der biometrischen Daten, die Art und Weise der Aufbewahrung dieser Daten oder deren Ableitungen (Templates), das Verfahren zur Erstellung der Dokumente und die praktische Anwendung sowie insbesondere die Risiken einer zentralen Datenspeicherung und die Maßnahmen gegen Datenmissbrauch aufgezeigt. Das gesamte Thema ist von äußerster Wichtigkeit. Deshalb gelten die vorgenannten Anmerkungen zum legitimierten Entscheidungsfindungsprozess für die präventive Aufbewahrung von Telekommunikationsdaten auch für die Aufnahme biometrischer Daten in Dokumente, die von unseren Bürgern benutzt werden müssen.

Die Datenschutzgruppe wirkt weiterhin richtungweisend bei sektorspezifischen Problemen. Die Verwendung genetischen Datenmaterials gewinnt immer größere praktische Bedeutung. Die Datenschutzgruppe hat unter Berücksichtigung der gesetzlichen Erfordernisse und bewährter Vorgehensweisen einen Richtlinienkatalog erstellt. Sie hat auch ein strukturelles Problem benannt, das zu einem späteren Zeitpunkt eingehender behandelt werden muss: die Eigentumsrechte an genetischen Daten als gemeinsames Erbe einer Gruppe von Menschen, die durch biologische Bande miteinander verbunden sind. Dies steht in klarem Widerspruch zur allgemeinen Auffassung, dass persönliche Daten ausschließlich zu ihrem Träger gehören, dem Betroffenen (WP 96).

Ferner wurden weitere sektorspezifische Dokumente zu den Themen Videoüberwachung (WP 89) und unerbetene Werbenachrichten (WP 90) erarbeitet. Ein eher technisches Dokument beschäftigt sich mit vertrauenswürdigen Rechnerplattformen (Trusted Computing Platforms) (WP 86).

In enger Zusammenarbeit mit der Industrie wurde ein Modell für mehrschichtige Informationsvermittlung entwickelt, das Informationen, die Internetnutzer über die Verwendung ihrer Daten erhalten, verständlich und vergleichbar macht (WP 100). Wir hoffen sehr, dass dies für mehr Klarheit innerhalb der Informationsfülle des Internets sorgt und die Benutzer zu fundierten Entscheidungen befähigt.

Eine einheitliche Durchsetzung ist neben der Vereinheitlichung der Rechtsgrundlagen ein ebenso wichtiger Teil des europäischen Datenschutzes. Die Datenschutzgruppe hat ein langfristiges Programm mit verschiedenen Durchsetzungsverfahren in den Mitgliedsstaaten eingeleitet. Mit diesem und anderen Dokumenten kommt die Datenschutzgruppe der Aufforderung der Europäischen

Kommission nach, einen Beitrag zu deren Arbeitsprogramm 2003-2004 für eine bessere Umsetzung der Datenschutzrichtlinie zu leisten (WP 101).

Die Mitglieder der Datenschutzgruppe hielten es für hilfreich, das eigene Verständnis ihrer Rolle als Teil der europäischen Institutionen, ihres Mandates und des technologischen, politischen und wirtschaftlichen Rahmens ihrer Arbeit in einem „Strategiepapier" darzulegen. Sie erläuterten auch die Arbeitsverfahren hinsichtlich der Tätigkeiten innerhalb der Datenschutzgruppe und der Zusammenarbeit mit Dritten. Der europäische Datenschutzbeauftragte, der seine Tätigkeit nun aufgenommen hat, ist neues Mitglied der Datenschutzgruppe. Die Koordination mit dem Datenschutzbeauftragten hat sich als besonders wichtig und nützlich erwiesen. Die allgemeine Zielsetzung ist eine Schärfung des Problembewusstseins und Erweiterung des Kenntnisstands auf allen Ebenen, die Unterstützung der europäischen Institutionen bei der Einbeziehung von Datenschutzerwägungen und –erfordernissen in ihre Entscheidungsfindungsprozesse und die einheitliche, effiziente und direkte Durchsetzung der Datenschutzbestimmungen in den Mitgliedstaaten und auf europäischer Ebene. Die Datenschutzgruppe möchte so kooperativ und transparent wie möglich arbeiten. Arbeitspapierentwürfe werden, sofern dies angebracht ist, Online-Beratungen unterzogen. Diese Praxis hat sich als sehr erfolgreich erwiesen. Die Datenschutzgruppe versucht, ihre Arbeit und ihre Ergebnisse einem möglichst breiten Publikum näher zu bringen. Sinn und Zweck des Strategiepapiers ist es, den Teamgeist innerhalb der Datenschutzgruppe zu festigen und einen Beitrag zur Transparenz für Partner und Öffentlichkeit zu leisten (WP 98).

Peter Schaar
Vorsitzender der Art. 29 Datenschutzgruppe

[1] Alle Dokumente, die von der Art. 29 Datenschutzgruppe angenommen wurden, finden Sie unter http://europa.eu.int/comm/justice_home/fsj/privacy/

Kapitel 1
Die Aufgaben der Art. 29 Datenschutzgruppe [1]

1.1 TRANSFER VON DATEN IN DRITTLÄNDER

1.1.1 Australien

Stellungnahme Nr. 1/2004 zu dem in Australien gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdatensätzen (Passenger Name Record data - PNR) von Fluggesellschaften

Die australische Gesetzgebung zum Schutz der nationalen Grenzen ermächtigt die australische Zollbehörde (Australian Customs) zur Gefahrenprüfung von Passagieren anhand von Fluggastdatensätzen (PNR) vor der Ankunft in beziehungsweise der Abreise aus Australien. Die Gesetzgebung beabsichtigt einen besseren Schutz der australischen Grenzen und dient vor allem der Umsetzung der im Wahlprogramm 2001 von der Regierung verlangten Erhöhung der nationalen Sicherheit.

Die Datenschutzgruppe gab eine positive Stellungnahme über das Schutzniveau ab, das die australische Zollbehörde bei der Übermittlung von PNR-Daten nach Australien bietet.

Diese Stellungnahme wurde unter der Bedingung abgegeben, dass die Einschränkung gemäß Artikel 41 Absatz 4 des Australian Privacy Act (australisches Datenschutzgesetz), der den Datenschutzbeauftragten bei der Untersuchung von Beschwerden nichtaustralischer Bürger oder Gebietsansässiger bezüglich Berichtigungsanfragen ausschließt, gestrichen wird. Das Gesetz wurde entsprechend geändert.

1.1.2. Kanada

Stellungnahme Nr. 3/2004 zu dem in Kanada gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdatensätzen (Passenger Name Records - PNR) und erweiterten Passagierdaten (Advanced Passenger Information – API) von Fluggesellschaften

Kanada hat eine Reihe von Gesetzen und Verordnungen erlassen, nach denen Fluggesellschaften mit dem Bestimmungsland Kanada die persönlichen Daten von Passagieren und Besatzungsmitgliedern zur Sicherung der Integrität der kanadischen Grenzen und zur Sicherheit Kanadas übermitteln müssen. Das kanadische API/PNR-Programm befand sich schon lange vor den Ereignissen vom 11. September 2001 in Vorbereitung, denn es wurde als Bestandteil der Programme für eine verbesserte Sicherung der kanadischen Grenzen betrachtet, die Kanada die Identifizierung von und die Konzentration auf Reisende mit einem hohen Risikoprofil ermöglichen und die Einreise von Personen mit einem geringen Risikoprofil erleichtern.

Laut der Datenschutzgruppe kann die Einhaltung der kanadischen Anforderungen aus mehreren Gründen zu Problemen im Hinblick auf die Richtlinie 95/46/EG über den Datenschutz führen. Die Zweckbestimmung der angeforderten Daten war zu weit gefasst und ging insbesondere eindeutig über den Zweck der Terrorismusbekämpfung hinaus. Die Datenschutzgruppe verlangte eine klar abgegrenzte Liste schwerwiegender Straftatbestände, die unmittelbar in Zusammenhang mit dem Terrorismus stehen.

Die Datenschutzgruppe vertritt die Auffassung, dass die Menge der Daten, die an die kanadischen Behörden übermittelt werden sollen, weit über das hinausgeht, was im Sinne von Artikel 6 Absatz 1 Buchstabe c der Richtlinie als angemessen, erheblich und nicht über den Zweck hinausgehend betrachtet werden kann. Die Datenschutzgruppe verlangte, dass die Menge der Daten dem jeweiligen öffentlichen Interesse, um das es geht, angepasst wird. Die Daten dürfen nur über einen kurzen Aufbewahrungszeitraum aufbewahrt werden, der einige Wochen oder Monate nach der Einreise in Kanada nicht überschreiten darf. Ein Aufbewahrungszeitraum von sechs Jahren, der von den kanadischen Behörden verlangt wurde, wurde als zu lang betrachtet.

1.1.3. Vereinigte Staaten von Amerika

Stellungnahme Nr. 2/2004 zur Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records – PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (US CBP – Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden sollen

Im Anschluss an ihre Stellungnahmen Nr. 6/2002 und Nr. 4/2003 gab die Datenschutzgruppe im Lichte der Entwicklungen in Bezug auf die Übermittlung von PNR-Fluggastdaten an die USA und insbesondere der Mitteilung der Europäischen Kommission vom Dezember 2003 über einen umfassenden PNR-Ansatz und der Ergebnisse der Verhandlungen zwischen der Europäischen Kommission und den US-Behörden eine neue Stellungnahme ab. Die Datenschutzgruppe empfahl der Kommission, die Übermittlung von PNR-Daten im Rahmen des CAPPS-II-Programms und aller anderen für die Massendatenverarbeitung geeigneten Systeme auszuschließen. Die Datenschutzgruppe machte auf die fehlende Rechtsverbindlichkeit der US-Verpflichtungen aufmerksam und forderte eine weitere Einschränkung der Zwecke, zu denen die Daten übermittelt werden, eine angemessene Datenmenge, ein Verbot für die Übermittlung sensibler Daten, die Bedeutung eines „Push"-Verfahrens für die Übermittlung, eine strenge Beschränkung der Weiterübermittlung von PNR-Fluggastdaten an andere Behörden der Vereinigten Staaten oder in anderen Ländern, Sonderrechte für Passagiere in Bezug auf Information, Datenzugang und Datenberichtigung sowie angemessene Aufbewahrungsfristen.

Stellungnahme Nr. 6/2004 zur Durchführung der Kommissionsentscheidung vom 14. Mai 2004 über die Angemessenheit des Schutzes der personenbezogenen Daten, die in den Fluggastdatensätzen (Passenger Name Records – PNR) enthalten sind, welche dem United States Bureau of Customs and Border Protection (US CBP – Zoll- und Grenzschutzbehörde der Vereinigten Staaten) übermittelt werden, und des Abkommens zwischen der Europäischen Gemeinschaft und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen und deren Übermittlung durch die Fluggesellschaften an das Bureau of Customs and Border Protection des United States Department of Homeland Security (US-Ministerium für Heimatschutz)

Stellungnahme Nr. 8/2004 zur Unterrichtung von Fluggästen anlässlich der Übermittlung persönlicher Daten bei Flügen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika

Nach der Kommissionsentscheidung vom 14. Mai 2004 gab die Datenschutzgruppe zwei Stellungnahmen ab. In ihrer Stellungnahme Nr. 6/2004 stellt die Datenschutzgruppe fest, dass die Kommission die Anforderungen, die die Datenschutzgruppe insbesondere an den Umfang der zu übermittelnden Daten, die Dauer ihrer Speicherung und die Art ihrer Verwendung gestellt hat, nur zum Teil berücksichtigt. Die Datenschutzgruppe verwies auf zwei Punkte, in denen sich alle Parteien einig sind: das „Push"-Verfahren und die Unterrichtung der Fluggäste. Die Datenschutzgruppe bat die Fluggesellschaften, das technische Verfahren der Datenübermittlung so schnell wie möglich vom „Pull"-Verfahren auf das „Push"-Verfahren umzustellen, da es den allgemeinen datenschutzrechtlichen Grundsätzen entspricht, dass der Empfänger nur diejenigen Daten erhält, die er tatsächlich benötigt.

Die Datenschutzgruppe begrüßte die regelmäßige Kontrolle der Einhaltung der Datenschutzvorschriften, die mit den Vereinigten Staaten von Amerika vereinbart wurden. Die Datenschutzgruppe betonte außerdem die Notwendigkeit einer angemessenen Unterrichtung der Flugpassagiere, insbesondere die Notwendigkeit der Homogenität der Informationen, die die

Fluggäste erhalten, und zwar unabhängig von der Fluggesellschaft, die sie benutzen, oder dem Reisebüro, in dem sie ihren Flugschein erwerben. Zu diesem Zweck hat die Datenschutzgruppe zwei Informationsschreiben verabschiedet, die ihrer Stellungnahme Nr. 8/2004 beiliegen, und Fluggesellschaften, Reiseveranstalter und Betreiber computerunterstützter Reservierungssysteme aufgefordert, diese Schreiben so weit reichend wie möglich anzuwenden.

Bericht über den „sicheren Hafen" (Safe Harbor)

Die Datenschutzgruppe unterstützte die Kommission bei der Vorbereitung des Berichts, dessen Inhalt zuvor eingehend von der Datenschutzgruppe besprochen wurde. Im Anschluss an die Annahme des Berichts arbeitete die Datenschutzgruppe mit der Kommission an der Behebung der im Bericht enthaltenen Mängel, sodass der sichere Hafen erwartungsgemäß funktioniert. Unter anderem traf sich die Datenschutzgruppe mit Mitgliedern der Federal Trade Commission (FTC) zur Erörterung von Durchsetzungsfragen im Allgemeinen und der Durchsetzung der sichere-Hafen-Grundsätze im Besonderen.

1.2. ERWEITERUNG DER EINHALTUNG DER DATENSCHUTZRICHTLINIE

Entschließung der Art. 29 Datenschutzgruppe zum Thema Rechtsdurchsetzung

Am 25. November 2004 hat die Datenschutzgruppe die vorgenannte Entschließung zum Thema Rechtsdurchsetzung, die die Ergebnisse der Debatten über die Rechtsdurchsetzung in den Arbeitsgruppen und im Plenum enthält, angenommen und gemeinsame Durchsetzungsaktionen für die Jahre 2005-2006 auf der Grundlage der Kriterien, die in diesem Dokument aufgeführt sind, angekündigt.

Die Datenschutzgruppe äußerte ihre Überzeugung, dass eine bessere Einhaltung der Datenschutzgesetze innerhalb der gesamten Europäischen Union notwendig sei. Sie erklärte, sie werde sich um die Verbesserung der gegenwärtigen Situation bemühen.

Stellungnahme zu einheitlicheren Bestimmungen über Informationspflichten

Die Stellungnahme zu einheitlicheren Bestimmungen über die Informationspflichten, die eine Vereinfachung und Vereinheitlichung der an die Unternehmen gestellten Anforderungen beinhaltet, die Bürger über die Verarbeitung ihrer Daten zu informieren, wurde am 25. November 2004 angenommen. Die Datenschutzgruppe bekräftigt in ihrer Stellungnahme die Bedeutung eines gemeinsamen Verfahrens für eine pragmatische Lösung, die der Umsetzung der allgemeinen Grundsätze der Richtlinie hinsichtlich einer einheitlicheren Informationspflicht einen praktischen Mehrwert verleihen soll. Die Datenschutzgruppe befürwortet das Prinzip, nach dem eine Erklärung über eine Verarbeitung nach Treu und Glauben nicht unbedingt in einem einzigen Dokument enthalten sein muss. Stattdessen könnten die Informationen für die Betroffenen auf bis zu drei Ebenen verteilt werden, solange die Gesamtheit dieser Ebenen den rechtlichen Anforderungen entspricht.

1.3. INTERNET UND TELEKOMMUNIKATION

Stellungnahme Nr. 5/2004 zu unerbetenen Werbenachrichten im Sinne von Artikel 13 der Richtlinie 2002/58/EG

Diese Stellungnahme behandelt die rechtlichen Grundlagen für die Übermittlung elektronischer Mitteilungen (zum Beispiel E-Mail, SMS, Fax, Telefon) an natürliche Personen zu Werbezwecken gemäß Artikel 13 der Richtlinie 2002/58/EG. Diese Stellungnahme dient in erster Linie zur Klärung einiger Punkte, die in Artikel 13 enthalten sind, beispielsweise zum Begriff der elektronischen Post, der vorherigen Einwilligung des Teilnehmers, der

Direktwerbung, der Ausnahme von der Opt-in-Regelung und der Regelung für Nachrichten, die an juristische Personen gerichtet sind.

Arbeitspapier über vertrauenswürdige Rechnerplattformen und insbesondere die Tätigkeit der Trusted Computing Group (TCG)

In diesem Arbeitspapier werden aus der Sicht des Datenschutzes die Tätigkeiten der Trusted Computing Group bewertet, eines eigens zu diesem Zweck gebildeten Industriekonsortiums, das die Spezifikationen für eine neue Klasse von Hardwaresicherheitschips, die „Trusted Platform Modules" (TPM), entwirft. Neben der Betonung der Notwendigkeit, dass gewährleistet sein muss, dass die neuen Protokolle und Systeme von vornherein die Privatsphäre schützen und den Schutz der Privatsphäre verbessern müssen, enthält das Arbeitspapier einige Anregungen für die Tätigkeiten der TCG. Unter anderem empfiehlt die Datenschutzgruppe die Einrichtung einer Best-Practices-Group innerhalb der TCG, die sich mit den wichtigsten Datenschutzthemen befasst und Richtlinien und bewährte Vorgehensweisen hinsichtlich des Datenschutzes erarbeitet.

Stellungnahme Nr. 9/2004 zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten einschließlich Terrorismus.

Diese Stellungnahme prüft die Vereinbarkeit des vorgenannten Rahmenbeschlusses mit Artikel 8 der Europäischen Menschenrechtskonvention. Zu diesem Zweck prüft die Datenschutzgruppe, ob die Vorratsspeicherung im Rahmen dieses Entwurfs eines Rahmenbeschlusses mit den Kriterien hinsichtlich der Rechtsgültigkeit der Überwachung des Fernmeldeverkehrs, die aus Artikel 8 hervorgehen, übereinstimmt. Diese Kriterien besagen, dass Überwachungen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein müssen und einem in der Konvention aufgeführten legitimen Ziel dienen müssen. Die Datenschutzgruppe schließt daraus, dass die vorgeschriebene Aufbewahrung aller Daten über die Verwendung von öffentlichen Kommunikationsdiensten aus Gründen der öffentlichen Ordnung unter den Bedingungen des Rahmenbeschlusses nicht im rechtlichen Rahmen von Artikel 8 akzeptiert werden kann.

1.4. SCHENGEN/VISA/FREIER PERSONENVERKEHR

Die Datenschutzgruppe hat die Entwicklungen in diesem Bereich intensiv verfolgt und den Initiativen zur Vorbereitung der Annahme der Vorschläge der Gemeinschaft über die Einführung eines europäischen Visainformationssystems (VIS), eines neuen Schengen-Informationssystems (SIS II) und die Anforderungen für Pässe und Reisedokumente, die von den Mitgliedstaaten ausgestellt werden, besondere Aufmerksamkeit geschenkt.

Die eigens zu diesem Zweck zusammengestellte Arbeitsgruppe der Datenschutzgruppe für Recht, Inneres und Sicherheitsangelegenheiten hat sich mit diesen Themen befasst.

Stellungnahme Nr. 7/2004 zur Aufnahme biometrischer Merkmale in Visa und Aufenthaltstitel unter Berücksichtigung des Aufbaus des Visa-Informationssystems (VIS)

Diese am 11. August 2004 angenommene Stellungnahme wurde nach der Präsentation der Entwürfe der Europäischen Kommission für Verordnungen des Rates über eine einheitliche Visagestaltung und eine einheitliche Gestaltung von Aufenthaltstiteln für Drittstaatenangehörige veröffentlicht. Die Datenschutzgruppe hat ebenfalls die Arbeit und die Initiativen im Hinblick auf die Einrichtung eines europäischen Visainformationssystems (VIS) berücksichtigt.

In ihrer Stellungnahme betont die Datenschutzgruppe die Bedeutung der Aufrechterhaltung eines Gleichgewichtes zwischen den Anforderungen der öffentlichen Sicherheit einerseits und der Achtung der im Rechtssystem der Gemeinschaft und der einzelnen Mitgliedstaaten verankerten persönlichen Freiheiten und somit der Achtung vor den Grundsätzen des Schutzes persönlicher Daten andererseits.

Im ersten Abschnitt ihrer Stellungnahme bezieht sich die Datenschutzgruppe auf ihr Arbeitspapier über Biometrie (WP 80/2003) und betont, dass aufgrund der besonderen Natur der Biometrie die Beachtung der Grundsätze der Richtlinie 95/46/EG für die Aufnahme biometrischer Daten in Visa und Aufenthaltstitel und die diesbezügliche Verarbeitung persönlicher Daten erforderlich ist. Die Stellungnahme bekräftigt die Notwendigkeit einer eindeutigen Definition der Zwecke, für die die biometrischen Daten erhoben und weiterverarbeitet werden, sowie der Angemessenheit des Systems. Sie erinnert auch daran, dass alle entsprechenden Maßnahmen zur Ausschließung einer Zweckentfremdung der Daten ergriffen werden müssen.

Im zweiten Teil des Dokuments untersucht die Datenschutzgruppe die Fragen, die der Vorschlag der Kommission aus der Sicht des Schutzes persönlicher Daten aufgeworfen hat. Hierbei werden Fragen zum Zweck der vorgeschlagenen Maßnahmen und der Einführung eines VIS behandelt, beispielsweise über den Zeitraum der Aufbewahrung persönlicher Daten, über die Notwendigkeit der Übereinstimmung der Information der betroffenen Personen bei der Datenerhebung mit den Grundsätzen der Richtlinie 95/46/EG, über den Zugang von Drittländern zur VIS-Datenbank sowie über die Kompatibilität der einzelnen Systeme (VIS, SIS, EURODAC), um ihren Mehrwert zu erhöhen und Synergieeffekte zu erzielen. Die Datenschutzgruppe erklärt, dass die europäische Datenbank VIS der Kontrolle des Europäischen Datenschutzbeauftragten (EDPS) unterstellt werden sollte. Die nationalen Operationen sollten unter die Kontrolle der nationalen Datenschutzbehörden gestellt werden. Die diesbezügliche Kooperation zwischen dem EDPS und den nationalen Aufsichtsbehörden sollte so geregelt sein, dass eine einheitliche Anwendung der Datenschutzbestimmungen gewährleistet ist.

Normen für Sicherheitsmerkmale und Biometrie in den Pässen der EU-Bürger

Am 18. August 2004 richtete der Vorsitzende der Datenschutzgruppe ein Schreiben an den Europäischen Rat sowie den Präsidenten des Europäischen Parlamentes und den Präsidenten der Europäischen Kommission, in dem er über die Bedenken der Datenschutzgruppe hinsichtlich der vorgeschriebenen Aufnahme von zwei biometrischen Identifikationsmerkmalen in die Pässe der EU-Bürger berichtete, die im Vorschlag für eine Verordnung des Rates über die Normen für Sicherheitsmerkmale und Biometrie in den Pässen von EU-Bürgern, den die Kommission im Februar 2004 vorlegte, enthalten ist. Das Schreiben enthielt mehrere konkrete Vorschläge zum Text der Kommission. Die meisten Vorschläge wurden in die endgültige Fassung der Verordnung eingearbeitet, die vom Rat am 13. Dezember 2004 verabschiedet wurde.

Am 30. November 2004 richtete der Vorsitzende der Datenschutzgruppe ein zweites Schreiben an den Rat, den Ratspräsidenten und den Ausschuss des Europaparlamentes für bürgerliche Freiheiten, Justiz und Inneres (LIBE), um diese über die Vorbehalte der Datenschutzgruppe gegenüber der Aufnahme von Fingerabdrücken als zweites biometrisches Identifikationsmerkmal in den Pässen von EU-Bürgern, die in dem offiziell vom Rat verabschiedeten Text vorgesehen ist, zu informieren. Es wurde betont, dass die Aufnahme einer zusätzlichen biometrischen Information umso mehr die Einrichtung eines effizienten, sicheren und hieb- und stichfesten Systems zur Wahrung des Grundrechtes auf den Schutz der Privatsphäre erfordert.

1.5. GENETISCHE DATEN

Arbeitspapier über genetische Daten

Am 17. März 2004 verabschiedete die Datenschutzgruppe ein Arbeitspapier über die Verarbeitung genetischer Daten. Eine der wichtigsten Schlussfolgerungen lautet, dass jede Verwendung genetischer Daten zu anderen Zwecken als der direkten Sicherung der Gesundheit der betroffenen Person oder zu Forschungszwecken nationalen Regelwerken, die mit den Datenschutzgrundsätzen in der Richtlinie 95/46/EG übereinstimmen, unterworfen sein muss. Die Verarbeitung genetischer Daten sollte im Zusammenhang mit Arbeitsverhältnissen und Versicherungen ausschließlich in gesetzlich vorgeschriebenen strikten Ausnahmefällen zugelassen sein, zum Beispiel zum Schutz vor Diskriminierung aufgrund genetischer Daten. Die Datenschutzgruppe erklärte abschließend, sie könnte unter Umständen das Arbeitspapier im Lichte der Erkenntnisse der nationalen Datenschutzbehörden überarbeiten und zu einem späteren Zeitpunkt den Schwerpunkt auf spezifische Bereiche legen, um auf dem Stand der technologischen Entwicklungen und Fortschritte in der Verarbeitung genetischer Daten zu bleiben.

1.6. VIDEOÜBERWACHUNG

Stellungnahme Nr. 4/2004 zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung

Im Anschluss an die öffentliche Beratung, bei der die Datenschutzgruppe ihr Arbeitspapier über die Jahre 2002-2003 vorstellte (siehe Bericht 7, Punkt 1.3.7), gab die Datenschutzgruppe ihre offizielle Stellungnahme zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung ab (siehe WP 89).

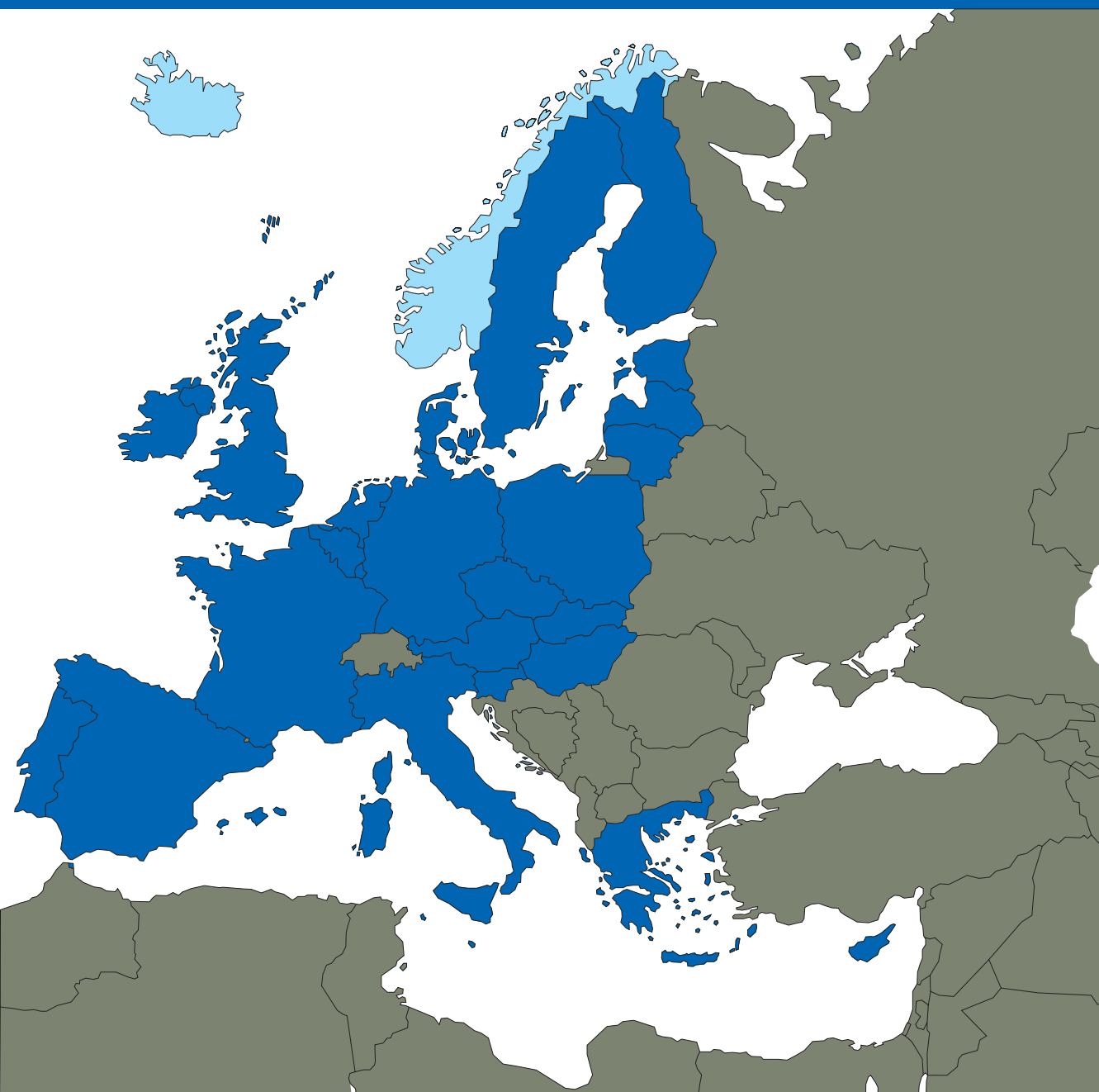
Die Datenschutzgruppe hält die Herausgabe dieser Stellungnahme für einen angemessenen Beitrag zur einheitlichen Ausführung der nationalen Maßnahmen im Rahmen der Richtlinie 95/46/EG über den Bereich der Videoüberwachung aufgrund der fortschreitenden Entwicklung der Videoüberwachungstechnik und deren Folgen für die Privatsphäre.

Die Datenschutzgruppe erinnert daran, dass mit Ausnahme der ausdrücklich in der Richtlinie 95/46/EG erwähnten Fälle (d.h. Datenverarbeitungen im Interesse der öffentlichen Sicherheit, Verteidigung, nationalen Sicherheit, mit Bezug auf das Strafrecht oder außerhalb des Geltungsbereichs des europäischen Rechtes, Datenverarbeitungen einer natürlichen Person für rein private Zwecke sowie Datenverarbeitungen zu rein journalistischen, literarischen oder künstlerischen Zwecken) die Verarbeitung personenbezogener Daten durch Videoüberwachungstechniken in den Geltungsbereich der Richtlinie 95/46/EG fällt und aus diesem Grunde die Prinzipien, die in dieser Richtlinie dargelegt werden, beachten muss, um ihre Rechtmäßigkeit zu erhalten.

Die Datenschutzgruppe weist auch darauf hin, dass die Mitgliedsstaaten unbedingt Richtlinien für die Tätigkeiten von Herstellern, Dienstleistern, Vertreibern und Wissenschaftlern im Hinblick auf die Entwicklung von Technologien, Software und technischen Systemen in Übereinstimmung mit den in diesem Papier erwähnten Grundsätzen herausgeben müssen.

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

■ Das Gerichtsorganisationsgesetz wurde geändert (vgl. Bundesgesetzblatt I, Nr. 128/2004). Hiermit wird ein spezielles Verfahren für die Erhebung von Beschwerden aufgrund der Verletzung von Datenschutzrechten durch Organe der Gerichtsbarkeit geschaffen. Das bedeutet, dass die österreichische Datenschutzkommission (DSK) den öffentlichen Sektor nur kontrollieren darf, wenn keine Organe der Gerichtsbarkeit (Gerichte) oder gesetzgebenden Organe (Parlament) davon betroffen sind.

■ Das Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (kurz: E-Government-Gesetz, E-Gov-G) wurde verabschiedet und trat am 01. März 2004 in Kraft (vgl. Bundesgesetzblatt I, Nr. 10/2004). Nach diesem Gesetz ist in Österreich die rechtserhebliche elektronische Kommunikation mit öffentlichen Stellen folgendermaßen geregelt:

➔ Im elektronischen Verkehr mit für die Datenverarbeitung Verantwortlichen des öffentlichen Bereichs darf Zugriff auf personenbezogene Daten nur dann gewährt werden, wenn die eindeutige Identität desjenigen, der Einsichtnahme begehrt, sowie die Berechtigung seines Ersuchens nachgewiesen sind. Zu diesem Zweck wurde die „Bürgerkarte" entwickelt, die als elektronischer Identitäts- und Authentizitätsnachweis im elektronischen Verkehr dient.

➔ Das wichtigste Datenschutzmerkmal dieses Systems besteht darin, dass die persönliche Stammzahl, die die elektronische Identität eines einzelnen Bürgers darstellt, Dritten nicht zugänglich ist. Die für die Datenverarbeitung Verantwortlichen des öffentlichen Bereichs können nur Identifikatoren speichern, die einseitige kryptographische Verschlüsselungen der (geheimen) Stammzahl darstellen und in den verschiedenen Bereichen der behördlichen Tätigkeiten unterschiedlich sind. Somit ist die Verknüpfung von Daten über eine betroffene Person aus mehreren Quellen mittels deren (individueller) Stammzahl nicht möglich. Die unbefugte Erhebung der Stammzahl wird zusätzlich dadurch verhindert, dass die Stammzahl nur auf der Bürgerkarte gespeichert ist, die sich im Besitz der betroffenen Person befindet. Beim Stammzahlenregister handelt es sich lediglich um ein virtuelles Register, das aus den (kryptographischen) Hilfsmitteln zur Generierung der Stammzahl im Moment der Einspeisung in die Bürgerkarte besteht. Die Stammzahl wird anschließend unmittelbar aus dem Register gelöscht.

B. Bedeutende Rechtsprechung

■ Das Finanzministerium hatte ein neues System zur elektronischen Überwachung der Arbeitszeit von Beschäftigten vorgestellt. Beginn und Ende der Arbeitszeit konnten nur durch Öffnen des Arbeitsplatzes im Büro in das elektronische System eingegeben werden. Der Öffnungszeitpunkt des Arbeitsplatzes diente der Glaubwürdigkeitskontrolle hinsichtlich Beginn und Ende der Arbeitszeit, die in das elektronische System eingegeben wurden.

Die DSK befand dieses System aufgrund seiner Unangemessenheit für unzulässig, denn es bestehen zahlreiche Gründe, aus denen ein Mitarbeiter seinen Arbeitstag nicht im Büro beginnen kann (z.B. Meetings außerhalb des Büros, Geschäftsreisen usw.), sodass dieses System als nicht für die zuverlässige Aufzeichnung von Arbeitszeiten geeignet betrachtet werden kann.

■ Ein Facharzt, der eine Person in behördlichem Auftrag untersuchte, hatte von den eventuellen Gebrechen der betreffenden Person, die deren

Fahrtüchtigkeit beeinträchtigten, erfahren und übermittelte diese Informationen an die Führerscheinbehörde. Nachdem die betroffene Person Beschwerde eingelegt hatte, befand die DSK, dass ein „vorrangiges rechtliches Interesse" nicht ohne eine spezifische gesetzliche Regelung, die dem Arzt die Weiterleitung dieser Informationen erlaubt, als gesetzliche Grundlage für die Übermittlung von Daten von einer öffentlichen Stelle zu einer anderen öffentlichen Stelle betrachtet werden könne. Aufgrund der eindeutig schwerwiegenden Gebrechen der betroffenen Person war die DSK im vorliegenden Fall jedoch der Ansicht, dass die Weiterleitung der Daten aufgrund „berechtigter Interessen der betroffenen Person", für die das Führen eines Fahrzeugs lebensgefährlich sein könne, rechtmäßig war. Die Verarbeitung vertraulicher Daten aufgrund berechtigter Interessen der betroffenen Person ist gemäß Artikel 8 Absatz 2 unter c der Richtlinie 95/46/EG (Artikel 9 Absatz 7 Datenschutzgesetz 2000) zulässig.

C. Wichtige spezifische Themen

■ In mehreren Fällen ersuchten betroffene Personen um ihre Löschung aus den Polizeiakten. Zum Zeitpunkt dieser Beschwerden wurden Polizeiakten auf lokaler Ebene in der Regel auf Papier und zusätzlich in Indexkarteien geführt. Die Polizei erklärte, die Dokumentation ihrer Arbeit nicht vollständig löschen zu können, da polizeiliche Ermittlungen aufgrund rechtsstaatlicher Prinzipien überprüfbar sein müssen. Die DSK befand, dass die zweckgebundene „Dokumentation" die (vollständige) Löschung von Aufzeichnungen innerhalb der in der nationalen Gesetzgebung vorgeschriebenen Aufbewahrungsfrist tatsächlich verbietet. Während dieser Frist müsse jedoch das Endergebnis der polizeilichen Ermittlungen festgehalten werden, um Fehlinformationen zu vermeiden. Ferner wurde befunden, dass Artikel 12 der Richtlinie 95/46/EG (Artikel 27 Datenschutzgesetz 2000) nicht greift, solange solche Informationen in Papierform vorliegen. Das Verwaltungsgericht war ebenfalls dieser Auffassung. Dieser Fall ist zurzeit beim Verfassungsgericht anhängig.

■ Die Ausübung des Zugriffsrechts auf Direktmarketingdaten war eines der häufigsten Probleme, die im Jahr 2004 Anlass für Beschwerden waren. Die Besonderheit von Direktmarketingdaten liegt darin, dass sie keinen Anspruch auf Richtigkeit der Informationen erheben, sondern vielmehr statistische Informationen über „mögliche Eigenschaften" einer Person (z.B. Einkommen, Zielgruppe, Zusammensetzung des Haushaltes usw.) enthalten.

■ Außerdem beruhen die Schlussfolgerungen aus den von den Marketingunternehmen gesammelten Daten häufig auf statistischen oder mathematischen Modellen, die das besondere Know-how des Direktmarketingunternehmens darstellen. Eine Pflicht zur Offenlegung dieser Daten im Rahmen eines Zugangsbegehrens kann im Sinne einer gerechten Abwägung zwischen Datenschutzrechten und Geschäftsgeheimnissen problematisch sein.

■ Bezüglich der internationalen Datenströme erteilte die DSK einem auf dem Balkan tätigen Bankenkonzern eine Genehmigung. Diese Genehmigung wurde aufgrund der unilateralen Erklärung der Konzernmitglieder zur Einhaltung einiger Datenschutzvorschriften erteilt, die in diesem Fall keinen besonderen Verhaltenscodex darstellen, da sich der Konzern zur Erfüllung der (nicht verfahrensrechtlichen) Bestimmungen des österreichischen Datenschutzgesetzes 2000 verpflichtete. (Der Fall ist auf der Website der DSK (www.dsk.gv.at) dokumentiert.)

■ Die DSK hat sich oft mit dem Problem der Mobilfunkbetreiber, die die Bonität potentieller Kunden vor einem Vertragsabschluss prüfen, befasst. Da Mobilfunkbetreiber erst bezahlt werden, nachdem sie ihre Dienstleistung erbracht

haben, muss ihr Bedarf an Kenntnissen über die Bonität potentieller Kunden als vorrangiges rechtliches Interesse und demzufolge als zulässig betrachtet werden. Weil Daten über die Bonität nicht gespeichert, aber bei der Entscheidung für oder gegen einen Vertragsabschluss berücksichtigt werden, kann eine betroffene Person falsche Informationen über ihre Bonität nur schwer berichtigen. Das Zugriffsrecht auf Daten gilt anscheinend nicht für Informationen über die Herkunft von Daten, weshalb es nicht immer möglich ist, die Herkunft falscher Bonitätsinformationen und den/die Verantwortliche/n, gegen den/die das Recht zur Datenberichtigung ausgeübt werden soll, zu ermitteln.

- Großes öffentliches Interesse galt einem neuen Register über den Bildungsstand der österreichischen Wohnbevölkerung. Das Register dient ausschließlich statistischen Zwecken, weshalb die Daten (gemäß der europäischen Richtlinie für statistische Erhebungen) 60 Jahre lang gespeichert werden. Solange eine Person eine Schule oder Universität besucht, werden diese Daten auch zu administrativen Zwecken von der Schulbehörde benutzt. Um die datenschutzrechtlichen Bedenken eines derartigen Registers, in dem die gesamte Bevölkerung enthalten ist, auszuräumen, wurde ein spezielles Verschlüsselungssystem (ohne Namensspeicherung!) entwickelt, das auf der Sozialversicherungsnummer der betroffenen Personen basiert. Dies hatte viele Befürchtungen und mehrere Beschwerden bei der DSK zur Folge. Die DSK leitete ein Untersuchungsverfahren ein, das noch nicht vollständig abgeschlossen ist. Mögliche Lösungen sind die Anpassung der Datenverwaltung des Registers an das neue Identifizierungssystem im Rahmen des E-Government-Gesetzes und die Verwendung spezieller Bildungsevidenzkennzahlen (BEKZ) anstelle der leicht zugänglichen Sozialversicherungsnummern.

- Die DSK wurde auch darauf aufmerksam gemacht, dass in der Veröffentlichung eines Urteils des Obersten Gerichtshofs die Identität einer beteiligten Person nicht korrekt unkenntlich gemacht wurde. Obwohl die DSK nicht zur Kontrolle der Organe der Gerichtsbarkeit befugt ist, konnte die Angelegenheit zur vollen Zufriedenheit der betroffenen Person gelöst werden.

Belgien

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

Richtlinie 95/46/EG
Keine Entwicklung

Richtlinie 2002/58/EG
Die belgische Datenschutzkommission wurde beim Entwurf des Gesetzes zur Umsetzung der Richtlinie 2002/58/EG hinzugezogen. (Das Gesetz wurde letztlich am 13. Juni 2005 verabschiedet).

Die Datenschutzkommission gab am 14. Juni 2004 eine Stellungnahme ab, in der Folgendes hervorgehoben wird:

- Eine allgemeine Verpflichtung zur vorrangigen Speicherung aller Verkehrsdaten, wie dies im Gesetzentwurf vorgesehen ist, würde im Widerspruch zu den Datenschutzgrundsätzen stehen, die bei mehreren Gelegenheiten von der Datenschutzkommission, der Art. 29 Datenschutzgruppe, in internationalen Dokumenten und in der Rechtsprechung des Europäischen Gerichtshofes für die Menschenrechte bestätigt wurden.

- Der Gesetzentwurf umfasst ein Verbot des Einsatzes technischer Mittel, die die Rückverfolgung von Anrufen oder das Abhören von Gesprächen verhindern, es sei denn, sie dienen der Gewährleistung der Vertraulichkeit von Mitteilungen oder der Sicherheit von Zahlungen. Die Kommission brachte ihre Besorgnis darüber zum Ausdruck, dass dadurch die Möglichkeiten der anonymen Verwendung von Telekommunikationsmitteln eingeschränkt oder vollständig aufgehoben werden.

Ferner fehlt im Gesetzentwurf die Umsetzung von Artikel 13 der Richtlinie 2002/58/EG über unerbetene Nachrichten, weil man davon ausgeht, dass dieser Artikel bereits im Gesetz vom 11. März 2003 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft umgesetzt wurde. Die Datenschutzkommission hat jedoch betont, dass dieses Gesetz dem Verbraucherschutz dienen sollte, weshalb sich sein Anwendungsbereich geringfügig von dem der Richtlinie unterscheidet. Das Gesetz gilt für Werbenachrichten und nicht für das Direktmarketing und deckt daher politische oder gemeinnützige E-Mails nicht ab. Dies gilt auch für Fax und automatische Anrufsysteme. Die Datenschutzkommission ersuchte um eine offizielle Klärung dieser Punkte unter Berücksichtigung des Anwendungsbereiches der Richtlinie 2002/58/EG.

B. Bedeutende Rechtsprechung

Ein Rechtsstreit über die Möglichkeit, Arbeitnehmer ohne deren Wissen mit einer Kamera aufzunehmen, gelangte unlängst zu einem kontroversen Ende. Der Streit begann im Jahr 2004 mit einem Urteil des Berufungsgerichts in Brüssel vom 24. November 2004, das am 02. März 2005 vom obersten Zivilgericht (Kassationshof) aufgehoben wurde. Das letztere Urteil besagt, dass ein Arbeitgeber unter der Hand gemachte Aufnahmen eines Mitarbeiters beim Diebstahl von Geld vor Gericht verwenden darf (Frage der Übereinstimmung mit der Informationsverpflichtung gegenüber Mitarbeitern).

Dieses Urteil warf zwei Fragen auf:

- Zum einen die Frage nach der Tragweite des Datenschutzgesetzes, denn der Richter urteilte, dass in diesem Fall das Datenschutzgesetz nicht greift (das gemeinsame Abkommen über die Videoüberwachung von Arbeitnehmern jedoch seine Gültigkeit behält), weil nicht der Mitarbeiter das Objekt der Überwachung sei, sondern die Registrierkasse. Es ist diesbezüglich fraglich, ob tatsächlich eine Überwachung der Registrierkasse oder eine Überwachung des Mitarbeiters beabsichtigt wurde, um dessen Fehlverhalten zu beweisen.

■ Zum anderen stellt sich die Frage nach der Gültigkeit von Beweismitteln (Bilder), die widerrechtlich aufgenommen wurden, und deren Berücksichtigung in einem Gerichtsverfahren. Hierbei geht es auch um die Frage der Rechtssicherheit, wenn ein Richter je nach den vorhandenen Interessen entscheiden kann, welche Beweismittel gültig sind.

C. Wichtige spezifische Themen

Datenschutz und Transparenz im Falle offizieller Dokumente

Die Datenschutzkommission erhält zunehmend Fragen in Bezug auf die Ausgewogenheit zwischen der Transparenz und der Vertraulichkeit offizieller Dokumente. Es wurde betont, dass offizielle Dokumente, die personenbezogene Daten beinhalten, nicht ohne vorherige Unkenntlichmachung der Daten weitergeleitet werden dürfen. Wenn die betreffende Person aufgrund der Art des Dokuments noch stets erkennbar ist, muss vor der Übermittlung der Daten an Dritte die Zustimmung der betreffenden Person eingeholt werden. Die Kommission bestand auf diesen Bedingungen, insbesondere hinsichtlich des Zugriffs und der Weiterverarbeitung der Daten zu Direktmarketingzwecken durch Dritte.

Die Bemühungen Belgiens um einen neuen Cybersicherheitsplan mit einer verbesserten Integration nationaler, kultureller und rechtlicher (auch datenschutzrechtlicher) Erfordernisse

Die Datenschutzkommission beschloss bereits im Jahre 2003, die belgische Informationssicherheitsbranche und die belgischen Universitäten zusammenzubringen, damit diese gemeinsam Grundanforderungen eines neuen Cybersicherheitsplanes mit einer verbesserten Integration der nationalen, kulturellen und rechtlichen (auch datenschutzrechtlichen) Erfordernisse erarbeiten sollten. Es fanden einige erfolgreiche Sitzungen statt. Ferner richtete die Datenschutzkommission ein Schreiben mit ihren Anliegen an die belgischen Universitäten. Anfang 2005 wurde eine Sonderarbeitsgruppe innerhalb der Datenschutzkommission eingerichtet, die die nächsten Schritte festlegen soll. Diese Arbeitsgruppe konzentriert sich zurzeit vor allem auf die Ausarbeitung von Sicherheitsrichtlinien.

Bekämpfung von E-Müll (Spam)

Im Streben nach einem kohärenten Ansatz bei der Umsetzung des Gesetzes über unerbetene Nachrichten vom 11. März 2003 finden auf nationaler Ebene Koordinationssitzungen zwischen der Datenschutzkommission, dem Wirtschaftsministerium und anderen zuständigen Gremien statt. Das Ziel ist die effizienteste Behandlung und/oder Weiterleitung von Beschwerden entsprechend ihrem Inhalt (Betrug, widerrechtliche Datensammlung usw.).

Die Ergebnisse der „Spam box"-Praxis, die seit dem Jahr 2002 von der Datenschutzkommission durchgeführt wird, motivierte das Wirtschaftsministerium zur aktiven Teilnahme am Projekt in Rücksprache mit der Datenschutzkommission.

Zypern

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

Das Gesetz über die Verarbeitung personenbezogener Daten (Schutz der Privatsphäre) trat im November 2001 in Kraft. Die Einführung des Gesetzes erfolgte im Zuge des Vereinheitlichungsprozesses, vor allem vor dem Hintergrund der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Zugleich ratifizierte das zypriotische Parlament die Konvention des Europarates über den Schutz von natürlichen Personen bei der automatisierten Verarbeitung personenbezogener Daten, die am 01. Juni 2002 in Kraft trat.

Das Gesetz über die Regulierung der elektronischen Kommunikationen und der Postdienstleistungen trat in Zypern 2004 in Kraft. Es setzte unter anderem die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation um. Laut den Bestimmungen in Artikel 107 wurden die Verantwortungsbereiche des Datenschutzbeauftragten erweitert, und zwar auf den Teil des Gesetzes, der die Vertraulichkeit von Mitteilungen, Verkehrs- und Ortungsdaten, Telefonbücher und unerbetene Nachrichten umfasst.

B. Bedeutende Rechtsprechung

E-Müll (Spam)

E-Müll (Spam, Junkmail) und andere unerbetene kommerzielle Nachrichten haben in Zypern im letzten Jahr erheblich zugenommen. Die zypriotische Datenschutzbehörde erhält jeden Monat zahlreiche telefonische Beschwerden, meist über unerbetene kommerzielle Nachrichten per SMS.

Das Gesetz über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation sieht vor, dass die Benutzung automatischer Anrufsysteme, von Faxgeräten oder elektronischer Post zu Direktmarketingzwecken nur erlaubt ist, wenn der Teilnehmer vorher seine diesbezügliche Zustimmung erteilt hat (Opt-in).

Die einzige Ausnahme, bei der Opt-outs verwendet werden dürfen, liegt vor, wenn eine natürliche Person oder ein Unternehmen beziehungsweise eine Institution die elektronischen Kontaktdaten oder E-Mail-Adressen seiner/ihrer Kunden im Rahmen eines Verkaufs oder für die direkte Vermarktung ihrer Produkte verwenden.

Die Ermittlungen im Rahmen dieser Beschwerden stellen aufgrund verfassungsrechtlicher und anderer rechtlicher Bestimmungen in Bezug auf das Recht jeder Person auf Achtung und Vertraulichkeit ihrer Kommunikation hin und wieder ein Problem dar.

Der Datenschutzbeauftragte führt derzeit Gespräche mit den Internet Service Providern (ISP), die sich zur Ermittlung von Spamversendern verpflichten und Letztere darauf aufmerksam machen, dass bei einer Fortsetzung ihrer illegalen Tätigkeiten die ISP-Dienstleistungen gesperrt werden.

Die zypriotische Börse

Anfang 2004 gingen zahlreiche Beschwerden bezüglich einer angeblichen Bekanntgabe personenbezogener Daten seitens der zypriotischen Börse (CSE) ein. Es wurde behauptet, dass die CSE personenbezogene Daten aus Börsentransaktionen im Zeitraum 1999 bis 2000 den Einkommenssteuerbehörden mitgeteilt habe.

Bei den Ermittlungen stellte sich heraus, dass der Ermittlungsausschuss, der mit der Prüfung der Transaktionen in den Jahren 1999 bis 2000 beauftragt worden war, Daten an den Ministerrat weitergeleitet

hatte. Der Ministerrat leitete aufgrund einer Empfehlung des Justizministers die betreffenden Informationen an das Finanzamt weiter.

Nach einer Prüfung des Auftrags des Ermittlungsausschusses und der Stellungnahme des Justizministers erklärte der Datenschutzbeauftragte, dass der Ministerrat nicht zu einer Weiterleitung von Informationen an das Finanzamt befugt sei, es sei denn, die betroffene Person habe gegen das Einkommenssteuerrecht verstoßen.

Den Beschwerdeführern wurde mitgeteilt, dass sie gegen Steuerforderungen seitens des Finanzamts, die auf Daten basieren, die widerrechtlich erhoben oder verarbeitet wurden, Widerspruch einlegen können.

C. Wichtige spezifische Themen

Öffentliches Bewusstsein

Abgesehen von Erklärungen in den Medien über Angelegenheiten, die derzeit von Interesse sind, fand im Jahr 2004 ein Seminar über das Gesetz über die Verarbeitung von Daten und die Verpflichtungen der für die Datenverarbeitung Verantwortlichen statt, das für den Verband der Gemeinden (Union of Municipalities) und die Steuerberatervereinigung (Association of Accountants) veranstaltet wurde.

Im selben Jahr wurden die Richtlinien für die Verwendung von Internet und Videoüberwachung verabschiedet und auf die Website der zypriotischen Datenschutzbehörde (nur in griechischer Sprache) www.dataprotection.gov.cy gestellt.

Ferner erschienen im selben Jahr die englische Fassung des Datenschutzgesetzes und Teil 14 des Gesetzes über die elektronische Kommunikation, das die Bestimmungen der Richtlinie 2002/58/EG in der nationalen Gesetzgebung umsetzt, auf der Website.

Zukünftig werden auch weitere Informationen in englischer Sprache auf der Website zu finden sein.

Meldepflicht

Anfang 2004 wurden drei Stadtverwaltungen zu Ordnungsstrafen verurteilt, weil sie es unterlassen hatten, dem Datenschutzbeauftragen über ihre Datenverarbeitung/ihr Registrierungssystem Auskunft zu geben.

Kommunikation

Es gingen eine große Zahl von telefonischen Anfragen von Unternehmen, für die Datenverarbeitung Zuständigen und Bürgern über die Verarbeitung personenbezogener Daten sowie Beschwerden ein. Hinsichtlich der Anfragen bot man den für die Datenverarbeitung Zuständigen Hilfe bei der Erfüllung der gesetzlichen Bestimmungen an. Hinsichtlich der Beschwerden wurden die Bürger gebeten, ihre Beschwerden schriftlich einzureichen, um die Ermittlungsarbeiten zu erleichtern.

Prüfungen und Felduntersuchungen

Im Jahr 2004 wurden fünf Prüfungen durchgeführt. Bei vier Prüfungen handelte es sich um Routineuntersuchungen, eine Prüfung fand im Rahmen der Ermittlungen in Bezug auf eine Beschwerde statt.

Die Routineuntersuchungen fanden in drei behördlichen Abteilungen, einer Auskunftei und einer Handelsgesellschaft statt.

Tschechische Republik

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

Das neue, moderne Gesetz Nr. 101/2000 Slg. über den Schutz personenbezogener Daten und über die Änderung einiger Gesetze (nachfolgend „Gesetz 101" genannt), in dem die Richtlinie 95/46/EG fast vollständig umgesetzt wird, trat am 01. Juni 2000 in Kraft. In diesem Gesetz wurden ebenfalls die Voraussetzungen für die Errichtung einer tschechischen Datenschutzbehörde mit allen erforderlichen Vollmachten und Funktionen einer unabhängigen Aufsichtsbehörde geschaffen. Dennoch waren einige Anpassungen erforderlich und wurde die hundertprozentige Erfüllung der Richtlinie erst im Jahr 2004 erreicht, in dem das Gesetz 101 mit dem Gesetz Nr. 439/2004 Slg. novelliert wurde.

Der Tschechischen Republik gelang eine komplette Umsetzung der Richtlinie 2002/58/EG im Jahr 2004 nicht. Es wurden lediglich einige Klauseln über unerbetene Nachrichten im Gesetz Nr. 480/2004 Slg. über einige Dienstleistungen der Informationsgesellschaft, das am 07. September 2004 in Kraft trat, umgesetzt. Das Gesetz gab der Datenschutzbehörde mehr Befugnisse bei der Bekämpfung unerbetener kommerzieller Nachrichten, einschließlich der Ermächtigung zur direkten Bestrafung. Die Umsetzung des restlichen Großteils der Richtlinie sowie mehrerer anderer Richtlinien aus dem „neuen Telekommunikationspaket" wurde mit der Vorbereitung eines neuen Gesetzes über die elektronische Kommunikation eingeleitet. Nach einigen Anfangsschwierigkeiten trat das Gesetz Nr. 127/2005 Slg. über die elektronische Kommunikation am 01. Mai 2005 in Kraft.

Im Jahr 2004 wurde die Behörde in Übereinstimmung mit der Änderung des Gesetzes Nr. 133/2000 Slg. über die Erfassung der Einwohner und die Geburtsnummer und über die Änderung einiger Gesetze (Gesetz Nr. 53/2004 Slg. über die Änderung einiger Gesetze über das Bevölkerungsregister) mit weit reichenden Befugnissen ausgestattet, unter anderem bezüglich der unerlaubten Verwaltung und Verwendung von Geburtsnummern.

B. Bedeutende Rechtsprechung

Die Datenschutzbehörde ist befugt, Urteile über Nachbesserungen und/oder Strafen zu begutachten, und zwar unbeschadet des Rechts aller Bürger, ein Verfahren direkt vor Gericht anhängig zu machen oder Berufung gegen ein Urteil der Datenschutzbehörde einzulegen.

Mehrere Gerichtsverfahren, in denen die Datenschutzbehörde Verfahrenspartei war, wurden im Laufe des Jahres abgeschlossen. Kein Gerichtsbeschluss fiel zu Ungunsten der Behörde aus – zum Beispiel in der Verfassungsklage des tschechischen Statistikamtes gegen die Datenschutzbehörde im Jahre 2002, in der es um die Untersagung der Verarbeitung bestimmter personenbezogener Daten, die während der Volkszählung zusammengetragen wurden, ging. Das Verfassungsgericht wies die Klage ab und untersagte dem Statistikamt die Verwendung bestimmter Volkszählungsdaten. Diese Daten sind nunmehr permanent gesperrt.

Drei Beschlüsse der Datenschutzbehörde über die Verhängung einer Strafe wurden Gegenstand eines Ordnungsstrafverfahrens. Zwei Klagen wurden bereits von einem Senat des Amtsgerichts in Prag zugunsten der Datenschutzbehörde abgewiesen. Das Gericht fand keine Fehler im Verfahren der Datenschutzbehörde bei der Verhängung von Strafen und bestätigte die rechtliche Argumentation der Datenschutzbehörde.

C. Wichtige spezifische Themen

Einige spezifische Themen boten der Datenschutzbehörde im Jahr 2004 besonderen Anlass zur Besorgnis über die Gefahr einer Verletzung der Privatsphäre im Hinblick auf den Schutz personenbezogener Daten, beispielsweise:

- elektronische Kommunikation und Telekommunikation (Abhörungen, Aufbewahrung von Daten, unerbetene kommerzielle Nachrichten),
- Videoüberwachungssysteme (Überwachungskameras),
- Kataster und andere öffentlich zugängliche Register,
- neue Technologien - RFID, biometrische Daten,
- Gesundheits- und Sozialsysteme

Im Jahr 2004 machte die Datenschutzbehörde 35 Verfahren anhängig, die mit Ordnungsstrafen endeten.

In den beiden nachfolgenden Verfahren wurde das höchstzulässige Strafmaß verhängt:

■ **Arbeitsvermittlung:** Eine Arbeitsvermittlung wurde zu einer Ordnungsstrafe in Höhe von 500.000 tschechischen Kronen (CZK) (rund 17.000 EUR) verurteilt, weil sie die ihr verfügbaren sensiblen personenbezogenen Daten von Arbeitssuchenden ohne die vorhergehende ausdrückliche Zustimmung der Arbeitssuchenden verarbeitet hatte, und zwar ohne dabei zu gewährleisten, dass die Rechte der betroffenen Personen und insbesondere das Recht auf Menschenwürde nicht verletzt werden. Ferner arbeitete die Arbeitsvermittlung ohne Sicherheitsmaßnahmen für die Datenverarbeitung. Das Ordnungsstrafverfahren gegen diese Arbeitsvermittlung wurde aufgrund der Tatsache anhängig gemacht, dass neben städtischen Abfalleimern Dokumente gefunden wurden, die personenbezogene Daten von Arbeitssuchenden enthielten. Diese schriftlichen Dokumente enthielten eine Vielzahl personenbezogener Daten von Arbeitssuchenden, unter anderem sensible Daten über den Gesundheitszustand, eventuelle Vorstrafen und die Staatsangehörigkeit der Arbeitssuchenden, sowie schriftliche medizinische Gutachten und Beurteilungen der Arbeitssuchenden durch die Mitarbeiter der Arbeitsvermittlung, die verschiedene subjektive, beleidigende und unhaltbare Bemerkungen beinhalteten.

Das Verfahren wurde schließlich mit der Ablehnung einer Klageschrift gegen diese Ordnungsstrafen beendet.

■ **Bank:** Eine Bank sammelte und verarbeitete als für die Verarbeitung personenbezogener Daten Verantwortliche im Rahmen einer Kundenwerbungskampagne personenbezogene Daten potentieller Kunden, und zwar unter Missachtung ihrer Verpflichtung, die betroffenen Personen darüber zu unterrichten. Ferner war die Bank hinsichtlich einiger personenbezogener Daten nicht in der Lage, die Zustimmung der betroffenen Personen zur Verarbeitung dieser personenbezogenen Daten zu beweisen. Anhand von Stichproben fand die Datenschutzbehörde heraus, dass die Bankangestellten personenbezogene Daten von Bekannten oder Geschäftspartnern sammeln mussten. Hierfür erhielten die Angestellten eine nicht-geldwerte Belohnung, wobei diesbezüglich zu wenig aktive Mitarbeiter zur Erfüllung dieser Aufgabe angehalten und in einigen Fällen sogar bedroht wurden. Die Bank wurde aufgrund der vorgenannten Verletzung ihrer Verpflichtungen gemäß dem Datenschutzgesetz zu einer Ordnungsstrafe in Höhe von 485.000 tschechischen Kronen (CZK) (rund 16.000 Euro) verurteilt.

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 01. Juli 2000 in Kraft. Die englische Fassung des Gesetzes finden Sie unter http://www.datatilsynet.dk/eng/index.html.

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

Die Richtlinie 2002/58/EG wurde ins nationale dänische Recht übertragen durch:
- die dänische Verfassung;
- das Gesetz über die Marketingpraktiken, Absatz 6a (vgl. Gesetz Nr. 450 vom 10. Juni 2003);
- das Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten;
- das Gesetz über die Wettbewerbsbedingungen und den Verbraucherschutz auf dem Telekommunikationsmarkt (vgl. Durchführungsverordnung Nr. 661 vom 10. Juli 2003), Artikel 34;
- die Durchführungsverordnung Nr. 666 vom 10. Juli 2003 über die Bereitstellung elektronischer Kommunikationsnetze und Dienstleistungen;
- Kapitel 71 des Gesetzes über die Rechtspflege, vgl. Durchführungsverordnung Nr. 777 vom 16. September 2002;
- Artikel 263 des Strafgesetzbuches, vgl. Durchführungsverordnung Nr. 779 vom 16. September 2002.

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

■ Im Jahr 2004 konzentrierte sich die Behörde insbesondere auf die bevorstehende Reform des öffentlichen Sektors. Die Datenschutzbehörde trug unter anderem zu mehreren Gesetzesinitiativen bei – 29 von 226 neuen Gesetzentwürfen, die der Behörde vorgelegt wurden, beziehen sich auf diese Reform.

Ein Bestandteil der bevorstehenden Reform ist die Einrichtung neuer Bürgerbüros, die den Bürgern einen direkteren Zugang zu den lokalen Behörden verschaffen sollen. Diesbezüglich bemerkte die Datenschutzbehörde, dass vor der Einrichtung dieser Büros unter anderem geklärt werden muss, welche Stelle die Daten verwaltet und auf welche Art und Weise die erforderlichen Sicherheitsvorkehrungen gemäß den Grundsätzen aus Artikel 17 der Richtlinie 95/46/EG gewährleistet werden. Außerdem wies die Behörde darauf hin, dass die Mitarbeiter, die die personenbezogenen Daten bearbeiten, hinsichtlich der Datenschutzstandards ausreichend geschult sein müssen.

■ Die Behörde wurde um ihre Stellungnahme zu den Änderungsvorschlägen zum Gesetz über eine zentrale DNA-Datenbank gebeten. Durch diese Änderung sollte die Möglichkeit der Nutzung der DNA-Datenbank im Rahmen von Verbrechensermittlungen erweitert werden.

Die Datenschutzbehörde war unter anderem der Ansicht, dass eine solche Erweiterung eine Lockerung der ursprünglich für die Datenbank festgelegten Erfassungskriterien darstellen würde und die Erhebung einer weitaus größeren Menge

biologischer Daten zur Folge hätte. Vor diesem Hintergrund zweifelte die Datenschutzbehörde an der Verhältnismäßigkeit zwischen der Zielsetzung der Gesetzesänderung einerseits und der zu erhebenden Menge biologischer Daten und deren Aufbewahrungsfrist andererseits.

■ Die Behörde wurde auch um eine Stellungnahme zu einem Gesetzentwurf ersucht, in dem öffentliche und private Institutionen ein so genanntes „Child Certificate" beantragen müssen, bevor sie eine Person mit der Betreuung von Kindern unter 15 Jahren beauftragen. Diese Zertifikate beinhalten Informationen darüber, ob die betroffene Person in der Vergangenheit aufgrund sexueller Vergehen an Kindern verurteilt wurde.

■ Die Datenschutzbehörde merkte dazu an, dass die Erstellung eines solchen Zertifikats nur mit der vorherigen schriftlichen Zustimmung der betroffenen Person möglich sein dürfe.

Die Datenschutzbehörde war aufgrund der Grundsätze des Datenschutzes und des Schutzes der Privatsphäre besorgt, dass auf diese Art und Weise Informationen über schwerwiegende Verbrechen einer großen Zahl privater Organisationen zugänglich werden können und dass die betreffenden Zertifikate ohne eine individuelle Prüfung der Notwendigkeit beantragt werden. Die Datenschutzbehörde stellte auch die Frage nach der Verpflichtung zur Meldung bei der Behörde gemäß Artikel 18 bis 20 der Richtlinie 95/46/EG.

Grundsätzlich war die Datenschutzbehörde der Ansicht, dass eine allgemeine Verpflichtung zur Beschaffung dieser Zertifikate für eine derart große Zahl von Personen nur dann in Kraft treten dürfe, wenn damit nachweislich maßgeblichen öffentlichen Interessen gedient wäre.

B. Bedeutende Rechtsprechung

■ Im Jahr 2004 urteilte die Datenschutzbehörde, dass die Überprüfung der Bonität aller Mitarbeiter über 18 Jahre durch eine große Supermarktkette einige datenschutzrechtliche Fragen aufwirft. Die Datenschutzbehörde war der Ansicht, dass Artikel 5 Absatz 1 bis 3 (Umsetzung von Artikel 6 der Richtlinie 95/46/EG) der Beschaffung von Informationen über die Bonität von Arbeitnehmern gewisse Grenzen setzt. Die Datenschutzbehörde urteilte deshalb, dass infolge des Inkrafttretens des dänischen Gesetzes über die Verarbeitung personenbezogener Daten Kreditinformationen nur über Mitarbeiter mit einer besonderen Vertrauensposition beschafft werden dürfen. In diesem Zusammenhang urteilte die Datenschutzbehörde, dass beispielsweise Positionen von eher praktischer Natur nicht als besondere Vertrauenspositionen betrachtet werden können.

■ Im Zusammenhang mit einer Beschwerde in Bezug auf das Recht auf Zugriff auf personenbezogene Daten erklärte die Datenschutzbehörde, dass die Verarbeitung und Aufbewahrung von Verkehrsdaten aus einem Internetchat nur mit der ausdrücklichen Zustimmung der betroffenen Person erfolgen dürften. Ferner urteilte die Behörde, dass eine Aufbewahrungsfrist für diese Daten bis zu einem Jahr gerechtfertigt ist, wenn die Verarbeitung der Daten der Gewährleistung der Sicherheit der Website dient und die Polizei bei der Ermittlung unsittlichen Verhaltens gegenüber Kindern unterstützt.

■ Die Datenschutzbehörde nahm auch Stellung zur Erhebung von Daten im Rahmen des amerikanischen Sarbanes Oxley Act, laut dem Wirtschaftsprüfer bei der Aufsichtsbehörde PCAOB (Public Company Accounting Oversight Board) registriert sein müssen. Die Informationen werden auf der PCAOB-Website veröffentlicht. Die Erhebung basiert auf der Zustimmung der betroffenen Person.

Die Datenschutzbehörde war der Ansicht, dass die Erhebung die allgemeinen Grundsätze gemäß Artikel 5 des Gesetzes über die Datenverarbeitung (Umsetzung von Artikel 6 der Richtlinie 95/46/EG) nicht erfüllt und dass die Zustimmung der betroffenen Person zu unspezifisch und aufgrund einer unzureichenden Unterrichtung im Sinne von Artikel 3 Absatz 8 des Gesetzes über die Verarbeitung personenbezogener Daten erteilt werde.

Die Datenschutzbehörde konnte die erforderliche Verhältnismäßigkeit zwischen der Menge der erhobenen Daten und dem Zweck der Registrierung bei der PCAOB auch angesichts der Tatsache, dass die Informationen auf der Website der PCAOB veröffentlicht werden, nicht feststellen.

C. Wichtige spezifische Themen

Im Jahr 2004 konzentrierte sich die Datenschutzbehörde auf so genannte Headhunter, nachdem über die Medien bekannt geworden war, dass viele dieser Unternehmen nicht über die erforderliche Genehmigung der Datenschutzbehörde verfügen.

Die Datenschutzbehörde nahm Kontakt zu rund 300 Unternehmen auf, erklärte diesen Unternehmen in Kürze die Grundsätze des Gesetzes über die Verarbeitung personenbezogener Daten und verlangte, dass diese Unternehmen gegebenenfalls eine Genehmigung beantragen.

Das Ergebnis waren fast 250 Anträge bis Ende 2004. Neben der Vergabe von Genehmigungen stellte die Datenschutzbehörde den betreffenden Unternehmen mehrere Informationsquellen über das Gesetz über die Verarbeitung personenbezogener Daten zur Verfügung und stellte insbesondere die Regeln für die Zustimmung der betroffenen Person und die Aufbewahrungsfrist der Daten in den Mittelpunkt.

Die Datenschutzbehörde ist der Ansicht, dass die geringe Zahl der Anträge in diesem Bereich auf Unkenntnis in Bezug auf den Datenschutz zurückzuführen ist. Deshalb ist das Ziel ihrer Bemühungen, die Industrie auf diese Regeln aufmerksam zu machen. Ein positiver Nebeneffekt dieser Bemühungen ist die zunehmende Zahl der Anträge aus ähnlichen Sektoren, beispielsweise Zeitarbeitsfirmen.

Estland

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

Im vergangenen Jahr blieb die neue Fassung des Datenschutzgesetzes (PDPA)[2] unverändert, jedoch plant die estnische Regierung Änderungen am PDPA und hat die Arbeitsgruppe bereits aufgestellt.

Im August 2004 erließ die Regierung neue Sicherheitsvorschriften für Informationssysteme.[3]

Die Verordnung umfasst nützliche Informations- und anschließende Sicherheitssysteme für die Pflege von Datenbanken staatlicher und kommunaler Behörden. Das Sicherheitssystem besteht aus der Festlegung spezifischer Sicherheitsanforderungen und der Beschreibung der organisatorischen, materiellen und informationstechnologischen Datenschutzmaßnahmen. Die Verordnung umfasst die Beschreibung der Sicherheitskategorien und –ebenen. Die Sicherheitskategorien bestehen aus vier Komponenten: zeitkritische Aspekte, Schwere der Verzugsfolgen, Integrität und Vertraulichkeit.

B. Bedeutende Rechtsprechung

Im Jahr 2004 war die estnische Datenschutzbehörde an zwei Verfahren beteiligt, die letztlich vor dem Obersten Gerichtshof verhandelt wurden. Beide bezogen sich auf den Zugriff auf öffentliche Informationen. Am ersten Verfahren waren die Datenschutzbehörde und die estnische Steuer- und Zollbehörde beteiligt. Es behandelte das Dokumentenregister dieser Behörde und die Zugriffsbeschränkung.[4] Der Oberste Gerichtshof bestätigte die vorhergehenden Urteile des Verwaltungsgerichts und des Berufungsgerichts. Dem Gerichtshof zufolge fällt die Beschwerde der Steuer- und Zollbehörde nicht in den Zuständigkeitsbereich des Verwaltungsgerichtes. Deshalb wurde der Beschluss der Datenschutzbehörde, dass die Zugriffsbeschränkung rechtswidrig sei, von den Gerichten nicht berücksichtigt. Im November 2004 erhielt die Zugriffsbeschränkung durch eine Änderung der Steuergesetze gesetzlichen Charakter.[5]

Am zweiten Verfahren waren die Datenschutzbehörde und eine natürliche Person beteiligt.[6] Es handelte sich um eine Beschwerde der natürlichen Person über den Berufungsbeschluss der Datenschutzbehörde. Laut diesem Beschluss hat die natürliche Person (die Mitglied eines Stadtrates war) kein Recht, Informationen über die Gehälter der Angestellten in städtischen Einrichtungen einzuziehen, weil diese keine Beamten sind. Das Oberste Gericht urteilte, dass die natürliche Person in ihrer Eigenschaft als Stadtratsmitglied Informationen zu erhalten wünschte und es sich deshalb nicht um einen Antrag im Rahmen des Gesetzes über die Meldepflicht öffentlicher Einrichtungen handelte.[7] Der Oberste Gerichtshof hob die vorherigen Urteile des Verwaltungsgerichts und des Berufungsgerichts auf und schloss das Verfahren, weil die Angestellten in städtischen Einrichtungen keine Beamten und ihre Gehälter nicht öffentlich sind. Das Urteil der Datenschutzbehörde wurde bekräftigt.

[2] Datenschutzgesetz: http://www.legaltext.ee/text/en/X70030.htm
[3] RTI 26.08.2004.63.443 : https://www.riigiteataja.ee/ert/act.jsp?id=791875
[4] Oberster Gerichtshof, 3-3-1-38-04: http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-38-04.html
[5] Änderung der Steuergesetze: https://www.riigiteataja.ee/ert/act.jsp?id=901885
[6] Oberster Gerichtshof, 3-3-1-55-04: http://www.nc.ee/klr/lahendid/tekst/RK/3-3-1-55-04.html
[7] Gesetz über die Auskunftspflicht öffentlicher Einrichtungen: http://www.legaltext.ee/text/en/X40095K2.htm

C. Wichtige spezifische Themen

Das herausragende Thema des letzten Jahres war das Problem der Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken.

Die jüngste Fassung des estnischen Datenschutzgesetzes trat im Oktober 2003 in Kraft. Laut diesem Gesetz ist die Zustimmung der betreffenden Person zur Verarbeitung ihrer Daten für wissenschaftliche, historische und statistische Untersuchungen erforderlich. Außerdem muss die Verarbeitung sensibler Daten bei der Datenschutzbehörde gemeldet werden. Dies setzt die Anwendung erforderlicher Sicherheitsmaßnahmen voraus, was zu einem Streit zwischen der Datenschutzbehörde und der Wissenschaft führte.

Die Gegenpartei argumentiert, dass Datenschutzbehörde und Datenschutzgesetz die Verarbeitung personenbezogener Daten grundlos behindern. Für die Datenschutzbehörde liegt das größte Problem im fehlenden Problembewusstsein bei der Verarbeitung personenbezogener Daten (die Gegenpartei setzt sich nicht mit den Gründen für die Beschränkung bei der Verarbeitung sensibler Daten auseinander). Weitere Gründe sind fehlende Ressourcen, fehlende IT-Kenntnisse und fehlende Kenntnis der Menschenrechte sowie die Starrheit gegenüber den Veränderungen innerhalb der Informationsgesellschaft.

Zurzeit wird eine Arbeitsgruppe eingerichtet, um Lösungen zu finden.

Finnland

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

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

Die Richtlinie des Europäischen Parlamentes und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) wurde in Finnland mit dem Datenschutzgesetz (523/1999), das am 01. Juni 1999 in Kraft trat, umgesetzt. Das Gesetz wurde am 01. Dezember 2000 überarbeitet, als Bestimmungen zum Entscheidungsfindungsprozess der Kommission und zur Verbindlichkeit der Entscheidungen bei der Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union im Rahmen der Datenschutzrichtlinie in das Gesetz aufgenommen wurden.

Der Schutz der Privatsphäre ist seit dem 01. August 1995 in Finnland ein Grundrecht. Gemäß der finnischen Verfassung wird der Schutz personenbezogener Daten durch ein separates Gesetz geregelt.

Die Umsetzung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation

Das Gesetz über den Datenschutz in der elektronischen Kommunikation (516/2004), das am 01. September 2004 in Kraft trat, setzte die Datenschutzrichtlinie für die elektronische Kommunikation (2002/58/EG) um. Zweck dieses Gesetzes ist die Gewährleistung der Vertraulichkeit und der Schutz der Privatsphäre in der elektronischen Kommunikation, die Verbesserung der Verkehrssicherheit in der elektronischen Kommunikation sowie die ausgewogene Entwicklung der elektronischen Kommunikationsdienste.

Die Verantwortung für die Durchsetzung des Gesetzes ist geteilt, sodass der Auftrag des Büros des Datenschutzbeauftragten folgende Aufgaben umfasst:

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

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

Die wichtigsten Entwicklungen in Bezug auf:

■ gesetzgebende Maßnahmen unter der ersten Säule

Das Gesetz über den Schutz der Privatsphäre im Berufsleben (759/2004) trat am 01. Oktober 2005 in Kraft. Das neue Gesetz trat an die Stelle der einschlägigen früheren Gesetzgebung. Das neue Gesetz beinhaltet Vorschriften zum Recht des Arbeitgebers zur Verarbeitung der Ergebnisse von Drogentests, zur Organisation der Videoüberwachung am Arbeitsplatz und zur Zusammenarbeit von Arbeitnehmern und Arbeitgebern im Bereich der Verarbeitung personenbezogener Daten.

Das neue Ausländergesetz (301/2004) trat am 01. September 2004 in Kraft. Zweck dieses Gesetzes sind die Einführung und Förderung einer verantwortungsbewussten Regierungsführung und des Rechtsschutzes in Ausländerfragen. Darüber hinaus soll das Gesetz die legale Einwanderung fördern und den internationalen Schutz der Menschenrechte und der Grundrechte sowie

der für Finnland verbindlichen internationalen Abkommen gewährleisten beziehungsweise verbessern. Das Gesetz regelt die Ermittlung von Verwandtschaftsverhältnissen mithilfe der DNS-Analyse. Die Verarbeitung personenbezogener Daten in der Ausländerbehörde wird im Gesetz über die Registrierung von Ausländern (1270/1997), das mit Einführung des neuen Ausländergesetzes überarbeitet wurde, geregelt. Das Gesetz über die Registrierung von Ausländern enthält spezielle Regeln für die Verarbeitung personenbezogener Daten bei der Ausländerbehörde.

Das Statistikgesetz (280/2004) trat am 01. Juli 2004 in Kraft. Das Gesetz beschreibt die Methoden und Prinzipien der Datenerfassung, der Statistikplanung und die geltenden Methoden für die Erstellung von Statistiken auf behördlicher Seite sowie die Verpflichtung zur Meldung von Datenerfassungen. Das Gesetz behandelt weiterhin die Vertraulichkeit und Veröffentlichung von und Meldepflicht über zu statistischen Zwecken gesammelten Daten und die Verwendung dieser Daten. Das Gesetz definiert ferner das Recht des finnischen Statistikamtes, vertrauliche und sensible personenbezogene Daten auf der Grundlage der Unterrichtung der Betroffenen zusammenzutragen. Das Gesetz ermächtigt das Statistikamt zur Übermittlung personenbezogener Daten an bestimmte Stellen in sehr wenigen, eindeutig definierten Situationen. Das finnische Statistikamt ist die vorrangig für die Führung nationaler Statistiken verantwortliche Behörde.

- Änderungen unter der zweiten und dritten Säule: Keine nennenswerten Änderungen

B. Bedeutende Rechtsprechung

Der Datenschutzbeauftragte wurde ersucht, die personenbezogenen Daten bestimmter Personen von den Websites verschiedener Stellen entfernen zu lassen. Die Meinung hierzu war, dass diese Themen vornehmlich auf der gesetzlichen Grundlage der Meinungsfreiheit und des Strafgesetzbuches behandelt werden sollten. Letztendlich ist der Schutz der Privatsphäre in diesen Fällen durch die Bestimmungen über Verstöße gegen die Privatsphäre, die öffentliche Ordnung und den Leumund gewährleistet, deren bewertung der Polizei und den Gerichten obliegt. Allgemein hat sich der Datenschutzbeauftragte regelmäßig mit Fragen der Veröffentlichung personenbezogener Daten über das Internet befasst. Im Zusammenhang mit der Tsunamikatastrophe in Asien wurde ein Bericht über die Nutzung des Internets zur Bereitstellung von Informationen in Krisenfällen, zum Beispiel durch die Veröffentlichung der Namen von Katastrophenopfern im Internet, in Auftrag gegeben.

Nach dem Gesetz über den Datenschutz bei der elektronischen Kommunikation erfordert das elektronische Direktmarketing grundsätzlich die vorhergehende Zustimmung des Empfängers der Marketingsendungen. Diese Zustimmung ist hingegen nicht notwendig, wenn der Dienstleistungsanbieter oder Produktverkäufer die Kundenkontaktinformationen per E-Mail, SMS, Voicemail oder Multimedia-Messaging im Zusammenhang mit dem Verkauf eines Produktes oder einer Dienstleistung erhält und wenn derselbe Dienstleistungsanbieter oder Produktverkäufer diese Kontaktinformationen für die direkte Vermarktung seiner Produkte oder Leistungen verwendet, die mit dem erworbenen Produkt oder Service verknüpft sind oder diesem ähneln. Der Datenschutzbeauftragte wurde bei mehreren Gelegenheiten um eine Stellungnahme zum elektronischen Direktmarketing ersucht.

Die Ähnlichkeit von oder die Verbindung mit per SMS angebotenen Produkten und Leistungen mit früher gelieferten Produkten und Leistungen ist nach dem Inhalt des Dienstes oder dem Zweck des Produktes und nicht nach dem zum Kauf oder zur Lieferung des Produktes oder Dienstes verwendeten Gerät oder System zu beurteilen. Wenn beispielsweise eine natürliche Person eine Nutzleistung per SMS erworben hat, ist die Vermarktung von Unterhaltungsdiensten per SMS bei dieser Person unzulässig. Soweit die Möglichkeit des Direktmarketings bei einer natürlichen

Person ohne deren vorhergehende Zustimmung besteht, hat der Dienstleistungsanbieter oder der Produktverkäufer dem Kunden die Möglichkeit zu gewährleisten, ohne weitere Probleme und Kosten die Verwendung seiner Kontaktinformationen in Verbindung mit Datenerhebungen und mit jeder E-Mail, SMS, Voice Mail oder Multimedia-Nachricht zu untersagen. Diese Möglichkeit muss dem Kunden eindeutig mitgeteilt werden.

Fragen zu den verschiedenen biometrischen Identifizierungssystemen wurden ebenfalls zunehmend erörtert. Vor dem Hintergrund der Einführung des biometrischen Passes bereitet Finnland eine Änderung des Ausweis- und Passrechtes vor, in der die Verarbeitung biometrischer Identifizierungsdaten gesondert behandelt wird.

C. Wichtige spezifische Themen

Viele Datenschutzfragen hatten ihren Ursprung im veränderten Tätigkeitsfeld, in der rasanten technologischen Entwicklung, im breiten Umfang der Tätigkeiten und deren Herausforderungen für die Regulierung und die Überwachung der Datenverarbeitung. Auslagerungen, vernetztes Arbeiten, die unterschiedlichen Formen des E-Business, Service- und Callcenter führen dazu, dass die Akteure und der Datenschutzbeauftragte vor immer größere Herausforderungen bei der Identifizierung der für die Verarbeitung von Daten verantwortlichen Stellen und der Aufgaben der Akteure, die an der Datenverarbeitung beteiligt sind, gestellt werden. Gleichzeitig haben die betroffenen Personen immer größere Schwierigkeiten, sich ein genaues Bild solcher Aktivitäten zu machen.

Diese Entwicklungen stellen neue Herausforderungen für das Büro des Datenschutzbeauftragten dar, weil es immer schwieriger wird, die Anwendungsmöglichkeiten der Datenschutzgesetze in den betreffenden Fällen herauszufinden. Was die Sache noch komplizierter macht, ist die Tatsache, dass in vielen Fällen ein Teil der betreffenden Dienstleistungen außerhalb Finnlands, manchmal sogar außerhalb der EU, generiert wird.

Ein Beispiel für die sich verändernden Dienstleistungsketten ist der Ortungsdatenservice. Bei diesen Leistungen werden die Daten, die den Standort eines vom Bediener gesteuerten Endgerätes angeben, zur Erbringung mehrerer mehrwertschöpfender Leistungen verwendet. Dies erfordert – mit Zustimmung der betroffenen Person – die Übermittlung von Ortungsdaten an einen anderen Dienstleister.

Laut dem Datenschutzgesetz ist der Staatsanwalt zur Rücksprache mit dem Datenschutzbeauftragten verpflichtet, bevor er Anklage im Fall einer Verletzung des Datenschutzgesetzes erhebt. Die Zahl dieser Rücksprachen ist erheblich angestiegen, und zwar aus den nachfolgenden Gründen:

- Die Bürger (die betroffenen Personen) sind sich ihrer Datenschutzrechte stärker bewusst.
- Stärkeres Bewusstsein für die Bedeutung des Datenschutzes.
- Bessere technische Standards in der Datensicherheit von Datenverarbeitungssystemen, die die Erfolgsquote bei der Verbrechensbekämpfung erhöhten.
- Öffentlichkeitsgrad, den die landesweit einschlägigen Strafsachen in Bezug auf die Vertraulichkeit von Mitteilungen in den letzten Jahren erreicht haben.

Das öffentliche Bewusstsein für den Datenschutz scheint stärker zu werden. Der Datenschutzbeauftragte beabsichtigt, diese Entwicklung im Rahmen seines Auftrages durch die Unterstützung der für die Datenverarbeitung Verantwortlichen und durch eine noch bessere Unterrichtung der betroffenen Personen zu unterstützen.

Im Jahr 2004 führte das Büro des Datenschutzbeauftragten zum dritten Mal das Projekt „Internetpolizei" durch. Eine der Hauptzielgruppen dieses Projektes sind Websites, die Dienstleistungen anbieten, bei denen davon ausgegangen werden muss, dass sie besonders

sensible Daten enthalten, und deren Betreiber. Dank dieses Projektes konnten einige Broschüren überarbeitet und aktualisieret werden. Das Projekt machte den Serviceprovidern die Wichtigkeit der Unterrichtung der betroffenen Personen gemäß den Bestimmungen des Datenschutzgesetzes deutlich.

Im Jahr 2004 wurden die ersten Folgen schädlicher Programme (z.B. Cabir), die sich auf mobilen Plattformen ausbreiten, entdeckt. Der Datenschutzbeauftragte hat auch die Aufgabe, Richtlinien zur Datensicherheit herauszugeben. Er erfüllte diese Aufgabe in Zusammenarbeit mit den Hauptverantwortlichen für Datensicherheit.

Der Datenschutzbeauftragte ist Mitglied einer Arbeitsgruppe des Lenkungsausschusses für die Datensicherheit bei staatlichen Behörden (VAHTI), der dem Finanzministerium untersteht. Die Arbeitsgruppe bereitete das Entwicklungsprogramm vor, das Anfang des Jahres genehmigt wurde. Vertreter des Büros des Datenschutzbeauftragten beteiligten sich an mehreren Projekten im Rahmen dieses Entwicklungsprogramms. Das National Data Security Advisory Board, ein weiteres wichtiges Forum für den Datenschutz in Finnland, setzte seine Arbeit unter der Aufsicht des Verkehrsministeriums fort. Der Datenschutzbeauftragte ist Mitglied dieses Beratungsgremiums. Das Beratungsgremium zeichnet sich durch die Teilnahme zahlreicher Vertreter aus der Wirtschaft aus. Eine der wichtigsten Errungenschaften des Beratungsgremiums, die landesweit und international starke Beachtung fand, war der nationale Informationssicherheitstag (National Information Security Day).

Ein Hinweis auf die zunehmende Bedeutung des Datenschutzes im Rahmen der polizeilichen Tätigkeiten ist die Arbeit von Herrn Jaakko Jonkka, einem Ein-Mann-Komitee, der vom Innenministerium ernannt wurde. In seinem Bericht über die Effizienz des Leistungsrichtliniensystems der Polizei und die Kontrolle der Rechtmäßigkeit bei der Polizei weist Jonkka darauf hin, dass der Datenschutz und die Sicherheit der Datenregister, zu denen die Polizei Zugang hat, besondere Aufmerksamkeit erfordern. Die Überwachung der Benutzung dieser Register, die Verhinderung ihres Missbrauchs sowie die Probleme infolge der gemeinsamen Nutzung der Register bei der Zusammenarbeit der Behörden sind Themen, die in diesem Bericht zur Sprache kommen. Jonkka schlägt weiterhin vor, dass die Polizei den Posten eines Datenschutzmanagers oder –überwachers schaffen sollte, der entweder direkt dem nationalen Polizeibeauftragten oder der Abteilung unterstellt ist, die die Rechtmäßigkeit kontrolliert.

Von besonderer Bedeutung ist die Tatsache, dass in Finnland Datenschutz sehr umfassend verstanden wird. Beim Datenschutz geht es dort nicht nur um Technologie, sondern auch um Ausbildung, Management und das Gewinnen des Kundenvertrauens mittels guter und sicherer Dienstleistungen und andere „sanfte" Ansätze. In Finnland hat man verstanden, dass sich der Status des Bürgers vom Subjekt zum Kunden gewandelt hat und dass die Öffentlichkeit gelernt hat, ein sicheres Tätigkeitsumfeld zu verlangen, und dass diese Entwicklung durch den breiten Einsatz vieler Methoden und Verfahren, die die Informationsgesellschaft, die Technik und die Rechtsprechung zu bieten haben, beurteilt und unterstützt werden muss.

Einer der Hauptentwicklungsbereiche im Jahr 2004 war die Aktualisierung unserer Website. Informationen sollten leichter zugänglich gemacht und aktuellere und interaktive Informationen geliefert werden. Es wurde auch das verfügbare Informationsvolumen über Einzelfälle und internationale Themen erweitert. Im Zuge dieser Entwicklungsarbeit wurde im Frühjahr 2004 eine Umfrage unter den Benutzern durchgeführt. Es nahmen insgesamt 350 Personen teil. Zu den Wünschen gehörten einfachere Suchmöglichkeiten, praktische Anleitungen und eine bessere Struktur der Website. Die neue Website wurde am 07. September 2004 ins Netz gestellt. Die Besucherzahl ist auch ein nützlicher Indikator bei der Beurteilung der Effizienz unserer Tätigkeiten und des Bewusstseins bezüglich des Datenschutzes.

Frankreich

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

Das Gesetz vom 06. August 2004 zur Umsetzung der Richtlinie 95/46/EG

Das französische Parlament übertrug die Richtlinie 95/46/EG vom 24. Oktober 1995 durch das lang erwartete Gesetz vom 06. August 2004 in die nationale Gesetzgebung. Das Gesetz über „Informatik und persönliche Freiheit" (Loi Informatique et Libertés) vom 06. Januar 1978 sollte zwar beibehalten, jedoch grundlegend novelliert werden. Die Gundsätze des Datenschutzes blieben erhalten, es wurden jedoch maßgebliche Änderungen an den Bestimmungen des Gesetzes vom 06. Januar 1978 über die Struktur und Philosophie des Datenschutzes (Umfang, Ernennung eines Datenschutzbeauftragten, neue Befugnisse der Datenschutzkommission CNIL) vorgenommen.

Zunächst wurden die formalen Verfahren, die vor der automatischen Datenverarbeitung durchlaufen werden müssen, grundlegend geändert.

Eine neue Klausel im neuen französischen Datenschutzgesetz, mit der die Auskunftspflicht privater und öffentlicher Einrichtungen gelockert wird, wenn diese einen Datenschutzbeauftragten ernennen, der den Titel „Beauftragter für Informatik und persönliche Freiheit" tragen könnte, stellt eine erste maßgebliche Änderung dar. Der Status und die Aufgaben des Beauftragten werden in einer Durchführungsverordnung festgelegt. Die CNIL leistete einen eigenen Beitrag zu den laufenden Diskussionen über die genaue Funktion dieses Beauftragten.

Generell sieht das Gesetz zahlreiche Bestimmungen für die Vereinfachung der Formalitäten vor, die vor der Datenverarbeitung erfüllt werden müssen und die im vergangenen Jahr umfassend von der CNIL angewandt wurden.

Zugleich wurden die Vorabkontrollen für die verschiedenen Arten der Datenverarbeitung erweitert. Einige dieser festgeschriebenen Kontrollen beziehen sich auf die Vorabkontrolle durch die CNIL (Stellungnahme oder Genehmigung), beispielsweise:

- Die Verarbeitung sensibler Daten, die schnell anonymisiert werden müssen, oder eine Verarbeitung, die aufgrund des öffentlichen Interesses gerechtfertigt ist.
- Die Verarbeitung genetischer Daten in bestimmten Fällen.
- Die Verarbeitung von Daten über Rechtsverletzungen, Gerichtsurteile oder Sicherheitsvorkehrungen durch Verwertungsgesellschaften zur Bekämpfung des widerrechtlichen Herunterladens von Dateien aus dem Internet.
- Die Verarbeitung von Daten, die aufgrund ihrer Natur, ihres Umfangs oder ihres Zwecks dazu führen könnte, dass natürliche Personen mangels gesetzlicher Regelungen auf Rechte, eine Zuwendung oder einen Vertragsabschluss verzichten.
- Die automatische Verarbeitung von Daten, die Einzelheiten über die sozialen Probleme von Einzelpersonen enthalten.
- Die Verarbeitung biometrischer Daten, die zur Identitätskontrolle usw. erforderlich sind.

Das Inkrafttreten des Gesetzes vom 06. August 2004 hatte ebenfalls Änderungen in den CNIL-Kontrollverfahren zur Folge. Die neue Kontrollstrategie der CNIL, die im März 2004 eingeführt wurde und sich durch den Wunsch nach der Erweiterung von Feldkontrollen zur intensiveren Kontrolle der Datenverarbeitung auszeichnet, griff den Veränderungen in der übrigen Kontrollgesetzgebung vor (weniger Vorabkontrollen, mehr Nachkontrollen). Die Kommission muss entscheiden, welche Tätigkeitsbereiche Feldkontrollen unterzogen werden, um

sicherzustellen, dass die Entscheidungen und Empfehlungen der CNIL erfüllt werden, um auf die zunehmende Besorgnis der Öffentlichkeit einzugehen und insbesondere, um die Anwendung von Sicherheitsmaßnahmen sicherzustellen, die die Vertraulichkeit der Daten gewährleisten sollen. Natürlich wird die CNIL weiterhin Kontrollen im Rahmen von Beschwerden, die natürliche Personen an sie richten, durchführen. Noch vor der Veröffentlichung der Durchführungsverordnung im November 2004 änderte die CNIL ihre Hausordnung, um Kontrollverfahren unter dem neuen Gesetz einzuführen, vor allem die Einführung von Berichten und die Bereitstellung von Informationen an die Staatsanwaltschaft, die für den betreffenden Gerichtsbezirk zuständig ist. Beide Maßnahmen sind in Artikel 44 des Gesetzes vorgesehen. Ferner sind laut Artikel 19 der Gesetzesnovelle bestimmte Kommissionsvertreter zur Durchführung von Kontrollen befugt.

Diese Kontrollpolitik wird zudem durch die neuen Befugnisse der CNIL zur Verhängung von Strafen unter dem neuen Gesetz unterstützt. Vor dem Inkrafttreten des neuen Gesetzes durfte die CNIL lediglich Verwarnungen gegen die betreffenden Unternehmen oder Einrichtungen aussprechen oder die Staatsanwaltschaft unterrichten. Das Gesetz vom 06. August 2004 verlieh der CNIL einschlägige Befugnisse, um Ordnungs- und Geldstrafen zu verhängen. Die Datenschutzkommission möchte alle Kontroll- und Zwangsmittel, die ihr zur Verfügung stehen, so schnell wie möglich zur effektiven Durchsetzung des Gesetzes einsetzen.

Es gibt eine Vielzahl von Zwangsmitteln und Strafmaßnahmen, nämlich Verwarnungen, Geldstrafen, ein Verbot der weiteren Verarbeitung von Daten und den Entzug von Zulassungen. Bei dringendem Handlungsbedarf kann die Kommission die einstweilige Unterbrechung der Datenverarbeitung oder eine (dreimonatige) Sperrung der Daten anordnen. Bestimmte Datenverarbeitungen der Regierung sind davon ausgenommen. Bei einer schwerwiegenden Verletzung von Rechten und Freiheiten kann der CNIL-Vorsitzende vor Gericht jede Sicherheitsmaßnahme zur Gewährleistung der betreffenden Rechte und Freiheiten beantragen. Bei Erstverstößen kann bei natürlichen Personen eine Geldstrafe in Höhe von € 150.000 und bei Unternehmen in Höhe von € 300.000 oder 5 % der Umsatzerlöse vor Steuern des Vorjahres, jedoch höchstens € 300.000, verhängt werden (Artikel 47 Absatz 2). Die Höhe dieser Geldstrafen muss „im Verhältnis zur Schwere der begangenen Straftaten und den Vorteilen, die aus diesen Straftaten gezogen wurden", stehen. Schließlich dürfen die Strafmaßnahmen gemäß Artikel 226 Absatz 16 und Artikel 226 Absatz 24 des Strafgesetzbuches nicht vergessen werden. Natürlich kann die CNIL die Staatsanwaltschaft über alle Verstöße gegen das Gesetz, über die die CNIL in Kenntnis gesetzt wird, unterrichten.

Die meisten Zwangsmittel werden nicht von der Vollversammlung der Kommission, sondern von einem sechsköpfigen Gremium festgelegt, das aus dem Vorsitzenden, zwei stellvertretenden Vorsitzenden und drei Mitgliedern, die von der Kommission für die Dauer ihres Mandates ernannt werden, besteht.

Umsetzung der Richtlinie 2002/58/EG

- *Gesetz vom 21. Juni 2004 über die digitale Wirtschaft*

Das Gesetz über das Vertrauen in die digitale Wirtschaft, das gewisse Bestimmungen der Richtlinie 2002/58/EG umsetzt, wurde am 21. Juni 2004 erlassen. Eine wichtige Neuerung im Rahmen des Gesetzes über die digitale Wirtschaft ist die erforderliche vorherige Zustimmung des Empfängers (Opt-in) zum Erhalt von kommerziellen Nachrichten per E-Mail, SMS (Short Message Service) oder MMS (Multimedia Messaging Services). Diese Zustimmung muss der Empfänger in vollkommener Kenntnis der Sachlage erteilen. So bedeutet zum Beispiel die Annahme der

allgemeinen Geschäftsbedingungen nicht, dass die betreffende Person auch dem Empfang kommerzieller Nachrichten zugestimmt hat. Darüber hinaus muss eine Person, die mit dem Empfang solcher Mitteilungen einverstanden ist, eindeutig über die Identität des Absenders informiert worden sein und die Möglichkeit haben, kommerzielle Nachrichten abzulehnen.

Wenn ein Unternehmen bereits Beziehungen zu einem Kunden unterhält, ist die vorhergehende Zustimmung des Kunden nicht erforderlich, wenn sich die vom Unternehmen versandten Nachrichten auf Produkte oder Leistungen beziehen, die den Produkten oder Leistungen, die der Kunde zuvor gekauft oder abonniert hat, ähnlich sind. Darüber hinaus muss der Kunde bei einer Bestellung die Möglichkeit haben, Werbematerial des Unternehmens kostenlos abzulehnen. Anlass zahlreicher Diskussionen im Jahr 2004 war die Frage, ob eine vorhergehende Zustimmung für den Versand kommerzieller Nachrichten zwischen Unternehmen erforderlich ist. Obwohl nicht bestritten wird, dass die geschäftliche E-Mail-Adresse von Mitarbeitern eines Unternehmens zu den personenbezogenen Daten zählt, wenn eine natürliche Person über diese Adresse identifiziert werden kann, ersuchten die Unternehmen um eine flexiblere Anwendung des Gesetzes im Geschäftsleben. Anfang des Jahres 2005 urteilte die CNIL, dass kommerzielle Nachrichten an die geschäftliche E-Mail-Adresse natürlicher Personen ohne deren vorhergehende Zustimmung versandt werden dürfen, wenn die Sendung im Zusammenhang mit ihrer Funktion im Unternehmen oder in der öffentlichen Einrichtung, das/die ihnen die E-Mail-Adresse zugeteilt hat, steht.

- *Gesetz vom 09. Juli 2004 über die elektronische Kommunikation*

Ein Erlass vom 01. August 2003 regelt die Rechte natürlicher Personen gegenüber allgemeinen Verzeichnis- oder Informationsdiensten, lässt jedoch eine Reihe von Fragen offen, unter anderem den Fall der Mobiltelefonabonnements. Die CNIL befand, dass allgemeine Verzeichnisse ausschließlich die Daten der Mobiltelefonabonnenten enthalten dürfen, die ausdrücklich um ihre Eintragung ins Verzeichnis gebeten haben. Bisher galt das Prinzip, dass natürliche Personen in die Verzeichnisse eingetragen werden, wenn sie eine Eintragung nicht ausdrücklich ablehnen. Nachdem die betreffenden Dienste ihre diesbezügliche Politik geändert hatten, ratifizierte das Gesetz vom 09. Juli 2004 über die elektronische Kommunikation einen Standpunkt, der sich dem Wunsch der CNIL nach einem System der vorhergehenden Zustimmung durch die Mobiltelefonabonnenten anschließt. Das Gesetz über die Postdienste und die elektronische Kommunikation wird durch einen neuen Erlass entsprechend angepasst, der weitere Angleichungen, die von einer von der CNIL eigens zu diesem Zweck eingerichteten Arbeitsgruppe ausgearbeitet wurden, beinhalten muss. Der neue Erlass, der im Jahre 2005 veröffentlicht werden soll, enthält die nachfolgenden Bestimmungen: Telefongesellschaften müssen ihre Abonnenten über deren Recht informieren, in einem (Mobiltelefonnummern-) Verzeichnis aufgeführt zu werden bzw. die Eintragung in ein (Festnetznummern-) Verzeichnis oder die Eintragung ihrer vollständigen Adresse abzulehnen, vom Vornamen nur den Anfangsbuchstaben eintragen zu lassen, sofern es keine Homonyme gibt, den Erhalt von Direktmarketing abzulehnen und die Möglichkeit ihrer Identifizierung durch eine Suche auf Telefonnummernbasis (umgekehrte Suche) auszuschließen. Auf Wunsch müssen die Abonnenten Daten über andere Benutzer ihrer Leitung und deren Beruf eintragen lassen können. Die Abonnenten haben die Möglichkeit, ihre Wünsche bis zu sechs Monaten nach ihrer Unterrichtung durch den Betreiber zu äußern. Die ersten allgemeinen Verzeichnisse werden Ende 2005 erscheinen.

Weitere Entwicklungen in der Gesetzgebung

- *Bekämpfung von Diskriminierung*

Die Bekämpfung von Diskriminierung aufgrund der ethnischen Herkunft, der Staatsangehörigkeit oder der Konfession war 2004 ein zentrales Thema. Eine Reihe von Berichten und Studien haben zur Diskussion über die Mittel und Wege zur Gewährleistung des Grundrechtes auf Gleichbehandlung aller Personen beim Zugang zum Arbeitsmarkt oder zu einer bestimmten beruflichen Funktion, zum Wohnungsmarkt oder bestimmten Dienstleistungen beigetragen. Die nationale Antidiskriminierungs- und Gleichheitsbehörde (HALDE), die per Gesetz vom 30. Dezember 2004 gegründet wurde, ist der eindeutige Beweis für den Wunsch der Behörden, in diesem Bereich tätig zu werden. Angesichts der Komplexität der Fragen bezüglich der Identität von Personen und der Achtung ihrer Rechte beschloss die CNIL im Rahmen ihrer Befugnisse einen Beitrag zur derzeitigen landesweiten Debatte über die Einsetzung einer Arbeitsgruppe zu leisten, die die Datenverarbeitung im Lichte der Staatsangehörigkeit oder ethnischen Herkunft untersuchen wird.

- *Automatische Erfassung von Triebtätern (FIJAIS)*

Die Artikel 706-53-1 bis 706-53-12 des Strafgesetzbuches, die in das Gesetzbuch durch eine Gesetzesänderung vom 09. März 2004 eingebracht wurden, legen die Bedingungen für die automatische oder auf ausdrücklichen Beschluss einer Behörde angeordnete Erfassung von bestimmten Triebtätern fest. Laut diesen Bestimmungen müssen Personen, die im FIJAIS registriert sind, jährlich einen Wohnsitznachweis vorlegen und jede Adressenänderung binnen zwei Wochen melden. Gefährliche Straftäter müssen ihren Wohnsitz alle sechs Monate melden oder bestätigen. Die Registrierung von Straftätern und die daran geknüpfte Verpflichtung zur Adressangabe dient dem doppelten Ziel dieser Erfassung, das im Gesetz dargelegt wird, nämlich erstens der Vorbeugung gegen Wiederholungstaten vorbestrafter Täter und zweitens der einfacheren Ermittlung dieser Täter.

- *Testverfahren mit biometrischen Visa in Frankreich*

Das Gesetz vom 26. November 2003 über die Einwanderung enthält Bestimmungen über die Aufzeichnung, Speicherung und Verarbeitung von Fingerabdrücken und Fotos nicht nur von – wie früher der Fall – Antragstellern von Aufenthaltsgenehmigungen und Ausländern in einer irregulären Situation, sondern auch von Visum-Antragstellern. Im Rahmen dieser Gesetze informierte das Innenministerium die Kommission von einem Erlassentwurf des Staatsrates, der probeweise für einen Zeitraum von zwei Jahren die Einrichtung einer Datenbank mit Fingerabdrücken und digitalen Aufnahmen von Visum-Antragstellern bei sieben Konsulaten sowie bei einigen Konsulaten die Erfassung dieser biometrischen Daten in einem elektronischen Chip im ausgestellten Visum erlaubt.

Die CNIL wurde über diesen Erlassentwurf informiert und gab ihre Stellungnahme über das Testverfahren am 05. Oktober 2004 ab. Während die Fingerabdruckspeicherung auf einem Visumchip keine grundsätzlichen Schwierigkeiten darstellt, sofern die entsprechenden Schutzmaßnahmen getroffen werden, äußerte die CNIL eine Reihe erheblicher Vorbehalte und Einwände zu den Bedingungen, unter denen das Experiment stattfinden sollte, insbesondere zur Einrichtung einer zentralen Datenbank.

Die Durchführungsverordnung übernimmt nur einige Anmerkungen und Empfehlungen der CNIL. Die Zielsetzungen des Experimentes wurden dargelegt und die Maßnahmen werden beurteilt. Die verarbeiteten Informationen werden nach Abschluss des Experimentes nicht aufbewahrt, wenn entschieden wird, dass die Maßnahmen nicht fortgeführt werden. Die Maßnahmen im Rahmen des Experimentes basieren jedoch

auf einer zentralen Datenbank, in der die Fingerabdrücke aller Visum-Antragsteller, gleich ob sie ein Visum erhalten oder nicht, gespeichert sind. Die Kommission ist der Ansicht, dass das Risiko besteht, dass Ausländer, deren Visumanträge abgelehnt wurden, stigmatisiert werden, obwohl die Ablehnung eines Antrages ein normales behördliches Verfahren ist, das nicht notgedrungen dem Ausgang eines neuen Antrages vorgreift und der abgelehnte Antragsteller folglich nicht verdächtig ist.

- *Personenbezogene medizinische Aufzeichnungen*

Das Gesetz vom 13. August 2004 über das Gesundheitswesen sieht die Erfassung personenbezogener medizinischer Aufzeichnungen vor. Die CNIL wurde von der Regierung um ihre Stellungnahme zum Gesetzentwurf gebeten und legte nach einer Debatte am 10. Juni 2004 ihren Standpunkt dar.

Laut diesem Gesetz müssen personenbezogene medizinische Aufzeichnungen entsprechend dem Arztgeheimnis aufbewahrt werden. Sie enthalten sämtliche gesammelten oder generierten Daten bezüglich der Vorsorge, Diagnose und Behandlung, vor allem Daten, die für die Überwachung medizinischer Leistungen notwendig sind. Der Zugang zu den Aufzeichnungen wird überwacht. Das Gesetz verbietet jede Vermarktung medizinischer Daten.

B. Bedeutende Rechtsprechung

Die rechtliche Nachfassung der Spam-Box-Initiative

Im Oktober 2002 informierte die CNIL nach ihrer „Spam-Box-Initiative" die Staatsanwaltschaft über fünf Firmen, die unerbetene Massen-E-Mails zu Werbezwecken (Spamming) verschickten. Im Urteil vom 18. Mai 2005 verurteilte das Berufungsgericht in Paris ein Unternehmen, das E-Mail-Adressen von öffentlichen Internetseiten sammelte, zu einer Geldstrafe von € 3.000, weil es personenbezogene Daten widerrechtlich oder auf unlautere Weise erworben hatte.

Ein Wendepunkt: die Verurteilung eines französischen Spammers

Am 05. Mai 2004 verurteilte das Handelsgericht in Paris ein französisches Unternehmen wegen Spamming nach einer gemeinsamen Klage von Microsoft, dem Betreiber des kostenlosen E-Mail-Service „Hotmail", und des Internetproviders AOL France. Sie beschuldigten das betreffende Unternehmen, ihre Dienstleistungen für den Versand einer Million unerbetener Fußballwerbemails über mehrere ihrer Webseiten missbraucht zu haben.

Der Richter verurteilte das Unternehmen zu Schadensersatzzahlungen in Höhe von € 10.000 sowie zur zahlung der Kosten des Verfahrens in Höhe von € 12.000 und untersagte dem Unternehmen den Versand unerbetener E-Mails über die Dienste der Unternehmen, die das Verfahren anhängig gemacht hatten.

Deutschland

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

Die Richtlinie 95/46/EG wurde größtenteils in das deutsche Recht übertragen, die Richtlinie 2002/58/EG wurde hingegen nur zum Teil umgesetzt. Das neue Telekommunikationsgesetz trat im Juni 2004 in Kraft. Im Rahmen der Gesetzesänderung regte der Bundestag an, dass Verkehrsdaten nicht nur im Hinblick auf die Durchsetzung des Rechtes durch die zuständigen Behörden gespeichert werden sollten. Im neuen Gesetz sind Vorschriften zu folgenden Punkten verankert:

- die obligatorische Registrierung von Prepaid-SIM-Karteninhabern;
- die Benutzung von Mobiltelefonortungsdaten;
- die Möglichkeit der Feststellung der Identität und der Adresse einer Person anhand einer Rufnummer (umgekehrte Suche).

Die Richtlinie wurde auf dem Gebiet der Tele- und Mediendienstleistungen noch nicht umgesetzt.

B. Bedeutende Rechtsprechung

Urteil des Bundesverfassungsgerichtes vom 03. März 2004 über das Abhören von Wohnräumen (BverfG 109, 279).

Das Verfassungsgericht urteilte, dass große Teile des Strafgesetzbuches im Bereich der Abhörung von Wohnräumen verfassungswidrig seien, weil sie gegen die Menschenwürde verstießen. Die Abhörung von Wohnräumen zu strafrechtlichen Zwecken dürfe nicht bis in die Privatsphäre vordringen. Die Privatsphäre stehe unter absolutem Schutz. Darüber hinaus müssten verfahrensrechtliche Absicherungen – vor allem die nachträgliche Unterrichtung der abgehörten Personen – bei der Anwendung von verdeckten Ermittlungsverfahren und bei anderen Ermittlungsmethoden gewährleistet sein. Ein neuer Katalog von Strafverfahrensvorschriften zur Durchsetzung der Entscheidung wurde am 17. Juni 2005 verabschiedet und sollte am 01. Juli 2005 in Kraft treten.

Urteil über das Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi)

Gemäß dem ersten Urteil des Bundesverfassungsgerichtes vom 08. März 2002 war es der Bundesbeauftragten für Stasiunterlagen strikt untersagt, Unterlagen über den Altbundeskanzler Helmut Kohl gegen dessen Willen zu veröffentlichen. Diesbezüglich kamen jedoch erneute Zweifel auf, nachdem am 06. September 2002 in Paragraph 32 des Fünften Gesetzes zur Änderung des Gesetzes über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik vom 06. September 2002 eine neue Fassung der Klausel über die Interessensabwägung angenommen wurde. Die beteiligten Parteien hatten die Angelegenheit zur Klärung erneut vor Gericht anhängig gemacht.

Das zweite Urteil des Bundesverfassungsgerichtes vom 23. Juni 2004 forderte, dass das geänderte Stasi-Unterlagen-Gesetz gemäß der Verfassung restriktiv interpretiert und angewandt werden müsse. Das Verfassungsgericht legte dazu eine Reihe von Kriterien fest. Die Bundesbeauftragte für Stasiunterlagen hat die internen Richtlinien ihres Hauses bezüglich der Veröffentlichung von Karteien und die diesbezüglichen Praktiken geändert. Die Veröffentlichung von Unterlagen ohne die Zustimmung der betroffenen Person muss noch sorgfältiger geprüft werden und ist nur in wenigen Ausnahmefällen möglich.

C. Wichtige spezifische Themen

Speicherung von Daten von EU-Bürgern im Ausländerzentralregister

Die Frage, ob Daten von Angehörigen von EU-Mitgliedstaaten, die in der Bundesrepublik wohnhaft sind, im Ausländerzentralregister (AZR) gespeichert werden dürfen und ob diese Datenspeicherung nicht im Widerspruch zur Datenschutzrichtlinie 95/46/EG steht, wurde bislang noch nicht endgültig geklärt. Das Bundesinnenministerium hat bisher nicht auf die wiederholten Ersuchen des Datenschutzbeauftragten des Bundes um das allgemeine Verbot der Speicherung solcher Daten reagiert.

Stärkung der Kooperation zwischen den Sicherheitsbehörden bei der Terrorismusbekämpfung

Die Kooperation zwischen der Polizei und dem Nachrichtendienst im Kampf gegen den internationalen Terrorismus wurde vertieft.

Ein wichtiges Element in dieser neuen Sicherheitsstruktur ist das Anti-Terror-Zentrum in Berlin (seit Dezember 2004). Es gibt eine Kooperation in zwei getrennten Analyse- und Auswertungszentren zwischen Sondereinheiten und Untersuchungseinheiten der Polizei und des Bundesnachrichtendienstes mit dem Ziel, potentielle Gefahren zu beurteilen und das Potential des islamistischen Terrorismus im Hinblick auf eventuell beteiligte Personen zu analysieren.

Ein weiterer Aspekt der verstärkten Kooperation zwischen den Sicherheitsbehörden ist die geplante Verwaltung gemeinsamer Projektdatenbanken, zu denen Polizeiorgane und der Nachrichtendienst im Rahmen eines Beurteilungsprojektes – inklusive Lese- und Schreibfunktionen – online Zugang haben werden.

Schließlich sind Diskussionen über die Einrichtung einer gemeinsamen Indexdatei im Gange, die Hinweise auf in den Registern der Polizei und des Nachrichtendienstes gespeicherte Informationen enthält. Diese Art der Kooperation ist aus der Sicht des Datenschutzes vertretbar, wenn die deutsche Verfassung beachtet wird, die eine Trennung von Polizei und Nachrichtendienst vorsieht und die Zusammenarbeit auf den Informationsbereich begrenzt. Mit anderen Worten, es müssen die geltenden Auftrags-, Befugnis- und Übermittlungsregeln streng befolgt werden. Die Dienste dürfen persönliche Daten nur dann in einer gemeinsamen Datenbank speichern, wenn sie allen anderen beteiligten Dienststellen in Übereinstimmung mit den geltenden Übermittlungsbestimmungen Zugang zu diesen Daten verschaffen.

Griechenland

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

Richtlinie 95/46/EG

Die Richtlinie 95/46/EG wurde mit dem Gesetz *2472/97 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten* (Staatsblatt Nr. A50/10-4-1997) in der nationalen Gesetzgebung umgesetzt. Eine begrenzte Änderung dieses Gesetzes wurde durch Artikel 8 des Gesetzes 2819/2000 (Staatsblatt Nr. 84/15-3-2000) angenommen, der bestimmte für die Datenverarbeitung Verantwortliche von der Auskunftspflicht befreit.

Im Jahr 2004 wurde per Dekret des Justizministers ein Sonderausschuss für die Überarbeitung des vorgenannten Gesetzes gebildet. Die Überarbeitung wurde vornehmlich zur Angleichung an den ersten Bericht der Europäischen Kommission im Hinblick auf die Umsetzung der Datenschutzrichtlinie vorgenommen.

Die englische Fassung des geänderten Textes finden Sie unter www.dpa.gr

Richtlinie 97/66/EG

Die Richtlinie 97/66/EG wurde mit dem Gesetz *2774/99 über den Schutz personenbezogener Daten im Telekommunikationssektor* (Staatsblatt Nr. A287/22-12-1999) in nationales Recht umgesetzt.

Die englische Fassung des geänderten Textes finden Sie unter www.dpa.gr

Richtlinie 2002/58/EG

Das Verfahren für die Umsetzung der Richtlinie 2002/58/EG in nationales Recht ist noch nicht abgeschlossen. Ein Gesetzesentwurf zur Umsetzung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation wird dem Parlament im September 2005 vom Justizminister zur Verabschiedung vorgelegt.

Wichtigste Entwicklungen:

- *Gesetzgebende Maßnahmen unter der ersten Säule:* Keine nennenswerten Entwicklungen.
- *Änderungen unter der zweiten und dritten Säule:* Gemeinsame Kontrollinstanz

Im Februar 2005 wurde Griechenland im Rahmen der Kompetenzen der Gemeinsamen Kontrollinstanz (GK) beurteilt. Die Beurteilung der griechischen Datenschutzbehörde als Aufsichtsbehörde des griechischen SIRENE-Büros wurde mit positivem Ergebnis am 08. und 09. Februar 2005 von einer Gruppe von Datenschutzbeauftragten und Polizeiexperten aus Luxemburg (Präsidentschaft), Belgien, Norwegen, Zypern, Estland und Schweden durchgeführt.

B. Bedeutende Rechtsprechung

Stellungnahmen 1/2004, 2/2004 und 3/2004

Die parlamentarische Kontrolle und das Recht auf den Schutz personenbezogener Daten sind in der Verfassung garantiert. Deshalb muss der Zugriff von Parlamentsmitgliedern auf öffentliche Dokumente im Rahmen ihrer Amtsausführung in einer Art und Weise geregelt sein, die die Gefahr einer Verletzung des Datenschutzrechtes minimiert. Daher kann der Antragsteller die erforderlichen Dokumente ausschließlich vor Ort einsehen und nicht um Übermittlung von Kopien einer vollständigen Datenbank an das Parlamentssekretariat ersuchen.

Entschließung 6/2004

In Bezug auf einen Antrag der sozialistischen Partei (PASOK) auf Anmeldung einer Datenbank von „Parteifreunden", die anlässlich des Nationalkongresses der Partei erstellt werden sollte, bei dem nicht nur die Parteimitglieder, sondern auch die Parteifreunde abstimmen durften, urteilte

die Datenschutzbehörde, dass der Status „Freund einer politischen Partei" zu den sensiblen Daten gehört, die aufgrund der Gefahr einer indirekten Verletzung des Wahlgeheimnisses nicht verarbeitet werden dürfen.

Entschließungen 28/2004, 63/2004 und 58/2005

- Die Entschließung 28/2004 der Datenschutzbehörde legt die Bedingungen fest, unter denen die griechische Polizei das Recht hatte, Überwachungskameras an öffentlichen Plätzen von Athen und Umgebung für die Sicherheit bei den Olympischen Spielen 2004 zu installieren.

- In der Entschließung 63/2004 der Datenschutzbehörde wurde dem Antrag der griechischen Polizei stattgegeben, die rechtmäßige Verwendung von Überwachungskameras nach dem Ende der Olympischen Spiele zum alleinigen Zweck der Verkehrsüberwachung unter strengen Bedingungen, unter anderem der Entfernung von Mikrofonen und allen Kameras, die an Stellen angebracht waren, die für die Verkehrsüberwachung nicht erforderlich sind, sowie der Verpflichtung, das Überwachungssystem während Demonstrationen usw. abzuschalten, um sechs Monate zu verlängern.

- Nach Ablauf dieser sechsmonatigen Frist beantragte die Polizei die Verlängerung derselben und die Erweiterung des Verwendungszwecks des Überwachungssystems für den Schutz von Personen und Gütern vor Verbrechen und terroristischen Handlungen (öffentliche Sicherheit). In der Entschließung 58/2005 (12-8-2005) lehnte die Datenschutzbehörde die Zweckerweiterung mit der Begründung ab, dass die Einrichtung eines umfassenden elektronischen Überwachungssystems nicht im Einklang mit dem Prinzip der Verhältnismäßigkeit stünde, da sie eine schwerwiegende Verletzung der Rechte des Menschen auf Schutz der Privatsphäre und des Datenschutzes darstelle, ohne dem Recht der Bürger auf Sicherheit dienlich zu sein.

Entschließung 61/2004

Der Eingriff des Arbeitgebers in die elektronische Kommunikation der Arbeitnehmer stellt eine Verarbeitung personenbezogener Daten dar und ist illegal, wenn der Arbeitnehmer nicht vorher über die Möglichkeit eines solchen Eingriffs, auch aus technischen Gründen, informiert wurde und nicht über die technischen Mittel, beispielsweise spezielle Software, zur Geheimhaltung seiner Mitteilungen verfügt.

Entschließung 67/2004

Gemäß Artikel 9 des griechischen Datenschutzgesetzes bedarf die Übermittlung von Daten an Nicht-EU-Länder der vorhergehenden Genehmigung der Datenschutzbehörde. Diese Genehmigung wurde Olympic Airways für die Übermittlung von Fluggastdatensätzen (PNR) an die Zoll- und Grenzschutzbehörde der Vereinigten Staaten von Amerika (CBP) gemäß dem Abkommen zwischen der EU und den USA und dem Beschluss des Europäischen Rates nach vorhergehender schriftlicher Benachrichtigung der Passagiere entsprechend der Stellungnahme der Art. 29 Datenschutzgruppe erteilt.

C. Wichtige spezifische Themen

Aufgrund des Personalmangels bei der Datenschutzbehörde, die ihre wichtigsten Aufgaben nicht ordnungsgemäß erfüllen konnte (sieben Anwälte und fünf IT-Experten), nahm das Justizministerium die vorgeschlagene Einstellung von 14 weiteren Prüfern (acht Anwälte und sechs IT-Experten) sowie von fünf weiteren Verwaltungskräften an. Das Verfahren soll im Herbst 2005 abgeschlossen sein.

Ungarn

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

Richtlinie 95/46/EG

Der Staat muss transparent sein, während die Bürger für den Staat nicht transparent sein sollten. Dieses Ideal wurde 1989 in der Verfassung der Republik Ungarn, die als erste der mittel- und osteuropäischen Länder den Schutz personenbezogener Daten und die Informationsfreiheit in der Verfassung verankerte, bestätigt. Seitdem hat das Verfassungsgericht diesen Grundsätzen stattgegeben, und das Parlament hat später das Gesetz LXIII von 1992 über den Schutz personenbezogener Daten und über die Offenlegung von Daten von öffentlichem Interesse verabschiedet.

Am 01. Januar 2004 trat eine neue Änderung für die bessere Umsetzung der EU-Richtlinie 95/46/EG in Kraft.

Die englische Fassung des Gesetzes finden Sie unter http://abiweb.obh.hu/dpc/index.htm

Richtlinie 2002/58/EG

Die Einführung der Richtlinie 2002/58/EG wurde 2004 teilweise abgeschlossen. Relevante Bestimmungen im Zusammenhang mit unerbetenen kommerziellen Nachrichten im Gesetz CVIII von 2001 über bestimmte Aspekte der elektronischen kommerziellen Dienste der Informationsgesellschaft (E-Commerce-Gesetz), das dieses Jahr in Kraft trat, wurden geändert. Dies bedeutet, dass bei einer Verletzung dieser Bestimmungen durch den Werbungsträger das Gesetz LVIII von 1997 über die wirtschaftliche Werbetätigkeit Anwendung findet.

Ein weiteres Gesetz, das übereinstimmend mit der Richtlinie 2002/58/EG abgeändert wurde, war das Gesetz C von 2003 über die elektronische Kommunikation im Hinblick auf die Datenverarbeitung im Telekommunikationssektor.

Wichtigste Entwicklungen:

- *Gesetzgebende Maßnahmen unter der ersten Säule*

Alle Gesetze und vorgeschlagenen Änderungen von Rechtsmitteln, die Datenschutzregeln beinhalten oder implizieren, müssen dem Datenschutzbeauftragten zur Begutachtung vorgelegt werden. Der Anhang zum Jahresbericht, der ausschließlich in ungarischer Sprache erhältlich ist, enthält immer die Liste der Gesetze und Rechtsmitteländerungen, die dem Datenschutzbeauftragten vorgelegt werden.

- *Änderungen unter der zweiten und dritten Säule*

Mit dem Beitritt Ungarns zur Europäischen Union am 01. Mai 2004 wurden eine Reihe rechtlicher Instrumente aufgrund der EU-Mitgliedschaft geändert. Neben diesen Änderungen halten wir folgende Änderungen für wichtig:

➔ Das ungarische Parlament erließ die Konvention über Cyberkriminalität des Europarates (Gesetz LXXIX von 2004).

➔ Das ungarische Verfassungsgericht hat in seinem Beschluss 44/2004 bezüglich der Vorschriften des Gesetzes XXXIV von 1994 über die Polizei die Bedeutung der Verfassungsrechte des Datenschutzes und der Sammlung von Daten von öffentlichem Interesse bekräftigt.

B. Bedeutende Rechtsprechung

■ Das Büro des Datenschutzbeauftragten führte landesweite Feldstudien in Bezug auf das individuelle Recht auf anonyme HIV-Untersuchungen durch. Anlass für die Untersuchung war ein Artikel in einer Wochenzeitung, in dem berichtet wurde, dass in mehreren Fällen Honorare für HIV-Tests und die Angabe personenbezogener Daten verlangt wurden. Die Kollegen des Datenschutzbeauftragten überprüften verdeckt eine Reihe von Einrichtungen, die HIV-Tests durchführen dürfen, und berichteten, dass einige Einrichtungen die Nummer des Ausweises und die Sozialversicherungsnummer der Antragsteller verlangten. Die Wahl eines anonymen HIV-Tests, mit anderen Worten ohne obligatorische Angabe personenbezogener Daten, ist laut §59 (5) des CLIV-Gesetzes von 1997 über das Gesundheitswesen gewährleistet. Die Identifizierung von Personen, die auf HIV getestet wurden, ist im Dekret des Ministeriums für Gesundheit, Soziales und Familie 18/2002 (XII.28) über die Vorgehensweise bei Ausschlusstests und über die Maßnahmen zur Vorbeugung einer Ausbreitung der HIV-Infektion vorgesehen. Laut dem vorgenannten Dekret müssen auf dem Deckblatt, das der ersten Blutprobe auf dem Weg zum Labor beiliegt, der medizinische Identifizierungscode und die Identifizierungsnummer sowie – getrennt – das Datum und der Ort der Blutprobenentnahme angegeben sein. Im Anschluss an die Untersuchung wandte sich der Datenschutzbeauftragte an den leitenden Medizinbeauftragten sowie an die Leiter und Aufsichtsgremien anderer Einrichtungen, die Blutproben gemäß dem vorgenannten Dekret durchführen, mit dem Ersuchen, Bedenken bezüglich des Schutzes der Privatsphäre durch tatsächlich anonyme HIV-Tests zu zerstreuen. Er erinnerte die betroffenen Personen daran, dass das Beratungsprinzip, das im Gesetz über das Gesundheitswesen verankert ist, als fester Bestandteil von HIV-Tests beachtet werden muss. Demzufolge ist das medizinische Personal verpflichtet, die Testpersonen über ihr Recht auf einen anonymen HIV-Test aufzuklären.

■ Der Datenschutzbeauftragte und der Bürgerrechtsbeauftragte führten eine gemeinsame Untersuchung zur Verbesserung des Schutzes von Neugeborenen durch, die in der Babyklappe von Krankenhäusern abgelegt werden. Die Beauftragten schlugen vor, dass der Justizminister die geltenden Verordnungen ändert, damit die Anonymität der Mutter, die auf diese Weise ihr Kind überlässt, gewährleistet ist. Der Standesbeamte bräuchte in dem Fall keine polizeiliche Ermittlung der Identität der Kinder unbekannter Eltern vor der Eintragung ins Geburtenregister mehr anzufordern. Die Initiative der Beauftragten wurde durchgesetzt. Ein weiteres rechtliches Problem bestand darin, dass die Mutter, indem sie das Neugeborene in der Babyklappe zurücklässt, den Straftatbestand der willkürlichen Veränderung des Familienstandes laut Strafgesetzbuch erfüllt. Aus diesem Grunde schlugen die Beauftragten neue Vorschriften vor, nach denen das Zurücklassen von Neugeborenen in der Babyklappe nicht mehr als Straftat betrachtet wird. Der Justizminister erkannte den Bedarf einer eingehenden Diskussion mit den Beauftragten und dem Ministerium für Gesundheit, Soziales und Familie, um die komplexen Auswirkungen auf die zwischenmenschlichen Beziehungen und die sensiblen Grundrechte des Kindes auf Leben und Würde beziehungsweise der Mutter auf Selbstbestimmung zu klären. Nach mehreren Diskussionen benannte das Ministerium für Gesundheit, Soziales und Familie die Bestimmungen, die abgeändert werden müssten, damit das Zurücklassen von Neugeborenen keine Straftat mehr darstellt. Die Beauftragten waren mit den vorgeschlagenen Änderungen zum Schutze des Grundrechtes des Kindes auf Leben und Menschenwürde ohne Beeinträchtigung des Rechtes der Mutter auf Selbstbestimmung einverstanden und traten dafür ein, dass diese bei nächster Gelegenheit in der Gesetzgebung verankert werden.

■ Der Datenschutzbeauftragte und der Bürgerrechtsbeauftragte gaben eine gemeinsame Empfehlung zur Regelung der Eizellenspenden ab. Sie verwiesen auf den Widerspruch zwischen der Bestimmung des Gesetzes über das Gesundheitswesen, die die In-Vitro-Befruchtung zulässt, und der äußerst strikten Datenschutzbestimmung desselben Gesetzes, die Eizellenspenden praktisch unmöglich macht. Das Gesetz erlaubt nur anonyme Spenden und verbietet somit Eizellenspenden von Verwandten. Der Datenschutzbeauftragte und der Gesundheits-, Sozial- und Familienminister schlugen die Änderung des Gesetzes vor.

C. Wichtige spezifische Themen

Das Gros der Beschwerden (die um 25 % zunahmen) betraf die beträchtliche Zunahme der rechtlichen Prüfungen, Beschwerden und Beratungen. Die Zahlen zeigen, dass die Zahl der Fälle, die in den sieben Jahren nach der Gründung der Datenschutzbehörde in Ungarn stetig zugenommen und die psychologische Schwelle von 1.000 im Jahre 2003 überschritten hat, mit 2.000 Beschwerden im Jahr 2004 einen weiteren Meilenstein erreichte. Dieser Trend weist eindeutig darauf hin, dass die Menschen immer empfänglicher für Themen werden, die die Privatsphäre berühren.

Irland

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

Die EU-*Datenschutzrichtlinie 95/46EG* wurde durch das Datenschutz(änderungs)gesetz von 2003, das vom Parlament (Oireachtas) im April 2003 verabschiedet wurde, vollständig in das irische Recht übertragen. Das Änderungsgesetz und das ursprüngliche Gesetz von 1988 stellen die Datenschutzgesetze von 1988 und 2003 dar und werden als ein gemeinsames Gesetz betrachtet.

Die *Richtlinie 2002/58/EG* über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation wurde im irischen Recht durch Sonderverordnungen (S.I. 535 von 2003) des Ministers für Verkehr, Marine und natürliche Ressourcen, die im November 2003 in Kraft traten, verankert. Die neuen Verordnungen übertragen die Richtlinie vollständig in die irische Gesetzgebung. Der Datenschutzbeauftragte ist das Aufsichtsorgan, das über die Durchsetzung der datenschutzrechtlichen Aspekte dieser Verordnungen wacht.

Es gab keine weiteren legislativen Entwicklungen im Jahr 2004.

B. Bedeutende Rechtsprechung

Erfolgreiche Strafverfolgungen fanden 2004 gegen zwei für die Datenverarbeitung Verantwortliche statt, die ihre Registrierung bei der Datenschutzbehörde (Meldepflicht) unterlassen hatten. Ein dritter für die Datenverarbeitung Verantwortlicher wurde aufgrund der Nichtbeantwortung einer Meldeaufforderung verfolgt, jedoch nicht verurteilt, weil er sich nach der Vorladung registrierte. Ende 2004 wurden die Anwälte der Behörde mit der Vorladung eines erstklassigen Dienstleistungsanbieters aufgrund der Verletzung der Bestimmungen über das unerbetene Direktmarketing in den Verordnungen über elektronische Kommunikation (S.I. 535 von 2003), mit denen die Richtlinie 2005/58/EG in nationales Recht umgesetzt worden war, beauftragt.

Die Behörde war an keinen weiteren Gerichtsverfahren beteiligt.

Der Datenschutzbeauftragte traf eine Reihe bedeutsamer Entscheidungen, die nicht vor Gericht angefochten wurden. Die wichtigsten hiervon waren:

- Eine natürliche Person stellte einen Antrag auf Zugang zu personenbezogenen Daten in Berichten ihres Arbeitgebers über eine Beschwerde, die sie aufgrund von Schikanen am Arbeitsplatz durch einen Kollegen vorgebracht hatte. Der Arbeitgeber hielt die Daten über die laufenden Mobbing-Ermittlungen zurück. Der Datenschutzbeauftragte befand, dass dies im Einklang mit den Ausnahmen von der Meldepflicht sei, die in Kraft treten, wenn es sich um Daten handelt, deren Offenlegung die Ermittlungen hinsichtlich einer Straftat stören würde. Er urteilte auch, dass diese Ausnahmeregelung nach Abschluss der Ermittlungen nicht mehr gültig sei.

- In einem anderen Fall entschied der Datenschutzbeauftragte, dass die Ausnahmen von der Meldepflicht im Zusammenhang mit der Ausübung eines Rechtsberufes nicht als Vorwand oder Rechtfertigung für eine Zugangseinschränkung in Fällen, in denen Letztere nicht gerechtfertigt ist, benutzt werden können.

- Der frühere Herausgeber des internen Tagebuches der Anwaltskammer benutzte die Datenbank, über die er im Rahmen seines Auftrages verfügte, für eine konkurrierende Veröffentlichung, nachdem er seinen Auftrag verloren hatte. Der Datenschutzbeauftragte befand, dass personenbezogene Daten, die für einen Datenverarbeitungsauftrag bereitgestellt

werden, nicht nachträglich zu einem anderen Zweck genutzt werden dürfen. Da der Betreffende unverzüglich reagierte und sich zur Erfüllung der Anforderungen des Datenschutzbeauftragten verpflichtete, wurde die strafrechtliche Verfolgung fallen gelassen.

■ Die Daten über die Mitgliedschaft in einer politischen Partei wurden von einem kommunalen Parteimitglied für Spendenaufrufe an eine wohltätige Organisation verwendet. Auf Anfrage seitens der Datenschutzbehörde bestätigte die Landeszentrale der Partei, dass das kommunale Mitglied die kommunale Parteidatenbank für den Versand von Spendenaufrufen benutzt hatte, und akzeptierte, dass diese Art der Datennutzung einen Verstoß gegen die Einschränkungs- und Geheimhaltungsbestimmungen der Datenschutzgesetze von 1988 und 2003 darstellte. Im Laufe der Behandlung dieser Beschwerde wies der Datenschutzbeauftragte die Partei auf ihre Verpflichtungen als für die Datenverarbeitung Verantwortliche hin, insbesondere in Form von Anweisungen bezüglich der Anforderungen des Datenschutzes an Mitglieder, die personenbezogene Daten verarbeiten.

■ Der Datenschutzbeauftragte urteilte in Bezug auf die kommunalen Behörden und deren Entscheidungen über die Zuteilung von Sozialwohnungen, dass ungeachtet einer Gesetzgebung, laut der diese Informationen aus Gründen der Offenheit und Transparenz öffentlich zugänglich sein müssen, dies nicht immer bedeute, dass es angebracht sei, personenbezogene Informationen auf eine Website zu stellen. Es müsse stets das erforderliche Gleichgewicht zwischen dem Anspruch der Öffentlichkeit auf bestimmte Informationen und dem Recht des Einzelnen auf den Schutz seiner Privatsphäre beachtet werden, insbesondere dann, wenn die angestrebten Zielsetzungen auch ohne die Offenlegung personenbezogener Daten verwirklicht werden können.

C. Wichtige spezifische Themen

Forschung

Im Laufe des Jahres befasste sich der Datenschutzbeauftragte mit einer Reihe von Fragen in Bezug auf medizinische und sozialwissenschaftliche Forschungsprojekte und verdeutlichte die zu erfüllenden Datenschutzanforderungen, damit wichtige Forschungsprojekte mit der erforderlichen Sicherheit durchgeführt werden können. Der Datenschutzbeauftragte rief das Pflegepersonal und die Forscher zu einem stärkeren Bewusstsein für die Datenschutzregeln auf und betonte gegenüber dem Gesundheitssektor, dass Forschungsdaten zur Einschränkung der Gefahr einer Offenlegung vertraulicher personenbezogener Daten anonym (oder unter Pseudonymen) geführt werden sollten, wenn personenbezogene Identifikatoren für den jeweiligen Zweck nicht notwendig sind. Er bekräftigte, dass die Technik einen Beitrag zur Verbesserung des Datenschutzes in diesem Bereich leisten könne und dass sie in breiterem Umfang eingesetzt werden sollte, um die medizinische und sozialwissenschaftliche Forschung zu erleichtern.

Der Gesetzesreformkommission, die ein Konsultationspapier über die Frage einer nationalen DNS-Datenbank (www.lawreform.ie) herausgab, wurde ein Vorschlag unterbreitet.

Kommunikationsverkehrsdaten

Aufgrund mangelnden Fortschritts bei der Verbesserung der unzureichenden rechtlichen Grundlage für die Aufbewahrung von Kommunikationsverkehrsdaten auf nationaler Ebene im Jahre 2004 forderte der Datenschutzbeauftragte Anfang Januar 2005 mithilfe von Durchsetzungsverordnungen drei Telekommunikationsgesellschaften auf, diese Daten ab dem 01. Mai 2005 zugunsten der nationalen Sicherheit höchstens 12 Monate zu speichern. Zwei der drei Gesellschaften legten Berufung beim Berufungsgericht ein. Der Minister für Justiz, Gleichheit und Gesetzesreformen

erarbeitete ein Gesetz, das eine dreijährige Aufbewahrungsfrist vorsieht. Weil dadurch eine rechtliche Grundlage für die Datenaufbewahrung durch die Unternehmen geschaffen wurde und der Datenschutzbeauftragte keine weiteren Kosten für sich selbst und für die Unternehmen verursachen wollte, nahm er die Verordnungen am 07. Februar 2005 zurück.

Public Service Card

Der Datenschutzbeauftragte legte der Regierung einen Vorschlag über den erforderlichen Datenschutz bei der Erstellung einer Karte für den öffentlichen Dienst (Public Service Card) vor. Mit dem Hinweis, dass er sich Erfolg für das Projekt wünsche, bat er um Klarheit über den Geltungsbereich des Vorschlages (nur auf den öffentlichen Dienst beschränkt?) sowie um Klarheit bezüglich der Benutzung der Personal Public Service Number (PPSN). Er empfahl der Regierung:

- alle konkreten oder potentiellen Zweckbestimmungen der Karte anzugeben;
- die Daten verarbeitenden Organisationen, die auf der Karte gespeicherten Datentypen und die Mittel und Instrumente zur Gewährleistung der Datenschutzrechte genau anzugeben;
- eine getrennte Gesetzgebung für dieses Programm nach einer umfassenden Debatte und Unterrichtung der Öffentlichkeit vorzusehen;
- von Anfang an offen und transparent zu sein und die Zweckbestimmungen der Karte zu nennen. Es wäre zu einfach, die Karte einzuführen und später die Zwecke zu erweitern. Das könnte zu Problemen mit dem Datenschutz führen.

Datenschutzerklärungen auf Websites

Im Jahr 2004 führte der Datenschutzbeauftragte eine Prüfung der Websites des öffentlichen Dienstes durch. Ingesamt wurden 242 Websites erfasst und hinsichtlich ihrer Datenschutzerklärungen kontaktiert. Wenn Unternehmen personenbezogene Daten online sammelten oder technische Mittel wie Cookies benutzten, forderte der Datenschutzbeauftragte, dass die betreffenden Unternehmen diesen Mangel beheben und bis spätestens 31. Januar 2005 eine angemessene Datenschutzerklärung auf ihre Websites stellen sollten. Diese Angelegenheit wird zurzeit geprüft. Die Untersuchung ergab, dass 53 Websites adäquate Datenschutzerklärungen, 46 eine unzureichende Datenschutzerklärung, 8 eine schlechte Datenschutzerklärung und 135 keine erkennbare Datenschutzerklärung hatten.

Das Büro des Datenschutzbeauftragten ist derzeit damit beschäftigt, Websites, die Schwierigkeiten mit ihrer Datenschutzerklärung oder überhaupt keine Datenschutzerklärung haben, zu kontaktieren.

Aufklärung und Bewusstseinsbildung

Die Datenschutzbehörde führte mehrere öffentliche Initiativen zur Bewusstseinsbildung sowie eine sechswöchige Werbekampagne in Bussen und Zügen im Herbst durch. Beide Aktionen fanden großen Anklang.

Italien

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

Das konsolidierte Datenschutzgesetz (Gesetz Nr. 196/2003), in dem beide Richtlinien in vollem Umfang umgesetzt wurden, trat am 01. Januar 2004 in Kraft. Das Gesetz Nr. 196/2003 wurde mit dem Gesetz vom 26. Februar 2004 über die Aufbewahrung von Daten zur Aufdeckung und Vereitelung von Verbrechen novelliert. Das Gesetz vom 26. Februar 2004 ersetzt Artikel 132 des Gesetzes Nr. 196/2003 und erweitert die Aufbewahrungsfrist für Telefonverkehrsdaten auf 24 Monate. Nach dieser Frist werden die Telefonverkehrsdaten für weitere 24 Monate vom Telekommunikationsunternehmen ausschließlich zu dem Zweck aufbewahrt, schwerwiegende Verbrechen wie zum Beispiel terroristische Straftaten aufzudecken und zu verhindern.

Das Datenschutzgesetz wurde im März 2004 hinsichtlich der Meldevorschriften erneut geändert. Es verlangt die Unterrichtung der betroffenen Personen über eine Verarbeitung ihrer Daten, die gegebenenfalls deren grundlegenden Rechte und Freiheiten beeinflussen kann, die im betreffenden Artikel (37) aufgeführt sind, und ermächtigt den Datenschutzbeauftragten *(Garante)*, die Liste der meldepflichtigen Datenverarbeitungen zu erweitern oder zu begrenzen. In der Entschließung, die im März angenommen wurde, befreite der Datenschutzbeauftragte für die Datenverarbeitung Verantwortliche von ihrer Meldepflicht, wenn die Verarbeitung der Daten mit Blick auf die Befugnisse der für die Datenverarbeitung Verantwortlichen oder auf den Zweck der Datenverarbeitung nicht geeignet erscheint, die Rechte und Freiheiten der betroffenen Personen gemäß Artikel 37 beeinflussen zu können.

Diesbezüglich sollte auch die Einführung allgemeiner Genehmigungen für die Verarbeitung sensibler Daten durch verschiedene Kategorien von für die Datenverarbeitung Verantwortlichen erwähnt werden. Das Datenschutzgesetz erlaubt die Verarbeitung sensibler Daten durch private Unternehmen mit der Zustimmung der betroffenen Person und der Genehmigung des Datenschutzbeauftragten, die auch in Form allgemeingültiger Genehmigungen für verschiedene Kategorien von für die Datenverarbeitung Verantwortlichen erteilt werden kann und den Rahmen für die Verarbeitung der sensiblen Daten, um die es geht, absteckt. Seit dem Jahr 1998 wurden sieben allgemeine Genehmigungen mit einer begrenzten Gültigkeitsdauer erteilt, die regelmäßig überprüft werden, um nachträgliche Entwicklungen zu berücksichtigen. Die im Jahre 2004 erteilten Genehmigungen laufen im Dezember 2005 aus.

Weitere Entwicklungen in der Gesetzgebung:

- Die Verordnungen vom Februar 2004 legen die Vorgehensweisen für die Ausstellung der so genannten „Service Card" fest, die den elektronischen Zugang der Bürger zu öffentlichen Verwaltungsdiensten erleichtern und das E-Government verbessern soll. Auf dieser Karte werden die Identifikationsdaten und die Steuernummer des Karteninhabers, aber keine biometrischen Daten erfasst.

- Im Haushalt 2004 ist ausdrücklich die Einführung einer elektronischen Gesundheitskarte (mit der Steuernummer des Karteninhabers) vorgesehen, mit der die Bürger Zugang zu allen Leistungen im Rahmen des nationalen Gesundheitswesens haben. Die relevanten Bestimmungen wurden in Artikel 50 des Gesetzes 326/2003 aufgenommen und anschließend in mehreren Verordnungen im Jahr 2004 erlassen. Diese Maßnahme sollte ausschließlich die Überwachung der Gesundheitsausgaben, insbesondere der Arzneimittelkosten, vereinfachen. Die Karte soll Ende 2005 allen italienischen Bürgern ausgehändigt worden sein.

B. Bedeutende Rechtsprechung

Im Jahr 2004 fällte der italienische Oberste Gerichtshof (Kassationshof) mehrere Urteile in Bezug auf den Datenschutz. Es kann dabei insbesondere auf die folgenden Urteile hingewiesen werden.

Zivilrecht

Ein einschlägiges Urteil wurde bezüglich eines Antrags auf Zugang zu Beurteilungsdaten, den eine Mitarbeiterin bei ihrem Arbeitgeber eingereicht hatte, gesprochen. Der Arbeitgeber hatte dies abgelehnt. Die Mitarbeiterin reichte daraufhin Beschwerde beim Datenschutzbeauftragten ein, der dem Antrag stattgab und den Arbeitgeber zur Auskunft der Daten verpflichtete. Der Arbeitgeber legte Berufung beim zuständigen erstinstanzlichen Gericht ein, das den Beschluss des Datenschutzbeauftragten mit der Begründung aufhob, dass Handlungen, die für den Abschluss der Beurteilung erforderlich sind, nicht zu den personenbezogenen Daten zählen, obwohl sie die Verarbeitung personenbezogener Daten und eventuell zusätzliche Beurteilungen umfassen. Ferner stellte das erstinstanzliche Gericht die rechtliche Stellung des Datenschutzbeauftragten im vorliegenden Fall in Frage. Der Oberste Gerichtshof bestätigte im Urteil vom Februar 2004 zwei wichtige Grundsätze, nämlich, dass Beurteilungsdaten zu den personenbezogenen Daten gehören und deshalb gemäß dem im Datenschutzgesetz verankerten Zugangsrecht von den betroffenen Personen eingesehen werden dürfen, und zwar ungeachtet des Zeitpunktes, zu dem diese Daten verarbeitet werden, und dass der Datenschutzbeauftragte eine rechtliche Stellung einnimmt, wenn es bei der betreffenden Sache um die Rechtmäßigkeit einer Entscheidung geht, die der Datenschutzbeauftragte im Hinblick auf die Feststellung des öffentliches Interesses getroffen hat, das nach dem Gesetz gewährleistet sein muss.

Mit dem Urteil vom Juni 2004 entschied das Gericht ausdrücklich, dass der gesetzliche Schutz personenbezogener Daten auch für „unstrukturierte" Daten einer Datenbank sowie für Daten aus öffentlichen Quellen gilt. Einige Journalisten der italienischen Fernsehanstalt RAI und RAI selbst hatten den Obersten Gerichtshof in Bezug auf das Urteil eines erstinstanzlichen Gerichts angerufen, in dem eine Beschwerde der Journalisten gegen eine Tageszeitung abgelehnt wurde. Die Tageszeitung hatte Artikel veröffentlicht, die personenbezogene Daten der betreffenden Journalisten enthielten, die unter Berufung auf das Datenschutzgesetz eine Löschung dieser Daten verlangten, da diese widerrechtlich verarbeitet worden seien. Das Gericht betonte, dass das Datenschutzgesetz dem Schutz natürlicher Personen und ihrer Grundrechte dient, die durch die Verarbeitung von Daten verletzt werden können, auch wenn diese Verarbeitung nur in der Veröffentlichung dieser Daten besteht und ungeachtet dessen, ob diese nachträglich eventuell in eine strukturierte Datei aufgenommen werden. Bei der Beurteilung der Rechtmäßigkeit der Verarbeitung von Daten sollten alle diesbezüglichen Aktivitäten berücksichtigt werden, um sicherzustellen, dass sie keine schwerwiegenden Verstöße gegen die Grundrechte des Menschen hervorrufen. Außerdem urteilte das Gericht, dass der Geltungsbereich des Datenschutzrechts eindeutig über personenbezogene Daten und Informationen hinausgeht und sich auch auf öffentlich verfügbare und/oder veröffentliche Daten erstreckt, weil „alle Einrichtungen, die Daten und/oder Informationen verarbeiten, mithilfe von Vergleichen, Anpassungen, Analysen, Verknüpfungen usw. den Daten zusätzliche Informationen entnehmen können" und weil diese Informationen einen „Informationsmehrwert" bieten, der nicht aus den einzelnen Dateneinheiten als solchen gewonnen werden kann und unter Umständen die Würde der betroffenen Person verletzt, die den fundamentalen Wert darstellt, für dessen Schutz das Datenschutzrecht einsteht.

Strafrecht

In einem Fall, in dem ein Mann seine frühere Verlobte durch SMS und die Veröffentlichung von Bildern über das Internet belästigte, betonte das Gericht, dass gemäß der betreffenden Bestimmung im konsolidierten Datenschutzgesetz (das das frühere Datenschutzgesetz Nr. 675/1996 ersetzt) das „Zufügen von Schaden" eine grundlegende Voraussetzung für das Bestehen einer Straftat ist beziehungsweise die in der betreffenden Bestimmung definierte Straftat verstärkt. Das bedeutet, dass die Verarbeitung von Daten ohne die Zustimmung der betroffenen Person, die gemäß Artikel 167 des Datenschutzgesetzes eine Straftat darstellt, im strafrechtlichen Sinn keine Straftat ist, wenn die betroffene Person hierdurch nicht geschädigt wird.

In einem anderen Urteil vom Juli 2004 über die Verarbeitung von Daten durch ein Mitglied einer humanitären Organisation, wobei ohne die Zustimmung der Empfänger Daten einer vertraulichen Mailingliste für den Versand von Wahlwerbung verwendet wurden, verdeutlichte der Oberste Gerichtshof die Definition der „Zufügung von Schaden" gemäß Artikel 167 des Datenschutzgesetzes. Das Gericht urteilte, dass „das Zufügen von Schaden", das einen objektiven Straftatbestand darstellt, im strafrechtlichen Sinn unerheblich ist, wenn der Identität oder Privatsphäre einer natürlichen Person nur geringfügiger Schaden zugefügt wurde und daraus nur ein geringfügiger Vermögensschaden entsteht.

C. Wichtige spezifische Themen

Videoüberwachung

Die Entschließung, die am 29. April vom Datenschutzbeauftragten angenommen wurde, befasste sich mit den Grundlagen der Videoüberwachung und beschreibt die allgemeinen Anforderungen, die alle Videoüberwachungssysteme erfüllen müssen. Es wurden auch Leitlinien für spezielle Anwendungen bereitgestellt, wie den Einsatz von Videoüberwachungssystemen in Schulen, Krankenhäusern, Verkehrsmitteln und am Arbeitsplatz. Die Datenschutzbehörde behielt sich das Recht vor, die in bestimmten Situationen zu ergreifenden Maßnahmen von Fall zu Fall festzulegen.

Ausgangspunkt ist die Beachtung der grundlegenden Rechte und Freiheiten sowie die Würde der Bürger unter besonderer Berücksichtigung des Schutzes von Privatsphäre, Identität und personenbezogenen Daten (siehe Artikel 2 Absatz 1 Datenschutzgesetz). Demgemäß wies der Datenschutzbeauftragte darauf hin, dass natürliche Personen ein Recht auf uneingeschränkte Bewegungsfreiheit haben, das ein grundlegendes Merkmal einer freien demokratischen Gesellschaft darstellt (siehe Artikel 8 der Europäischen Konvention über die Menschenrechte, die von Italien mit dem Gesetz Nr. 848/1955 ratifiziert wurde) und deshalb nicht durch eine in die Privatsphäre eingreifende und gewaltsame Erhebung von Daten über die Aufenthaltsorte und Bewegungen einer natürlichen Person, die durch den zunehmenden Einfluss des Internets und des Intranets erleichtert wird, entzogen werden darf. Der Datenschutzbeauftragte lehnte sich auch an die Richtlinien mehrerer internationaler und europäischer Foren an, insbesondere an die Dokumente der Europäischen Datenschutzbehörde im Rahmen der von der Art. 29 Datenschutzgruppe und dem Europarat herausgegebenen Richtlinien über die Videoüberwachung vom 20. bis 23. Mai 2003.

Wahlwerbung

Der Datenschutzbeauftragte bekräftigte, dass betroffene Personen grundsätzlich eindeutige Informationen erhalten müssen, wenn Daten aus Volkszählungen, die in öffentlichen und/oder öffentlich zugänglichen Datenbanken zugänglich sind, für Wahlwerbung verwendet werden. Für die Europa- und Parlamentswahlen im Juni 2004 befreite der Datenschutzbeauftragte die Kandidaten und Parteien, die am Wahlkampf

beteiligt waren, von der Meldepflicht, die als eine unverhältnismäßige Verpflichtung betrachtet wurde, wenn die Daten ausschließlich öffentlichen Listen entnommen und die betroffenen Personen nicht weiter kontaktiert wurden. Die Zustimmung der betroffenen Person war nicht erforderlich, wenn die Daten Listen, Registern, Unterlagen und Instrumenten entnommen wurden, die von öffentlichen Einrichtungen verwaltet werden und nach den Gesetzen oder Verordnungen frei verfügbar sind (z.B. Wahlregister bei den städtischen Gemeinden, Listen von Mitgliedern von Fachverbänden usw.) oder wenn Telefonverzeichnisse als Quelle für den Versand von Standardpostsendungen oder direkte Anrufe verwendet wurden. In allen anderen Fällen ist die vorhergehende Zustimmung der betroffenen Person durch eine Informationsmitteilung, in der die Zweckbestimmung der Daten angegeben ist, erforderlich.

„Institutionelle" SMS-Mitteilungen

Der Datenschutzbeauftragte betonte die Prinzipien, die von TLC-Betreibern und öffentlichen Verwaltungsagenturen beim Versand von SMS-Mitteilungen „institutioneller" Natur, das heißt von Mitteilungen, die von nationalen beziehungsweise kommunalen Behörden für Informations- und Bewusstseinsbildungskampagnen oder zur Verbreitung öffentlich relevanter Informationen verwendet werden, unbedingt erfüllt werden müssen.

In einer Entschließung vom 07. Juli 2004 über SMS-Nachrichten der italienischen Regierung zur Information der Bürger über die Wahlverfahren vom 13. Juni 2004 (Europawahlen) bestätigte der Datenschutzbeauftragte seinen Standpunkt aus einer Entschließung vom März 2003 und erinnerte daran, dass institutionelle SMS-Mitteilungen nur dann rechtmäßig sind, wenn ein Notfall oder eine Ausnahmesituation vorliegt. Es sollte insbesondere ein deutlicher Unterschied zwischen Mitteilungen von Telefonbetreibern auf Wunsch öffentlicher Verwaltungsagenturen und Mitteilungen öffentlicher Stellen gemacht werden. Im ersteren Fall ist die ausdrückliche Zustimmung der betroffenen Person nicht erforderlich, wenn die Mitteilungen im Rahmen von Naturkatastrophen und anderen Notsituationen gesendet werden, nachdem die betreffende öffentliche Stelle, falls gesetzlich gestattet, eine Notmaßnahme im Hinblick auf die öffentliche Ordnung, Gesundheit und Hygiene verabschiedet hat. Im letzteren Fall, wenn SMS-Mitteilungen direkt von öffentlichen Stellen gesendet werden, ist keine Zustimmung zu „institutionellen" Mitteilungen als solchen erforderlich. In beiden Fällen müssen die Telefonbetreiber und die öffentlichen Stellen vorher den Benutzern angemessene Informationen über die Systeme und Zweckbestimmungen der durchgeführten Verarbeitungen personenbezogener Daten sowie über die Möglichkeit des Empfangs institutioneller Mitteilungen zukommen lassen.

Dieser Standpunkt wurde auch nach dem Tsunami am 26. Dezember 2004 vertreten, als das Amt des Premierministers und das Außenministerium den Datenschutzbeauftragten um Mitwirkung bei der Aufgabe ersuchten, Informationen über italienische Bürger, die sich möglicherweise in den Tsunami-Gebieten aufhielten, von den betreffenden Mobil telefonbetreibergesellschaften zu erhalten. Damit sollte insbesondere dem Ministerium erlaubt werden, SMS-Mitteilungen an die betreffenden Personen zu verschicken, in denen diese aufgerufen wurden, ihren Aufenthaltsort mitzuteilen.

Telefonverzeichnisse

Laut dem Datenschutzgesetz hat der Datenschutzbeauftragte die Aufgabe, durch eine unabhängige Entscheidung die Verfahren zur Eingabe und Benutzung von Daten über Netzteilnehmer (und Inhaber von Prepaid-Karten) in öffentlichen Papier- und/oder elektronischen Verzeichnissen (siehe Artikel 129) darzulegen.

Am 15. Juli 2004 erließ der Datenschutzbeauftragte deshalb einen Beschluss, in dem er insbesondere

die jeweiligen Verfahren angab, wie die betroffenen Personen ihre Zustimmung sowohl zur Aufnahme ihrer Daten in Verzeichnisse als auch zur weiteren Verwendung der betreffenden Daten zu kommerziellen oder Marketingzwecken, Umfragen usw. zu erteilen hatten. Ein entsprechendes Musterformular wurde erstellt und von allen Telefonbetreibern an die Netzteilnehmer geschickt (Januar 2005). Somit werden die Netzteilnehmer in angemessener Weise über den Zweck der eventuellen Aufnahme ihrer Daten in Telefonverzeichnisse informiert und können entscheiden, ob sie mit dieser Datenverarbeitung (vor allem mit dem Empfang von kommerziellen Informationen und mit deren Übermittlung, z.B. per E-Mail bzw. Telefon, angedeutet durch entsprechende Symbole neben jedem Eintragsfeld) einverstanden sind. Es ist für jede Organisation gesetzeswidrig, unerbetene Mitteilungen an einen Teilnehmer zu senden, der sich mit diesem Formular dagegen entschieden hat.

Verhaltenskodex mit Bezug auf die Verarbeitung persönlicher Daten zu statistischen und wissenschaftlichen Zwecken

Am 16. Juni 2004 erließ der Datenschutzbeauftragte den Verhaltenskodex und die beruflichen Praktiken für öffentliche und private Körperschaften, die Daten zu statistischen und/oder wissenschaftlichen Zwecken verarbeiten, wenn diese Daten nicht beim Landesstatistikamt (Sistan) erfasst sind.

Neben der Festlegung von Anforderungen und Sicherheiten für die Verarbeitung von Daten für statistische und wissenschaftliche Zwecke trifft dieser Kodex eine wichtige Unterscheidung zwischen Marktsondierungen zu statistischen Zwecken und Marktumfragen zu kommerziellen Zwecken. Der Text des Kodex wurde der konsolidierten Datenschutzgesetzgebung beigelegt, wie gesetzlich verlangt. Die englische Fassung steht unter www.garanteprivacy.it

Verhaltenskodex für private Kreditbeurteilungsagenturen

Nach einer öffentlichen Konsultation, die vom Datenschutzbeauftragten initiiert worden war, wurde der Kodex für Verhaltens- und Berufspraktiken, der sich auf private Informationssysteme zur Erfassung der Bonität, Zuverlässigkeit und Zahlungsmoral von Kunden bezieht, schlussendlich am 12. November 2004 von allen betroffenen Handelsorganisationen und mehreren Verbraucherschutzverbänden angenommen. Dieser Kodex wird gesetzlich verbindlich sein, da die Einhaltung seiner Regeln eine Voraussetzung für die gesetzlich zugelassene Verarbeitung personenbezogener Daten ist und weil jede Zuwiderhandlung zu Sanktionen und Geldstrafen führt.

Die Hauptkennzeichen des Kodex sind folgende:

a) Banken und Finanzgesellschaften (d.h. Körperschaften, die an Kreditinformationssystemen beteiligt sind und Zugang zu den Letzteren haben) müssen eine vereinfachte Standard-Informationsmitteilung verschicken, die gemeinsam mit dem Datenschutzbeauftragten erarbeitet wurde und in der die angewandten Risikobeurteilungsmethoden sowie die Verfahren, durch die betroffene Personen ihre Rechte in der Praxis wahrnehmen können, dargelegt werden.

b) Es dürfen lediglich objektive, nicht vertrauliche persönliche Daten verarbeitet werden. Die Benutzung versteckter Codes zur Kunden/Antragstellerkategorisierung ist untersagt.

c) Regelmäßige Sicherstellung, dass die Daten genau, aktuell und nicht zu ausführlich sind. Speicherung von Daten über Zahlungsunterlassungen getrennt von Datenzugängen aus öffentlichen Quellen. Vor allem dürfen lediglich Daten über den Schuldner verarbeitet werden, und die betroffene Person muss vor der Eingabe ihrer Daten ins System informiert werden.

d) Einhaltung der gesetzlich vorgeschriebenen Aufbewahrungsfristen, mit anderen Worten: 1) Daten über Zahlungsunterlassungen, die behoben wurden, dürfen bis zu einem Jahr oder zwei Jahre lang – je nachdem, ob zwei oder mehr Ratenzahlungen vorgesehen waren – aufbewahrt werden. 2) Darlehensinformationen dürfen während 180 Tagen aufbewahrt werden, müssen jedoch nach 30 Tagen gelöscht werden, wenn die Darlehen nicht gewährt oder vom Antragsteller nicht in Anspruch genommen werden. 3) Daten über nicht behobene Zahlungsunterlassungen dürfen bis zu 3 Jahre nach dem Ablauf des jeweiligen Vertrages/ Auftrages aufbewahrt werden.

e) Nur diejenigen Banken und Finanzgesellschaften, die am CIS teilnehmen, haben Zugang zu den dort gespeicherten Daten. Es müssen Schutzmaßnahmen zur Verhinderung von Sammelanfragen getroffen werden.

f) Daten aus dem CIS dürfen nicht zu Marketingzwecken, Umfragen oder für Werbung verwendet werden.

g) Die CIS-Manager haften bei Sanktionen (einschließlich strafrechtlicher Verurteilungen) laut Datenschutzgesetzgebung neben den Sanktionen, die von den betroffenen Handelsorganisationen auferlegt werden können.

Der Text der Gesetzgebung wurde gesetzesgemäß der konsolidierten Datenschutzgesetzgebung hinzugefügt. Die englische Fassung ist unter www.garanteprivacy.it einsehbar.

Öffentliche Debatte über 4 Hauptthemen: Loyalitätsprogramme, interaktives Fernsehen, RFID und Videophone

Im Hinblick auf die Verabschiedung weit reichender Bestimmungen zu oben stehenden Themen initiierte der Datenschutzbeauftragte im Dezember 2004 eine öffentliche Debatte. Benutzer- und Verbraucherorganisationen, Handelsorganisationen und Bürger wurden um ihre Ansicht zu einigen der Hauptpunkte bei der Entwicklung der Datenschutzrichtlinien für diese sehr wichtigen Bereiche gebeten. Es wurden vor allem Kommentare und Anregungen für die Festlegung der zu sammelnden Kategorien von Daten, der Verarbeitungszwecke, der Informationen, der Erwirkung von Genehmigungen und des Anwendungsbereichs von Schutzmaßnahmen gesucht. Stichtag für die Antworten war der 31. Januar 2005.

Perspektiven

Neben dem wöchentlichen Newsletter, der seit 1999 mit Informationen über die Tätigkeiten des Datenschutzbeauftragten erscheint, und der halbjährlichen CD-ROM mit einem digitalen Archiv derselben Tätigkeiten zuzüglich der Referenzgesetzgebung – genannt: „Die Bürger und die Informationsgesellschaft" (zwölfte Ausgabe im Jahre 2004) – setzte die Behörde ihr Ausbildungsprogramm (In-house-Datenschutzgruppen) zu den Merkmalen und/oder Anwendungen der Datenschutzgesetzgebung bei privaten und öffentlichen Verantwortlichen für die Datenverarbeitung fort.

Erwähnt sei außerdem noch die internationale Konferenz bei der Datenschutzbehörde am 17. und 18. Juni 2004 zum Thema "Privacy and Technological Innovations", welche Gelegenheit zum Meinungsaustausch bezüglich Datenschutzthemen und Spitzentechnologien bot. Die Konferenzprotokolle wurden Anfang 2005 veröffentlicht.

Die Webseite der Behörde steht unter www.garanteprivacy.it. Die Unterlagen sind zum Teil auf Englisch erhältlich.

Lettland

Allgemeine Informationen über die Datenschutzbehörde

Die Datenschutzbehörde ist eine Behörde unter der Aufsicht des Justizministeriums und nahm ihre Tätigkeit 2001 gemäß der Datenschutzgesetzgebung auf. Ihre Aufgaben sind in der Datenschutzgesetzgebung, im Gesetz über elektronische Dokumente und im Gesetz über die Informationsfreiheit verankert. Die Datenaufsichtsbehörde handelt unabhängig in ihren gesetzlichen Aufgaben. Berufung gegen ihre Entscheidungen kann nur vor Gericht eingelegt werden.

Die Richtlinie 95/46/EG wird durch die Datenschutzgesetzgebung, die am 06. April 2000 in Kraft trat, umgesetzt. Bezüglich der Überwachung des Datenschutzes in Lettland übt die Datenschutzbehörde die nachstehenden Aufgaben aus:

- Sie wacht über die Übereinstimmung der Verarbeitung von personenbezogenen Daten mit der Datenschutzgesetzgebung.
- Sie trifft Entscheidungen und prüft Beschwerden bezüglich des Datenschutzes.
- Sie registriert Datenverarbeitungssysteme.
- Sie unterbreitet und führt Aktivitäten zur Verbesserung der Effizienz des Datenschutzes durch und legt Berichte über die Übereinstimmung von Datenverarbeitungssystemen der Regierung und örtlicher Regierungseinrichtungen mit den Datenschutzvorschriften vor.
- Gemeinsam mit dem Amt des Generaldirektors der Staatsarchive der Republik Lettland entscheidet sie über den Transfer von Datenverarbeitungssytemen an die Staatsarchive zu deren Verwahrung.
- Sie akkreditiert Personen, die eine Überprüfung der Datenverarbeitungssysteme der Regierung und der örtlichen Regierungseinrichtungen unter Anwendung der Verfahren, die vom Kabinett der Minister festgelegt werden, durchzuführen wünschen.

Im Bereich der elektronischen Unterschrift übt die staatliche Datenschutzbehörde folgende Aufgaben aus:

- Zulassung von Zertifizierungsdienstleistern gemäß den Prinzipien der freiwilligen Akkreditierung;
- Prüfung der Einhaltung der Zertifizierungsdienstleistungsvorschriften seitens des Zertifizierungsdienstleistungserbringers;
- Überwachung der Sicherheit des zugelassenen Zertifizierungsdienstes und dessen Informationssystems sowie dessen Informationsverfahren, deren Übereinstimmung mit dem Gesetz, den Verordnungen und der Beschreibung des betreffenden Informationssystems, der Ausrüstung und der Verfahrenssicherheit;
- Sicherstellung, dass der akkreditierte Zertifizierungsdienstleister in einem Register, in dem auch Informationen über Zertifizierungdienstleister anderer Länder aufgeführt sind, sofern die von ihnen ausgestellten Zertifikate von einem seitens der Republik Lettland akkreditierten Zertifizierungdienstleister garantiert wurden, aufgeführt ist und dieses Register ständig online abrufbar ist.

Neben den vorgenannten Aufgaben überwacht die Datenschutzbehörde seit 01. Januar 2004 die Anwendung des Informationsfreiheitsgesetzes.

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

Wie bereits erwähnt, wurde die Richtlinie 95/46/EG durch die am 06. April 2000 in Kraft getretene Datenschutzgesetzgebung umgesetzt. Um jedoch die Anforderungen des Artikels 28 der besagten Richtlinie 95/46/EG zu erfüllen, hat die Datenschutzbehörde Lettlands in Zusammenarbeit mit österreichischen und deutschen Datenschutzexperten das Phare Twinning Projekt Nummer LV/2002/IB/OT-01 „Datenschutzbehörde" (Einführungsfrist – 15. September 2004 bis 15. September 2005) eingeführt. Das Hauptziel dieses Twinning-Projektes ist die Stärkung der administrativen Kapazität der Datenschutzbehörde bei der Gewährleistung des Datenschutzes, vor allem durch eine bessere rechtliche Grundlage und Ausbildung der Mitarbeiter. Nach der Einführung des Projektes werden Änderungen am nationalen Recht vorgenommen, damit es die Anforderungen gemäß Artikel 28 der Richtlinie 95/46/EG erfüllt.

Die Richtlinie 2002/58/EG wurde durch das Gesetz über elektronische Kommunikation vom 17. November 2004 und das Gesetz über die Dienstleistungen der Informationsgesellschaft vom 04. November 2004 in die nationale Gesetzgebung übertragen.

B. Bedeutende Rechtsprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Die Mitarbeiter der Datenschutzbehörde nahmen an mehreren Arbeitsgruppen auf nationaler Ebene teil, bei denen es um Datenschutzprobleme ging. Die Ergebnisse waren verschiedene Rechtshandlungen.

Die Haupttätigkeiten im Jahre 2004 betrafen die Erarbeitung eines Gesetzesentwurfs zu Patientenrechten, der dem Parlament Anfang 2005 zur Verabschiedung vorgelegt wurde.

Darüber hinaus wurde aktiv an der Ausarbeitung des Gesetzes über die Dienstleistungen der Informationsgesellschaft, das am 04. November 2004 in Kraft trat, gearbeitet. Das Kernstück dieses Gesetzes ist das Verbot unerbetener Sendungen an Personen, die dem Versand nicht vorher zugestimmt haben.

Es wurde an den Grundsätzen des Datenschutzes weitergearbeitet, damit diese besser im Sozialbereich, im Pharmasektor und in der Genforschung zum Tragen kommen.

Litauen

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

Richtlinie 95/46/EG

Die jüngste Änderung des Gesetzes, das vom Seimas am 13. April 2004 verabschiedet worden war und sich auf die Vorprüfung bezog, trat am 24. April 2004 in Kraft. Das Gesetz engt den Umfang der Vorprüfung auf die Verarbeitung vertraulicher personenbezogener Daten durch automatische Mittel für die interne Verwaltung oder in den Fällen, die unter dem Artikel 10 und Paragraphen 2(6) und (7) von Artikel 5 aufgeführt werden, ein, d.h. wenn der für die Datenverarbeitung Verantwortliche mittels automatischer Mittel öffentliche Dateien verarbeiten darf, sofern Gesetze usw. nicht die Prozedur für die Offenlegung der Daten vorschreiben.

Richtlinie 2002/58/EG

- Das Gesetz über elektronische Kommunikation trat am 1. Mai 2004 in Kraft und setzt die Richtlinie 2002/58/EG um.

- Am 22. April 2004 wurden die Gesetzesbestimmungen über administrative Verletzungen des Rechtes der Republik Litauen um Gesetzesbestimmungen mit Bezug auf die Haftung von Verwaltungen bei ungesetzlicher Behandlung personenbezogener Daten und bei der Verletzung des Datenschutzes in der elektronischen Kommunikation ergänzt. Die Datenschutzaufsichtsbehörde der Republik Litauen wacht darüber, wie die Bestimmungen des neunten Kapitels „Verarbeitung personenbezogener Daten und Schutz der Privatsphäre sowie Datenschutz" des Gesetzes über elektronische Kommunikation angewandt werden, und prüft Beschwerden in Fällen, die in diesem Gesetz vorgesehen sind und im Behördenrecht ausgeführt werden. Diese ergänzenden Bestimmungen traten am 1. Mai 2004 in Kraft.

- Am 6. Dezember 2004 verabschiedete die litauische Regierung ihre Resolution über die Vergabe von Genehmigungen für die Umsetzung des Gesetzes über die elektronische Kommunikation.

- Am 24. Januar 2005 verabschiedete die litauische Regierung die Resolution über die Abänderung der Verordnungen mit Bezug auf die Datenschutzbehörde. Auf diese Weise wurden der Datenschutzbehörde neue Funktionen zuteil, und zwar gemäß dem Gesetz über elektronische Kommunikation, dem Europol-Abkommen und dem Abkommen über den Einsatz der Informationstechnologie zu Zollverwaltungszwecken.

Weitere Entwicklungen in der Gesetzgebung

- Am 22. April 2004 ratifizierte der Seimas der Republik Litauen das Europol-Abkommen. Das Gesetz über die Ratifizierung des Europol-Abkommens trat am 1. Mai 2004 in Kraft.

- Am 28. Juni 2004 ernannte die Regierung der Republik Litauen das nationale Aufsichtsamt der Datenschutzaufsichtsbehörde, dessen Aufgaben die unabhängige Überwachung und Prüfung der Zulässigkeit von Dateneingaben und –einzügen und Mitteilungen personenbezogener Daten an Europol sowie die Verhinderung von Verletzungen der Rechte der betroffenen Person sein werden.

- Am 8. März 2004 ratifizierte der Seimas der Republik Litauen das Abkommen über den Einsatz der Informationstechnologie zu Zollverwaltungszwecken, das auf der Basis des Artikels K.3 des EU-Vertrages zustande kam.

Am 15. Juli 2004 setzte die Regierung der Republik Litauen die Aufsichtsbehörde ein, die für die unabhängige Überwachung und Aufsicht personenbezogener Daten im Zollinformationssystem verantwortlich ist. Sie übt eine unabhängige Aufsichts- und Prüfungsfunktion aus und wacht darüber, dass die Daten, die im

Zollinformationssystem gespeichert sind, nicht unter Verletzung der Rechte des Betroffenen verwendet oder verarbeitet werden.

- Die neue Fassung des Gesetzes über die Staatsregister wurde am 15. Juli 2004 verabschiedet und trat am 7. August 2004 in Kraft.

- Am 19. April 2004 verabschiedete die Regierung der Republik Litauen die Resolution über die Annahme der Regeln über die Einrichtung und Legitimierung staatlicher Informationssysteme.

- Am 2. Juni 2004 verabschiedete die Regierung der Republik Litauen eine Resolution über die Kompensationsregeln bei der Offenlegung von Daten zugunsten der betroffenen Person und über die Annahme der Kompensationsregeln für den Dateneinzug bei registrierten Datenverwaltern.

B. Bedeutende Rechtsprechung

- Anfang 2004 unterrichtete der Parlamentarische Sicherheits- und Verteidigungsausschuss die Datenschutzbehörde über eventuelle Verletzungen des Gesetzes über den gesetzlichen Schutz personenbezogener Daten beim Sonderermittlungsdienst.

Das Korruptionsbekämpfungsgesetz beinhaltet die Einschränkungen der Sammlung und Verwendung von Informationen über eine Person, die sich für eine staatliche oder kommunale Stelle bewirbt oder eine derartige Position innehat. Die Entscheidung, beim Sonderermittlungsdienst Informationen über eine Person zu erhalten, trifft der Vorgesetzte der betreffenden Einrichtung oder ein Politiker, der die betreffende Person einzustellen wünscht oder eingestellt hat.

Während der Inspektion wurde festgestellt, dass personenbezogene Daten an Personen geleitet wurden, die nicht das Recht hatten, diese Informationen zu erhalten. Weitere Gesetzesübertretungen wurden bei der Datenverarbeitung entdeckt: Der Sonderermittlungsdienst verarbeitete geheime Daten ohne jede vorhergehende Prüfung, nahm widerrechtlich gesammelte Daten von Einrichtungen entgegen und teilte der Datenschutzbehörde nicht die Fälle mit, bei denen personenbezogene Daten automatisch verarbeitet wurden. Die Datenschutzbehörde ordnete dem Sonderermittlungsdienst die Wiedergutmachung der festgestellten Zuwiderhandlungen innerhalb einer festgesetzten Frist an. Der Sonderermittlungsdienst legte gerichtliche Berufung gegen diese Anordnung ein. Der Kern des Problems war die Anwendung des Gesetzes, insbesondere der Aspekt der Verarbeitung strukturierter Datenverarbeitungssysteme ohne automatische Mittel.

Der Sonderermittlungsdienst bestritt das Recht der Datenschutzbehörde, das unter dem Artikel 32 §1, 5 des Gesetzes über den gesetzlichen Schutz personenbezogener Daten verankert ist, Empfehlungen und Anordnungen an den für die Datenverarbeitng Verantwortlichen mit Bezug auf die Verarbeitung personenbezogener Daten und den Datenschutz zu erteilen, weil der Sonderermittlungsdienst nicht die für die Datenverarbeitung verantwortliche Dienststelle sei. Das Gericht verwarf dieses Argument und erklärte, dass ein für die Datenverarbeitung Verantwortlicher eine juristische oder natürliche Person ist, die allein oder mit anderen die Zweckbestimmungen und die Mittel der Verarbeitung personenbezogener Daten festlegt. Sind die Ziele der Verarbeitung personenbezogener Daten in Gesetzen oder anderen Rechtsgrundlagen festgelegt, können der für die Datenverarbeitung Verantwortliche und/oder das Verfahren seiner Bestellung auch in Gesetzen oder anderen Rechtsgrundlagen festgelegt sein. Die Datenverarbeitung ist jede Operation, der personenbezogene Daten unterzogen werden, d.h. Sammlung, Aufzeichnung, Anhäufung, Klassifizierung, Gruppierung, Kombination, Veränderung (Ergänzung oder Berichtigung), Enthüllung, Bereitstellung usw.,

logische und/oder arithmetische Operationen, Suche, Verbreitung, Vernichtung und andere Operationen. Das Gericht argumentierte, dass der Sonderermittlungsdienst durch seine Aufgabe der Bekämpfung von Korruption und die Verarbeitung privater Daten zu einer für die Datenverarbeitung verantwortlichen Stelle würde. Ein Argument des Dienstes lautete, das Gesetz über den gesetzlichen Schutz personenbezogener Daten gelte nicht für seine Tätigkeiten, während der Artikel 1 §5 desselben Gesetzes besagt, dass, wenn personenbezogene Daten für die Sicherheit oder Verteidigung des Staates verarbeitet werden, dieses Gesetz gelte, wenn andere Gesetze dem nicht widersprechen. Das Gericht erklärte hingegen, dass es keinen Grund dafür gebe, dass das Gesetz über den Datenschutz keine Anwendung fände. Die einzige Ausnahme laut dem Datenschutzgesetz sei, dass die Datenschutzbehörde nicht das Recht habe, die Verarbeitung personenbezogener Daten vor Gericht zu beaufsichtigen.

- Anfang Mai 2004 wandte sich der Berater des Interimspräsidenten der Republik Litauen an die Datenschutzbehörde mit der Bitte, nachzuprüfen, ob die größten Supermärkte nicht dem Datenschutzgesetz zuwiderhandelten, wenn sie Käufer um Ausweisunterlagen bitten und die sieben ersten Zahlen der Ausweisnummer in die Registrierkasse eingeben.

Das Alkoholkontrollgesetz, das am 1. Mai 2004 in Kraft trat, sieht vor, dass der Verkauf alkoholischer Getränke an Käufer unter 18 Jahren verboten ist. Die Verkäufer alkoholischer Getränke sind beim Verdacht, dass der Käufer unter 18 Jahre alt ist, berechtigt und sogar verpflichtet, den Käufer um den Nachweis seines Alters zu bitten. Legt der Käufer keinen solchen Nachweis vor, darf der Verkäufer alkoholischer Produkte ihm keine alkoholischen Produkte verkaufen. Die gleichen Bestimmungen zum Verkauf von Rauchwaren sind im Tabakkontrollgesetz verankert.

Die Supermärkte begannen also, alle Bürger um ihren Ausweis zu bitten, um zu verhindern, dass Alkohol oder Rauchwaren Minderjährigen verkauft werden.

Im Mai 2004 prüfte die Datenschutzbehörde nach, ob das Datenschutzgesetz nicht beim Verkauf von Alkohol und Rauchwaren verletzt würde. Zuwiderhandlungen wurden nicht festgestellt. Ein Supermarkt gab die ersten Zahlen des Ausweises lediglich ein, um das Alter eines Käufers zu schätzen. Es war – den Aussagen dieses Supermarktes zufolge – unmöglich, direkt oder indirekt die Person auf diese Weise zu identifizieren.

- Das Aufsichtsamt erhielt Beschwerden von zwei Personen über die Datenverarbeitung beim Generalstaatsanwalt der Republik, im Sekretariat des Seimas-Vorsitzenden der Republik und bei der Korruptionsbekämpfungskommission des Seimas.

Im Verlauf der Ermittlungen wurde festgestellt, dass die Kommission, die das Exemplar der Verdachtsanzeige Medienvertretern übermittelt hatte, die überschüssigen Daten über den Antragsteller, mit anderen Worten persönlichen Code, Aufenthaltsort und Anschrift, ebenfalls weiterleitete – ohne organisatorische und technische Mittel zum Schutz der personenbezogenen Daten vor unfreiwilliger und ungesetzlicher Enthüllung anzuwenden.

Für diese Zuwiderhandlungen wurde ein Protokoll aufgestellt und ans Gericht weitergeleitet. Das Gericht strich den Fall wegen der nicht nachgewiesenen Verletzung des Gesetzes seitens der betreffenden Verwaltung.

■ Das Aufsichtsamt erhielt eine Anfechtungsklage über die Gesetzesmäßigkeit der Verarbeitung personenbezogener Daten bei einer Aktiengesellschaft (im Folgenden Firma X). Der Antragsteller behauptete, Firma X biete eine Karte mit Vorteilen und einem persönlichen Code.

Im Laufe der Ermittlungen stellte sich heraus, dass Firma X, die eine persönliche Kundenkarte „Blank" bot, die Angabe der nachstehenden Informationen verlangte: Name, Vorname, persönlicher Code, Geschlecht, Wohnsitz, Telefonnummer und E-Mail-Adresse. Die Gesellschaft X verarbeitet die persönlichen Codes der Kunden, obwohl der persönliche Code nicht zu irgendeinem speziellen Zweck gebraucht wird, weder für die Zahlung von Gebühren noch für etwas anderes. Es wurde festgestellt, dass Sinn und Zweck der Verarbeitung der einzugebenden Daten die Berechnung der „Punkte" war, die der Karteninhaber bei Zahlungen oder Geschäften mit der Kundenkarte in den Geschäften der Firma X erhielt. Außerdem erhielt der Karteninhaber Informationen über Werbeevents und absatzfördernde Aktionen in diesen Geschäften. Laut den allgemeinen Benutzungsbedingungen der Kundenkarte, Punkt 4.3, erhält der Kunde gegen erstmalige Vorlage seiner Karte der Gesellschaft X bei der Zahlung von Einkäufen in Geschäften der Gesellschaft X eine Ermäßigung von 10 % auf den geschätzten Gesamtpreis des Einkaufs. Demzufolge ist der Sinn und Zweck der Verarbeitung der in das Kartenantragsformular einzutragenden Daten nicht allein die Berechnung der „gewonnenen Punkte" bzw. der Versand von Informationen über Werbeaktionen an den Karteninhaber, sondern auch die Gewährung von Ermäßigungen an die treuen Kunden der Gesellschaft X. Es wurde ermittelt, dass die personenbezogenen Daten der Kunden der Gesellschaft X zu direkten Marketingzwecken sowie zur Gewährung von Rabatten verarbeitet wurden. Firma X verarbeitet eine Art „unnützer personenbezogener Daten": den persönlichen Code des Kunden.

Bezüglich der Kundenkarten der Gesellschaft X und der allgemeinen Bedingungen, Punkt 4.6, wird der Karteninhaber mit seiner Erlaubnis über Topneuheiten, Werbeaktionen und Sonderangebote per E-Mail, SMS und Post unterrichtet. Die Firma X liefert dem Kunden keinerlei Informationen über sein Recht, sich der Nutzung seiner personenbezogenen Daten zur Direktmarketingzwecken widersetzen zu dürfen.

Über diese Zuwiderhandlungen der Firma X wurde ein Protokoll über administrative Zuwiderhandlungen erstellt und der Direktor von Firma X zu 600 Lt Geldstrafe verurteilt.

■ Die Vorschriften zum Staatsregister der für die Datenverarbeitung Verantwortlichen beinhalten die Anforderung für den für die Datenverarbeitung Verantwortlichen, anzugeben, wer für den Datenschutz zuständig ist. Der für die Datenverarbeitung Verantwortliche gibt in der Mitteilung über die Verarbeitung von personenbezogenen Daten an, dass er eine Person bezeichnet hat, die sich um den Datenschutz kümmert. Diese Information wurde von der Datenschutzbehörde im Register verzeichnet.

Im Verlauf der Überprüfung der Gesetzesmäßigkeit der Datenverarbeitung des betreffenden Datenverwalters wurden Zuwiderhandlungen festgestellt, und die Verletzung des Verwaltungsrechtes zu Lasten des Unternehmensleiters wurde zu Protokoll gebracht. Das Unternehmen legte Berufung ein mit dem Argument, dass das Protokoll nicht stichhaltig sei. Das Verwaltungsgericht entschied, dass, wenngleich die Gesetze nicht ausdrücklich die Funktion des „für den Datenschutz Zuständigen" beschreibe, die vom Unternehmensleiter bezeichnete Person, die mit dem Datenschutz befasst ist, als solcher betrachtet werden könne und im Falle einer Zuwiderhandlung gegen das Datenschutzgesetz eine Verletzung des Verwaltungsrechtes zu Lasten dieser Person zu Protokoll gebracht werden müsse.

C. Wichtige spezifische Themen

Persönliche Erkennnungsnummer

Das litauische System der Staatsregister und Informationssysteme bei staatlichen Einrichtungen basiert im Wesentlichen auf der Ausgabe einer persönlichen ID-Nummer (PIN) an jeden Ansässigen. Diese PIN ist einmalig und unveränderlich.

Die Struktur der PIN wird unter Artikel 8 des Gesetzes über das Bevölkerungsregister sowie in Klausel 18 der Verordnungen über das Bevölkerungsregister beschrieben. Es ist ein elfstelliger Code mit Informationen über das Geburtsdatum und das Geschlecht. Entsprechend Artikel 8 des Gesetzes über das Bevölkerungsregister, §2, ist die Struktur der PIN zum Zeitpunkt ihrer Zuteilung folgende: Die erste Zahl entspricht dem Geschlecht und dem Geburtsjahrhundert, die zweite und dritte dem Geburtsjahr, die vierte und fünfte dem Geburtsmonat, die sechste und siebente dem Geburtstag, die achte, neunte und zehnte die laufende Nummer im Register der Personen, die am selben Tag geboren wurden, die elfte ist die Kontrollzahl der zehn ersten Zahlen. Die PIN steht auf persönlichen Unterlagen (zum Beispiel Ausweis, Pass, amtlicher Reisepass, Führerschein). Das Bevölkerungsregister erstellt und teilt die persönliche Nummer zu und bereitet die Anordnung ihrer Zuweisung vor, die vom Innenminister genehmigt werden muss.

Die Benutzung der PIN ist gemäß Artikel 7 des Datenschutzgesetzes Beschränkungen unterworfen. Entsprechend Artikel 7 §2 dieses Gesetzes hängt die Benutzung der persönlichen Identifizierungsnummer für die Verarbeitung personenbezogener Daten von der Zustimmung der betroffenen Person ab. Die persönliche Identifizierungsnummer darf ohne die vorhergehende Zustimmung der betroffenen Person zur Datenverarbeitung benutzt werden, wenn:

- dieses Recht in diesem Gesetz und anderen Gesetzen steht;
- zu Forschungs- oder Statistikzwecken in den Fällen laut Artikel 12 (Verarbeitung von personenbezogenen Daten für wissenschaftliche Forschung) und 13 (Verarbeitung personenbezogener Daten zu Statistikzwecken) dieses Gesetzes;
- in Staatsregistern und Informationssystemen, sofern sie amtlich und gesetzlich genehmigt wurden;
- sie von juristischen Personen benutzt wird, die an der Gewährung von Darlehen, Schuldeneintreibungen, Versicherungen oder Leasing, Pflegeleistungen, Sozialversicherungen sowie an den Tätigkeiten anderer Sozialeinrichtungen, Bildungsanstalten, Forschungs- und Studieneinrichtungen und an der Verarbeitung geheimer Daten in den gesetzlich vorgesehenen Fällen beteiligt sind.

Weil die PIN wie ein Schlüssel zu einer Menge weiterer (und zum Teil vertraulicher) Informationen über die betroffene Person funktioniert, wurde gründlich nachgeprüft, zu welchem Zweck die PIN von den für die Datenverarbeitung Verantwortlichen verwendet werden darf.

In Litauen ist es im privaten Sektor und in Staatsregistern und Informationssystemen von staatlichen Einrichtungen möglich, eine Datensuche allein per PIN durchzuführen. Eine Änderung dieses Suchsystems würde gewaltige finanzielle Aufwendungen verursachen.

Es sollte ebenfalls erwähnt werden, dass die PIN-Benutzung nicht allein dem Datenschutzgesetz, sondern auch anderen Sondergesetzen und untergeordneten Gesetzgebungen unterworfen ist. In der Praxis gibt es Fälle, in denen die untergeordnete Gesetzgebung die PIN-Benutzung vorsieht, obwohl das Gesetz dies nicht direkt vorsieht.

Im Juli 2004 führte das Human Rights Monitoring Institute eine Untersuchung „Recht auf Achtung des Privatlebens: Benutzung des ID-Codes in Litauen" durch. Diese Untersuchung wurde dem Vorsitzenden des Seimas und Vertretern anderer Regierungs- und Nicht-Regierungseinrichtungen, die sich mit den Menschenrechten befassen, vorgestellt. Die Schlussfolgerungen dieser Untersuchung waren folgende: Die Struktur der ID-Codes in Litauen ist mangelhaft. In Litauen offenbart der ID-Code persönliche Daten (Geschlecht, Geburtsdatum). Im litauischen Recht wird kein moderner Standard des Rechtes auf Privatsphäre bei der Benutzung der ID-Codes angewandt. Die PIN ist zu vielen Personen zugänglich, so dass sie als Identifikator nutzlos wird, weil sie bei den meisten gesetzlichen Handlungen erfragt wird, jedoch nicht als Beweis dient. Die PIN wird auf diese Weise zu leicht öffentlich zugänglich. Damit werden dem Missbrauch der PIN Tür und Tor geöffnet. Das Institut empfahl: „Die Regel ‚Offenlegung nur wenn nötig' muss in die litauische Datenschutzgesetzgebung aufgenommen werden. Die Zahl der Aufforderungen zur Offenlegung der Ausweisnummer bei anderen gesetzlichen Handlungen muss eingeschränkt werden, um der exzessiven Offenlegung von privaten Informationen Einhalt zu bieten. Die Struktur des Identifizierungscodes muss geändert werden (z.B. zufällige Zahlenfolge), damit personenbezogene Daten wie Alter, Geschlecht usw. geheim bleiben. Der ID-Code darf nur benutzt werden, wenn es angebracht ist. Die obligatorische Angabe von ID-Codes in den Medien muss unterbunden werden."

Die Gesetzgebung der Republik Litauen im Bereich des Datenschutzes bei den staatlichen Registern wurde von den Experten des PHARE-Projektes analysiert. Fazit war, dass die Gesetzgebung über die Staatsregister zwar die EU-Datenschutzstandards erfüllt, aber die Befugnisse für Personen des Justizapparates laut Artikel 7 §3, 4 des Gesetzes über den gesetzlichen Schutz von personenbezogenen Daten recht weit reichen. Aufgrund der Zahl der Personen, die die PIN benutzen dürfen, bewirkt diese Bestimmung das Gegenteil des eigentlichen Zieles, nämlich eine noch breitere Benutzung der PIN.

Eine entsprechende Abänderung des Artikels 7 des Gesetzesentwurfs über den gesetzlichen Schutz von personenbezogenen Daten ist vorgesehen.

Staatsregister

Die Datenschutzbehörde äußerte sich zum Gesetzesentwurf über Staatsregister des Parlamentes bzw. den darin gehandhabten Datenschutz. Das wichtigste Thema ist der öffentliche Charakter der Informationen der Staatsregister. Das Parlament trug der Meinung der Datenschutzbehörde Rechnung. Die neue Fassung des Gesetzes über die Staatsregister wurde am 15. Juli 2004 verabschiedet und trat am 7. August 2004 in Kraft.

Phare-Projekt

Ende März 2004 wurde das Doppelprojekt Nr. LT02/IB-JH-02/-03 „Stärkung der administrativen und technischen Kapazitäten des Datenschutzes" bei der Datenschutzbehörde eingeläutet. Zu den Hauptzielsetzungen dieses Projektes zählten die Stärkung des öffentlichen Bewusstseins für diese Materie, die Vorbereitung von Schulungen für für die Datenverarbeitung Verantwortliche und für diejenigen, die die Datenschutzgesetzgebung durchsetzen und Entscheidungen treffen (Richter, Beamte) und die Vorbereitung der Anmerkungen zur Datenschutzgesetzgebung.

Die Gesetzgebung der Republik Litauen auf dem Gebiet des Datenschutzes auf Ebene der Staatsregister wurde von Experten des PHARE-Projektes analysiert. Fazit: Die litauische Gesetzgebung über den Datenschutz bei den Staatsregistern entspricht den EU-Anforderungen, doch reichen die Befugnisse von Justizmitarbeitern laut Artikel 7 §3, 4 des Gesetzes über den gesetzlichen Schutz personenbezogener Daten doch recht weit. Aufgrund der Zahl der Personen, die zur Benutzung des PIN zugelassen

sind, bewirkt diese Bestimmung das Gegenteil des eigentlichen Zieles, nämlich eine noch breitere Benutzung der PIN.

Eine entsprechende Abänderung des Artikels 3 des Gesetzes über das Bevölkerungsregister im Sinne einer genaueren Festlegung der Zweckbestimmungen des Registers muss ins Auge gefasst werden. Der Öffentlichkeit müssen Informationen über die vornehmlichen Zielsetzungen sowie über die Hauptempfänger von offengelegten Informationen bekannt gemacht werden. Das Bevölkerungsregister muss eine ausführliche Beurteilung der Notwendigkeit der Offenlegung personenbezogener Daten, der entsprechenden Zeiträume und der jeweiligen Ziele vorlegen. Die Empfänger der freigegebenen Daten sowie die ausführlichen Datenfreigabebedingungen und –zwecke sowie die Datenmenge müssen im Gesetz stehen.

Der Datenumfang laut den Verordnungen über dingliches Eigentum sollte kritisch unter die Lupe genommen werden, nicht nur im Hinblick auf Effizienz und Kundenorientierung, sondern auch im Hinblick auf den strikten gesetzlichen und wirtschaftlichen Zweck des Registers. Das Prinzip der Notwendigkeit fand seinen Ausdruck in der EU-Richtlinie und ist ein Hauptaspekt des Datenschutzes.

Zumindest die Regeln der Verordnungen sollten durch eine präzise Beschreibung der zu registrierenden Daten vervollständigt werden.

Die Verordnungen könnten folgendermaßen geändert werden: Es sollte festgelegt werden, dass bei Anfragen ein berechtigtes Interesse bestehen muss, insbesondere bei Zugriff über das Internet in jedem Einzelfall, wobei das legitime Interesse des Benutzers abgefragt und im Hinblick auf Datenschutzebelange gespeichert werden muss. Es sollte ausdrücklich festgelegt werden, dass jede Nachforschung aufgezeichnet werden muss, damit eine Kontrolle der Gesetzmäßigkeit des Antrages im Nachhinein möglich ist. Außerdem sollte jeder Benutzer dazu verpflichtet werden, die Daten ausschließlich im Rahmen der legitimen Zwecke, die er angegeben hat, zu verwenden. Zudem könnte die kommerzielle und politische Nutzung der Daten generell untersagt werden. Die Offenlegung von Informationen sollte auf den Umfang, der für das Register notwendig ist, beschränkt werden.

Luxemburg

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

Gesetz vom 2. August 2002 bezüglich des Schutzes von Personen bei der Verarbeitung von personenbezogenen Daten

Das Koalitionsprogramm der am 4. August 2004 neu gebildeten Regierung beinhaltet die Absicht der Regierung, das Datenschutzrahmengesetz vom 2. August 2002 klarer zu gestalten und zu vereinfachen, insbesondere die formalen Anforderungen und Verfahren, die nicht wesentlich für einen guten Schutz der Grundfreiheiten und der Privatsphäre der Bürger sind.

Gesetz vom 30. Mai 2005 bezüglich der besonderen Regeln des Schutzes der Privatsphäre im elektronischen Kommunikationsbereich

Der Gesetzentwurf zur Umsetzung der Richtlinie 2002/58/EG wurde in mehreren Punkten vor der Erörterung im Parlament geändert.

Er sah eine obligatorische Aufbewahrungsfrist für die Verbindungsdaten von 12 Monaten vor, obwohl der Entwurf besagt, dass die Betreiber und Serviceanbieter die Daten zu ihren eigenen technischen, operativen und Verrechnungszwecken höchstens sechs Monate aufbewahren dürfen.

Für Telefon- und Telekommunikationsverzeichnisse sah der Entwurf nur das Opt-Out-Prinzip vor.

Die nationale Datenschutzkommission veröffentlichte ihre Stellungnahme zu diesem Gesetzentwurf am 20. Februar 2004.

Das Gesetz wurde schließlich vom Parlament am 30. Mai 2005 verabschiedet und trat am 1. Juli 2005 in Kraft.

Gesetz vom 8. Juni 2004 über die Pressefreiheit und die Meinungsfreiheit in den Medien

Dieses Gesetz ersetzt ein altes Gesetz über die Pressefreiheit, die Haftung und Pflichten von Herausgebern und Journalisten.

Die eingangs vorgesehenen Bestimmungen zu den Ausnahmen und Abweichungen vom Datenschutzgesetz wurden letzten Endes aus dem Text herausgenommen. Das Parlament beschloss, die spezifischen Regeln bezüglich der Verarbeitung von personenbezogenen Informationen bei Tätigkeiten, die den Grundsätzen der Meinungsfreiheit unterworfen sind, bei der Verabschiedung der Reform des Datenschutzgesetzesentwurfs neu zu regeln.

Gesetz vom 6. Juli 2004, das das Gesetz vom 15. Februar 1955 über die Verkehrsregeln ändert

Die nationale Datenschutzkommission gab eine kritische Stellungnahme zu bestimmten spezifischen Bestimmungen dieses Gesetzes ab, vor allem zur Regelung der Verarbeitung von Daten betreffend Straftaten und gerichtliche Verurteilungen durch eine private Auftragsverarbeiterorganisation, der die Behörden bestimmte Tätigkeiten im Zusammenhang mit der Ausstellung und dem Einzug von Führerscheinen und der technischen Fahrzeugüberwachung anvertraut haben.

Die nationale Datenschutzkommission wurde vor der Verabschiedung dieses Gesetzes nicht zu Rate gezogen.

Erlasse und untergeordnete Gesetze

Mehrere Dekrete wurden zur Anwendung des Datenschutzgesetzes erlassen, unter anderem bezüglich der Aufgaben der betrieblichen Datenschutzbeauftragten, bezüglich der personenbezogenen Daten, die von bestimmten Pflegeleistenden verarbeitet werden, des Zugangs der Polizei und von Notdiensten zu Telefonnummern und Adressen sowie der polizeilichen Verarbeitung persönlicher Daten zu Strafverfolgungszwecken.

Weitere Entwicklungen der Gesetzgebung

- Am 4. März 2004 wurde ein Gesetzentwurf zur Ratifizierung des Zusatzprotokolls der Konvention 108 des Europarates (ETS Nr. 181) über die Einsetzung von nationalen Überwachungsbehörden und den grenzüberschreitenden Datenverkehr seitens des Parlamentes verabschiedet.

- Ein Gesetzentwurf zur Verarbeitung genetischer Daten zwecks Identifizierung von Personen zur Aufklärung von Straftaten und im Rahmen der Strafverfolgung wurde von der nationalen Datenschutzkommission eingehend kommentiert.

Die Datenschutzbehörde schlägt insbesondere Nachbesserungen bei den Bestimmungen betreffend die individuellen Rechte der betroffenen Personen und zur Verbesserung der unabhängigen Überwachung des Schutzes der Privatsphäre bei der Datenverarbeitung vor.

B. Bedeutende Rechtsprechung

Es gibt bislang keine einschlägigen Gerichtsurteile mit Bezug auf die Anwendung des Datenschutzgesetzes vom 2. August 2002, weder in zivilrechtlichen noch strafrechtlichen Angelegenheiten.

Am 15. Dezember 2004 erging jedoch ein wichtiges Urteil bei dem Verwaltungsgericht, das einen Antrag auf Annullierung eines Beschlusses der nationalen Datenschutzkommission verwarf, durch den die Videoüberwachung von Angestellten einer Schuster- und Schlüsseldienstfirma verboten wurde. Das Berufungsgericht bestätigte im Juli 2005 dieses Urteil und lehnte die Einwände des Arbeitgebers gegen die Interpretation des Gesetzes seitens der nationalen Datenschutzkommission ab. Dies ist eine wichtige Rechtsprechung, insofern sie bei der vorherigen Prüfung der Rechtmäßigkeit einer geplanten Videoüberwachung ausdrücklich die Bewertung von Notwendigkeit und Angemessenheit als Schlüsselkriterien hervorhob.

C. Wichtige spezifische Themen

Die nationale Datenschutzkommission kündigte im Oktober auf einer Pressekonferenz an, dass sie sich in den kommenden Monaten verstärkt auf die Öffentlichkeitsarbeit konzentrieren werde, zur Verbesserung des Kenntnisstandes und Bewusstseins der Bürger.

Eine Informationsbroschüre wurde in drei Sprachen herausgegeben und dank der Unterstützung des Informations- und Pressedienstes der Regierung in großer Anzahl verteilt.

Die Verfassung von Anleitungen und thematischen Orientierungshilfen für Personen, die für die Datenverarbeitung verantwortlich sind, und die Behandlung von Beschwerden werden weitere Schwerpunkte der Arbeit der Datenschutzbehörde in den Jahren 2005 und 2006 sein. Sie unterstützt die Absicht der Regierung, die Kontrollverfahren und Notifizierungssysteme von Anfang an zu vereinfachen.

Die nationale Datenschutzkommission gab - im Anschluss an eine öffentliche Debatte zu diesem Thema, das intensiv in den Medien behandelt wurde - eine Pressemitteilung über die Auslegung der Gesetzesbestimmungen in Bezug auf den Einsatz genetischer Vaterschaftstests heraus.

Die Verbreitung von Videoüberwachung und deren geplanter Einsatz zur Verbesserung der Sicherheit im öffentlichen Raum, die Überwachung am Arbeitsplatz durch den Arbeitgeber sowie die Benutzung von Kundenprofilen in den neuen aggressiven Marketingstrategien zählen weiter zu den wichtigsten Themen, die von der Presse aufgegriffen wurden und zu denen der Standpunkt der nationalen Datenschutzkommission dargestellt wurde.

Malta

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

Die Richtlinie 95/46/EG wurde per Gesetz XXVI von 2001 – abgeändert durch Gesetz XXX1 von 2002 und Gesetz IX von 2003 in das Kapitel 440 des Malteser Rechtes integriert. Dieses Gesetz wurde im Juli 2003 in Kraft gesetzt und enthält eine Benachrichtigungspflicht ab Juli 2004. Einige Bestimmungen über manuelle Karteisysteme treten im Oktober 2007 in Kraft.

Die Richtlinie 2002/58/EG wurde durch die rechtlichen Mittel L.N. 16 von 2003 und L. N. 19 von 2003 übertragen und im Juli 2003 in Kraft gesetzt.

Weitere Entwicklungen in der Gesetzgebung

Vor der gesetzten Frist für die Benachrichtigungspflicht wurden im Jahre 2004 Verordnungen über Gebühren veröffentlicht (L.N. 162 von 2004). Die Gebühren wurden auf einen Pauschalbetrag von Lm10 (24 Euro) pro Jahr gesenkt. Mehrere Sektoren wurden von der Zahlung von Gebühren befreit.

Gleichzeitig wurde das Benachrichtigungsverfahren vereinfacht. Die Verpflichtung zur jährlichen Benachrichtigung entfällt. Nur neue Prozesse und Änderungen müssen angezeigt werden, und zwar ohne Gebührenzahlung.

Im März 2004 (L.N. 142 von 2004) wurden Verordnungen zur Anwendung der polizeilichen Bestimmungen mit Bezug auf die Verarbeitung persönlicher Informationen zu polizeilichen Zwecken erlassen.

B. Bedeutende Rechtsprechung

Fehlanzeige.

C. Wichtige spezifische Themen

Wie bei der Einführung eines jeden neuen Systems gab es diverse Startschwierigkeiten in der Einführungsphase der Datenschutzgesetzgebung.

Anfangs standen die für die Datenverarbeitung Verantwortlichen der Zahlung hoher Anzeigegebühren ablehnend gegenüber. Dieses Problem wurde durch eine Überarbeitung der Gebührenordnung gemildert. Über 8.000 Benachrichtigungsformulare trafen ein.

Die Umsetzung machte auch eine Aufklärung der für die Datenverarbeitung Verantwortlichen über ihre Pflichten nach dem neuen Gesetz erforderlich, damit sie den zunehmenden Erwartungen und Anforderungen der Bürger gerecht werden können.

Ein weiteres Thema war der Schutz von Minderjährigen, wenn Kinder die Opfer ihrer eigenen Eltern werden und sich in der Schule hierüber äußern. Mit einer entsprechenden Verordnung (L.N. 125 von 2004) wurde die Notwendigkeit der Zustimmung und das Zugangsrecht von Eltern aufgehoben, wenn es nicht im Interesse des Kindes ist.

Niederlande

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

Die Richtlinie 95/46/EG wurde durch ein Gesetz vom 6. Juli 2008 in nationales Recht übertragen und trat am 1. September 2001 in Kraft. Es ersetzt das alte Datenschutzgesetz Wet persoonsregistraties (Wpr) vom 28. Dezember 1988.

Die Richtlinie 2002/58/EG wurde ins niederländische Recht vornehmlich durch Änderungen am so genannten *Telecommunicatiewet* (Telekommunikationsgesetz), das am 19. Mai 2004 in Kraft trat[9], übertragen. Weitere Gesetze, die Teile dieser Richtlinie aufnehmen, sind unter anderem das Wet op de Economische Delicten (Wirtschaftskriminalitätsgesetz), das Artikel 13(4) der Richtlinie 2002/58/EG übernimmt.

Bekämpfung des Terrorismus

Die Bomben in Madrid und der Mord an Theo van Gogh führten zu intensiveren Bemühungen um die Sicherheit der Gesellschaft vor allem beim Kampf gegen den Terrorismus. Kurzfristig wurden eine Reihe von Befugnissen der Polizei und des Justizministeriums erweitert bzw. deren Erweiterung angekündigt. Das Ergebnis sind immer mehr Informationen über unverdächtigte Bürger in den Akten der Polizei. Jahrelang wurde eine Erweiterung der Befugnisse der Justiz gefordert, doch erst die größere terroristische Bedrohung seit dem 11. September 2001 führte zur Überzeugung, dass dies in der Tat erforderlich ist.

Selbstverständlich unterstützt die Datenschutzbehörde die Regierung bei ihren Maßnahmen zur Bekämpfung des Terrorismus. Internationale Verträge, europäische Regeln, die niederländische Verfassung und Gesetze verlangen jedoch, dass die neu hinzugekommenen Befugnisse die Kriterien der Notwendigkeit und Verhältnismäßigkeit erfüllen. Auch gesetzlicher Schutz muss gewährleistet sein.

Es mag sein, dass mehrere Richtungen bei der Bekämpfung des Terrorismus eingeschlagen werden müssen, doch gilt immer noch die Ansicht, dass die Ausübung von Macht und Gesetzen in einem System der Prüfung und Abwägung stattfinden muss. Macht ohne Notwendigkeit und Verhältnismäßigkeit und ohne Kontrolle darf nicht sein.

In ihrem Terrorismusmemorandum an die Abgeordneten am 10. September 2004 kündigten der Justizminister und der Innenminister neue Methoden und Befugnisse zur Bekämpfung des Terrorismus an. Unter andere erwog die Regierung die umfassende Sammlung, Verknüpfung und Analyse von Informationen über Gruppen und Personen als Schlüssel zur Verhinderung terroristischer Aktivitäten. Zu diesem Zweck erachtete die Regierung es für notwendig, die Befugnisse im Bereich der Ermittlung und Erfassung auszudehnen. Sie wollte die Tragweite und den Umfang des gesetzlichen Kriteriums „Verdacht oder berechtigter Anlass zu Verdacht" im Hinblick auf die Genehmigung von Aktionen wie das Abhören von Anrufen, Internetüberwachung und Überwachungen nach „Hinweisen" ändern. Der Informationsaustausch zwischen den Sicherheitsdiensten, der Polizei, der Staatsanwaltschaft und dem Einwanderungs- und Einbürgerungsdienst sollte durch eine Informationsschnittstelle, die Informationsbox zur Bekämpfung des Terrorismus, in der Dateien miteinander kombiniert und analysiert werden, intensiviert werden. Dem Memorandum des Ministers zufolge ist für die Regierung allein schon verdächtiges

[8] Gesetz vom 6. Juli 2000 mit den Regeln über den Schutz personenbezogener Daten (Datenschutzgesetz), Staatsblatt 2000 302. Eine inoffizielle Übersetzung des Gesetzes steht auf der Website der niederländischen Datenschutzbehörde www.dutchDPA.nl / www.cbpweb.nl.

[9] Gesetz vom 19. Oktober 1998 mit den Telekommunikationsregeln (Telecommunicatiewet), Staatsblad 2004, 189.

Verhalten eines Bürgers ein ausreichender Grund für seine Überwachung, damit beurteilt werden kann, ob der Verdacht gerechtfertigt ist.

In einer öffentlichen Reaktion auf all diese Vorschläge kam die niederländische Datenschutzbehörde zu der Schlussfolgerung, dass kein Bedarf an erweiterten Befugnissen für die Informationssammlung bestehe. Die neuen Befugnisse würden die Antiterrorismusgesetzgebung vom 1. September 2004 erweitern. Der Umfang des Strafrechtes wurde um neue Strafen und Sanktionen für terroristisch motivierte Verbrechen erweitert. Konspiration im Hinblick auf die Verübung terroristischer Akte wurde auch zum Verbrechen. Es wurden noch keine Erfahrungen mit diesen neuen gesetzlichen Regelungen der Informationsverarbeitung gemacht, so dass die Notwendigkeit und Verhältnismäßigkeit der vorgeschlagenen Maßnahmen nicht bekannt sind. Hinzu kommen die unlängst eingeführten oder anstehenden Befugnisse zum Abhören und zur Anforderung von Informationen bei Firmen und anderen Organisationen.

Außerdem wird bei der vorgeschlagenen weit reichenden Koordination der Datensammlung die gesetzlich verankerte Trennung der Verantwortungen und Befugnisse der Nachrichtendienste und der Polizei missachtet. Der Schutz der Sicherheit des Staates ist hauptsächlich Aufgabe der Nachrichtendienste. Diese Dienste besitzen weit reichende Befugnisse, Informationen beim geringsten Verdachtsmoment auf Gefährdung der Staatssicherheit einzuholen. Die Polizei kann nur dann Informationen vom allgemeinen Nachrichten-/Geheimdienst erhalten, wenn ihr damit bei der Erfüllung ihrer Aufgabe geholfen ist. Die Datenschutzbehörde warnte daher vor der Tendenz, dass Informationen über viele unbescholtene Bürger in Polizeiakten enden würden.

In den vorgeschlagenen Plänen fehlt ein Vorschlag für eine angemessene und strukturierte Kontrolle der Datensammlung und –mitteilung. Es wäre ein schwerwiegendes Versäumnis, wenn die Regierung keine derartige Kontrolle vorsehen würde. Eine Menge Informationsflüsse blieben im Dunkeln, auch für Personen, gegen die ungerechtfertigter Weise ermittelt würde.

Es ist deshalb umso notwendiger, Kontrollen bei der Ausübung dieser weit reichenden Regierungsbefugnisse einzubauen. Die Bürger müssen vor Terroristen geschützt werden, dürfen aber dabei nicht das Vertrauen in die Regierung verlieren.

Die Identifizierungsaufgabe

Anfang 2004 riet die Datenschutzbehörde dem Justizminister von einem Gesetzesvorschlag zur Erweiterung der bürgerlichen Pflicht, sich zu identifizieren, ab. Das wichtigste Argument der Datenschutzbehörde lautete, dass auf diese Weise den Bürgern eine generelle Identifizierungspflicht auferlegt würde – gegenüber der Polizei und anderen Aufsichtsinstanzen, während der Gesetzgeber keine ausreichenden Gründe und Rechtfertigungen für eine solche allgemeine Verpflichtung vorlegen könne.

Erst vor einigen Jahren hatte die Regierung beschlossen, dass eine allgemeine Identifizierungspflicht der Bürger zu weit gehen würde. Das Memorandum zum Gesetzesvorschlag zur Erklärung dieser Haltung wurde nicht durch neue Argumente gestärkt, und die Regierung erfüllte somit nicht Artikel 8 §2 der europäischen Menschenrechtskonvention, nach dem jeder Eingriff in das Recht auf Privatsphäre triftig begründet sein muss. Zudem wurde die sich daraus eventuell ergebende Diskriminierung und Stigmatisierung verkannt. Am 1. Januar trat die erweiterte und faktische allgemeine Identifizierungspflicht der Bürger in Kraft.

Neues Polizeiinformationssystem

Vor einigen Jahren schufen die Polizeikräfte ein buntes Allerlei an IKT-Anwendungen für die Erfüllung ihrer Aufgaben. Letzten Endes wurde beschlossen, diese Anwendungen landesweit unter einen Hut zu bringen. Die Datenschutzbehörde, die über die Verarbeitung von Daten seitens der

Polizei wacht, wurde um Rat bei der Erarbeitung der Regeln für die neuen Systeme gebeten.

Darüber hinaus wurde mit der Überarbeitung des gesetzlichen Rahmens für ein Polizei-Informationssystem begonnen. 2004 erhielt der Justizminister ein Gutachten über den Gesetzentwurf über Polizeidaten. Die niederländische Datenschutzbehörde ist mit einem Datenverarbeitungssystem einverstanden, wenn mehr Sicherheiten geboten werden, weil die Datenverarbeitung größere Risiken für die betroffenen Personen mit sich bringt. Drei Kritikpunkte drängten sich auf. Erstens muss die Qualität der polizeilich verarbeiteten Daten verbessert werden. Zweitens widersetzt sich die Datenschutzbehörde vehement den so genannten thematischen Dateien, die unzählige Daten über Bürger enthalten, die sich nichts zuschulden haben kommen lassen. Drittens sind klare Regeln für die Aufbewahrungsfristen vonnöten. Nicht mehr erforderliche Daten sollten vernichtet und nicht unbegrenzt „für den Fall des Falles" aufbewahrt werden.

Krankenversicherungsgesetz

Das neue Krankenversicherungsgesetz stellt eine obligatorische Krankenversicherungsnorm für alle Bürger bereit. 2004 riet die Datenschutzbehörde im Gesetzesvorschlag zu konkreteren Regeln und Normen für die Benutzung und den Austausch von personenbezogenen Daten im Rahmen der Krankenversicherung. Die strukturelle Überwachung von Krankenversicherungsgesellschaften würde sich sonst nur auf die Hervorhebung ungesetzlicher Situationen auf versicherungstechnischem, finanziellem und administrativem Gebiet beschränken.

Weiterhin muss die Überwachung der Verarbeitung personenbezogener Daten ausdrücklich im Gesetzesvorschlag erwähnt sein, weil die Verarbeitung von personenbezogenen Daten durch die Krankenversicherungsgesellschaften eine strukturelle Aufsicht erfordert. Zudem muss der Nachtragsentwurf des Verbandes der niederländischen Krankenversicherer dem Verhaltenskodex für die Verarbeitung von personenbezogenen Daten bei Finanzanstalten angepasst werden.

Das neue Arbeitsunfähigkeitsversicherungsgesetz und die Versicherungsgesellschaften

Bezüglich des neuen Arbeitsunfähigkeitsversicherungssystems wünschte die Datenschutzbehörde mehr Klarheit in den wechselseitigen Standpunkten der diversen Parteien (Arbeitgeber, Arbeitnehmer, Angestelltenversicherungsbehörde, Wiedereingliederungsagenturen und Versicherungsgesellschaften) und Haltungen, wenn es um die Verwendung personenbezogener Daten geht. Die Behandlung personenbezogener Daten durch die Versicherungsgesellschaften im neuen System ist nach wie vor nicht deutlich, und diese Situation ist nicht wünschenswert.

Im Rahmen der neuen Aufgaben laut dem Gesetz über Arbeit und Einkommen auf Arbeitsfähigkeitsbasis und auch des neuen Krankenversicherungsgesetzes haben die Konzerne, zu denen die Versicherungsgesellschaften gehören, Zugang zu noch mehr (medizinischen) privaten Daten. Dies ist der Nährboden für eine mächtige und einflussreiche Informationsposition.

Den Versicherungsgesellschaften ist jedoch die Notwendigkeit einer sorgfältigen Datenverarbeitung durchaus bewusst. Wenn aber die Regierung keine Regeln für diese Datenverarbeitung aufzustellen imstande ist, verlieren die an der Datenverarbeitung Beteiligten unnötig Zeit. Die Datenschutzbehörde hat deshalb den dringenden Appell an den Minister für Soziales und Beschäftigung gerichtet, Klarheit in der einschlägigen Gesetzgebung bezüglich der Möglichkeiten und Einschränkungen der Verarbeitung von personenbezogenen Daten zu schaffen.

B. Bedeutende Rechtsprechung

Einhaltung der Notifizierungsverpflichtung

Gemäß dem Datenschutzgesetz (WBP) sind Unternehmen, Organisationen und Einrichtungen dazu verpflichtet, die Verarbeitung personenbezogener Daten der Datenschutzbehörde oder dem Datenschutzbeauftragten zu melden (bis auf Ausnahmen). War die Anmeldung unrichtig oder unvollständig oder wurde sie unterlassen, kann die niederländische Datenschutzbehörde ein Bußgeld von maximal 4.500 Euro erheben. Notifizierungen aus bestimmten Sektoren oder über bestimmte Arten von Datenverarbeitungen werden regelmäßig eingehender untersucht. Die niederländische Datenschutzbehörde betreibt solche Untersuchungen, nachdem sie Beschwerden von betroffenen Personen erhalten hat.

2004 lag der Untersuchungsschwerpunkt auf drei Sektoren: Telekommunikation, geistige Gesundheit und Schuldeneintreibung. Die Nachforschungen werden 2005 abgeschlossen. Es können Sanktionen auferlegt werden.

Im Zusammenhang mit spezifischen Informationen, die zum Telekomsektor gelangen, prüfte die Datenschutzbehörde nach, ob bestimmte Telekombetreiber (Festnetz, Mobiltelefon und Internet) der Notifizierungsverpflichtung nachkamen. Diese Nachforschungen konzentrierten sich insbesondere auf die Notifizierung über die Verarbeitung von Telekomverkehrsdaten.

Bei vielen lokalen Gesundheitsbehörden (GGD) untersuchte die Datenschutzbehörde die Anmeldung der Verarbeitung personenbezogener Daten im Rahmen der öffentlichen geistigen Gesundheitspflege (OGGZ). Der Gesetzgeber ist der Ansicht, dass diese Verarbeitung besondere Risiken für die Privatsphäre der betroffenen Bürger in sich birgt. Bei der Information der Datenschutzbehörde über die Datenverarbeitung muss der für die Datenverarbeitung Verantwortliche eine Untersuchung der Gesetzmäßigkeit der Datenverarbeitung, die so genannte Voruntersuchung, beantragen.

Die Analyse der WBP-Anmelderegister zeigte, dass die Zahl der Notifizierungen seitens Inkassoagenturen hinterherhinkte. Die Untersuchungen in diesem Sektor zielten auf die Prüfung des Umfangs der Verarbeitung von personenbezogenen Daten durch Inkassoagenturen und des Umfangs der von ihnen unterlassenen Anzeige der Verarbeitung personenbezogener Daten.

Sanktionen gegen Kommunalverwaltungen und Gesellschaften

2003 führte die Datenschutzbehörde die erste Zufallsprüfung der Einhaltung der WBP-Notifizierungsverpflichtung unter zahlreichen Kommunalverwaltungen, Krankenversicherungen, internen und externen Diensten für Gesundheit und Sicherheit am Arbeitsplatz (arbodiensten) sowie Direktmarketingfirmen durch. Die Zahl der WBP-Anmeldungen nahm nach diesen ersten Prüfungen stark zu, und zwar nicht nur in den geprüften Sektoren, sondern auch bei privaten Detekteien, der Polizei und im Gesundheitsbereich.

Insgesamt 50 Untersuchungen wurden im Rahmen dieser ersten Prüfung durchgeführt. In einer Reihe von Fällen wurde eine Zusatzprüfung vor Ort durchgeführt, um die Fakten zu erhärten. Ende 2003 führte die Stichprobe zu den ersten Sanktionen gegenüber einer Kommunalverwaltung und zwei Unternehmen.

Im Jahre 2004 verhängte die Datenschutzbehörde insgesamt 29 Strafen zwischen 3.000 € und 15.000 €. In einer Reihe von Fällen machte die Datenschutzbehörde von ihrer Befugnis Gebrauch, Strafen zu senken, vor allem wenn - wie im Falle von Kommunalbehörden - große Mengen personenbezogener Daten verarbeitet wurden. Die Hauptüberlegung lautete, dass auch eine abgemilderte Strafe zum Ziele führen würde und einen besonderen und allgemeinen vorbeugenden Effekt habe.

Die oben erwähnten Strafen wurden gegen 14 Kommunalbehörden, 3 Direktmarketinggesell schaften, 3 Krankenversicherungen und 9 Dienste für Gesundheit und Sicherheit am Arbeitsplatz verhängt. Die meisten Kommunalbehörden setzten sich gegen die Strafe zur Wehr. Eine Reihe von Kommunalbehörden haben die Strafe inzwischen bezahlt. Nur eine der privaten Organisationen brachte Einwände vor, und fast alle haben mittlerweile bezahlt. Alle beteiligten Organisationen haben nunmehr der Datenschutzbehörde ihre Verarbeitung von personenbezogenen Daten angezeigt.

Verbrechensermittlungseinheiten

2003 und 2004 führte die Datenschutzbehörde Untersuchungen bei speziellen Polizeiregistern von Verbrechensermittlungszellen (CIE) der regionalen Polizeikräfte durch. Entsprechend dem Polizeiaktengesetz (Wpolr) hat die Datenschutzbehörde die regulierende Aufsicht über Polizeiakten inne. In dieser Position hat die Datenschutzbehörde Zugang zum Inhalt der CIE-Dateien. Wegen ihrer vertraulichen Natur sind diese Dateien zu Recht weitgehend vor Zugang durch registrierte Personen und durch gerichtliche Aufsicht geschützt. In diesem Kontext sieht es die Datenschutzbehörde als besondere Verantwortung an, die CIE-Dateien besonders zu überwachen.

Bei ihren Nachforschungen konzentrierte sich die Datenschutzbehörde vornehmlich auf Prüfungen auf Dateninhaltsgrundlage. Eine Reihe technischer und organisatorischer Aspekte wurden ebenfalls berücksichtigt. Das allgemeine Bild, das sich aus den Nachforschungen ergibt, ist positiv. Die wichtigen Aspekte, die untersucht wurden, erwiesen sich als in Ordnung. Bezüglich der untersuchten technischen und organisatorischen Aspekte stellte sich heraus, dass in vielen Punkten die gesetzlichen Regeln und Verordnungen nicht eingehalten werden. Die Polizeikräfte gaben an, dass sie in Erwartung eines Informationssystems auf nationaler Grundlage keinerlei Anpassungen bei den derzeitigen Systemen und Methoden vornehmen würden.

Nationalregister im Gesundheits- und Pflegebereich

2004 schloss die Datenschutzbehörde ihre Prüfung der Nationalregister im Gesundheitsbereich mit einem Protokoll ab, das im April 2005 veröffentlicht wurde. Die Kernfragen der Nachforschungen lauteten: Was weiß der Patient über die Registrierung seiner Daten bei nationalen Datenbanken, zu welchen Zwecken werden diese Register benutzt und können die Informationen in diesen Registern auf den einzelnen Patienten zurückverfolgt werden? Weil die Informationen vertraulich sind und wegen des Arztgeheimnisses lässt das Gesetz zurzeit nur begrenzte Möglichkeiten bei der Verarbeitung von (indirekt) rückverfolgbaren Patientendaten zu.

Die Nachforschungen bei fünf Nationalregistern hinterließen bei der Datenschutzbehörde den Eindruck, dass die Nationalregister im Allgemeinen verantwortungsbewusst mit den Daten umgehen. Es stellte sich aber auch heraus, dass in fast allen Fällen Verbesserungen möglich und notwendig sind. Die wichtigste durchzuführende Maßnahme ist die Einschränkung der Rückverfolgbarkeit der Daten bis auf einzelne Patienten. Eine Reihe von Empfehlungen wurden inzwischen von den Registern übernommen.

C. Wichtige spezifische Themen

Kameras in der Öffentlichkeit

Das Interesse an Videoüberwachung hat in den letzten Jahren zugenommen. Die Öffentlichkeit akzeptiert Kameras und wünscht sich eine effiziente Videoüberwachung. Videoüberwachung, insbesondere von Seiten der Regierung, hat in den letzten Jahren erheblich zugenommen. Aus diesem Grunde führte die Datenschutzbehörde 2003 eine Studie über Art und Umfang der Videoüberwachung in den Gemeinden durch. Unter anderem zeigte diese Studie, dass 20 Prozent der Gemeinden Videokameras benutzen und dass in vielen Körperschaften die Wirksamkeit der Videoüberwachung (noch) nicht beurteilt

wurde. In der Folgezeit wurde eine Studie – Kameras in der Öffentlichkeit – im November 2004 herausgegeben. Sie umfasst Faustregeln für Entscheidungen und Ausgangspunkte für die Anbringung und den Einsatz von Kameras, für die Rechte der Überwachten und für die Überwachung und Auswertung.

Bürgerdienstnummer

Die Politik des „electronic government", einer Regierung, die die Informationstechnologie optimal einsetzt, auch das Internet, wurde im Jahre 2004 im Programm „Eine andere Regierung" beschrieben. Die Einführung der so genannten Bürgerdienstnummer (BSN) ist eine unbedingte Voraussetzung für den Erfolg des Programms. Die BSN-Programmagentur wurde mit dem Auftrag gegründet, den Ende 2003 abgeschlossenen Plan durchzuführen.

Die Regierung traf die unerwartete Entscheidung – entgegen ihren früheren Versprechen - die BSN auch im Gesundheitssektor einzuführen. Gesundheitsinrichtungen und Krankenversicherungen sind zur Benutzung dieser Nummer verpflichtet. Die Benutzung einer einzigen ID-Nummer im Gesundheitssektor birgt inhärente Risiken in sich. Die umfassende Verknüpfung von Patientendaten wird einfacher und damit auch der Missbrauch. Eine getrennte Erkennungsnummer für den Gesundheitsdienst – Sicherheit vor einer zu einfachen Weitergabe von Daten von Patienten und Pflegeleistungsempfängern – erwies sich im politischen und sozialen Bereich als nicht mehr vertretbar. Die Datenschutzbehörde genehmigte die Benutzung der BSN im Gesundheitssektor, sofern mit dieser Nummer ausgleichende Garantien verbunden sind, einschließlich zuverlässiger Genehmigungsverfahren für die Benutzung medizinischer Daten, die mit Hilfe dieser Nummer zugänglich werden.

2005 wurde die „Nationale Vertrouwensfunctie" (nationale Vertrauensfunktion) geschaffen, an der die Datenschutzbehörde beteiligt ist. Diese Organisation sorgt für eine strukturierte Beaufsichtigung unter anderem in Form eines Büros, in dem Bürger Fragen zur BSN stellen und Beschwerden über BSN einreichen können.

Verhaltensregeln

2004 konnten fünf sektorielle Verhaltenskataloge verabschiedet werden. Nach einer Vorbereitungsphase von mehreren Jahren, in der die Datenschutzbehörde den sektoriellen Verband unterstützte, wurden Anfang 2004 die Verhaltensregeln für private Ermittlungsagenturen verabschiedet.

Der Königliche Berufsverband der Gerichtsanwälte entwickelte einen Verhaltenskodex mit Regeln für die besondere Situation, in der Gerichtsanwälte als Beamte fungieren und zugleich kommerzielle Dienste erbringen (zum Beispiel Inkasso). Es ist wichtig, dass sie dabei keinesfalls Informationen verwenden, die sie aufgrund ihres besonderen Statuts als Beamte in der Ausübung ihrer nichtöffentlichen Tätigkeiten erhalten haben.

Der Branchenverband für Personalbeschaffung, Suche und Auswahl (OAWS) überarbeitete und aktualisierte seinen Verhaltenskodex hinsichtlich der zulässigen Verarbeitung von Daten potentieller Kandidaten. Diese „guten Verhaltensregeln", ein Verhaltenskodex für die medizinische Forschung, wurden ebenfalls überarbeitet und mit Regeln für die Verarbeitung von Patientendaten in der Gesundheitsforschung versehen. Neu ist der Verhaltenscodex für die Verarbeitung personenbezogener Daten in der Forschung und in der Statistik. Er wurde von drei Organisationen ausgearbeitet: dem Verband für politische Forschung, dem Verband für Statistik und Forschung sowie einem Berufsverband von Marktforschern (MarktOnderzoekAssociatie.nl).

2004 begann Zorgverzekeraars Nederland, der Branchenverband der Krankenversicherer, mit der Formulierung von Verhaltensregeln unter anderem für den Umgang mit den großen Mengen von medizinischen Daten, die bei Krankenversicherern

im Rahmen von medizinischen Schadensersatzforderungen anfallen. Regeln werden auch für die Nachforschungen bei Betrug seitens einer Einrichtung, Gesundheitsdienstleistern oder Versicherern erstellt. Sie stellen einen Nachtrag zu den Verhaltensregeln für die Verarbeitung personenbezogener Daten von Finanzeinrichtungen dar. Es wird damit gerechnet, dass diese Verhaltensregeln Ende 2005 verabschiedet werden.

Arbeits- und Unterstützungsgesetz

Im Hinblick auf die Überwachung der Einhaltung des neuen Arbeits- und Unterstützungsgesetzes von 2004 brachten das IWI (Arbeits- und Einkommensaufsicht) und die Datenschutzbehörde ihren Wunsch nach einem Kooperationsabkommen zum Ausdruck. Dieses wurde 2005 geschlossen. Durch Kooperation und Weitergabe von Wissen wird eine effizientere Überwachung möglich. Die Zusammenarbeit fördert weiterhin eine bessere Überwachung, weil die von den Regelungsinstanzen angewandten Normen koordiniert werden können. Dies mindert auch den Regelungsdruck der beaufsichtigten Organisationen. So beinhaltet das Abkommen auch Vereinbarungen mit Bezug auf die Weitergabe von Überwachungsinformationen und den gegenseitigen Austausch von Informationen über die Untersuchungsergebnisse.

Spam

Unerwünschte Massen-E-Mails, besser bekannt unter der Bezeichnung Spam, sind ein Ärgernis, sind schwierig zu entfernen und bringen für die Internetanbieter – und somit auch für deren Kunden – hohe Kosten mit sich. Jüngeren Schätzungen zufolge sind etwa drei Viertel aller weltweit versandten E-Mails Spam. Die europäische Richtlinie über elektronische Kommunikation (2002/58) untersagt den Versand unerwünschter kommerzieller Nachrichten. Die europäischen Überwachungsinstanzen, die über die Einhaltung dieses Verbots wachen, arbeiten im so genannten Verbindungsnetz der Spam-Behörden zusammen, wo sie Informationen austauschen und die Zusammenarbeit bei der Umsetzung des Verbots in der EU intensivieren. Ein Kooperationsvertrag wurde ebenfalls zu diesem Zweck erstellt.

In den Niederlanden unterzeichneten das OPTA (unabhängige Post- und Telekommunikationsbehörde) und die Datenschutzbehörde am 19. Oktober 2004 Abkommen über die Zusammenarbeit auf dem Gebiet der Unterbindung von Spam-Mitteilungen. Das Abkommen ist seit 19. Mai 2004 in den Niederlanden in Kraft. Die Datenschutzbehörde legt den Schwerpunkt auf die Überwachung der Sammlung und Benutzung von E-Mail-Adressen. Einzelbeschwerden über Spam-Mitteilungen können beim OPTA über www.spamklacht.nl eingereicht werden. Die praktischen Vereinbarungen über die Behandlung von Spam waren die Einleitung zu einem umfassenderen Kooperationsprotokoll, das die beiden Behörden im Juli 2005 unterzeichneten.

Private Ermittlungen

2004 wurde ein besonderes Überwachungssystem für den privaten Ermittlungssektor geschaffen. Das Gesetz über private Schutzorganisationen und Detekteien liefert einen Standard für die Branche, doch fehlten Regeln für die Durchführung von Ermittlungen und die weitere Verarbeitung von Daten, die bei solchen Ermittlungen gesammelt werden. Der Geltungsbereich des Verhaltenskodexes des Verbandes der privaten Sicherheitsorganisationen wurde erweitert, weil der Justizminister diesen Verhaltenskodex per Ministererlass für alle privaten Ermittlungsagenturen obligatorisch machte. Die niederländische Datenschutzbehörde und der Justizminister haben eine Zusammenarbeit bei der Überwachung der Einhaltung dieser Verhaltensregeln vereinbart.

Polen

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

Zu Beginn des Jahres 2004 wurden die Änderungen am Gesetz über den Schutz personenbezogener Daten abgeschlossen. Diese Verordnungen traten am 1. Mai 2004 in Kraft, und zwar zum Zeitpunkt des Beitritts Polens zur Europäischen Union. Die Tätigkeiten zur Verbesserung der Bestimmungen ergaben sich aus der Notwendigkeit der kompletten Anpassung des Gesetzes an die Anforderungen der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (im Folgenden als die Richtlinie bezeichnet) sowie aus der Notwendigkeit, einige in ihrer praktischen Umsetzung problematische Bestimmungen anzupassen.

Die wichtigsten Änderungen infolge der Änderung des Datenschutzgesetzes, dessen Bestimmungen der Richtlinie angepasst wurden, umfassen folgende Punkte:

- Unzweideutiger Hinweis darauf, dass das Gesetz auch Anwendung auf Fälle findet, in denen personenbezogene Daten außerhalb von Computerdateisystemen verarbeitet werden oder werden können;
- Sicherung des freien Datenverkehrs zwischen den Mitgliedsländern der EU und Staaten außerhalb der EU, die Mitglieder des EWR sind, wobei gilt, dass die Bedingungen der Datenübertragung nach außerhalb des polnischen Hoheitsgebietes gemäß Kapitel 7 des Gesetzes ausschließlich für den Transfer personenbezogener Daten an Drittländer, mit anderen Worten an Länder, die nicht im europäischen Wirtschaftsraum liegen, gelten;
- Begrenzung des subjektiven Geltungsbereichs des Gesetzes in der Weise, dass Personen ausgenommen sind, die ihren (Wohn-)Sitz in einem Drittland haben und technische Systeme innerhalb des polnischen Hoheitsgebietes nur zum Datentransfer einsetzen;
- Begrenzung der Anwendbarkeit der Bestimmungen des Gesetzes, wenn sich die Datenverarbeitung auf journalistische, literarische oder künstlerische Tätigkeiten bezieht, soweit nicht die Ausübung der Meinungsfreiheit und die Verbreitung der Informationen eine schwere Verletzung der Rechte und Freiheiten der betroffenen Person darstellen.
- Einführung der Verpflichtung für die für die Datenverarbeitung Verantwortlichen, die einen Firmen- oder Wohnsitz im Drittland haben und Daten auf dem Hoheitsgebiet der Republik Polen verarbeiten, einen Stellvertreter in der Republik Polen zu bestellen.
- Einführung der so genannten Vorprüfung der Datenverarbeitungsgenauigkeit, nach der die für die Verarbeitung vertraulicher Daten Verantwortlichen, die unter Art. 27 §1 des Gesetzes genannt werden, die Verarbeitung in einem Dateisystem erst nach einer Registrierung des Dateisystems aufnehmen dürfen, sofern sie nicht von der Verpflichtung zur Anzeige und Registrierung eines Dateiensystems nach dem Buchstaben des Gesetzes befreit sind.

Zudem wurde der Generalinspektor im Rahmen der Änderung dazu ermächtigt, bei einer Zuwiderhandlung gegen die Datenschutzbestimmungen die Anordnung zur Wiederherstellung des gesetzlichen Zustandes nicht nur dem für die Datenverarbeitung Verantwortlichen, sondern allen Personen zu erteilen, die personenbezogene Daten verarbeiten. Der Umfang der verfügbaren Informationen im offenen Register der Dateiensysteme, das vom Generalinspektor geführt wird, ist begrenzt (so gibt es keine Informationen über technische und organisatorische Schutzmaßnahmen), jedoch wurde das Problem der Notifizierung von Änderungen an Informationen, die in der Notifizierung des zu registrierenden Dateisystems vorgenommen wurden, beseitigt.

Infolge der Änderungen, die am Datenschutzgesetz vorgenommen wurden, wurden am 1. Mai 2004 die nachstehenden Durchführungsgesetzbestimmungen eingeführt:

- Verordnung vom 29. April 2004 des Ministers des Innern und für Verwaltungsfragen bezüglich der Modelle für die Notifizierung von Dateisystemen beim Generalinspektor für den Datenschutz (Anzeiger Nr. 100, Punkt 1025);
- Verordnung vom 22. April 2004 des Ministers des Innern und für Verwaltungsfragen bezüglich der Modelle für persönliche Genehmigungen und Betriebsausweise der Inspektoren des Büros des Generalinspektors für den Datenschutz (Anzeiger Nr. 94, Punkt 923);
- Verordnung vom 29. April 2004 des Ministers des Innern und für Verwaltungsfragen bezüglich der Dokumentation zur Datenverarbeitung und der technischen und organisatorischen Bedingungen, die Datenverarbeitungssysteme zu erfüllen haben (Anzeiger Nr. 100, Punkt 1024).

Die letztgenannte Verordnung führte spezifische Sicherheitsebenen für die Verarbeitung personenbezogener Daten mithilfe von Computersystemen ein.

Es gilt mindestens die Basis-Sicherheitsebene, wenn keine vertraulichen Daten (Art. 27 des Gesetzes) mithilfe eines Computersystems verarbeitet werden und keines der Computersysteme, die für die Datenverarbeitung eingesetzt werden, ans öffentliche Netz angeschlossen ist.

Es gilt mindestens die mittlere Sicherheitsebene, wenn Daten entsprechend Artikel 27 mithilfe des Computersystems verarbeitet werden und keines der Computersysteme für die Datenverarbeitung ans öffentliche Netz angeschlossen ist.

Es gilt die hohe Sicherheitsebene, wenn zumindest eines der Computersysteme, die für die Datenverarbeitung eingesetzt werden, ans öffentliche Netz angeschlossen ist.

Am 16. Juli 2004 wurde das neue Telekommunikationsgesetz eingeführt (Anzeiger Nr. 171, Punkt 1800) und trat am 3. September in Kraft. Das Gesetz hat die vollständige Umsetzung u. a. der Forderungen der Richtlinie 2002/58/EG des Europäischen Parlamentes und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Datenschutz im Bereich der elektronischen Kommunikation im polnischen Rechtssystem zum Ziel .

2004 wurde auf die Ratifizierung des Zusatzprotokolles der Konvention Nr. 108 des Europarates durch die polnische Republik hingearbeitet. Die Ratifizierung durch den Präsidenten der polnischen Republik wird voraussichtlich im Jahre 2005 vorgenommen werden.

B. Bedeutende Rechtsprechung

Am 13. Juli 2004 stellte das Verfassungsgericht die Diskrepanz zwischen der Verfassung und bestimmten Regeln des Gesetzes vom 23. November 2002 zur Abänderung des Gesetzes über die kommunale Selbstverwaltung und zur Abänderung einiger anderer Korruptionsschutzgesetze fest. Das Gesetz verlangte von Beratern und Beauftragten in den ausführenden Gremien der territorialen Selbstverwaltungseinheiten (stellvertretender Bürgermeister, Schatzmeister und Direktoren von organisatorischen Einheiten von Selbstverwaltungen) eine schriftliche Erklärung über die beruflichen Tätigkeiten des Ehepartners, der Nachkommen, Vorfahren und Geschwister. Diese Erklärung ist öffentlich.

Nach Ansicht des Verfassungsgerichtes ist die Offenlegung von Informationen über Nachkommen, Vorfahren und Geschwister nicht unabdingbar für die angemessene Funktionsweise des demokratischen Rechtsstaates, d.h. es besteht eine Verletzung des Verfassungsgrundsatzes der Verhältnismäßigkeit (Art. 31 der Verfassung der Republik Polen) im Zusammenhang mit dem

rechtsstaatlichen Prinzip der Demokratie (Artikel 2). Außerdem kann die Offenlegung der laut dem betreffenden Gesetz erforderlichen Informationen die Privatsphäre von Personen verletzen, die keine öffentlichen Aufgaben wahrnehmen (Art. 47 der Verfassung).

Das Verfassungsgericht hat die Ehepartner von Beamten der territorialen Selbstverwaltungseinheiten getrennt behandelt, weil das Leben unter einem Dach (und oftmals in einer Gütergemeinschaft) die Situation hervorrufen kann, dass das Einkommen jedes Ehepartners das Einkommen eines Beamten der territorialen Selbstverwaltung sein kann. Mangels Initiative des Beauftragten für den Schutz der bürgerlichen Rechte äußerte das Verfassungsgericht keinen Standpunkt mit Bezug auf das Problem des öffentlichen Zugangs zu den erwähnten Einkommenserklärungen.

Am 25. August 2004 verwarf das Warschauer Verwaltungsgericht der Provinz den Beschluss des Generalinspektors zur Streichung der personenbezogenen Daten des Schuldners bei der Kreditinformationsagentur (BIK S.A.) nach Beendung des Vertrages. Die Banken und die Kreditinformationsagentur rechtfertigten die Praxis der Verwahrung der Schuldnerdaten nach der vollständigen Tilgung der Schuld mit vertraglichen und obligatorischen Regeln bezüglich der Datensammlung und der Veröffentlichungspflicht seitens der Agentur. Entsprechend diesen Verordnungen ist die Agentur dazu verpflichtet, die ihr von der Bank übermittelten Daten fünf Jahre lang aufzubewahren (fünf Jahre ab der Schließung des Kontos, wenn das Konto keine Außenstände von über 30 Tagen aufweist) bzw. 7 Jahre (ab dem Tage der Schließung des Kontos, wenn das Konto Außenstände von über 30 Tagen aufweist). Das Gericht schloss sich der Meinung des Generalinspektors an, laut der die Regeln das verpflichtende Gesetz nicht enthalten und somit die Rechte und Pflichten der Bankkunden nicht darin verankert sind.

In der Rechtsprechung des Obersten Verwaltungsgerichtes gab es einen Fall bezüglich des Umfangs personenbezogener Daten, die von den Banken im Rahmen eines Kreditvertrages verarbeitet werden dürfen. In diesem Fall vertrat das Oberste Verwaltungsgericht den Standpunkt, dass es zulässig sei, dass der Generalinspektor die Verhältnismäßigkeit des Umfangs der von Banken gesammelten Daten festlegt.

Am 13. Juli 2004 verkündete das Oberste Verwaltungsgericht ein Urteil im Zusammenhang mit der Berufung des Generalinspektors gegen ein früheres Urteil einer anderen Abteilung desselben Gerichtes über die Entscheidung des Generalinspektors, dass die Bank es zu unterlassen hat, private Daten von Kopien von Ausweisen zu verarbeiten mit dem Ziel, Informationen über das Aussehen, Namen, frühere Wohnsitze, Kinder und andere Menschen, die von der betroffenen Person betreut werden, oder über die Löschung aus dem Schuldnerregister zu gewinnen.

Das Oberste Verwaltungsgericht lehnte die letzte Berufung des Generalinspektors unter Vorbringung der Argumente der ersten Gerichtsinstanz ab, dass es nämlich nicht hingenommen werden könne, dass die Datenschutzbehörde bei der Erstellung des Kataloges der verarbeitungsfähigen personenbezogenen Daten bei einer Krediteröffnung an die Stelle des Gesetzgebers tritt. Mit anderen Worten: Wenn es keine spezielle Regelung bezüglich des Umfangs der personenbezogenen Daten gibt, kann die Datenschutzbehörde nicht bestimmen, ob die Daten angemessen sind.

C. Wichtige spezifische Themen

Per Gesetz vom 1. April 2004 zur Abänderung des Bankengesetzes wurde der Artikel 112b zu den Bestimmungen des Bankengesetzes hinzugefügt. Dieser Artikel erlaubt es Banken, personenbezogene Daten Ausweisen zu entnehmen, indem sie die Ausweise kopieren.

Die bisherige Verfahrensweise der Banken, d.h. das Kopieren von Unterlagen zur Identitätsbestätigung eines Kunden, wurde in den Protokollen des Generalinspektors beanstandet, weil die gesetzliche Grundlage für diese Praxis fehlet. Zurzeit dürfen laut den Bestimmungen des Gesetzes zur Änderung des Bankengesetzes die Banken Daten von Ausweisen natürlicher Personen ausschließlich für ihre Banktätigkeiten verwenden. Die Erfassung der Daten dieser Dokumente durch die Banken ist entsprechend dem Datenschutzgesetz, dem die Verarbeitung personenbezogener Daten unterworfen ist (Artikel 23 §1 und 2), zulässig.

2004 befasste sich der Generalinspektor wiederholt mit dem Problem der Bereitstellung von Schuldnerdaten an Inkassofirmen, die mit der Beitreibung einer Forderung beauftragt wurden. Sehr oft agierten diese Firmen am Rande des Gesetzes, indem sie Schuldner einschüchterten oder nach Belieben ihre Honorare änderten.

Vom Standpunkte des Datenschutzgesetzes aus betrachtet ist die Legalität der Datenverarbeitung durch Inkassofirmen von oberster Bedeutung.

Die Forderungsabtretung ist in Art. 509 ff des Gesetzes vom 23. April 1964 (Bürgerliches Gesetzbuch – Anzeiger Nr. 16, Punkt 93) geregelt. In diesem Fall können auch die Verbraucherschutzregelungen angewandt werden, und zwar im Anwendungsbereich der so genannten Missbrauchsklausel. Nach Artikel 385 §5 des Bürgerlichen Gesetzbuches ist es der Vertragspartei untersagt, die Rechte und Pflichten eines Verbrauchers ohne dessen Zustimmung zu übertragen. Der Vorsitzende des Verbraucher- und Wettbewerbsschutzamtes nahm die Haltung ein, dass unter Berücksichtigung der Realität des Geschäftsverkehrs die Praxis der Forderungsabtretung an Inkassogesellschaften „die Sicherheiten und Rechte der Verbraucher schmälert".

Nach Maßgabe des Vorhergehenden vertrat der Generalinspektor wiederholt den Standpunkt, dass die Zurverfügungstellung von Daten von Verbrauchern im Zusammenhang mit einer Forderungsabtretung ausschließlich mit der Zustimmung der betroffenen Person möglich ist. In dem Fall kann keine der verbleibenden Legalitätsvoraussetzungen laut Artikel 23 §1 des Datenschutzgesetzes angewandt werden.

Die Fälle von Datenverarbeitungen im Zusammenhang mit Forderungsabtretungen waren Gegenstand von Verhandlungen vor dem Verwaltungsgerichtshof der Woiwodschaft in Warschau sowie vor dem Obersten Verwaltungsgericht. Es muss dabei unterstrichen werden, dass diese Fälle in der Rechtsprechung der Verwaltungsgerichte höchst widersprüchlich behandelt werden.

Im Jahre 2004 und in den Jahren davor behandelte der Generalinspektor viele Klagen über Direktmarketinggesellschaften. Diese Einrichtungen hatten ein Problem mit dem Beweis der Legalität der Datenverarbeitung oder mit der Informationspflicht gegenüber den Personen, deren Daten sie verarbeiteten. In diesen Fällen versuchten viele für die Datenverarbeitung Verantwortliche, die polnischen Datenverarbeitungsbestimmungen zu umgehen, indem sie (zumindest formal) die Datenverarbeitung in anderen Ländern (Vereinigte Staaten oder Zypern) durchführten. Wegen des begrenzten Zugangs zu den Direktmarketingfirmen zeigte der Generalinspektor Letztere bei den Strafverfolgungsbehörden an.

Portugal

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

Das Gesetz 43/2004 vom 18. August beinhaltet spezifische Regeln der Organisation und Arbeitsweise der Datenschutzbehörde und liefert einen autonomen Rahmen für das Personal. Er bietet der Behörde die Möglichkeit, eine Gebühr für Anzeigen und den Verkauf von Veröffentlichungen und Formularen zu erheben. Der selbständige Statuts der Mitglieder bzw. Beauftragten und die administrative Autonomie bleiben unverändert.

Die Richtlinie 2002/58/EG wurde durch zwei unterschiedliche Rechtsmittel in nationales Recht übertragen:

- Gesetzesdekret 7/2004 vom 7. Januar zur Übertragung der e-Commerce-Richtlinie und des Art. 13 der Richtlinie über elektronische Kommunikation;
- Gesetz 41/2004 vom 18. August zur Übertragung der Richtlinie.

Das Gesetzesdekret 35/2004 vom 21. Februar über den Einsatz der Videoüberwachung zum Schutz von Personen und Gütern schafft die gesetzliche Grundlage für die Genehmigung der Videoüberwachung zu diesem Zweck, unbeschadet der obligatorischen Fall-zu-Fall-Beurteilung, insbesondere der Beurteilung der Verhältnismäßigkeit.

Das Gesetz 35/2004 vom 29. Juli regelt die Arbeitsgesetzgebung. Vor der Verarbeitung personenbezogener Daten durch die Biometrietechnik oder durch Videoüberwachung am Arbeitsplatz muss die Meinung des Betriebsrates eingeholt werden.

B. Bedeutende Rechtsprechung

Gegen Beschlüsse der Datenschutzbehörde kann beim Verwaltungsgericht oder Strafgericht (Schnellverfahren) Berufung eingelegt werden, wenn Strafen verhängt wurden. 2004 gab es vier Gerichtsbeschlüsse bezüglich der Auferlegung von Bußgeldern. Drei hielten den Beschluss des Amtes aufrecht, eines senkte das Strafmaß von einem Bußgeld auf eine Verwarnung.

Ein interessanter Fall betraf die Weitergabe von Kundendaten durch einen Telekombetreiber ohne Zustimmung der Kunden an einen Dritten, der hieraus Kundenprofile erstellte und zu kommerziellen Zwecken verwendete.

Ein weiterer Fall betraf eine Website mit einer Liste von Namen und Fotos angeblicher Schuldner und geplatzter Schecks.

C. Wichtige spezifische Themen

RFID

Die portugiesische Datenschutzbehörde erließ eine Empfehlung zur Verarbeitung personenbezogener Daten durch Funkidentifizierung. Die Behörde befand, dass es sich um eine Verarbeitung personenbezogener Daten handelt, wenn der RFID-Einsatz die Verknüpfung mit persönlichen Informationen mit sich bringt. Folglich muss diese Datenverarbeitung der Datenschutzbehörde gemeldet werden. Die Daten müssen zu eindeutigen und legitimen Zwecken gesammelt werden und dürfen nicht zu anderen Zwecken verwendet werden. Die Daten müssen adäquat, stichhaltig und auf das strikt Notwendige beschränkt sein. Sie müssen auf eine transparente Art und Weise gesammelt werden, wobei der betroffenen Person das Recht auf Information einzuräumen ist. Der für die Datenverarbeitung Verantwortliche hat auf den Produkten und in den Räumen, in denen die RFID-Technik angewandt wird, einen entsprechenden Hinweis anzubringen.

Bei jeder Fernaktivierung oder Ferneinlesung muss die betroffene Person vorher informiert werden. Die personenbezogenen Daten müssen gelöscht werden, sobald sie nicht mehr dem angegebenen Zweck dienen, ebenso jede Verknüpfung, die inzwischen hergestellt wurde. Dieses Dokument steht auf Portugiesisch auf unserer Website: http://www.cnpd.pt/bin/decisoes/2004/htm/del/del009-04.htm

Biometrische Daten

Die portugiesische Datenschutzbehörde erließ einige Richtlinien für die Benutzung biometrischer Daten am Arbeitsplatz für die Zugangskontrolle und aus dienstlichen Gründen. Eine englische Version des Dokuments steht auf unserer Website: http://www.cnpd.pt/english/bin/guidelines/guidelines.htm

Videoüberwachung

Die Datenschutzbehörde erließ die allgemeinen Grundsätze für die Videoüberwachung unter Berücksichtigung des erneuerten gesetzlichen Rahmens in dieser Materie. Legitimät, die Ausübung des Zugangsrechtes sowie die Registrierung bei Justizbehörden wurden in diesem Papier behandelt. Es ist in portugiesischer Fassung unter http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm nachzulesen.

Die Datenschutzbehörde befasste sich mit einem spezifischen Fall bezüglich der Videoüberwachung in Kindergärten in beinahe jedem Raum, so dass die Eltern im Internet nach Eingabe eines Kennwortes den Alltag ihrer Kinder im Kindergarten verfolgen konnten. Die Behörde untersagte diese Datenverarbeitung wegen ihres nicht angemessenen Charakters, weil sie das Recht der Kinder auf Privatsphäre verletzte und weil das Personal unter ständiger Überwachung stünde.

Audit bei Krankenhäusern

Die portugiesische Datenschutzbehörde führte 2004 bei 38 öffentlichen und privaten Krankenhäusern überall im Land ein gründliches Audit durch. Das allgemeine Ziel war ein Einblick in die Verarbeitung von Gesundheitsdaten und die Einhaltung der Rechte der betroffenen Personen. Die internen Informationsübermittlungsverfahren innerhalb der Krankenhäuser, die Ebenen des Informationszugangs, die Analyseanfragen und die Sammlung von Informationen, der Zugang zur individuellen Krankenakte des Patienten, Telemedizinerfahrungen, Videoüberwachung usw. waren die wichtigsten Auditthemen. Die Datenschutzbehörde erstellte ein Auditprotokoll mit spezifischen Schlussfolgerungen und Empfehlungen und schickte es an die beteiligten Krankenhäuser, ans Parlament, an die Regierung und an Berufs- und Fachverbände. Das Protokoll kann auf unserer Website in portugiesischer Sprache abgerufen werden: http://www.cnpd.pt/bin/relatorios/outros/Relatorio_final.pdf

Europameisterschaft 2004

Die Datenschutzbehörde spielte eine sehr aktive Rolle und überwachte die Organisation der Europameisterschaft sehr genau. Es wurde hierbei eine große Fülle von Daten verarbeitet. Dies wurde von der Datenschutzbehörde ordnungsgemäß registriert und genehmigt. Die Organisation der Euro 2004 schickte regelmäßig Protokolle an die Datenschutzbehörde.

E-Abstimmung

Die Datenschutzbehörde autorisierte und überwachte vor Ort den ersten Pilotversuch der elektronischen Abstimmung bei den Wahlen zum Europaparlament. Es war eine unverbindliche persönliche Wahl, die an neun verschiedenen Orten durchgeführt wurde. Nach der herkömmlichen Abstimmung konnte der Wähler auf freiwilliger Basis das elektronische Verfahren testen.

Slowakische Republik

Die Slowakische Republik wurde am 1. Mai 2004 Mitglied der Europäischen Union. Offizieller Name der Datenschutzbehörde (Ges. 428/2002 Coll. über den Datenschutz, abgeänderte Fassung, in Kraft seit 1. Mai 2005):

- Datenschutzbehörde der Slowakischen Republik (vormals einfach „Datenschutzbehörde").

Herr Gyula Veszelei ist Vorsitzender der Datenschutzbehörde der Slowakischen Republik.

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

Umsetzung der Richtlinie 95/46/EG

Gemäß dem Plan für die gesetzgebenden Aufgaben der slowakischen Regierung für 2004 bereitete die Datenschutzbehörde einen Gesetzentwurf vor, der das Gesetz 428/2002 Coll. über den Datenschutz abändert. Im September 2004 verabschiedete das slowakische Kabinett in seiner 101. Sitzung seine Resolution Nr. 895 und genehmigte somit den Gesetzentwurf. Der Gesetzentwurf wurde dem slowakischen Nationalrat am 30. September 2004 unterbreitet und am 3. Februar 2005 verabschiedet. Der Präsident der slowakischen Republik unterzeichnete das Gesetz am 28. Februar 2005. Das Gesetz wurde im Staatsanzeiger als das Gesetz Nr. 90/2005 Coll. veröffentlicht und trat am 1. Mai 2005 in Kraft (im Folgenden die „Euro-Gesetzesänderung").

Das Ziel dieser Euro-Gesetzesänderung war die Erfüllung des Inhaltes des Beurteilungsprotokolls der Europäischen Kommission vom November 2003, des umfassenden Begleitungsprotokolls über die Beitrittsvorbereitungen der slowakischen Republik, die zur vollständigen Harmonisierung des Datenschutzgesetzes mit der Richtlinie des Parlamentes und des Rates 95/46/EG über den Schutz von Einzelpersonen im Rahmen der Datenverarbeitung und über den freien Verkehr solcher Daten (im Folgenden als die Richtlinie 95/46/EG bezeichnet) führen sollen. Im Beurteilungsprotokoll steht die klare Aufforderung an die slowakische Republik, unverzüglich den Anforderungen der Europäischen Kommission gerecht zu werden, damit ihr Überwachungsgremium im Bereich des Datenschutzes über Untersuchungs- und Interventionsrechte verfügt und seine Aufgaben vollkommen unabhängig nicht nur von der Exekutive, sondern auch von anderen staatlichen Stellen ausüben kann. Unabhängigkeit wurde auch im Finanzbereich und in der Personalpolitik erwartet, die ausschließlich Sache des Vorsitzenden des Büros sein soll.

Die Euro-Änderung berücksichtigte auch Kommentare der Europäischen Kommission.

Die Hauptgrundsätze der verabschiedeten Änderung:

- Verdeutlichung einiger Konzepte und Umsetzung neuer Konzepte im Einklang mit dem Inhalt der Richtlinie 95/46/EG,
- Anwendung der Artikel der Konvention 108 und der Empfehlungen des Europäischen Rates hinsichtlich des Datenschutzbereiches,
- Angabe und Verdeutlichung der Grundpflichten des für die Datenverarbeitung Verantwortlichen,
- Beschränkte schriftliche Registrierung von Informationssystemen im Kontext der Stärkung der Position eines delegierten Verantwortlichen in Übereinstimmung mit der Richtlinie 95/46/EG,
- Einführung einer speziellen Registrierung bestimmter riskanter Operationen gemäß der Richtlinie 95/46/EG,
- Beschreibung des Prozesses der Verarbeitung und Annahme von Notifizierungen natürlicher Personen,
- Verdeutlichung von Bestimmungen über die grenzüberschreitende Übermittlung personenbezogener Daten in Drittländer und innerhalb der EU.

Der Gesetzesänderungsentwurf, der den einzelnen Ressorts zur Überprüfung zugeleitet wurde, trug dem letzten Beurteilungsprotokoll der Europäischen Kommission vom November 2003 Rechnung, auch in dem Abschnitt, in dem es darum

geht, dass die slowakische Republik die Forderung der Europäischen Kommission zu erfüllen hat, dass die Überwachungsinstanz auf dem Gebiet des Datenschutzes – die Datenschutzbehörde – das Recht haben muss, ihre Aufgaben in voller Unabhängigkeit nicht nur von der ausführenden Gewalt, sondern auch von anderen staatlichen Instanzen auszuüben. Diese Unabhängigkeit wurde auch erwartet bei der Finanzierung der Tätigkeit der Datenschutzbehörde und der Personalpolitik, die ausschließlich Sache des Vorsitzenden der Datenschutzbehörde sein sollte. Der Artikel 1 §3 des Zusatzprotokolls zur Konvention 108 verpflichtet die Parteien der Konvention dazu, den mit dem Datenschutz betrauten Aufsichtsbehörden in den einzelnen Staaten eine solche Position einzuräumen – wir zitieren: „Die Aufsichtsbehörden üben ihre Funktionen in vollkommener Unabhängigkeit aus". Die gleiche Forderung steht in Artikel 28 §1 der Richtlinie 95/46/EG.

Die völlig unabhängige Position der Datenschutzbehörde, die am Schutz der Grundrechte und Grundfreiheiten des Einzelnen mitwirkt, wenn es um die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre geht, kann übereinstimmend mit der verfassungsmäßigen Ordnung der slowakischen Republik sichergestellt werden, wie sie soeben in der slowakischen Verfassung festgelegt wurde. Deshalb muss die Datenschutzbehörde denjenigen Behörden zugerechnet werden, deren Unabhängigkeit die slowakische Verfassung bekräftigt. Im Zusammenhang mit den erwähnten Forderungen der Europäischen-Kommission bereitete die Datenschutzbehörde diese in Form eines Gesetzentwurfs vor und unterbreitete diesen im Januar 2004 dem Vorsitzenden des slowakischen Nationalrates. Mit diesem Gesetzentwurf sollte die Datenschutzbehörde als individuelle staatliche Behörde in der slowakischen Verfassung verankert werden. Das Amt hielt diesen Gesetzentwurf nicht mehr aufrecht, nachdem der Verfassungsänderungsentwurf verworfen worden war.

Das Gesetz 576/2004 Coll. über das Gesundheitswesen, Gesundheitsdienstleistungen und über die Abänderung und Ergänzung bestimmter Gesetze bewirkte eine so genannte indirekte Änderung des Datenschutzgesetzes.

Das Gesetz trat am 1. Januar 2005 in Kraft. Es betrifft den Abschnitt 9 des Gesetzes Nr. 428/2002 Coll. (Befreiung von Einschränkungen bei der Verarbeitung besonderer Kategorien von personenbezogenen Daten). Die Datenschutzbehörde lehnte diese Änderungen bei der ressortübergreifenden Überprüfung ab und verlangte, dass sie nicht in dieser Form ins Datenschutzgesetz integriert würden, weil die Änderung in Form einer vorbereiteten Euro-Abänderung erwartet wurde, wie sie vom Sachverständigen der Europäischen Kommission vorgeschlagen wurde.

Das slowakische Gesundheitsministerium bereitete trotz dieser klaren Forderung der Datenschutzbehörde die indirekte Änderung des Gesetzes Nr. 428/2002 Coll. über den Datenschutz vor, das durch das Gesetz Nr. 602/2003 Coll. abgeändert wurde, und setzte diese ohne die Beteiligung des Amtes durch.

Umsetzung der Richtlinie 2002/58/EG

Angesichts der Tatsache, dass die Richtlinie 2002/58/EG die Rechte und Pflichten im Rahmen des Datenschutzes speziell für den Bereich der elektronischen Kommunikation festlegt, wurde sie innerhalb des neuen Verordnungspakets für die elektronische Kommunikation ins Gesetz Nr. 610/2003 über die elektronische Kommunikation integriert. Die Zuständigkeit für diese Richtlinie liegt beim Minister für das Verkehrs-, Post- und Fernmeldewesen der slowakischen Republik.

Das Gesetz über die elektronische Kommunikation trat am 1. Januar 2004 in Kraft. Die Slowakei hat somit ihre Verpflichtung, die slowakische Gesetzgebung zu harmonisieren, rechtzeitig erfüllt. Der Datenschutz und der Schutz der Privatsphäre sind im vierten Abschnitt des Gesetzes geregelt. Die Verpflichtungen von Unternehmen zum Schutz der Privatsphäre und die Fragen zu unerwünschten Mitteilungen sind ebenfalls in diesem Teil enthalten. Das Gesetz weist

u. a. dem Fernmeldeamt der slowakischen Republik die Rolle einer nationalen Regelungsbehörde für das elektronische Kommunikationswesen sowie die Befugnis zu, Sanktionen zu verhängen, wenn die gesetzlichen Verpflichtungen nicht erfüllt werden.

Die Europäische-Kommission hat die vollständige Umsetzung der Richtlinien mit den neuen Verordnungen in der slowakischen Gesetzgebung geprüft. In diesem Kontext stellte die Kommission einige Mängel im zehnten Umsetzungsprotokoll (Regulierung und Märkte des europäischen Kommunikationswesens 2004) über die Gesetze über die elektronische Kommunikation fest, die im November 2004 erlassen wurden. Zu Beginn des Jahres 2005 schickte die EU-Kommission eine offizielle Notiz über die unvollständige Übertragung der Richtlinie 2002/58/EG. Die Notiz bezog sich auf fehlende Bestimmungen zu „Cookies" und auf unvollständige Bestimmungen zu unerwünschten Mitteilungen. Die slowakische Republik hat innerhalb der gestellten Frist geantwortet und eine Lösung vorgeschlagen. Derzeit wird die Abänderung des Gesetzes über die elektronische Kommunikation vorbereitet und werden alle fehlenden Bestimmungen in dieses Gesetz eingefügt Die Änderung befindet sich im Gesetzgebungsverfahren und wird voraussichtlich am 1. Januar 2006 in Kraft treten.

B. Bedeutende Rechtsprechung

Da es in der slowakischen Republik kein Präzedenzfall-/Entscheidungsrecht gibt, stellen wir einige Fälle vor, die unserer Ansicht nach typisch für Beitrittsbewerberländer oder neue Mitgliedstaaten der Europäischen Union sind.

Ungesetzliche Veröffentlichung personenbezogener Daten

Der Kläger hatte sich als Richter für das Sondergericht beworben. Klagegegenstand war der Verdacht auf unerlaubte Weitergabe von Informationen über den Umstand, dass das Nationale Sicherheitsamt die Sicherheitsüberprüfung für die betroffene Person nicht abgeschlossen hatte. Mit solchen Überprüfungen wird untersucht, ob ein Kandidat die gesetzlichen Voraussetzungen für den Umgang mit geheimhaltungsbedürftigen Informationen erfüllt. Der Grund waren angeblich Probleme mit dem Nachweis des Eigentumsursprungs. Die Meldung über die Sicherheitsüberprüfung beim Kläger wurde von einem privaten Fernsehsender in den Hauptnachrichten ausgestrahlt. Daten wie Name, Vorname, Arbeitgeber und Position können im Zusammenhang mit diesem Verfahren als persönliche Daten betrachtet werden.

Gemäß dem Gesetz Nr. 215/2004 Coll. über den Schutz vertraulicher Informationen und über die Änderung und Ergänzung bestimmter Gesetze ist die Nationale Sicherheitsbehörde dazu verpflichtet, den Schutz registrierter Daten vor unerlaubter Verwendung gemäß Gesetz Nr. 428/2002 Coll. über den Datenschutz zu gewährleisten.

Dies sowie die oben erwähnten Fakten zeigen, dass Informationen über die Sicherheitsüberprüfung des Klägers nicht offiziell vom Nationalen Sicherheitsamt angekündigt (veröffentlicht) und genehmigt worden waren.

Wahrscheinlicher ist, dass die Informationen dem Fernsehen von einer Person zugespielt wurden, die diese Daten direkt aus der Datei des Nationalen Sicherheitsamtes entnommen hatte oder von jemand anderem, der Zugang zu diesen Informationen hatte und hiervon Kenntnis erhalten hatte.

Nach Meinung der Datenschutzbehörde besteht der begründete Verdacht, dass ein Unbekannter Daten unbefugterweise offen gelegt hatte oder Daten über den Kläger im Zusammenhang mit seiner Sicherheitsüberprüfung beim Nationalen Sicherheitsamt der unbekannten Person zugänglich gemacht hatte. Dieser Unbekannte machte sich dadurch bestimmter gesetzwidriger Handlungen schuldig.

Gemäß Kapitel 38 §1 j) des Gesetzes Nr. 428/2002 Coll., gefolgt von Kapitel 38 §2 desselben Gesetzes, legt der Vorsitzende der Datenschutzbehörde den Vollzugsorganen eine entsprechende Mitteilung vor, wenn der Verdacht auf einen Gesetzesverstoß besteht.

Ausgehend von den mitgeteilten Fakten zeigte die Behörde den Strafermittlungsbehörden den Verdacht auf einen Gesetzesverstoß an.

Unerlaubter Umgang mit personenbezogenen Daten von Betroffenen (Verwitweten) – Rechtsnachfolger/Erben.

Anfang Juli 2003 wurde bei der Datenschutzbehörde eine Beschwerde gegen eine Aktiengesellschaft in Bratislava eingereicht. Beschwerdeführer war ein privates Forschungsinstitut in Bratislava. Gegenstand der Beschwerde war der Verdacht, dass die Aktiengesellschaft das Datenschutzgesetz verletzt hatte und personenbezogene Daten ohne gesetzliche Grundlage verarbeitete. Diese Tätigkeiten standen im Zusammenhang mit der Verarbeitung personenbezogener Daten der Betroffenen (zertifizierte Sachverständige). Gegenstand der Verarbeitung waren personenbezogene Daten (Titel, Name, Vorname, Adresse und Ergebnisse von theoretischen und praktischen Prüfungen sowie Prüfungsprotokolle).

Der Beschwerde zufolge war ein privates Forschungsinstitut, das die Beschwerde einreichte, Rechtsnachfolger der staatlichen Organisation geworden, die sich ebenfalls mit Schulungen und Zertifizierungen von Sachverständigen befasste.

Die Datenschutzbehörde, die nachprüfte, wie die personenbezogenen Daten übermittelt und verarbeitet wurden, fand heraus, dass eine Aktiengesellschaft die personenbezogenen Daten ohne Rechtsgrundlage verarbeitete und daher gegen Kapitel 7 §1 und §3 des Datenschutzgesetzes verstieß (Verstoß gegen Artikel 7 a) und Artikel 7 c) der Richtlinie 95/46/EG). Die Aktiengesellschaft war nicht Rechtsnachfolger der sich in staatlichem Besitz befindenden Organisation geworden und war deshalb nicht zur Dokumentation von zertifizierten Mitarbeitern berechtigt. Dies bedeutet, dass sie die Dokumentation nicht wie ein für die Datenverarbeitung Verantwortlicher hätte behandeln dürfen, der dazu laut Sondergesetz Nr. 264/1999 Coll. über die technischen Produktanforderungen und die Konformitätsbeurteilung und laut später abgeänderten Verordnungen bestellt wurde. Die Aktiengesellschaft konnte bei der Durchführung von Kontrollen nicht den Nachweis über die Zustimmung der Betroffenen – von zertifiziertem Personal - erbringen, weil kein einzelner Betroffener die Aktiengesellschaft um die Ausstellung von Zertifikaten gebeten hatte und ihre Protokolle weder einzeln noch gemeinsam eingereicht hatte.

Angesichts des Umstandes, dass im Laufe der Ermittlungen ein Verstoß eines ehemaligen Angestellten der staatlichen Organisation festgestellt wurde, hielt die Datenschutzbehörde sich an Kapitel 38 §1 j) des Datenschutzgesetzes und informierte die Strafverfolgungsbehörden über den Verstoß einer bestimmten Person entsprechend den Abschnitten 257a und 178 des Strafgesetzbuches. Abschnitt 257a des Strafgesetzbuches legt die Bestrafung der betreffenden Person fest, die nachweislich vorsätzlich die auf dem Informationsträger befindliche Liste zweckentfremdet hat, und Abschnitt 178 des Strafgesetzbuches bestimmt die Bestrafung der betreffenden Person, die nachweislich personenbezogene Daten, die sie in der Ausübung ihres Berufes, im Rahmen ihrer Beschäftigung oder in ihrem Büro zusammengetragen hat, zugänglich gemacht und somit Vertrauensmissbrauch begangen hat.

C. Wichtige spezifische Themen

Beschwerde über die Datenverarbeitung beim Landesarchiv der slowakischen Republik

Im Laufe des Jahres 2004 regelte die Datenschutzbehörde die Beschwerde einer Betroffenen bezüglich der Datenverarbeitung beim Landesarchiv, einer öffentlichen Einrichtung, die durch das Gesetz über das Landesarchiv eingerichtet wurde. Laut diesem Gesetz besteht das Ziel der Einrichtung darin, Unterlagen über die Tätigkeiten der Staatssicherheitsdienste in den Jahren 1939-1989 zugänglich zu machen.

Die Betroffene brachte in ihrer Beschwerde vor, das slowakische Informationssystem habe eine persönliche Datei des Landesarchivs ohne ihre Genehmigung, ohne ihr Wissen und ohne ihre Zustimmung herausgegeben.

Laut Kapitel 7 §6 des Gesetzes Nr. 428/2002 Coll. können personenbezogene Daten nur geliefert, zugänglich gemacht oder veröffentlicht werden, wenn die Zustimmung der Betroffenen vorliegt. Diese Regel gilt nicht, wenn die Strafverfolgungsbehörden diese Daten für ihre Aufgabenerfüllung benötigen oder wenn personenbezogene Daten an ein Informationssystem auf der Grundlage eines getrennten Gesetzes geliefert werden, das eine Liste der personenbezogenen Daten, den Zweck ihrer Verarbeitung und die Bedingungen ihrer Lieferung, ihrer Zugänglichmachung oder Veröffentlichung festlegt oder wenn diese personenbezogenen Daten gesetzlichen Einheiten, natürlichen Personen oder Einheiten im Ausland geliefert oder zugänglich gemacht werden.

Ein solches Gesetz ist das Gesetz 553/2002 Coll. über die Freigabe von Dokumenten über die Tätigkeiten der Sicherheitsorgane des Staates in der Zeit von 1939 - 1989 und die Gründung des Landesarchivs, das bestimmte andere Gesetze abändert oder vervollständigt (im Folgenden „das Gesetz Nr. 553/2002 Coll"). Laut Kapitel 27 §1 des Gesetzes Nr. 553/2002 Coll. müssen der Innenminister der slowakischen Republik, der Verteidigungsminister der slowakischen Republik, das Justizministerium der slowakischen Republik und der slowakische Nachrichtendienst die Unterlagen über die Tätigkeiten der Sicherheitsbehörden, die sich in ihrem Besitz befinden, ihr Eigentum sind oder sich in ihrer Verwaltung befinden innerhalb von acht Monaten nach dem Inkrafttreten des Gesetzes an das Landesarchiv aushändigen. Daraus kann gefolgert werden, dass der slowakische Nachrichtendienst nicht gegen das Gesetz Nr. 428/2002 Coll. verstoßen hat, indem es Dateien über die Betroffene an das Landesarchiv weitergeleitet hat.

Der Beschwerdeführer protestierte in seiner Beschwerde ebenfalls dagegen, dass das Landesarchiv seine persönliche Akte ohne seine Genehmigung behandelt und vorsätzlich zurückbehält.

Der Beschwerdeführer bringt weiterhin vor, dass er das Landesarchiv um die Rückgabe seiner persönlichen Datei gemäß Kapitel 20 §1 e) des Gesetzes Nr. 428/2002 Coll. gebeten habe.

Der Zweck der Verarbeitung solcher personenbezogener Daten ist in Kapitel 1 b) des Gesetzes Nr. 553/2002 Coll. beschrieben. Es ist die Erfassung, Sammlung, Offenlegung, Veröffentlichung, Verwaltung und Benutzung der Unterlagen der Staatssicherheitsbehörden des Dritten Reiches und der Union der sozialistischen Sowjetrepubliken sowie der Sicherheitsbehörden des Staates, die in der Zeit zwischen dem 18. April 1939 und 31. Dezember 1989 (im Folgenden die „entscheidende Zeit") erzeugt und gesammelt wurden und Verbrechen gegen slowakische Staatsangehörige oder slowakische Bürger betreffen, die eine andere Staatsangehörigkeit besitzen.

Daraus folgt, dass die Rechte der Betroffenen entsprechend Kapitel 20 §1 e) des Gesetzes Nr. 428/2002 Coll. nach der Erfüllung des Zwecks der Verarbeitung personenbezogener Daten eingeklagt werden können. Im vorliegenden Fall war die Verarbeitung der personenbezogenen Daten nicht abgeschlossen. Deshalb war das Landesarchiv als für die Datenverarbeitung verantwortliche Instanz nicht befugt, die angeforderten Dateien zurückzugeben, sondern musste die personenbezogenen Daten der Betroffenen nach dem Gesetz 553/2002 Coll. weiterverarbeiten.

Empfang von personenbezogenen Daten, die für die Archivierung im Rahmen der Verarbeitung erforderlich sind, durch Kopieren, Scannen oder andere Aufzeichnung der amtlichen Dateien auf Trägern des öffentlichen Kommunikationssektors

2003 und 2004 gingen bei der Datenschutzbehörde mehrere Beschwerden über die Verarbeitung personenbezogener Daten bei Datenverwaltern ein, die im Telekommunikationssektor tätig sind.

Das Problem der Verarbeitung personenbezogener Daten im Telekommunikationsbereich wurde

geregelt per Gesetz 195/2000 Coll. über die Telekommunikation (im folgenden „Gesetz 195/2000 Coll."), an dessen Stelle das Gesetz. 610/2003 Coll. über elektronische Kommunikation (im Folgenden „Gesetz 610/2003 Coll.") trat und am 1. Januar 2004 in Kraft trat. Beide Gesetze wurden als getrennte Gesetze bei der Anwendung des Gesetzes Nr. 428/2002 Coll. betrachtet.

Gesetz 195/2000 Coll. enthielt nicht das, was laut Gesetz 428/2002 Coll. notwendig war. Trotzdem durften die für die Datenverarbeitung Verantwortlichen die personenbezogenen Daten von Betroffenen in dem Umfang behandeln, dass ein bestimmtes Ziel verwirklicht werden konnte, weil die Bestimmungen unter Kapitel 52 §2 des Gesetzes Nr. 428/2002 Coll. sie dazu berechtigten.

Das Gesetz 610/2003 Coll. enthielt die Aspekte, die laut dem Gesetz Nr. 428/2002 Coll. notwendig sind, nämlich eine Liste personenbezogener Daten, den Zweck ihrer Verarbeitung, die Bedingungen für den Empfang und den Kreis der Betroffenen. Weiterhin änderte das Gesetz die Datenverarbeitung in mehreren Bestimmungen.

Die Datenschutzbehörde befasste sich mit Anforderung und Kopieren amtlicher Dateien und der Anforderung anderer Unterlagen vor deren Weiterleitung an Telekommunikationsdienste.

Eine Prüfung ergab, dass der für die Datenverarbeitung Verantwortliche das Gesetz verletzt hatte.

Gesetz 428/2002 Coll., Kapitel 10 §6 bestimmt, dass „personenbezogene Daten, die für die Datenverarbeitung erforderlich sind, durch Fotokopieren, Scannen oder andere Arten der Aufzeichnung amtlicher Unterlagen auf einem Informationsträger nur mit schriftlicher Zustimmung der Betroffenen oder wenn ein Sondergesetz ausdrücklich die Gewinnung dieser Daten ohne Zustimmung der Betroffenen vorsieht, gewonnen werden dürfen. Weder der für die Datenverarbeitung Verantwortliche noch der Datenverarbeiter dürfen die Zustimmung der Betroffenen erzwingen oder von dieser Zustimmung eine Vertragsbeziehung, eine Dienstleistung, Güter oder die Erfüllung einer Verpflichtung des für die Datenverarbeitung Verantwortlichen oder des Datenverarbeiters, die im Gesetz verankert sind, abhängig machen."

Während der Prüfung wurde festgestellt, dass die vom für die Datenverarbeitung Verantwortlichen beauftragte Person gegen diese Bestimmung verstoßen hatte. Auch die Vorgehensweise des Datenverarbeiters bei der Gewinnung personenbezogener Daten im Rahmen dieses Vertrages aus den unterbreiteten Unterlagen und das Kopieren dieser Unterlagen ohne vorherige Zustimmung der Betroffenen zur Anfertigung von Kopien amtlicher Dokumente waren ungesetzlich. Gleichzeitig wurde festgestellt und bewiesen, dass der für die Datenverarbeitung Verantwortliche Kopien von amtlichen Dokumenten ohne schriftliche Zustimmung der Betroffenen angefertigt hatte.

Im Rahmen der Verarbeitung von Kopien amtlicher Unterlagen wurde festgestellt und bewiesen, dass der für die Datenverarbeitung Verantwortliche sich auch personenbezogene Daten über andere Personen als Teilnehmer und Benutzer, die nicht für die Verwirklichung der oben erwähnten Zwecke laut dem Gesetz Nr. 610/2003 Coll. erforderlich waren, beschafft und verarbeitet hatte. Somit hatte er der Bestimmung unter Kapitel 6 §1 und §3 des Gesetzes Nr. 428/2002 Coll. zuwidergehandelt.

Bei der Prüfung wurde festgestellt und bewiesen, dass der für die Datenverarbeitung Verantwortliche nicht nur Kopien amtlicher Dokumente, die nicht allein personenbezogene Daten über Betroffene enthielten, die den Vertrag mit für die Datenverarbeitung Verantwortlichen unterzeichnet hatten, sondern auch Kopien personenbezogener Daten anderer Betroffener ohne deren Zustimmung angefertigt hatte. Durch die Fotokopie z.B. einer Heiratsurkunde erlangte der für die Datenverarbeitung Verantwortliche auch personenbezogene Daten anderer Personen, u.a. eine Geburtsnummer. Diese Daten sind weder nach Umfang noch nach Inhalt mit den Datenverarbeitungszwecken laut Gesetz

610/2003 Coll. vereinbar. Auch die Verarbeitung und Benutzung sind nicht im Einklang mit dem Sinn und Zweck ihrer Verarbeitung.

Die Fotokopien, die während der Inspektion angefertigt wurden, bewiesen, dass der für die Datenverarbeitung Verantwortliche mehr Fotokopien von persönlichen Unterlagen als nötig angefertigt hatte. Beim Fotokopieren benutzte er keine Folien zum Abdecken der nicht erforderlichen personenbezogenen Daten, beispielsweise die personenbezogenen Daten des Ehepartners, der kein Kunde des für die Datenverarbeitung Verantwortlichen ist.

Da nicht alle Betroffenen ihre Zustimmung zum Fotokopieren ihrer personenbezogenen Daten gegeben hatten, hatte der für die Datenverarbeitung Verantwortliche den Bestimmungen der Bestimmung unter Kapitel 7 §1 des Gesetzes Nr. 428/2002 Coll., laut dem die Verarbeitung personenbezogener Daten ausschließlich mit der Zustimmung der Betroffenen erfolgen darf, zuwidergehandelt. Der für die Datenverarbeitung Verantwortliche hat dafür zu sorgen, dass der Nachweis für eine solche Zustimmung erbracht werden kann.

Bei der Prüfung wurde nicht festgestellt, dass die Zustimmung zum Fotokopieren von amtlichen Unterlagen seitens eines Befugten durch Androhung einer Versagung von vertraglichen Beziehungen, Leistungen, Waren oder Aufgaben des für die Datenverarbeitung Verantwortlichen oder Datenverarbeiters erzwungen worden wäre.

Es wurde festgestellt und nachgewiesen, dass der für die Datenverarbeitung Verantwortliche andere Unterlagen mit personenbezogenen Daten über die Betroffenen angefordert hatte, z.B. das Militärbuch, aus dem die Beauftragten auf Anweisung des für die Datenverarbeitung Verantwortlichen Fotokopien anfertigen sollten.

Da die Datenschutzbehörde den Verdacht einer Verletzung eines Sondergesetzes hatte, wurde das Verteidigungsministerium der slowakischen Republik darum gebeten, sich zu diesem Problem zu äußern.

Das Verteidigungsministerium befürwortete den Inhalt der Erklärung der Datenschutzbehörde, in der diese den oben erwähnten Standpunkt begründet hatte, dass die persönliche Identifizierungskarte (frühere Militärkarte oder früheres Militärbuch – es ist das gleiche Dokument) nicht als Nachtrag beigefügt und einem Unbefugten ausgehändigt werden darf, weil die persönliche Identifizierungskarte des Soldaten ausschließlich im Rahmen der Erfüllung seiner Aufgaben dazu dient, seine Mitgliedschaft bei der Armee zu beweisen, sowie zur Erfassung von Personen im Register , die ihren obligatorischen Wehrdienst ableisten. Deshalb darf sie nicht für andere Zwecke verwendet werden.

Die für die Datenverarbeitung Verantwortlichen wurden weiterhin darauf hingewiesen, dass sie den Bestimmungen des getrennten Gesetzes Nr. 162/1993 Coll. über Ausweise (geändertes Gesetz, im Folgenden „Gesetz 162/1993 Coll.") zuwidergehandelt hatten. Laut diesem Gesetz ist der Ausweis ein öffentliches Dokument, das ein Bürger der slowakischen Republik zum Nachweis seiner Identität, seiner Eigenschaft als Bürger der slowakischen Republik oder anderer im Ausweis festgehaltener Merkmale benutzt, wobei er nicht dazu verpflichtet ist, ein anderes Dokument zum Nachweis der Daten auf seinem Ausweis vorzulegen, sofern in den Kapiteln 1 und 5 §2 des Gesetzes Nr. 162/1993 Coll. nichts anderes bestimmt ist.

Die Datenschutzbehörde hat ausgehend von den vorgefundenen und bewiesenen Fakten die Bestimmung erlassen, dass der für die Datenverarbeitung Verantwortliche zur Vereinheitlichung der Datenverarbeitung mit dem Gesetz 428/2002 Coll. und zur Überarbeitung der entsprechenden Methodik verpflichtet ist, mit der auch das Verfahren für Beauftragte des für die Datenverarbeitung Verantwortlichen im Rahmen der Anforderung amtlicher und sonstiger Unterlagen und der Anfertigung von Kopien geregelt wird.

Slowenien

I. ALLGEMEINE EINFÜHRUNG

A. Verfassungsbestimmungen für den Schutz personenbezogener Daten in der Slowenischen Republik

Die verfassungsrechtliche Grundlage für die Annahme und den Inhalt des Datenschutzgesetzes der Republik Slowenien (von 2004) ist Artikel 38 der Verfassung der Republik Slowenien vom 23. Dezember 1991 (zuletzt abgeändert am 23. Juni 2004), der Folgendes besagt:

„Der Schutz von personenbezogenen Daten ist garantiert. Die Benutzung personenbezogener Daten entgegen dem Zweck ihrer Zusammentragung ist untersagt.

Die Sammlung, Verarbeitung, Zweckbestimmung, Überwachung und der Schutz des vertraulichen Charakters personenbezogener Daten können gesetzlich geregelt werden.

Jeder hat das Recht auf Kenntnisnahme der personenbezogenen Daten über ihn und das Recht auf gerichtlichen Schutz im Falle einer Zweckentfremdung dieser Daten".

Die verfassungsrechtliche Grundlage für die Verabschiedung des Datenschutzgesetzes im Rahmen der Mitgliedschaft der Republik Slowenien in der Europäischen Union ist im dritten Paragraphen des Artikels 3.a der Verfassung der Republik Slowenien verankert. Dieser lautet wie folgt:

„Rechtshandlungen und –beschlüsse im Rahmen internationaler Organisationen, denen Slowenien die Ausübung eines Teils seiner Hoheitsrechte übertragen hat, werden in Slowenien in Übereinstimmung mit den gesetzlichen Regeln dieser Organisationen angewandt".

Aus allgemeiner systemischer Sicht bedeutet der Artikel 38 der Verfassung der Republik Slowenien, dass die Verfassungsväter für die Regelung des Schutzes von personenbezogenen Daten das sog. „Verarbeitungsmodell" und nicht das so genannte „Missbrauchsmodell" herangezogen haben, da dieser Verfassungsartikel allgemeine Regeln für die angemessene (rechtmäßige) Verarbeitung personenbezogener Daten auf gesetzlicher Ebene und nicht den Grundsatz der Freiheit der Verarbeitung personenbezogener Daten festlegt, die ausnahmsweise ausdrücklich gesetzlich eingeschränkt werden kann.

Der zweite Paragraph des Artikels 38 der Verfassung der Republik Slowenien legt die Verpflichtung zur gesetzlichen Regelung der Sammlung, Verarbeitung, Zweckbestimmung, Überwachung und zum Schutz des vertraulichen Charakters von personenbezogenen Daten fest. Dies bringt speziell nicht nur die Verpflichtung zur Regelung des Schutzes von personenbezogenen Daten in einem allgemeinen Datenschutzgesetz, sondern auch die Möglichkeit der Behandlung dieser Themen in sektoriellen Gesetzen mit sich, die ebenfalls den Bestimmungen des Artikels 38 der Verfassung der Republik Slowenien gerecht werden müssen und aus dem Grunde für ein angemessenes Maß an Schutz personenbezogener Daten – vergleichbar mit den Bestimmungen des Datenschutzgesetzes – sorgen müssen. Natürlich bedeutet dieser zweite Paragraph des Artikels 38 der Verfassung der Republik Slowenien nicht, dass alle rechtlichen Beziehungen bis ins letzte Detail in sektoriellen Gesetzen über den Datenschutz geregelt werden müssen: Erstens, weil im Fall eventueller Lücken in den sektoriellen Gesetzen die Bestimmungen des allgemeinen (systemischen) Datenschutzgesetzes Anwendung finden und gelten, und zweitens, weil das Datenschutzgesetz bzw. die sektoriellen Gesetze die Ausnahmen von der allgemeinen Regelung des Schutzes personenbezogener Daten festlegen, wie im Falle von Vertragsschließungen zwischen Privatleuten.

Die Frage des Schutzes personenbezogener Daten in der Republik Slowenien wurde bereits als verfassungsrechtliches Thema im Jahre 1969 gestellt, als das Verfassungsgericht der Sozialistischen Republik Slowenien einen Antrag auf die Überprüfung der Verfassungsmäßigkeit beim ehemaligen Verfassungsgericht Jugoslawiens einreichte. Es ging um den Beschluss des damaligen Statistikbundesamtes Jugoslawiens zur obligatorischen Sammlung von angeblich statistischen Daten (Schulbildung und berufliche Tätigkeit von Einzelpersonen, die Organisation, in der sie beschäftigt waren, ihr Einkommen aus einzelnen Einkommensquellen, die Zahl der Mitglieder ihres Haushaltes und deren Einkommen sowie Ferienwohnungen und Motorfahrzeuge der Betreffenden und der Mitglieder ihres Haushaltes), die von den Personen in direktem Zusammenhang mit deren Einkommen gewonnen wurden.

Das Verfassungsgericht Ex-Jugoslawiens entschied 1971[10], dass „der geschäftsführende Direktor des Statistikbundesamtes nicht durch seinen Beschluss zur Sammlung von Daten über Beitragsleistende aus gemeinsamen Einkommenserklärungen von Ansässigen im Jahre 1968 (Amtsblatt des damaligen Jugoslawien 55/68) und zur Anordnung der Sammlung von Daten über Steuerpflichtige aus den gemeinsamen Einkommenserklärungen für 1968 befugt war" und: „Während des Verfahrens und der öffentlichen Anhörung wurde festgestellt, dass gemäß dem Beschluss des Direktors Daten über Steuern auf gemeinsame Einkommen von Ansässigen gesammelt und verarbeitet wurden. Hierbei entstand die Frage nach der Zulässigkeit und Notwendigkeit einer Veröffentlichung dieser statistischen Daten. Das Gericht äußerte sich nicht zu dieser Frage, weil es sich hierzu nicht befugt hielt. Ob die erwähnten Daten veröffentlicht werden sollten oder Sachverhalte wirklich genau wiedergeben, ob sie nützlich seien und andere Fragen im Zusammenhang mit der Veröffentlichung sollten Gegenstand einer gesonderten Überprüfung und Entscheidung sein. Aus dem Standpunkt des Verfassungsgerichtes Jugoslawiens ergab sich jedoch deutlich, dass diese Daten durch ungesetzliche Handlungen zusammengetragen worden waren."[11]

Auf diesen Beschluss folgten theoretische Debatten und rechtswissenschaftliche Beiträge in der Sozialistischen Republik Slowenien über die Notwendigkeit einer Regelung des Datenschutzes als einem getrennten Feld des Schutzes der Privatsphäre. So war beispielsweise die Terminologie des Datenschutzes in der slowenischen Sprache bereits 1984 fest verankert und wird größtenteils noch heute in der slowenischen Gesetzgebung und Rechtsprechung angewandt.

Nach diesen Debatten verabschiedete die Sozialistische Republik Slowenien am 27. September 1989 die Änderung XLIV[12] zur Verfassung der Sozialistischen Republik Slowenien von 1974. Sie wurde eigentlich als neue verfassungsrechtliche Bestimmung zwischen Art. 209 und 210 der Verfassung eingeschoben und definierte zum ersten Mal auf verfassungsrechtlicher Ebene das Recht auf Datenschutz:

1. Der Schutz personenbezogener Daten wird gewährleistet. Die Sammlung, Verarbeitung und Zweckbestimmung personenbezogener Daten wird gesetzlich festgelegt. Die Benutzung privater Daten entgegen dem Zweck der Datensammlung ist untersagt.

2. Diese Änderung ergänzt Kapitel IV des zweiten Teils der Verfassung der Sozialistischen Republik Slowenien."

[10] Beschluss des Verfassungsgerichtes Jugoslawiens, Aktenzeichen U 167/69, 17. März 1971.

[11] Dieser Beschluss wurde weniger als zwei Jahre nach dem Beschluss des Bundesverfassungsgerichtes der Bundesrepublik Deutschland im Jahre 1969 zur repräsentativen Volkszählung getroffen: „Mikrozensus"-Fall (27 BverfGE 1, 16. Juli 1969), eine Art Ansatz eines Verfassungspräzedenzfalles, der die rechtlichen Grundlagen in der Bundesrepublik Deutschland gegen die uneingeschränkte Erfassung personenbezogener Daten schuf.

[12] Staatsblatt der SR Slowenien, Nr. 32/1989.

Die siebte Unterklausel der ersten Klausel der Änderung LXVII der Verfassung der Sozialistischen Republik Sloweniens, die am selben Datum wie die Verfassungsänderung XLIV verabschiedet wurde, bestimmte, dass das Parlament der SR Slowenien den Datenschutz persönlicher und anderer Daten gesetzlich regelt.

Nach der Änderung XLIV der Verfassung wurde im Jahre 1990 das erste Datenschutzgesetz der Republik Slowenien verabschiedet, und zwar nach mehreren Gesetzentwürfen zu dieser Materie, die schon mindestens seit 1983 in der damaligen Sozialistischen Republik Slowenien auf dem Tisch waren. Slowenien war somit der einzige Staat des ehemaligen Jugoslawien, der den Datenschutz regelte. Das Gesetz wurde faktisch Ende 1991 wirksam (nachdem die Polizei- und Verteidigungsgesetzgebung zum Teil entsprechend angepasst wurden) und verstärkt 1992, als der erste Datenschutzbeauftragte seine Überwachungstätigkeit aufnahm.

Am 24. Oktober 1995 verabschiedete die EU die Richtlinie 95/46/EG über den Schutz von Einzelpersonen im Rahmen der Verarbeitung personenbezogener Daten und über den freien Verkehr solcher Daten. Sie regelte sowohl den Schutz personenbezogener Daten als auch den freien Verkehr personenbezogener Daten in der Europäischen Union. Dies war notwendig, um in allen Mitgliedsländern der Europäischen Union den freien Verkehr von Waren und Dienstleistungen und wenigstens annähernd dasselbe Maß an Schutz personenbezogener Daten zu gewährleisten.

Diskussionen über die Umsetzung dieser Richtlinie in der Gesetzgebung gab es in der Republik Slowenien schon 1996, und der Entwurf der Richtlinie 95/46/EG von 1990 wurde schon 1992 inoffiziell ins Slowenische übersetzt.

1999 verabschiedete das Parlament der Republik Slowenien das neue Datenschutzgesetz, das weitgehend mit der Konvention zum Schutze von Einzelpersonen im Rahmen der automatischen Datenverarbeitung von 1981[13], die von der Republik Slowenien am 25. Januar 1994 ratifiziert wurde, vereinheitlicht wurde. 2001 wurde dieses Gesetz zur Vereinheitlichung mit den Bestimmungen der Richtlinie 95/46/EG geändert. Ein wichtiges Merkmal des geänderten Gesetzes (Stand 2001) war die Schaffung von zwei Datenschutzorganen in der slowenischen Republik – des Ombudsmanns für die Menschenrechte und des Datenschutzbeauftragten der slowenischen Republik als Organ innerhalb des Justizministeriums der Republik Slowenien. Der Ombudsmann für die Menschenrechte wurde durch dieses abgeänderte Gesetz zur unabhängigen Aufsichtsinstitution für den Datenschutz erklärt, besaß jedoch keine direkten (konkreten) Befugnisse zur Ausübung dieser Aufsicht. Andererseits besaß die Datenschutzbehörde der Republik Slowenien direkte Befugnisse zur Überwachung des Datenschutzes, war jedoch an und für sich nicht unabhängig. Ihre Beschlüsse und Regelungen (in erster Instanz) konnten Gegenstand von Berufung beim Justizminister sein (zweite Instanz). Der Justizminister konnte sie abändern, aufheben oder an die Datenschutzbehörde zurückverweisen. Das Recht auf gerichtliche Berufung wurde geschädigten Parteien zuerkannt. Sie konnten administrative Streitigkeiten vor das Verwaltungsgericht der Republik Slowenien bringen (spezialisierter Gerichtsbereich / spezialisiertes Gericht für verwaltungsrechtliche Angelegenheiten). Berufungen konnten beim Obersten Gerichtshof der Republik Slowenien eingereicht werden (Verwaltungsrechtsabteilung).

B. Rechtsprechung in der Zeit von 1992 bis 2003

Allgemein kann gesagt werden, dass die Hauptinitiative zur Schaffung einer Rechtsprechung mit Bezug auf den Datenschutz in der Republik Slowenien in der Zeit zwischen 1992 und 2002 vom Verfassungsgericht der Republik Slowenien

[13] CETS Nr.: 108.

ausging. 1992[14] hob es eine Bestimmung in den Ausweisausstellungsregeln wegen fehlender gesetzlicher Grundlage auf – die obligatorische Abgabe von Fingerabdrücken war nicht im Ausweisgesetz, sondern in den Satzungen über diese Verpflichtung festgelegt. Diese Bestimmung wurde für verfassungswidrig und ungesetzlich erklärt.

2000 entschied das Verfassungsgericht[15], dass einige Bestimmungen des Rundfunkgesetzes Sloweniens verfassungswidrig seien, weil sie eine unverhältnismäßige Sammlung und Nutzung von personenbezogenen Daten zum Zwecke des obligatorischen Gebühreneinzugs für den (öffentlichen) slowenischen Rundfunk erlaubten. In der Entscheidung heißt es ausdrücklich: „Das Recht auf Privatsphäre endet erst dann und dort, wo es in Konflikt mit den gesetzlich gebilligten stärkeren Interessen anderer gerät."

2002 beschloss das Verfassungsgericht ebenfalls[16], dass die Bestimmungen des Gesetzes über das zentrale Bevölkerungsregister bezüglich der Verarbeitung der einheitlichen persönlichen Registrierungsnummer (Kürzel EMŠO auf Slowenisch), die jeder Bürger der Republik Slowenien obligatorisch vom Staat erhält, nicht verfassungswidrig seien. Es erklärte, dass die einheitliche persönliche Registrierungsnummer keine solche Gefahr darstelle, dass sie nicht vom Staat verarbeitet werden dürfte. Es bestehe auch keine besondere Gefahr dadurch, dass das Dateisystem, in das diese Nummer obligatorisch aufgenommen werden muss (zentrales Bevölkerungsregister), vom Innenminister verwaltet wird; es gebe hierfür weitere angemessene Absicherungen im damaligen Datenschutzgesetz von 1999/2001 (Verbot der Verwendung desselben Verbindungscodes für den Zugriff auf personenbezogene Daten aus Dateien der öffentlichen Sicherheit, der nationalen Sicherheit, der Verteidigung usw.). In den Fällen, in denen es um Datenschutz gehe, sei die angemessene Norm für die verfassungsmäßige Überprüfung der Gesetzgebung über diesen empfindlichen Bereich Strenge und Präzision. Die Verhältnismäßigkeit wurde geprüft.

2002 prüfte das Verfassungsgericht weiterhin die Verfassungsmäßigkeit des Volkszählungsgesetzes von 2001 und entschied[17], dass die Frage im Volkszählungsformular über die Religionszugehörigkeit keine verfassungswidrige Beeinträchtigung des Rechtes auf Trennung von Staat und Religionsgemeinschaften darstelle (Artikel 7 der Verfassung), noch der Gewissensfreiheit (Artikel 41 der Verfassung), noch des Rechts auf Privatsphäre (Artikel 35) oder des Rechts auf Datenschutz (Artikel 38). Diejenigen, die diese Angaben machen sollten, hatten das Recht, die Beantwortung dieser Frage abzulehnen. Die Angaben über Abwesende unter 14 Jahren konnten nur mit deren schriftlicher Zustimmung gemacht werden. Das Gericht entschied weiterhin, dass die bei der Volkszählung zu statistischen Zwecken gesammelten Daten nicht zu anderen Verwaltungszwecken verwendet werden dürfen.

Weitere Beschlüsse des Verfassungsgerichtes bleiben hier unerwähnt, z.B. über steuerspezifische personenbezogene Daten, weil sie dem beschriebenen Muster der Beschlussfassung und Argumentation des Verfassungsgerichtes folgen.

2002 bestätigte das Oberste Verfassungsgericht[18] die Verurteilung eines Beamten, der personenbezogene Daten missbraucht hatte (Art. 154 Strafgesetzbuch) und lieferte dazu eine Interpretation dieser Straftat vor dem Hintergrund der Datenschutzgesetzgebung.

[14] Beschluss des Verfassungsgerichtes der Republik Slowenien, Nr. U-I-115/92, 24. Dezember 1992
[15] Beschluss des Verfassungsgerichtes der Republik Slowenien, Nr. U-I-238/99, 9. November 2000
[16] Beschluss des Verfassungsgerichtes der Republik Slowenien, Nr. U-I-69/99, 23. Mai 2002
[17] Beschluss des Verfassungsgerichtes der Republik Slowenien, Nr. U-I-92/01, 5. März 2002.
[18] Urteil des Obersten Gerichtshofes der Republik Slowenien, Az. I Ips 121/2000, 11. Dezember 2002

Im Jahre 2003 fällte das Verfassungsgericht eine wichtige Entscheidung über den Zugang eines Patienten zu seinen medizinischen Daten[19]: Unter bestimmten besonderen Umständen kann dieses Recht verweigert werden, wenn dies zur Vermeidung schädlicher Konsequenzen für die Gesundheit des Patienten dringend geboten ist. Die Verhältnismäßigkeit wurde geprüft.

Es gibt noch weitere Beschlüsse ordentlicher und spezialisierter Gerichte über den Datenschutz, aber da in diesen Beschlüssen keine wirklich wichtigen Grundsätze des Datenschutzes formuliert sind, werden sie in diesem Bericht nicht erwähnt.

II. WICHTIGSTE ENTWICKLUNGEN IN DER REPUBLIK SLOWENIEN IM JAHRE 2004

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

Im Mai 2003 begannen ausführliche Gespräche mit dem entsprechenden Gremium der EU-Kommission (mit der damaligen Medien- und Datenschutzzelle der GD Binnenmarkt) über die korrekte Vereinheitlichung des slowenischen Datenschutzgesetzes mit den Bestimmungen der Richtlinie 95/46/EG. Der Entwurf von Änderungen am bestehenden Gesetz von 1999 begann Juli 2003 beim Justizministerium der Republik Slowenien. Im November 2003 wurde beschlossen, dass ein von Grund auf neues Datenschutzgesetz für die angemessene Vereinheitlichung mit der Richtlinie 95/46/EG erforderlich sei. Die Bestimmungen des Gesetzentwurfs wurden von den Experten des Justizministeriums und der Datenschutzbehörde der Republik Slowenien formuliert. Anschließend wurde der Gesetzentwurf Anfang März 2004 in die ressortübergreifenden Beratungen geschickt und der gesetzgebenden Abteilung der Regierung zugeleitet, wobei laufende Konsultationen mit dem entsprechenden Organ bei der Europäischen Kommission stattfanden. Auch der Ombudsmann für die Menschenrechte und der Beauftragte für den Zugang zu öffentlichen Informationen legten Stellungnahmen vor. Am 25. März 2004 legte die Regierung der Republik Slowenien der Nationalversammlung den Entwurf des Datenschutzgesetzes vor. Dort durchlief der Gesetzesentwurf drei Lesungen und wurde am 15. Juli 2004 verabschiedet[20]. Er trat am 1. Januar 2005 in Kraft.

In der Zwischenzeit wurde die Republik Slowenien am 1. Mai 2004 Mitglied der EU.

Das Hauptziel des neuen Datenschutzgesetzes der slowenischen Republik war die Vereinheitlichung mit den Bestimmungen der Richtlinie 95/46/EG, die durch dieses Gesetz erzielt wurde.

Das neue Gesetz hebt jede Berufungsmöglichkeit und jeden Einfluss des Justizministeriums auf die Überwachung im Bereich des Datenschutzes auf. Die derzeitige Datenschutzbehörde der Republik Slowenien bleibt übergangsweise innerhalb der Organisation des Justizministeriums, übt jedoch bereits den größten Teil der Gerichtsbarkeit und gerichtlichen Befugnisse einer unabhängigen Datenschutzbehörde aus (mit Ausnahme des direkten Zugangs zum Verfassungsgericht). Das neue staatliche Aufsichtsgremium für den Datenschutz, in das die Datenschutzbehörde umgewandelt werden sollte, sollte voll und ganz am 1. Januar 2006 als unabhängiges Gremium (außerhalb des Justizministeriums) seine Tätigkeit aufnehmen. Der unabhängige Ombudsmann für die Menschenrechte behielt bestimmte Beratungs- und Aufsichtsfunktionen bezüglich der Tätigkeit der staatlichen Datenschutzbehörde.

Das Gesetz trifft eine gewisse Unterscheidung zwischen der Datenverarbeitung im öffentlichen und privaten Sektor.

[19] Beschluss des Verfassungsgerichtes der Republik Slowenien, Nr. U-I 60/03, 4. Dezember 2003

[20] Staatsanzeiger der Republik Slowenien. 86/2004.

Weitere wichtige Themen dieses Gesetzes sind die sektorielle Regelung der Videoüberwachung, die Biometrik, das Direktmarketing, öffentliche Register, Besucherlisten, Aufsicht durch Experten und Verknüpfung von Datenablagesystemen.

Die Beschlussfassung über den Transfer personenbezogener Daten in Drittländer und darüber, ob Drittländer ein angemessenes Maß an Schutz personenbezogener Daten gewährleisten, liegt in der Hand der Datenschutzbehörde.

Es liegt weiterhin in der Zuständigkeit der Aufsichtsbehörde, Datenablagesysteme zu verwalten. Zurzeit stellt jedoch noch das Justizministerium die technischen Mittel für die Verwaltung zur Verfügung.

Bezüglich der Richtlinie 2002/58/EG kann erklärt werden, dass sie durch das Gesetz über die elektronische Kommunikation[21], das am 9. April 2004 verabschiedet wurde und am 1. Mai 2004 in Kraft trat, umgesetzt wurde. Kapitel X dieses Gesetzes regelt weitgehend den Schutz personenbezogener Daten, den Schutz der Privatsphäre und der Geheimhaltung im Bereich der elektronischen Kommunikation. Die Übergangsbestimmung des neuen Datenschutzgesetzes nahm die vereinheitlichte persönliche Registrierungsnummer (EMŠO im Slowenischen) aus dem Gesetz Telefonbücher heraus, weil sie aufgrund des Fehlers des Gesetzgebers in Telefonbüchern veröffentlicht werden musste. Weil die Steuernummer bereits laut einer Bestimmung dieses Gesetzes für die Bezahlung von Telefonrechnungen eingeholt und verarbeitet werden musste, vertrat man die Ansicht, dass demnach die Verarbeitung der vereinheitlichten persönlichen Registrierungsnummer durch Betreiber von elektronischen Kommunikationsdiensten für die Bezahlung von Telefonrechnungen unangemessen sei. Folglich wurde die persönliche Registrierungsnummer aus dem Gesetz über die elektronische Kommunikation gestrichen.

B. Bedeutende Rechtsprechung

Wichtige Entscheidungen der Datenschutzbehörde der slowenischen Republik im Jahre 2004 fielen in verschiedenen Bereichen.

Im Fall der Bank von Slowenien, der Zentralbank von Slowenien, verbot das Datenschutzamt die Veröffentlichung des Bankkontenregisters im Internet, bis die so genannte Datenrückverfolgung (wem Daten übermittelt wurden, welche Daten übermittelt wurden, auf welcher rechtlichen Grundlage und wann) gewährleistet war. Die betreffenden Daten von Kunden (Informationen über natürliche Personen, z.B. Name, Vorname, Adresse, Steuerregisternummer, Kontonummer usw.) wurden obligatorisch von Geschäftsbanken übermittelt. Dieses Register wurde also aus Bankkonten erstellt, die bei Geschäftsbanken eröffnet worden waren. Sinn und Zweck der Veröffentlichung dieses Registers im Internet, also zugänglich für jeden ohne jede Erfordernis des Nachweises eines rechtlichen Interesses oder der Verwendung eines Passworts, war angeblich die einfachere Durchsetzung zivilrechtlicher Urteile und die leichtere Beschaffung von Daten für private Klagen vor Gericht. Diese Zweckbestimmung war jedoch nicht ausdrücklich im betreffenden Gesetz genannt. Das Justizministerium, das damals noch für Berufungen zuständig war, änderte den Beschluss der Datenschutzbehörde und verbot jede Verarbeitung von Daten über natürliche Personen in diesem Register im Internet, weil es keine gesetzliche Grundlage für diese Verarbeitung gab. Die Artikel 2 (b), 6 §1, (b) und 5 (b) der Richtlinie 95/46/EG wurden bei diesem zweiten Beschluss als Argument angeführt. Die Verfassungsmäßigkeit der Veröffentlichung des Registers im Internet ist zurzeit beim Verfassungsgericht zur Entscheidung anhängig.

[21] Staatsanzeiger der Republik Slowenien, Nr. 43/2004 und 86/2004.

Ein weiterer wichtiger Fall für die Datenschutzbehörde im Jahre 2004 betraf die Steuerverwaltung. Das Amt untersagte die Verwendung ungeeigneter Umschläge für den Versand von Steuerschuldbescheiden an Steuerpflichtige (natürliche Personen). Diese Umschläge waren so durchsichtig, dass man den Inhalt bei Tageslicht lesen konnte. Es wurde außerdem entschieden, dass die für die Datenverarbeitung Verantwortliche (die Steuerverwaltung) nicht schon deshalb von ihrer Verantwortung für die gesetzliche Verarbeitung personenbezogener Daten entbunden war, weil sie mit dem Datenverarbeiter einen Vertrag über die Datenverarbeitung geschlossen hatte. Die Datenschutzbehörde schlug weiterhin ein Verfahren gegen den Verantwortlichen bei der Steuerverwaltung wegen geringer Übertretung vor. Die Berufung, die die Steuerverwaltung beim Justizministerium einleitete, wurde abgelehnt. In seinem Beschluss zitierte das Ministerium auch die Richtlinie 95/46/EG bezüglich der Rolle des Datenverarbeiters.

Auch einige Referate bzw. unverbindliche Stellungnahmen des geschäftsführenden Datenschutzbeauftragten hatten Auswirkungen in der Öffentlichkeit. Sein Referat vom Dezember 2003 bei der Polizei bewirkte die Aufhebung der polizeilichen Praxis der Bekanntmachung von Daten von natürlichen Personen bei Strafanzeigen. Es gab diesbezüglich teilweise heftige Kritik in den Medien. Der Datenschutzbeauftragte erklärte hierzu, dass eine Bekanntmachung solcher personenbezogener Daten möglich sei, wenn dies nach Meinung von Experten erforderlich ist. In diesem Fall müsse dies genauestens gesetzlich geregelt sein, auch unter Berücksichtigung bestimmter Kriterien wie des Rechts auf Unschuldsvermutung.

Eine ähnliche Wirkung hatte seine öffentliche Erklärung im Jahre 2004 über die Praxis bestimmter Gerichte, personenbezogene Daten von Parteien, die an einem Gerichtsverfahren beteiligt waren, im Internet bekannt zu geben. Diese Praxis wurde weitgehend gestoppt. Das Gerichtsgesetz wurde 2004 entsprechend geändert und erlaubt nur eine begrenzte Veröffentlichung solcher Daten. Demgemäß dürfen nur mehr Name und Vorname einer Verfahrenspartei (nur in Verfahren ohne Ausschluss der Öffentlichkeit) vor Gericht bekannt gemacht werden. Diese dürfen auch in elektronischer Form veröffentlicht werden, so dass sie öffentlich zugänglich werden (nicht notwendigerweise im Internet). Es wurde auch festgelegt, dass Name und Vorname eines Richters oder Gerichtsvorsitzenden auf die gleiche Art und Weise mit Verweis auf den jeweiligen Gerichtsfall veröffentlicht werden dürfen. Außerdem können das Aktenzeichen des Falles und eine allgemeine Beschreibung der Angelegenheit, Datum und Uhrzeit der Anhörung oder Sitzung sowie der Ort veröffentlicht werden - Daten, über die die Verfahrensparteien informiert werden müssen.

C. Wichtige spezifische Themen

Das Hauptthema, bei dem es nur langsame Fortschritte im Datenschutzbereich gibt, ist der Gesundheitssektor, die Sicherheit von Gesundheitsdaten (vertrauliche Daten laut Datenschutzgesetzgebung). Eine Zusammenarbeit der Datenschutzbehörde mit den jeweiligen Gesundheitseinrichtungen im informationstechnischen Bereich könnte die Fortschritte beschleunigen. Zum anderen kann als positiver Aspekt angeführt werden, dass die Verarbeitung personenbezogener Daten im Gesundheitswesen sehr detailliert in der Gesundheitsgesetzgebung behandelt wird.

Ein weiteres bedeutendes Thema ist zurzeit die geringe Zahl von Datenschutzbeauftragten, doch dürfte dieses Problem in nächster Zukunft behoben sein.

Wichtige Vorhaben für die Zukunft sind die Vorbereitung sektorieller Richtlinien für bestimmte Arten der Verarbeitung personenbezogener Daten wie z.B. Videoüberwachung und Empfehlungen

für die Verarbeitung von medizinischen Daten im Gesundheitssektor.

Es laufen in der Republik Slowenien auch bedeutende Vorbereitungen zum Datenschutz im Zusammenhang mit dem Schengen-Acquis.

Neue Entwicklungen, vor allem im Jahre 2004, waren bestimmte Konflikte praktischer und theoretischer Natur zwischen dem Recht auf Datenschutz (Artikel 38 der Verfassung) und dem Recht auf Zugang zu Informationen öffentlicher Natur bzw. der Informationsfreiheit (Artikel 39 §2 der Verfassung) im Zusammenhang mit dem Gesetz über den Zugang zu öffentlichen Informationen, das im März 2003 verabschiedet wurde und im Juli 2005 erheblich geändert wurde. Das Datenschutzgesetz sieht ein Sonderverfahren für die Lösung dieser Konflikte in Verfahren vor dem Verwaltungsgericht der Republik Slowenien vor.

Auf Regierungsebene wird zurzeit die Zusammenlegung der Zuständigkeit für den Datenschutzbereich und den Zugang zu öffentlichen Informationen in einem Organ erwogen, dem Informationsbeauftragten. Demgemäß sollen die künftige Datenschutzbehörde der Republik Slowenien und der derzeitige Beauftragte für den Zugang zu öffentlichen Informationen zu einer einzigen Einrichtung zusammengefasst werden. Diese Einrichtung wäre nichtsdestoweniger vollkommen unabhängig von der Exekutive und Legislative. Ihr Leiter würde von der Nationalversammlung der Republik Slowenien auf Vorschlag des Präsidenten der Republik ernannt werden.

Spanien

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

Die Richtlinie des Europäischen-Parlamentes und Rates 95/46/EG wurde unter dem organischen Gesetz 15/1999 über den Datenschutz (LOPD) in die spanische Gesetzgebung integriert.

Bezüglich der Normen zum Datenschutzgesetz und im Hinblick auf eine größere Transparenz der Tätigkeiten der spanischen Datenschutzbehörde wurde die Anordnung (untergeordnete Gesetzgebung) 1/2004 über die Veröffentlichung von Resolutionen verabschiedet, und zwar als Folge der Änderung, die durch das Gesetz 62/2003 über steuerliche, administrative und soziale Maßnahmen verabschiedet wurde. Letztgenanntes Gesetz bestimmt die Veröffentlichung der Resolutionen der spanischen Datenschutzbehörde (Agencia Española de Protección de Datos – AEPD bisher) nach der gebührenden Unterrichtung der Betroffenen.

Zum anderen gehörte zu den Prioritäten der AEPD für das Jahr 2004 der Beginn der Arbeiten für den Entwurf allgemeiner Verordnungen zur Umsetzung des LOPD. Außerdem wurde mit dem Entwurf neuer Amtsstatuten begonnen. Diese sollen den verabschiedeten königlichen Erlass 428/1993 infolge der Anwendung des LOPD und der neuen Zuständigkeiten laut dem allgemeinen Gesetz über Telekom- und Informationsgesellschaftsleistungen und laut dem E-Commerce-Gesetz ersetzen. Eine Aufstockung der AEPD-Mitarbeiter von 15,59 % infolge der Übernahme dieser neuen Verantwortungsbereiche wurde genehmigt.

Neben der Entwicklung des organischen Datenschutzgesetzes wird der gesetzliche Rahmen, den dieses Gesetz schafft, durch mehrere allgemeine oder sektorielle Regelungen in verschiedenen gesetzlichen Bereichen vervollständigt, die den geltenden Rechtsrahmen darstellen. Unter diesen Regelungen können vor allem folgende hervorgehoben werden:

- Königlicher Erlass 2/2004, 5. März, zur Ergänzung des Gesetzes über das lokale Finanzamt.
- Königlicher Erlass 6/2004, 29. Oktober, zur Verabschiedung der Zusatzgesetzgebung über private Versicherungsaufträge und –aufsicht.
- Königlicher Erlass 183/2004, 30. Januar, zur Regulierung der persönlichen Gesundheitskarte.
- Königlicher Erlass 2393/2004, 30. Dezember, zur Genehmigung der Regelungen des organischen Gesetzes 4/2000, 11. Januar, über die Rechte und Freiheiten von Ausländern in Spanien und deren Integration in die Gesellschaft.
- Königlicher Erlass 424/2005, 15. April, zur Genehmigung der Regelung zur Umsetzung des allgemeinen Telekommunikationsgesetzes GLT (Übertragung der Richtlinie 2002/58/EG). Diese wichtige Regelung legt die Grundsätze des Datenschutzes in verschiedenen Telekommunikationsbereichen dar:

  ➔ Verarbeitung von Verkehrsdaten, Rechnungen und Ortung der Teilnehmer und Benutzer bei Telekombetreibern,

  ➔ unerwünschte kommerzielle Mitteilungen,

  ➔ Ausarbeitung von Telefonnummernverzeichnissen und Nutzung fortgeschrittener Telefondienstleistungen wie zum Beispiel Anruferidentifizierung und die automatische Anrufabweisung.

- Regionale Regelungen

Gesetz 2/2004, 25. Februar, über Dateien mit personenbezogenen Daten in öffentlichem Besitz und die Schaffung der baskischen Datenschutzbehörde.

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 in der elektronischen Kommunikation, die ausdrücklich an die Stelle der Richtlinie 97/66/EG trat, wurde in die spanische Gesetzgebung durch das allgemeine Telekommunikationsgesetz 32/2003 vom 3. November übertragen.

B. Bedeutende Rechtsprechung

Entsprechend Kapitel 48.2 des spanischen Datenschutzgesetzes beenden die Entscheidungen des Direktors den Prozess bei der Regierung. Aus diesem Grund und ungeachtet der Unterbreitung eines Verschiebungsantrages können solche Entscheidungen nur administrativ angegangen werden. 2004 wurden insgesamt 84 Urteile von den Oberen Gerichten und nationalen oberinstanzlichen Gerichten sowie 9 Urteile vom Obersten Gericht über Anträge auf die Vereinheitlichung der Rechtsdoktrin verkündet. An dieser Stelle erwähnen wir nur die Paragraphen, die Präzedenzfälle für kontroverse Materien und Datenschutzgesichtspunkte schaffen, die schwierig zu interpretieren sind:

Benutzung von Verkehrs- und Fakturierungsdaten ohne Zustimmung der betroffenen Personen und Anwendbarkeit des LOPD auf Fachleute und -unternehmen

Die Entscheidung vom 11. Februar 2004 war die Antwort auf die Bitte um Bestätigung der Kriterien der Datenschutzbehörde, laut denen ein Telekombetreiber für die Benutzung professioneller Verkehrsdaten zu inkompatiblen Zwecken ohne die Zustimmung der betroffenen Person und für die Weiterleitung dieser Daten an Dritte bestraft werden kann. Bei der kommerziellen Förderung dieser Leistungen und Produkte ist die Verarbeitung von Verkehrs- und Fakturierungsdaten zur Werbung für eigene Telekomdienstleistungen gestattet, wenn der Teilnehmer vorher seine Zustimmung dazu erteilt hat.

Verletzung der Verpflichtung zur Gewährung des Streichungsrechtes

Die Entscheidung vom 3. April 2004 bestätigt die Doktrin der spanischen Datenschutzbehörde und verwirft die Berufung gegen die Entscheidung der Datenschutzbehörde wegen Verletzung des LOPD, Kapitel 16, über die Streichung von Daten, da die Streichung, die von der betreffenden Partei beantragt wurde, nicht vorgenommen worden war. Die prozessführende Partei war der Meinung, dass die Streichung laut Kapitel 16 LOPD nicht für die Zerstörung oder physische Löschung steht, sondern dass die Daten durch ein Passwort gesperrt werden sollen. Das Gericht prüfte die Argumente und kam zum Schluss, dass kein Datensperrungsdatum gefunden noch bestätigt werden konnte.

Versand von SMS ohne Zustimmung und ausdrückliches Verbot der betroffenen Partei

Das Gesetz vom 17. März 2004 bestätigte die Entscheidung der Datenschutzbehörde bezüglich der Verletzung des Zustimmungsrechtes. Der Berufungskläger verarbeitete personenbezogene Daten und sendete entgegen dem ausdrücklichen Verbot des Betroffenen, das dieser zwei Monate vor der Werbekampagne ausgesprochen hatte, eine Werbebotschaft an ein Mobiltelefon. Diese Zeit hätte ausgereicht, um mithilfe der verfügbaren technischen Mittel die Daten zu löschen. Das Gericht war der Ansicht, dass es rücksichtslos sei, eine Werbekampagne einzuleiten, wenn man weiß, dass man damit Kundenrechte verletzt.

Anwendbarkeit des LOPD auf Dateien und nicht automatisierte Datenverarbeitung

Das Gesetz vom 19. Mai 2004 verwirft die Berufung gegen die Entscheidung der Datenschutzbehörde wegen einer Verletzung der Geheimhaltungspflicht.

Das spanische Datenschutzgesetz gilt sowohl für automatisierte als auch nicht-automatisierte Dateien und fügt hinzu, dass sich die prozessführende Partei unter keinen Umständen auf diesen

Anpassungszeitraum berufen kann, weil sich die erste Zusatzbestimmung des Datenschutzgesetzes auf Dateien bezieht, die vor dem Inkrafttreten des betreffenden Gesetzes generiert wurden.

Verpflichtung zur Einholung der Zustimmung von Betroffenen zur Verarbeitung und Abtretung ihrer Daten

Die Entscheidung vom 30. Juni 2004, mit der die Berufung gegen die Entscheidung der Datenschutzbehörde wegen einer Verletzung der Kapitel 11 und 6.1 des LOPD (Abtretung und Zustimmung) verwirft, beruht auf der Doktrin, die bereits in den Entscheidungen vom 24. Januar und 9. Mai 2003 mit Bezug auf die Notwendigkeit der empfängerseitigen Bestätigung von Mitteilungen des für die Datenverarbeitung Verantwortlichen dargelegt wird.

Datenverarbeitung durch Dritte und Auslagerung

Der Beschluss des Verwaltungsgerichtes des nationalen Oberen Gerichtes vom 21. Juli 2004 akzeptiert zum Teil die Berufung gegen den Beschluss der Datenschutzbehörde vom 26. September 2001. Das Gericht prüfte Artikel 12 des LOPD und untersuchte die gemeinsamen und anderen Verantwortungen von Unternehmen. Laut LOPD muss das Unternehmen die seitens mehrerer Parteien zu erfüllenden Pflichten aufführen und bei Bedarf entscheiden, ob eine bestimmte Person oder Einheit für die Vorbeugung von administrativen Zuwiderhandlungen, die angeblich von einer oder mehreren Personen begangen wurden, verantwortlich ist. Dies hat es ausführlich unter Festlegung des Umfangs und der Bedeutung, der bzw. die bei einer derartigen Anklage angemessen ist, zu tun.

Anwendung des Königlichen Erlasses 994/1999, 11. Juni, auf Daten und Verarbeitungen von Ärzten

Der Beschluss des Verwaltungsgerichtes des nationalen Oberen Gerichtes vom 20. Oktober 2004 verwirft den Antrag vom 20. Mai 2002 und erklärt, dass Computerdateien und Datenverarbeitungen von Ärzten mit Bezug auf die Gesundheit ihrer Patienten dem organischen Gesetz 15/1999, 13. Dezember, und den Regeln zu den Sicherheitsmaßnahmen unterworfen sind.

Einfügung von Daten in eine Bonitätsdatei

Der Beschluss des Verwaltungsgerichtes des nationalen Oberen Gerichtes vom 1. Dezember 2004 gibt der Berufung gegen den Beschluss der Datenschutzbehörde bezüglich der Zuwiderhandlung gegen Punkt 4.3 des LOPD statt.

Es geht um die Einfügung von Kundendaten in eine Bonitätsdatei. Im angefochtenen Entscheid wird ausgesagt, dass der Berufungskläger das Prinzip der Datenqualität verletzt habe, indem er die Daten des Antragstellers im Hinblick auf eine unechte, fällige und eintreibbare Schuld in eine Bonitätsdatei aufgenommen habe, weil es Zweifel über die Existenz einer solchen Schuld gab. Die Datenschutzbehörde war der Ansicht, dass dies ein Fall miteinander verbundener Verträge unter dem Schutz des Gesetzes 7/1995 über Darlehen sei und daher, weil der Vertrag unwirksam war, die bestehende Schuld nicht gelte.

C. Wichtige spezifische Themen

Transparenz

Vor dem Parlament: Anhörung bei der Verfassungskommission der Abgeordnetenkammer

Im Dezember 2004 wurde der AEPD-Direktor (auf seine Initiative) von der Abgeordnetenkammer angehört. Er stellte den Geschäftsbericht der AEPD vor und beantwortete Fragen der Abgeordneten wie zum Beispiel:

- Normung der Kultur des Schutzes personenbezogener Daten.
- Weiterentwicklung des Gesetzes 15/1999, 13. Dezember, über private Daten (LOPD).
- Personal- und Mittelaufstockung für die Datenschutzbehörde.

- Ausbau präventiver Maßnahmen: Ex-officio-Sektorenpläne und Standardcodes.
- Förderung und Verbesserungen in der Zusammenarbeit zwischen der AEPD und regionalen Datenschutzstellen.
- Verstärkung der internationalen Präsenz der Datenschutzbehörde.

Vor Bürgern – Veröffentlichung aller AEPD-Resolutionen

Wie bereits im Zusammenhang mit der Umsetzung der Richtlinie 95/46/EG für mehr Transparenz bei den Tätigkeiten der AEPD erwähnt, wurden die Tätigkeiten der AEPD durch die Anordnung (untergeordnete Gesetzgebung) 1/2004 der Veröffentlichung der definitiven Beschlüsse der Datenschutzbehörde genehmigt.

Durchsetzung

- *Spam-Bekämpfung*

Es ist wichtig, die Beziehungen der AEPD mit den Vereinigten Staaten über die Federal Trade Commission zu beleuchten, wenn es um unerwünschte geschäftliche Mitteilungen oder „Spam" geht, weil hierduch Instrumente geschaffen werden können, die die Spam-Bekämpfung effizienter machen. Die Spam-Bekämpfung fällt in Spanien laut dem allgemeinen Telekommunikationsgesetz unter die AEPD-Zuständigkeit. Im Jahre 2004 wurden Kontakte zur genannten US-amerikanischen Kommission geknüpft, um eine spezielle Zusammenarbeit zu vereinbaren, die in einem so genannten „Memorandum of Understanding" (Absichtserklärung) ihren Niederschlag fand (das beim Abschluss dieses Geschäftsberichtes bereits unterschrieben war).

- *Förderung der Vorbeugung: Sektorielle Inspektionen 2004*

Zur Förderung der Vorbeugung gehören zu den grundlegenden Tätigkeiten der Datenschutzbehörde die sektoriellen Inspektionsprogramme, die jährlichen Audits verschiedener öffentlicher und privater Instanzen, die zur Abfassung entsprechender Empfehlungen führen. Diese müssen obligatorisch erfüllt werden, damit die Arbeitsweise der betreffenden Sektoren den Anforderungen der Datenschutzgesetzgebung angepasst wird.

2004 wurden die Schlussfolgerungen und Empfehlungen über die sektoriellen Inspektionen beim nationalen Institut der öffentlichen Verwaltungen und bei den Krankenhauslabors genehmigt.

➔ INAP (Instituto Nacional de Administración Pública – Nationales Behördeninstitut)

Die Organisation ist mit der Förderung und Entwicklung der Ausbildungs-, Weiterbildungs- und Forschungspolitik innerhalb der Zentralregierung beauftragt. 2003 führte INAP über tausend Aktionen mit über 23.000 Studenten und 3.000 Lehrern durch. Diese Zahlen belegen das Volumen der Bearbeitung personenbezogener Daten.

Allgemein sind die Informationen und Dokumente, die das INAP bekommt, nützlich und stichhaltig. Es wurde jedoch die Erstellung eines dokumentierten Verfahrens empfohlen, das dem Recht auf Zugang, Berichtigung und Streichung von Daten entgegenkommt.

➔ Krankenhauslabors

Während der Inspektion im Jahre 1996 in öffentlichen Krankenhäusern wurde festgestellt, dass externe Einheiten, die in den Labors mitarbeiteten, Zugang zu personenbezogenen Daten hatten. 2003 und 2004 wurde eine erneute sektorielle Inspektion durchgeführt, um tiefgreifend zu prüfen, wie diese Zugänge erfolgten. Die Folgerungen und Empfehlungen der Inspektion wurden 2004 genehmigt. Diese Inspektion weist aus dem Grunde sehr spezifische Eigenschaften auf, weil sie sich auf die Aspekte von Sicherheitsmaßnahmen beim

Zugang seitens Dritter konzentriert.

Die Inspektion wird ergänzt um eine Empfehlung mit Bezug auf die Ausübung des Rechts auf Zugang, Streichung und Einspruch bezüglich der Datenschutzregelungen und Pflegeregelungen.

- *Förderung der Selbstverwaltung*

2004 registrierte das Amt die nachstehenden Verhaltensregeln für den Datenschutz im öffentlichen und privaten Bereich.

➔ Verhaltensregeln der Zahnärzte und Stomatologen in Spanien

Diese Verhaltensregeln, die vom allgemeinen spanischen Rat der offiziellen Schulen von Zahnärzten und Stomatologen entworfen wurden, enthalten spezifische Regeln für die Verarbeitung personenbezogener Daten in ihrer Berufssparte. Sie legen die Bedingungen für die Organisation, die Arbeitsweisen, die geltenden Prozeduren sowie die Regeln für die Ausübung der Rechte der jeweiligen Patienten fest.

➔ Verhaltenscodex der Castilla-La Mancha-Universität

Dieser Verhaltenscodex verfolgt ein dreifaches Ziel: Übereinstimmung mit der einschlägigen Gesetzgebung auf die einfachste und schnellste Art und Weise durch ein einziges Dokument, das alle wichtigen Elemente enthält, besserer Schutz der in automatisierten Dateien gespeicherten Daten und Erweiterung der gesetzlichen Sicherheitsmaßen sowie Verwendung als didaktisches Material für die Universität, insbesondere für die Studenten.

➔ Verhaltenscodex des katalonischen Verbandes der Unterstützungsdienste (ACRA)

Der Verhaltenscodex ist ein Qualitätsmerkmal bei der Verarbeitung personenbezogener Daten, die für Unterstützungsdienste und für daran geknüpfte Leistungen notwendig sind. Er ist eine Garantie für Gebietsansässige und Behörden für die korrekte Führung des Zentrums oder der Einrichtung in Sachen Datenschutz.

➔ Codex für den Immobilienvermittlungssektor (AEGI)

Die Hauptzielsetzungen dieses Codex sind: Aufklärung von Kunden über ihre Rechte, Beseitigung von Zweifeln, die bei der Umsetzung der Datenschutzverordnung auftauchen können, Gewährleistung von Zuverlässigkeit und Garantie der praktischen und operativen Normen von Unternehmen, die an der Verarbeitung personenbezogener Daten und der Umsetzung des Gesetzes beteiligt sind.

Steigerung des Datenschutzbewusstseins und Förderung der Kooperation mit regionalen Ämtern

Zur weiteren Steigerung des Datenschutzbewusstseins nach 2003 hat der Direktor der AEPD seine direkte Beteiligung an zahlreichen Sitzungen und Versammlungen verstärkt. Zur Normierung der Datenschutzkultur hat die AEPD 2004 mehrere Kooperationsprotokolle mit öffentlichen und privaten Einheiten unterzeichnet: der ONCE-Stiftung, dem spanischen Komitee der Vertreter von Behinderten, dem Verband „Comisión de Libertades e Informática" und der Antonio de Nebrija-Universität.

Zum anderen wurde 2004 die dritte regionale Datenschutzbehörde geschaffen, die baskische Datenschutzbehörde (die ähnliche Befugnisse wie die madrilenische und katalonische besitzt).

Zur Fortsetzung und Förderung der institutionellen Zusammenarbeit wurde ein Kooperationsprotokoll zwischen der AEPD und den drei regionalen Behörden für die Schaffung eines Kommunikationssystems für den Austausch von Informationen über Datenverarbeitungsmitteilungen unterzeichnet.

Spanische Tätigkeiten im iberoamerikanischen Datenschutznetzwerk

Im iberoamerikanischen Kontext richten sich die Bemühungen auch auf die Zusammenarbeit und die Förderung im Datenschutzbereich. Wie wir bereits in den letzten Jahresberichten (2002-2003) schrieben, wurde dazu auf die Initiative der AEPD[22] das iberoamerikanische Datenschutznetzwerk gegründet. Die spanische Datenschutzbehörde wirbt für eine jährliche iberoamerikanische Datenschutzkonferenz. Im Mai 2004 fand diese Konferenz in Cartagena de Indias (Kolumbien) statt.

Am Treffen 2004 nahmen mehr als 40 Behörden und prominente Vertreter öffentlicher und privater Kreise aus 15 iberoamerikanischen Ländern teil. Im Verlauf der Arbeitssitzungen wurde der Datenschutz im Finanzsektor untersucht. Unter anderem wurden die europäischen und iberoamerikanischen Ansichten bezüglich der internationalen Datentransfers, der Angriffe auf die Privatsphäre im Telekom- und Internetbereich und die Spam-Bekämpfung und die Nutzung finanzieller Informationen zu Marketingzwecken im kommerziellen Bereich behandelt. Das Ergebnis dieser Treffen war die Verabschiedung mehrerer Schlussfolgerungen in der Cartagena-Abschlusserklärung, in der gemeinsame Standpunkte zu den in der Sitzung behandelten Themen zusammengefasst wurden.

[22] Weitere Informationen über IDPN stehen unter https://www.agpd.es/index.php?idSeccion=349, auch auf Englisch.

Schweden

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

Die EU-Richtlinie 95/46/EG wurde in Schweden durch das Datenschutzgesetz (1998:204) (PDA), das am 24. Oktober 1998 in Kraft trat, umgesetzt. Das PDA wird vervollständigt durch den Datenschutzbeschluss, der zur gleichen Zeit in Kraft trat. Das Gesetz findet auf die automatisierte und manuelle Datenverarbeitung Anwendung, wobei jedoch die Grundsätze der Datenverarbeitung und darüber, wann eine Verarbeitung erlaubt ist, nicht für manuelle Datenverarbeitung gelten, die vor dem Inkrafttreten des Datenschutzgesetzes am 1. Oktober 2007 begonnen wird. Das Gesetz gilt zwar grundsätzlich für die Verarbeitung privater Daten in allen Bereichen der Gesellschaft, jedoch gibt es mehrere spezielle Gesetze und Beschlüsse für die Datenverarbeitung in bestimmten Bereichen, entweder anstelle des Datenschutzgesetzes oder ergänzend zu diesem. Auch beim Entwurf dieser Sondergesetze und –beschlüsse wurde der Richtlinie Rechnung getragen.

Im Februar 2004 legte ein mit der Überprüfung des Datenschutzgesetzes befasstes Gremium, das nachprüfen sollte, ob ein „Missbrauchsmodell" auf das Datenschutzgesetz im Rahmen der Anforderungen der EU-Richtlinie angewandt werden könnte, seinen Bericht vor. Das Gremium schlug vor, die Verarbeitung personenbezogener Daten in unstrukturiertem Material wie z.B. fortlaufendem Text, Ton und Bild usw. von der großen Mehrheit der Datenhandhabungsregeln des Datenschutzgesetzes auszunehmen.

Diese Regeln würden demnach keine Anwendung auf alltägliche Verarbeitungen, z.B. Schreiben durchgehender Texte mit einem Textverarbeitungsprogramm, deren Veröffentlichung im Internet und in E-Mails usw. finden. Die Ausnahme würde jedoch nur dann gelten, wenn die Informationen nicht zur Aufnahme in eine Datenbank mit einer personendatenbezogenen Struktur dienen würden. Es würde stattdessen eine einfache Regel gelten: Die Datenverarbeitung ist nicht erlaubt, wenn sie einen unangemessenen Eingriff in die Privatsphäre darstellt. Dieser Vorschlag wurde mehreren Organisationen zur Prüfung vorgelegt. In einer Stellungnahme vom September 2004 erklärte die Datenschutzbehörde, den Vorschlag dahingehend annehmen zu wollen, dass Formen der Datenverarbeitung, die keine Risiken für die Privatsphäre mit sich bringen, von einigen Regeln des Datenschutzgesetzes ausgenommen würden. Die Datenschutzbehörde kritisierte jedoch die Komplexität der vorgeschlagenen Regeln und befürchtete, dass es schwierig zu entscheiden wäre, ob das Datenschutzgesetz Anwendung findet oder nicht. Der Vorschlag wird zurzeit weiter beim Justizministerium bearbeitet.

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

B. Bedeutende Rechtsprechung

Nach der Vorentscheidung des Europäischen Gerichtshofes im November 2003 über die Offenlegung personenbezogener Daten im Internet verkündete der schwedische Göta hovrätt (ein Berufungsgericht) im April 2004 sein abschließendes Urteil in einem Fall, in dem ein ehrenamtlicher Jugendleiter der schwedischen

Kirche personenbezogene Daten über andere Angestellte und Beamte der örtlichen Organisation ohne deren vorhergehende Zustimmung im Internet veröffentlicht hatte. Einige Daten umfassten auch Gesundheitsdaten. Die Absicht war, Kindern auf eine einfache und humorvolle Art und Weise Informationen anzubieten. Als sich zeigte, dass einige Personen, auf die sich diese Informationen bezogen, dies nicht billigten, wurden diese Informationen unverzüglich gelöscht. Ein Bezirksgericht urteilte, dass der Ehrenamtliche bestimmten Bestimmungen des Datenschutzgesetzes zuwidergehandelt hatte. Der Fall wurde vor den Göta hovrätt gebracht, der sich mit Fragen über die Interpretation der EU-Richtlinie 95/46/EG an den europäischen Gerichtshof wandte. Der Gerichtshof befand u. a., dass diese Datenverarbeitung in den Geltungsbereich der Richtlinie fiele und vertrauliche Daten verarbeitet worden seien, dass aber die Handlungen des betreffenden Ehrenamtlichen keinen Datentransfer in Drittländer darstellten. Auf diese Erklärung des europäischen Gerichtshofes hin zog der Ankläger später den Vorwurf des Datentransfers in Drittländer zurück. In seinem Urteil vom April 2004 befand der Göta hovrätt, dass der Ehrenamtliche bestimmten anderen Bestimmungen des Datenschutzgesetzes fahrlässig zuwidergehandelt habe, diese Zuwiderhandlung jedoch so unerheblich sei, dass keine Strafe verhängt werden müsse.

Im Juni 2004 entschied das Komitee der Datenschutzbehörde, dass die Sammlung und Verarbeitung von Fingerabdrücken von Schülern für die Zugangsprüfung an der Schulkantine nicht angemessen und sachdienlich sei, und zwar ungeachtet der Tatsache, dass die Einverständniserklärung der Schüler eingeholt wurde.

Drei Mitglieder des Komitees einschließlich des Generaldirektors äußerten sich anders lautend, nämlich dass diese Vorgehensweise zulässig sei, wenn die Schüler sich damit einverstanden erklärten. Die Mehrheit im Komitee vertrat hingegen die Ansicht, dass solche Prüfungen auch anders durchgeführt werden könnten, ohne derart in die Privatsphäre einzudringen. Diese Ansicht wurde seither auch in ähnlichen Fällen von der Datenschutzbehörde vertreten. Gegen die Entscheidungen der Datenschutzbehörde wurde beim örtlichen Verwaltungsgericht Einspruch eingelegt.

C. Wichtige spezifische Themen

Im April 2004 wurde Herr Göran Gräslund Generaldirektor der Datenschutzbehörde.

Die Behörde hat bestimmte Aufsichtstätigkeiten in Form spezifischer Projekte fortgesetzt. Es wurden Inspektionen bei mehreren für die Datenverarbeitung Verantwortlichen desselben Sektors durchgeführt. Die Inspektionsergebnisse wurden in Protokollen zusammengefasst und veröffentlicht. 2004 veröffentlichte die Datenschutzbehörde drei Berichte über folgende Themen: Die Behandlung von Zugangsanträgen bei Banken (2004:3), Biobanken und Datenschutzgesetz (2004:2) und die Verarbeitung personenbezogener Daten bei öffentlichen Sozialhilfezentren sowie ökologische Themen (2004:1).

Die Debatte in Schweden 2004 hat die Problematik der Datenverarbeitung mithilfe neuer Techniken, wie zum Beispiel Biometrie und RFID, ins Rampenlicht gerückt. Ein Untersuchungsausschuss schlug die verstärkte Verwendung von DNA-Profilen beim Gesetzesvollzug vor. Einige forderten, dass Schweden ein DNA-Register über die gesamte Bevölkerung zur Identifizierung von Verbrechern und Unfallopfern anlegen solle. Ein weiteres Diskussionsthema war die zunehmende Videoüberwachung. Es wurde vorgeschlagen, dass die Datenschutzbehörde bestimmte Überwachungsaufgaben in diesem Bereich übernimmt, der zurzeit unter die Aufsicht der Bezirksverwaltungsgerichte fällt. Weitere Schwerpunkte waren Mobiltelefone mit Kameras und das damit verbundene Risiko, dass private Aufnahmen

gemacht und im Internet gezeigt würden. Medieninteresse fand auch der EU-Vorschlag bezüglich der Speicherung von Verkehrsdaten. Das Thema der Anwendung der Informationstechnik in Medizin und Gesundheitswesen wurde diskutiert, und die Datenschutzbehörde stellte einen Trend zur automatischen Verarbeitung vertraulicher Daten (elektronische Patientendateien usw.) in großen Systemen mit weiter gefassten Zugangsregeln fest.

Bezüglich der Selbstverwaltung gab die Datenschutzbehörde Stellungnahmen zu zwei Verhaltensvorschlägen ab, einen mit Bezug auf eine Abänderung des bestehenden Kodexes über Marktforschungstätigkeiten und einen über Inkassotätigkeiten.

Im April 2004 leitete das Justizministerium eine Untersuchung der bestehenden Datenschutzgesetzgebung daraufhin ein, inwieweit sie die Privatsphäre angemessen schützt. Vor allem analysiert wird das Verhältnis zwischen Zwangsmaßnahmen und Überwachungsmethoden einerseits und dem Schutz der Privatsphäre andererseits. Ebenfalls untersucht wird, ob die verfassungsrechtlichen Bestimmungen über das Recht auf Privatsphäre im Rahmen der automatisierten Datenverarbeitung abgeändert werden müssen, damit sie das gleiche rechtliche Gewicht wie andere in der Verfassung verankerte Rechte und Freiheiten bekommen. Die Untersuchung wird von Abgeordneten und Datenschutzexperten durchgeführt. Die Ergebnisse dieser Untersuchung werden gegen Ende März 2007 vorgestellt.

Vereinigtes Königreich

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

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

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

B. Bedeutende Rechtsprechung

2004 gab es keine bedeutende Rechtsprechung bei den britischen Gerichten, die sich auf 95/46/EG und 2002/58/EG bezogen hätte.

C. Wichtige spezifische Themen

Nach der Beratung über die Berechtigungskarten im vorigen Jahr gab die britische Regierung ihr Ausweisgesetz 2004 heraus. Das Gesetz sieht einen Ausweis mit biometrisch aktiviertem Chip vor, der sich auf eine zentrale Datenbank mit einer Vielzahl an Informationen über Einzelpersonen stützt. Informationen im Register wären u. a. Name, Geburtsdatum, Adresse, frühere Adressen, biometrische Merkmale und ein Nachverfolgungsaudit darüber, wie oft die Identität anhand des Registers überprüft wurde.

Der Datenschutzbeauftragte versuchte, einen Informationsbeitrag zur Diskussion über den vorgeschlagenen Ausweis zu leisten und diese dahingehend zu beeinflussen, dass dieser das Datenschutzgesetz 1998 erfüllt. Zu dem Zweck hat der Datenschutzbeauftragte auf die Beratungen des Innenministeriums über den Ausweisgesetzesentwurf reagiert, mit dem Innenministerium gesprochen, an den Untersuchungen des parlamentarischen Ausschusses bezüglich der Vorschläge teilgenommen und Informationen für die Parlamentsdebatte geliefert. Der Datenschutzbeauftragte wies nachdrücklich auf die von ihm wahrgenommenen Probleme mit dem Vorhaben hin, unter anderem den Umfang und die Bedeutung der aufbewahrten Informationen, den Zugang zur Datenbank und die Notwendigkeit einer stärkeren Beachtung der Datenschutzmaßnahmen.

Der Datenschutzbeauftragte hat Gespräche mit dem Ministerium für Handel und Industrie geführt, um die ihm eingeräumten Vollmachten bei der Bekämpfung unerwünschter Marketingmails aus dem Vereinigten Königreich zu erweitern. Der Datenschutzbeauftragte ist sich bewusst, dass dies ein Bereich ist, in dem eine effiziente Zusammenarbeit erforderlich ist. Er hat eine Absichtserklärung mit anderen relevanten Stellen im Vereinigten Königreich, in Australien und in den Vereinigten Staaten unterzeichnet.

Der Datenschutzbeauftragte ist sich der Bedeutung der Prävention und Behandlung von Kindesmissbrauchfällen und der Notwendigkeit eines Informationsaustauschs unter den mit den entsprechenden Fällen befassten Stellen bewusst. Dennoch gibt der Vorschlag Anlass zu großer Sorge, Datenbanken oder Verzeichnisse aller Kinder im Vereinigten Königreich (Kindergesetz 2004) anzulegen. Der Beauftragte hegt folgende Bedenken: Die Begründung für ein solch weit reichendes Vorhaben ist unzureichend; es kann erhebliche Schwierigkeiten bei der Sicherung und Aktualisierung der Datenbank geben; es besteht große Unsicherheit und die Gefahr negativer Folgen im Zusammenhang mit der Verwendung von Verdachtsindikatoren, und es besteht die konkrete Gefahr, dass die Privatsphäre von Kindern und Eltern beeinträchtigt wird.

2004 unterrichtete der Datenschutzbeauftragte die nachstehenden parlamentarischen Ausschüsse :

- Ausschuss für innere Angelegenheiten (Untersuchung über Ausweise).
- Ausschuss für Verfassungsangelegenheiten (Untersuchung der Arbeit des Datenschutzbeauftragten. Dazu gehörte die frühere Zwangsmaßnahme des Datenschutzbeauftragten gegen Bonitätsauskunfteien und gegen die Übertragung personenbezogener Daten an Datenverarbeiter außerhalb Europas.)

2004 beantwortete der Datenschutzbeauftragte die nachstehenden Regierungsanfragen:

- Übersicht über die Zivilverfahren seitens der und gegen die Krone. April 2004.
- Rechtsmittelanträge und Rechtsmittelüberprüfung. April 2004.
- Beratung über den Ausweisgesetzentwurf. Juli 2004.
- Polizei: Modernisierung der Polizei zwecks Anpassung an die Bedürfnisse der Gemeinschaft. Oktober 2004.

Kapitel 3

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. DIE EUROPÄISCHE KOMMISSION

3.1.1. Eurobarometer

Anfang 2004 wurden zwei Meinungsumfragen veröffentlicht, die Eurobarometer im Herbst 2003 durchgeführt hatte. Die erste Umfrage untersuchte mittels persönlicher Befragung die Meinung der EU-Bürger bezüglich der Tatsache, dass öffentliche und private Organisationen ihre persönlichen Daten besitzen, sowie zu diesbezüglichen Datenschutzthemen. Bei der zweiten Umfrage wurde die Meinung europäischer Unternehmen zum Datenschutz über Telefoninterviews eingeholt. Es zeigten sich erhebliche Informationsdefizite bei den Bürgern wie bei den Unternehmen.[23]

3.1.2. Bericht über die Schweiz

Wie in Artikel 4 Absatz 1 der Angemessenheitsentscheidung 2000/518/EG gefordert, haben die Kommissionsdienststellen eine Untersuchung über die Anwendung dieser Entscheidung seitens der Schweizer Behörden im Zeitraum von Mitte Juli 2000 bis Mitte April 2004 angestellt (Arbeitsdokument vom 20. Oktober 2004, SEC (2004) 1322[24]).

Die Kommissionsdienste haben keine größeren Probleme mit Bezug auf das derzeitige Schweizer Datenschutzsystem festgestellt und sind der Ansicht, dass das Schweizer Datenschutzsystem weiterhin ein angemessenes Maß an Schutz personenbezogener Daten im Sinne des Artikels 25 der Richtlinie gewährleistet. Die Kommissionsdienste sind vor allem mit der Situation der internationalen Datentransfers in Drittländer zufrieden, weil im Falle des Datentransfers von der Schweiz in Länder, die die Konvention 108 des Europarates nicht ratifiziert haben, laut Artikel 6 Absatz 1 des Schweizer Datenschutzgesetzes diese Länder einen gleichwertigen Schutz wie das Schweizer Datenschutzgesetz bieten müssen.

3.1.3. Bericht über den „sicheren Hafen" (Vereinigte Staaten von Amerika)

Am 20. Oktober 2004 gab die Kommission einen Bericht über die Umsetzung des Safe-Harbour-Beschlusses („Arbeitsdokument der Dienststellen der Kommission, SEC (2004) 1323 – Umsetzung des Kommissionsbeschlusses 520/2000/EG über den angemessenen Schutz personenbezogener Daten im Rahmen der Grundsätze des „sicheren Hafens" und die diesbezüglichen „Häufig gestellten Fragen" (FAQ), vorgelegt vom Handelsministerium der Vereinigten Staaten von Amerika"[25]) heraus. Während die Umsetzung des Safe-Harbour-Beschlusses im Wesentlichen den Schutz des Rechtes auf die Privatsphäre gewährleistet, wurden verbesserungswürdige Mängel bei der vollen Umsetzung des Beschlusses festgestellt. Eine kurze Zusammenfassung der im Bericht festgestellten Mängel: (a) Laut Bericht sollte das US-Handelsministerium („DoC") bei der Untersuchung von amerikanischen Firmen, die ihre Einhaltung der Datenschutzprinzipien selbst zertifizieren, größere Sorgfalt walten lassen, damit keine Unternehmen auf die Safe-Harbour-Liste gelangen, die keine öffentlich verfügbare Datenschutzpolitik vorweisen können. Die Kommission sieht dies als einen der Fälle, in denen die FTC eine aktivere Rolle bei der Überwachung der Einhaltung der Datenschutzgrundsätze seitens Firmen spielen und bei Bedarf Ermittlungen anstellen sollte. (b) Bezüglich der Funktion des DoC als für die Eigenzertifizierung zuständiges Gremium ist die Kommission der Meinung, dass das DoC verschiedene Änderungen an seiner

[23] Zusammenfassung und vollständiger Bericht: siehe http://europa.eu.int/comm/justice_home/fsj/privacy/lawreport/index_en.htm#actions

[24] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy/sec-2004-1322_en.pdf

[25] http://europa.eu.int/comm/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf

Website vornehmen sollte bzw. unter anderem deren Transparenz verbessern sollte. (c) Bezüglich der alternativen Rückgriffsysteme beleuchtet der Bericht bestimmte Mängel in der Arbeitsweise derselben und regt in Anbetracht ihirer Bedeutung bei der Umsetzung des Safe-Harbor-Programmes eine rasche Lösung dieser Probleme an.

3.1.4. Beschluss über die Angemessenheit der Übertragung von Fluggastdatensätzen an die Vereinigten Staaten

Die Übermittlung personenbezogener Daten in Drittländer muss entsprechend Artikel 25 erfolgen oder andernfalls durch die Ausnahmen von Artikel 25, die durch Artikel 26 zugelassen sind, abgedeckt sein. Bei der Prüfung der Abweichungen von Artikel 26 kam die Arbeitsgruppe zu dem Ergebnis, dass keine dieser Bestimmungen eine angemessene Grundlage für den Transfer von Fluggastdatensätzen zu Zwecken der US-Behörden bildet[26].

Die Kommission schloss sich dieser Auffassung an und verabschiedete am 14. Mai 2004[27] einen Beschluss gemäß Art. 25 der Richtlinie 95/46/EG, laut dem das United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten) ein angemessenes Maß an Schutz für die personenbezogenen Daten bietet, die in den Fluggastdatensätzen von Flugpassagieren enthalten sind und die von der Europäischen Union bezüglich der Flüge in die und aus den USA übermittelt werden. Der Beschluss legt genaue Bedingungen für die Verarbeitung von Fluggastdatensätzen durch die US-Zoll- und –Grenzschutzbehörden fest. Der Beschluss wurde nach langwierigen Verhandlungen mit den USA getroffen.

Die Datenverarbeitung von Fluggastdatensätzen durch Fluggesellschaften in der EU, d.h. die Sammlung in der EU und die Weiterleitung an die USA, ist den Bestimmungen der Richtlinie ungeachtet der Staatsangehörigkeit der Fluggesellschaften unterworfen. Das bedeutet, dass nicht nur EU-Fluggesellschaften den Entscheidungen bezüglich der Fluggastdatensätze unterliegen, sondern alle Fluggesellschaften, die in der EU personenbezogene Daten im Hinblick auf Flüge aus der EU in die USA und aus den USA in die EU verarbeiten.

3.2. DER RAT

Die Übermittlung von Fluggastdatensätzen an das United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten).

Neben der Angemessenheitsentscheidung der Kommission schien ein internationales Abkommen erforderlich, um Fluggesellschaften die Erfüllung von US-Anforderungen von Fluggastdatensätzen als legale Verpflichtung laut Artikel 7 c der Richtlinie zu ermöglichen. Die Angemessenheitsentscheidung der Kommission besagt lediglich, dass angemessene Sicherheit gewährleistet ist und kann dieser Erfordernis nicht genügen. Der Rat schloss am 17. Mai 2004[28] ein internationales Abkommen, das Fluggesellschaften die Übermittlung von Fluggastdatensätzen an die US-Zollbehörden erlaubt und den Fluggesellschaften die notwendige Rechtsgrundlage für die Verarbeitung von Fluggastdatensätzen in der EU entsprechend den US-Anforderungen bietet.

3.3. DAS EUROPÄISCHE PARLAMENT

Bericht über den ersten Bericht über die Umsetzung der Datenschutzrichtlinie

Im März 2004 verabschiedete das Europäische-Parlament eine Resolution über den ersten Bericht über die Umsetzung der Datenschutzrichtlinie, die von der Kommission im Mai 2003 verabschiedet

[26] Stellungnahme 6/2002 zu §2.5
[27] OJ L235, 6.7.2004, Seite 11
[28] OJ L183, 20. Mai 2004, Seite 83

worden war. Die Resolution unterstützte den Befund der Kommission nachdrücklich und forderte alle Betroffenen zur Zusammenarbeit und zur Gewährleistung der korrekten Umsetzung der Richtlinie auf. Auch andere Themen wie die Übermittlung von Fluggastdatensätzen an die US-Behörden, die Notwendigkeit eines umfassenden, auf mehreren Säulen ruhenden europäischen Datenschutzsystems, die Bedenken wegen Ausnahmen zu den Datenschutzgesetzen und viele andere Themen wurden angeschnitten.

3.4. DER EUROPÄISCHE GERICHTSHOF

Die Übermittlung von Fluggastdatensätzen an das United States Bureau of Customs and Border Protection (Zoll- und Grenzschutzbehörde der Vereinigten Staaten)

Das Europäische Parlament beschloss die Einleitung eines Verfahrens beim Gerichtshof gegen den Rat und die Kommission wegen der Verabschiedung eines Rechtsrahmens (eine Angemessenheitsentscheidung und ein internationales Abkommen) für die Weiterleitung von Fluggastdatensätzen an die USA (Rechtssachen C-317 und 318/04). Der Beschluss basierte auf der Auffassung, dass zum einen dieser Rechtsrahmen die Rechte des Parlamentes nicht angemessen berücksichtigt und zum anderen die Vereinbarungen keinen angemessenen Datenschutz bieten. Ein früherer Parlamentsbeschluss, den vorgeschlagenen rechtlichen Rahmen dem Europäischen Gerichtshof zur Einholung einer gerichtlichen Meinung zu unterbreiten, wurde wegen der Verabschiedung beider Instrumente fallen gelassen.

3.5. DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

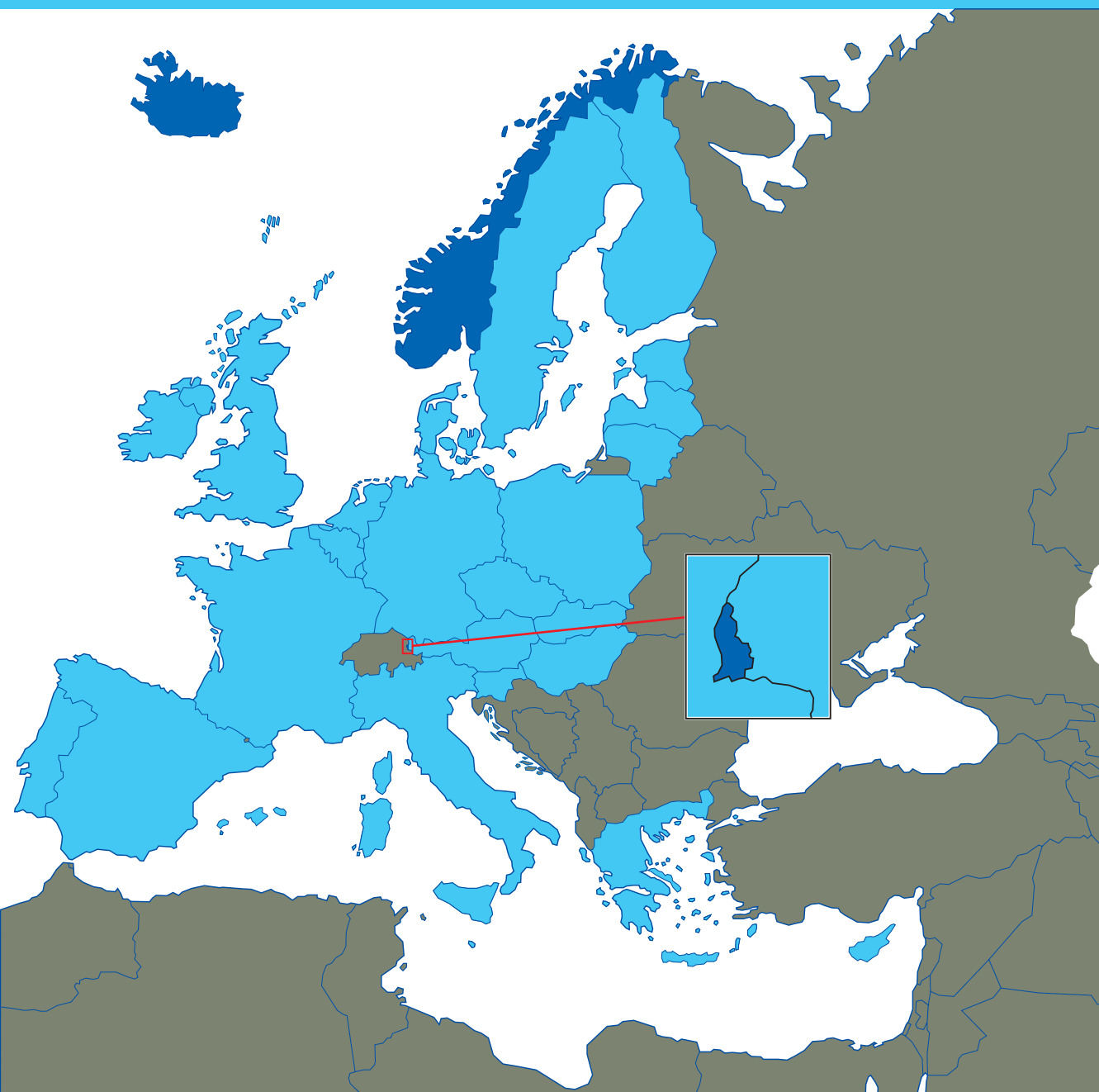
Der Europäische Datenschutzbeauftragte wurde gemäß dem Beschluss 2004/55/EG des Europäischen Parlamentes und des Rates vom 22. Dezember 2003, der am 17. Januar 2004 in Kraft trat, nominiert. Weitere Informationen sowie der Jahresbericht 2004 stehen unter http://www.edps.eu.int.

3.6. DIE EUROPÄISCHE KONFERENZ

Die jährliche Frühjahrskonferenz der Datenschutzbehörden in der Europäischen Union, die im Jahr 2004 von der niederländischen Datenschutzbehörde in Rotterdam organisiert wurde, konzentrierte sich auf effiziente Überwachungsmethoden und -vereinbarungen. Die dreitägige Konferenz wurde am 22. April von Justizminister J.P.H. Donner eröffnet, der zu einer weiteren Zusammenarbeit bei der Überwachung von Recht und Ordnung in Europa innerhalb der dritten Säule, dem Zuständigkeitsbereich der Justiz- und Innenministerien, aufrief. Die europäischen Datenschutzregulierungsinstanzen haben ihre Zusammenarbeit bei der Überwachung und Beratung in den Verantwortungsbereichen der Polizei und der Justizministerien verstärkt.

Kapitel 4

Wichtigste Entwicklungen im Europäischen Wirtschaftsraum



Island

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

Im Jahre 2004 wurden eine Reihe Gesetze, Verwaltungsregeln und –verordnungen verabschiedet. Die wichtigsten waren Folgende:

1. Versicherungsvertragsgesetz Nr. 30/2004. – Laut Artikel 82 §2 dieses Gesetzes hat eine Versicherungsgesellschaft nicht das Recht, vor oder nach Abschluss einer Lebens-, Krankheits- oder Unfallsversicherung Daten über die genetischen Eigenschaften von Menschen sowie über ihr Krankheitsrisiko anzufordern, sich in anderer Weise zu beschaffen, entgegenzunehmen oder zu verwenden. Sie darf auch keine Untersuchungen anfordern, die für die Erlangung solcher Daten erforderlich sind. Dieses Verbot gilt jedoch nicht für Beobachtungen des aktuellen oder früheren Gesundheitszustandes des Antragstellers oder anderer Personen. Die isländische Datenschutzbehörde Persónuvernd kritisierte diese Ausnahme in ihrer Stellungnahme zum parlamentarischen Gesetzentwurf, der später verabschiedet wurde, begrüßte jedoch andere Bestimmungen von Artikel 82 §2.

2. Verordnung über klinische Erprobung von Arzneimitteln an Menschen, Nr. 443/2004. – Diese Verordnung des Gesundheitsministeriums auf der Grundlage von Artikel 9 und 47 des Arzneimittelgesetzes Nr. 93/1994 enthält u. a. Bestimmungen über die Informationen, die einem Studienteilnehmer bei einer klinischen Erprobung von Arzneimitteln mitgeteilt werden müssen. Dies betrifft auch die Verarbeitung personenbezogener Daten. Die Verordnung enthält außerdem eine Bestimmung zur Aufbewahrungsfrist der Daten im Rahmen solcher Studien. In Übereinstimmung mit der internationalen Norm „Good Clinical Practice" sind die Daten für 15 Jahre nach der Erstellung des Studienabschlussberichtes aufzubewahren.

3. Vorschriften für die Melde- bzw. Genehmigungspflicht bezüglich der Verarbeitung personenbezogener Daten 698/2004. – Diese Vorschriften, die vom „Persónuvernd" im Einklang mit dem Gesetz 77/2000, Art. 31 und 33, erlassen wurden, sind auf Englisch auf der Website der Behörde zu finden. Sie ersetzen die Vorschriften 90/2001. Die wichtigste Änderung ist, dass elektronische Überwachung, die nur der Sicherheit und dem Eigentumsschutz dient, nicht mehr gemeldet werden muss.

4. Vorschriften für die elektronische Überwachung am Arbeitsplatz, in Schulen und anderen Bereichen, die von einer begrenzten Zahl von Menschen frequentiert werden, 888/2004. – Diese Vorschriften wurden vom „Persónuvernd" im Einklang mit dem Gesetz 77/2000, Art. 37, erlassen. Sie enthalten unter anderem Bestimmungen darüber, in welchen Fällen elektronische Überwachung erlaubt ist, wie lange Daten, die während der Überwachung gespeichert wurden, aufbewahrt werden dürfen, über die Nutzung des Internets am Arbeitsplatz, die automatische Aufzeichnung von Führerscheindaten der Mitarbeiter, die Überwachung zu Arbeitsaufsichtszwecken, die Verpflichtung eines Überwachungsverantwortlichen, die betroffenen Personen zu informieren, und die Verpflichtung eines Überwachungsverantwortlichen, bei dessen Tätigkeiten persönliche Daten verarbeitet werden, Überwachungsregeln aufzustellen.

B. Bedeutende Rechtsprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Eine der Hauptaufgaben des Persónuvernd im Jahre 2004 waren Inspektionen. Es wurden formelle administrative Entscheidungen mit Bezug auf Inspektionen gefällt, die 2002 und 2003 begannen: über die Gesetzesmäßigkeit der Datenverarbeitung bei drei Biobanken und beim Straßenverkehrsamt, das unter anderem persönliche Daten mit Bezug auf Verkehrsunfälle verarbeitet. Es wurden keine Gesetzwidrigkeiten bei der Datenverarbeitung und nur einige geringfügige Fehler bei der Sicherheit festgestellt.

Neben diesen Beschlüssen gab „Persónuvernd" drei Stellungnahmen mit den Ergebnissen von Überprüfungen der Rechtmäßigkeit der Verarbeitung von Stellenbewerberdaten bei Arbeitgebern heraus. Diese Inspektionen, mit denen im Jahr 2003 begonnen wurde, sind Teil eines panskandinavischen Projektes. Alle drei untersuchten Parteien, d.h. ein Pharma-Unternehmen, ein Sicherheitsunternehmen und die Zollverwaltung in Reykjavik, erhielten eine Reihe Empfehlungen zu Reformen in der Datenverarbeitung.

Liechtenstein

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

Das Datenschutzgesetz (DSG) wurde geändert, und zwar in zwei wichtigen Punkten. Der erste betrifft die Einführung der Möglichkeit einer Einsichtnahme in das Datenregister über das Internet. Es dürfen also moderne Kommunikationsverfahren eingesetzt werden. Die Arbeitsbelastung der Verwaltung wird dadurch entsprechend verringert. Der Zweite betrifft die Verlängerung einiger Übergangsbestimmungen. Die neue Bestimmung lautet, dass die Behörden bis 01. August 2007 mit der Verarbeitung persönlicher Profile und geheimer privater Daten fortfahren können, ohne dass eine bestimmte gesetzliche Bestimmung sie dazu ermächtigt. Diese Verlängerung war nötig geworden, weil die erforderlichen Gesetzesänderungen zum 01. August 2004 noch nicht fertig gestellt waren.

Die Datenschutzverordnungen (DSV) wurden ebenfalls geändert. Laut dem neuen Abschnitt 28 muss das Register nicht mehr in regelmäßigen Abständen veröffentlicht werden, sondern kann im Internet eingesehen werden. Weiterhin wurde der Abschnitt 5 (Datentransfer in andere Länder) an die Richtlinie 95/46/EG angepasst. Artikel 25 Absatz 2 der Richtlinie wurde übernommen. Die Liste der Länder im Anhang, die angemessenen Datenschutz bieten, wurde angepasst.

Stellungnahmen zu gesetzgebenden Instrumenten

Neben den Überarbeitungen des DSG und der DSV wurde die Datenschutzbehörde zu weiteren 21 Gesetzentwürfen um Rat gebeten. Folgende Entwürfe sind erwähnenswert:

- Verordnung über die Krankenversicherungskarte im Zusammenhang mit der europäischen Krankenversicherungskarte. Diese Verordnung stellt die Grundlage für die Krankenversicherungskarte und die Gesundheitskarte dar. Zu Beginn werden nur administrative Daten verarbeitet.

Anschließend eventuell auch Gesundheitsdaten – jedoch nur mit der vorhergehenden ausdrücklichen Zustimmung der betroffenen Person. Ende 2004 befand sich die Verordnung noch im Entwurfsstadium.

- Kommunikationsgesetz: Dieses setzt eine Reihe von Richtlinien um, unter anderem 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. Die Stellungnahme des Amtes wurde im Rahmen einer öffentlichen Beratung abgegeben. Der Entwurf wird anschließend dem Landtag unterbreitet.

- Vertrag zwischen der Schweiz und Liechtenstein über die gemeinsame Benutzung von Fingerabdruck- und DNA-Profildatenbanken. Dieser Vertrag schafft die rechtliche Grundlage für Datentransfers, die bereits in der Praxis stattfinden. Darüber hinaus werden sämtliche Bestimmungen des Schweizer DNA-Profil-Gesetzes in die Gesetzgebung von Liechtenstein übernommen. Dies ist eine weitere Datenschutzmaßnahme, weil sie klare gesetzliche Regeln enthält.

- Vertrag zwischen der Regierung von Österreich, dem Schweizer Bundesrat und der Regierung des Fürstentums Liechtenstein über den Austausch in Asylangelegenheiten. Ende 2004 war dieses Instrument noch im Entwurfsstadium. Es stellt ebenfalls eine angemessene Rechtsgrundlage für Datentransfers in Asylangelegenheiten dar.

B. Bedeutende Rechtsprechung

Der erste Bericht der Datenschutzkommission (DSK) wurde in diesem Jahr herausgegeben. Er unterstützt eine Empfehlung der DSB an die örtlichen Behörden und enthält den Beschluss, dass die örtlichen Behörden künftig nicht mehr ohne weiteres Baugenehmigungen veröffentlichen dürfen. Die Datenschutzbestimmungen müssen nun eingehalten werden. Bisher veröffentlichten die Behörden sämtliche von ihnen genehmigten Baugenehmigungsanträge aus Gründen der Transparenz und machten sich dabei die unterschiedlichsten Medien zunutze, z.B. Anschläge, Aufzeichnungen von Stadt-/Gemeinderatssitzungen, lokale Fernsehsender, Newsletter und Websites. Das DSK entschied, dass es keine gesetzliche Grundlage für die regelmäßige Bekanntmachung von genehmigten Bauanträgen ohne vorherige Zustimmung der Antragsteller gibt.

C. Wichtige spezifische Themen

Im zweiten Berichtsjahr lag der Schwerpunkt auf der Prüfung der zentralen Personalverwaltung (ZPV), einer zentral verwalteten Datenbank der Liechtensteiner Nationalverwaltung, auf deren Übereinstimmung mit den Datenschutzbestimmungen. Die Prüfung bezog sich auf das Recht der Behörden auf den Zugang zu privaten Datenfeldern. Die Datenbank, die die administrativen Prozeduren erleichtern soll, enthält im Wesentlichen die gesamte Bevölkerung mit sämtlichen persönlichen Daten. Das Kernelement ist eine Nationalcodenummer, die jeder Person und jeder Körperschaft zugeteilt wird. Eine umfassende Datenbank wie diese, die zur Verarbeitung persönlicher Profile eingesetzt wird, wurde bisher ohne gesetzliche Grundlage betrieben. Artikel 8 Absatz 7 der Datenschutzrichtlinie 95/46/EG wurde nicht erfüllt. Laut diesem Artikel müssen die Mitgliedsländer die Bedingungen bestimmen, unter denen eine nationale ID-Nummer bzw. andere allgemeine Identifikatoren verarbeitet werden dürfen. Zu Beginn des Jahres 2004 richtete die Regierung eine Arbeitsgruppe zur Untersuchung des Datenschutzes bei der ZPV ein. Die Arbeitsgruppe, in der Datenschutzmitarbeiter vertreten sind, vereinbarte ein Zugangsantragsverfahren für Befugte. Zugangsgenehmigungen wurden nach den Kriterien der rechtlichen Grundlage und der Verhältnismäßigkeit erteilt. Aus diversen Gründen konnte die Untersuchung nicht bis Ende 2004 abgeschlossen werden.

Die Arbeitsgruppe versucht, eine gesetzliche Grundlage für die Datenbank zu schaffen. Ähnliche Fragen stellen sich bei den lokalen Behörden, da diese ebenfalls persönliche Daten der Bevölkerung speichern.

Die Webseite der Datenschutzbehörde www.sds.llv.li wurde mehr oder weniger fortlaufend erweitert und aktualisiert. Zu den spezifischen Themen gehörten der Datenschutz in der Schule, Datenschutz und E-Government, Spam, Videoüberwachung, die Präzisierung der Richtlinien der Datenschutzbehörde über die Freigabe von personenbezogenen Daten zu Bevölkerungskontrollzwecken, der DSB-Bericht 2003 usw.

Register: Das Datenregister wurde noch nicht auf die Webseite der Datenschutzbehörde geladen, wenngleich die rechtliche Grundlage dafür nach der Überarbeitung des Datenschutzgesetzes geschaffen wurde.

Norwegen

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

Bedeutende Änderungen in Datenschutzgesetzen bzw. Gesetzen zum Schutz der Privatsphäre

2004 erarbeitete die norwegische Datenschutzbehörde Vorschläge zur Änderung der Datenschutzverordnungen. Ziel dieser Vorschläge ist die Erleichterung bestimmter Aspekte der Lizenzpflichten für bestimmte Forschungsprojekte, die von einer Ethikkommission empfohlen werden. Die Änderungen traten am 01. Juli 2005 in Kraft.

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

➔ *Das Devisenkontrollgesetz*

Ein neues Register wurde im Devisenkontrollgesetz zu Kontroll- und Nachforschungszwecken im Zusammenhang mit dem Währungsumtausch und den Geldströmen aus dem Land und ins Land vorgesehen.

Die Datenschutzbehörde vertrat die Ansicht, dass der ursprüngliche Vorschlag einer ausführlichen Registrierung geringer Beträge und der Datenspeicherung über einen Zeitraum von über zehn Jahren zu weit in die Privatsphäre hineinreichen würde. In seiner Debatte über den Gesetzgebungsentwurf beschloss der Storting, das norwegische Parlament, eine Verkürzung des Aufbewahrungszeitraumes und des Umfangs an Details bei der Registrierung geringer Beträge.

➔ *Das Gesetz über das Arbeitsumfeld*

Eine Gesetzesbestimmung wurde dem Gesetz über das Arbeitsumfeld hinzugefügt. Sie enthält die Verordnung, dass alle Mitarbeiter spezielle ID-Karten erhalten müssen.

Während der Beratungsrunde konnte die Datenschutzbehörde nicht nachvollziehen, wie eine solche ID-Karte bei der Vorbeugung von Sozialdumping und bei der Verbesserung des Arbeitsumfeldes – den Zielen der Initiative – helfen könne.

Zudem wurde eine gesetzliche Handhabe eingeführt, derzufolge Arbeitgeber eine stärkere Kontrolle über ihre Beschäftigten ausüben können. Dazu gehört auch das Recht, die Mitarbeiter unter bestimmten Bedingungen auf Rauschmittel zu untersuchen.

B. Bedeutende Rechtsprechung

Keine nennenswerten Entwicklungen.

C. Wichtige spezifische Themen

Es wurden Initiativen ergriffen, um Organisationen und Agenturen bei der Erfüllung ihrer Datenschutzverpflichtungen oder bei der allgemeinen Verbesserung des Schutzes der Privatsphäre zu unterstützen.

Richtlinien

Die Datenschutzbehörde wirkte an der Formulierung von drei Industrienormen für eine Dachorganisation von ehrenamtlichen Fachgremien und Industriegremien, einer Industrienorm für die Informationssicherheit im Gesundheitssektor und einer Norm für die Verarbeitung persönlicher Informationen im Sport mit.

Beratungen

Polizeimethoden

Ein öffentlicher Ausschuss, der die Erfordernis bestimmter Methoden bei der Polizei beurteilte, stellte seinen Bericht im Frühjahr 2004 vor. Einer der leitenden Berater der Datenschutzbehörde saß im Komitee und erhob einige grundlegende Einwände gegen die Vorschläge der Mehrheit.

Im Beitrag der Datenschutzbehörde zur Beratungsrunde gab es vor allem Einwände gegen die Vorschläge mit Bezug auf das Einlesen von Daten und elektronische Raumüberwachungen. Das Einlesen von Daten ist eine Methode, die die Privatsphäre stark beeinträchtigt. Bei dieser Methode können auch nicht mitgeteilte Informationen von der Polizei genauer unter die Lupe genommen werden. Dies kann zum Beispiel durch Spyware der Polizei auf dem Computer eines Verdächtigen erfolgen. Die Software speichert jeden Tastenanschlag, auch nachträglich gelöschte Daten. Die Datenschutzbehörde sieht es als problematisch an, dass Gedanken, Assoziationen und Wünsche, die nicht zur Weitergabe gedacht waren, dazu verwendet werden könnten, um die Schuld einer Person nachzuweisen.

Verschlankter öffentlicher Sektor

Im Laufe des Jahres wurde die Datenschutzbehörde in Angelegenheiten, die wesentliche Fragen bezüglich der Verarbeitung persönlicher Informationen im öffentlichen Sektor aufwerfen, um Rat gebeten. Vielen Initiativen ist der Wunsch nach einer kosteneffizienteren und kundenrientierten öffentlichen Verwaltung entsprechend dem Modernisierungsprogramm der Regierung gemeinsam. Einige der vorgeschlagenen Maßnahmen würden dazu führen, dass viele persönliche Daten in zentralen Datenbanken gespeichert und Portale für den Austausch von persönlichen Daten zwischen verschiedenen Verwaltungen eingerichtet werden. Beispiele sind die Pläne des Modernisierungsministeriums für eine gemeinsame IT-Architektur und die Einrichtung einer behördlichen Datenbank, die von verschiedenen Behörden benutzt werden kann. Außerdem wurden das „norwegische Patientenregister" des Gesundheitsministeriums sowie das Zentralregister des Unterrichts- und Forschungsministeriums für landesweite Prüfungen in Schulen gebildet.

Die Datenschutzbehörde ist der Ansicht, dass rigorose Mechanismen eingebaut werden müssen, um zu verhindern, dass persönliche Daten unnötig verbreitet oder zweckentfremdet werden, wenn es sich um große Datenbanken handelt.

In mehreren Fällen fand praktisch keinerlei Beurteilung des Datenschutzes und der Informationssicherheit statt.

Die Berichte plädieren für das Prinzip der Wiederverwendung und die effiziente Nutzung verschiedener Basisdaten in allen Behörden. Ein beachtlicher Teil des Informationsaustauschs besteht natürlicherweise aus persönlichen Daten. Der Umstand, dass die Behörden auf diese Weise einfacheren Zugang zu den zunehmenden Informationsmengen über die Bürger erhalten, ohne dazu in unmittelbarem Kontakt mit ihnen zu stehen, könnte in isolierter Betrachtung die Effizienz der Verwaltung steigern. Allerdings könnte dies auch zu einer effektiven Machtübertragung von den einzelnen Bürgern auf die Behörden beitragen.

Norwegisches Patientenregister

2004 schlug das Gesundheits- und Sozialministerium die Änderung des norwegischen Patientenregisters in ein identitätsabhängiges Register vor. Dies lehnt die Datenschutzbehörde entschieden ab. Im Laufe der Beratungsrunde machte die Datenschutzbehörde deutlich, dass sich ein personenspezifisches norwegisches Patientenregister mit zentraler Erfassung des Gesundheitszustandes jedes einzelnen Bürgers Norwegens und dessen Benutzung von Krankenhäusern von seiner Geburt bis zu seinem Tod negativ auf die Privatsphäre eines jeden Einwohners Norwegens auswirken würde. Das vorgeschlagene Patientenregister wäre ein Schlüsselregister. Mithilfe einiger weniger Informationen aus dem Register könnten die Bürger in den meisten anderen Gesundheitsregistern identifiziert werden – ganz gleich, ob diese Register grundsätzlich anonym sind oder

unter Pseudonymen geführt werden. Wenn bestehende Register mit dem vorgeschlagenen Patientenregister verknüpft werden, wird die Informationskartographie fast allumfassend.

Zielgerichtetere Inspektionen

Die Datenschutzbehörde beschloss 2004, einige ihrer Inspektionstätigkeiten schwerpunktmäßig auf bestimmte Projekte auszurichten. Dieses Verfahren wurde für Sektoren gewählt, in denen es wichtig ist, Instrumente und Mittel für eine besonders gründliche und somit auch ressourcenintensive Erfassung anzuwenden. Projektinspektionen wurden in folgenden Bereichen durchgeführt:

- Frauenhäuser
- Elektronische Kommunikation im Gesundheitssektor
- Nationaler Versicherungsdienst
- Medizinische Forschung

Die Datenschutzbehörde bestellte eine Projektgruppe, die im Frühjahr 2004 fünfzig Forschungsprojekte durrchführte. Untersucht wurden 26 verschiedene Unternehmen im Gesundheitsbereich, Bildungseinrichtungen, Forschungsinstitute und Arzneimittelhersteller. Das Projekt deckte mehrere Probleme auf, die die Datenschutzbehörde für schwerwiegend hält. Die Datenschutzbehörde stellte Zuwiderhandlungen gegen Lizenzierungsbedingungen, illegal gespeicherte sensible personenbezogene Daten, unzureichende interne Kontrollen und nicht klar abgesteckte Verantwortungsbereiche fest.

Es wurde ein separater Bericht auf Norwegisch über die Ergebnisse und Tendenzen im Zusammenhang mit dem betreffenden Projekt erstellt.

Vollautomatische Mautstationen

Auch wenn an den vollautomatischen Mautstationen keine sensiblen personenbezogenen Daten verarbeitet werden, beschloss die Datenschutzbehörde im Herbst 2004, dass vollautomatische Mautstationen eine Lizenz erwerben müssen. Die Begründung für diese Forderung lautet, dass diese Art der Datenverarbeitung eindeutig wichtige persönliche Interessen verletzt. Nach Ansicht der Datenschutzbehörde werden wichtige persönliche Interessen immer dann verletzt, wenn Personen nicht selbst entscheiden können, ob sie bei ihren Fahrten auf norwegischen Straßen Spuren hinterlassen möchten. Die derzeitigen Systeme bieten den Straßenverkehrsteilnehmern keine echten Alternativen hinsichtlich Informationen, Verfügbarkeit, Kosten und Funktionalitäten.

Untersuchung auf Rauschmittel

Securitas hat ein System für die Untersuchung ihrer Mitarbeiter auf Rauschmittel mit deren Zustimmung entwickelt. Die Datenschutzbehörde ist jedoch der Auffassung, dass das Weisungsrecht des Arbeitgebers und die Zustimmung der Arbeitnehmer keine ausreichende Rechtsgrundlage für solche Untersuchungen darstellen. Auch wenn die Datenschutzbehörde nicht ohne weiteres die Freiwilligkeit einer gewährten Zustimmung anzweifeln darf, steht andererseits auch fest, dass sich viele Arbeitnehmer gezwungen fühlen könnten, einem solchen Eingriff in ihre Privatsphäre zuzustimmen. Wenn sie in eine solche Untersuchung nicht einwilligen, könnte dies ohne weiteres bedeuten, dass ihnen eine Stelle verwehrt wird.

Kapitel 5

Mitglieder und Beobachter der Art. 29 Datenschutzgruppe

MITGLIEDER 2004

ÖSTERREICH Frau Dr. Waltraut KOTSCHY Österreichische Datenschutzkommission	**BELGIEN** Herr Paul THOMAS Präsident Commission de la Protection de la Vie privée (Datenschutzkommission)
ZYPERN* Frau Goulla FRANGOU Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Datenschutzbeauftragte)	**TSCHECHISCHE REPUBLIK*** Dr. Karel NEUWIRT Präsident Úřad pro ochranu osobních údajů (Datenschutzbehörde)
DÄNEMARK Frau Janni CHRISTOFFERSEN Director Datatilsynet (Dänische Datenschutzagentur)	**ESTLAND*** Herr Urmas KUKK Generaldirektor Andmekaitse Inspektsioon (Estnische Datenschutzbehörde)
FINNLAND Herr Reijo AARNIO Tietosuojavaltuutetun toimisto (Büro des Datenschutzombudsmannes)	**FRANKREICH** Frau Anne DEBET Leiterin der Abteilung für europäische, internationale und prospektive Angelegenheiten Commission Nationale de l'Informatique et des Libertés (CNIL) (Nationaler Ausschuss für EDV und Freiheiten)
DEUTSCHLAND Herr Peter SCHAAR Vorsitzender Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit	**GRIECHENLAND** Herr Nikolaos FRANGAKIS Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Griechische Datenschutzbehörde)
UNGARN* Herr Attila PETERFALVI Parlamentarischer Beauftragter Adatvédelmi Biztos Irodája (Büro des parlamentarischen Beauftragten für den Datenschutz und die Informationsfreiheit)	**IRLAND** Herr Joe MEADE Datenschutzbeauftragter (Irish Life Centre)
ITALIEN Prof. Stefano RODOTA Präsident Garante per la Protezione dei Dati personali (Datenschutzbeauftragter/-gewährsmann)	**LETTLAND*** Frau Signe PLUMINA Direktorin Datu valsts inspekcija (Datenschutzbehörde)
LITAUEN* Frau Ona JAKSTAITE Direktorin Valstybinė duomenų apsaugos inspekcija (Staatliche Datenschutzbehörde)	**LUXEMBURG** Herr Gérard LOMMEL Präsident Commission nationale pour la Protection des Données (Nationale Datenschutzkommission)

* zum 01. Mai 2004

MALTA*	**NIEDERLAND**
Herr Paul MIFSUD-CREMONA Data Protection Commissioner (Datenschutzbeauftragter)	Herr Ulco VAN DE POL College Bescherming Persoonsgegevens (CBP) (Niederländische Datenschutzbehörde)
POLEN*	**PORTUGAL**
Frau Ewa KULESZA Generalinspektorin Biuro Generalnego Inspektora Ochrony Danych Osobowych (Büro des Generalinspektors für den Datenschutz)	Herr Luís DA SILVEIRA Präsident Comissão Nacional de Protecção de Dados (Nationale Datenschutzkommission)
SLOWAKISCHE REPUBLIK*	**SLOWENIEN***
Herr Pavol HUSAR Úrad na ochranu osobných údajov Slovenskej republiky (Datenschutzbehörde)	Herr Jernej ROVSEK Stv. Ombudsman Republik Slowenien Ombudsman für Menschenrechte
SPANIEN	**SCHWEDEN**
Herr José Luis PIÑAR MAÑAS Vizevorsitzender Director Agencia de Protección de Datos (Datenschutzbehörde)	Herr Göran GRÄSLUND Director General Datainspektionen (Datenschutzaufsichtsrat)
VEREINIGTES KÖNIGREICH	**EUROPÄISCHER DATENSCHUTZAUFSICHTS-BEAUFTRAGTER**
Herr Richard THOMAS Datenschutzbeauftragter The Office of the Information Commissioner Executive Department (Büro des Datenschutzbeauftragten Exekutivabteilung)	Herr Peter HUSTINX Europäischer Datenschutzaufsichtsbeauftragter

* Stand vom 01. Mai 2004

BEOBACHTER 2004

ISLAND	**NORWEGEN**
Frau Sigrun JOHANNESDOTTIR Direktorin Icelandic Data Protection Agency (Isländische Datenschutzbehörde)	Herr Georg APENES Generaldirektor Datatilsynet (Datenbüro)
LIECHTENSTEIN	
Herr Dr. Philipp MITTELBERGER Stabsstelle für Datenschutz	

MITGLIEDER AM 25. NOVEMBER 2005

ÖSTERREICH Frau Dr. Waltraut KOTSCHY Österreichische Datenschutzkommission Ballhausplatz 1 - A - 1014 WIEN Tel.: +43 1 531 15 26 79 - Tel.: +43 1 531 15 25 25 Fax: +43 1 531 15 26 90 E-Mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	**BELGIEN** Herr Michel PARISSE Präsident Commission de la Protection de la Vie privée (Datenschutzkommission) Rue Haute, 139 - B - 1000 BRÜSSEL Tel.: +32 2 213.85.40 Fax: +32 2 213.85.65 E-Mail: commission@privacycommission.be Website: http://www.privacy.fgov.be
ZYPERN Frau Goulla FRANGOU Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Datenschutzbehörde) 40, Themistokli Dervi str. Natassa Court, 3. Stock - CY - 1066 NIKOSIA OR P.O. Box 23378 - 1682 Nikosia Tel.:+357 22 818 456 Fax +357 22 304 565 E-Mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy	**TSCHECHISCHE REPUBLIK** Herr Igor NEMEC Präsident Úřad pro ochranu osobních údajů (Datenschutzbehörde) Pplk. Sochora 27 - CZ - 170 00 PRAG 7 Tel.: +420 234 665 281 Fax: +420 234 665 501 E-Mail: info@uoou.cz Website: http://www.uoou.cz/
DÄNEMARK Frau Janni CHRISTOFFERSEN Direktorin Datatilsynet (Dänische Datenschutzagentur) Borgergade 28, 5. Stock - DK – 1300 KOPENHAGEN V Tel.: +45 33 19 32 36 Fax: +45 33 19 32 18 E-Mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	**ESTLAND** Herr Urmas KUKK Generaldirektor Andmekaitse Inspektsioon (Estnische Datenschutzbehörde) Väike - Ameerika 19 10129 TALLINN - ESTLAND Tel.: +372 6274 135 Fax: +372 6274 135, 627 4137 E-Mail: urmas.kukk@dp.gov.ee, info@dp.gov.ee Website: http://www.dp.gov.ee
FINNLAND Herr Reijo AARNIO Tietosuojavaltuutetun toimisto (Datenschutzombudsmann) P.O. Box 315 - FIN-00181 HELSINKI Tel.: +358 10 36 66700 Fax: +358 10 36 66735 E-Mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi	**FRANKREICH** Herr Georges de La LOYERE Beauftragter für den internationalen Aufgabenbereich Commission Nationale de l'Informatique et des Libertés (CNIL) (Nationale Kommission für EDV und Freiheiten) Rue Saint Guillaume, 21 - F - 75340 PARIS CEDEX 7 Tel.: +33 1 53 73 22 31 - Tel.: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-Mail: laloyere@cnil.fr Website: http://www.cnil.fr

DEUTSCHLAND Herr Peter SCHAAR Vorsitzender Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 - D-53117 BONN Tel.: +49 228 81995 0 Fax: +49 228 81995 550 E-Mail: peter.schaar@bfdi.bund.de Website: http://www.bfdi.bund.de	**GRIECHENLAND** Herr Nikolaos FRANGAKIS Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Griechische Datenschutzbehörde) Kifisias Av. 1-3, PC 115 23 Ampelokipi - ATHEN Tel.:+30 210 6475601 - Tel.: 30 210 33 52 602 Fax: +30 1 33 52 617 E-Mail: sofralaw@otenet.gr Website: http://www.dpa.gr
UNGARN Dr. Attila PETERFALVI Parlamentarischer Beauftragter Adatvédelmi Biztos Irodája (Büro der parlamentarischen Beauftragten) Nador u. 22 - H - 1051 BUDAPEST Telefon: +36 1 475 7186, +36 1 475 7100 Telefax: +36 1 269 3541 E-Mail: adatved@obh.hu Website: http://abiweb.obh.hu	**IRLAND** Herr Billy HAWKES Datenschuztbeauftragter Irish Life Centre, Block 6 Lower Abbey Street - IRL - DUBLIN 1 Tel.: +353 1 8748544 Fax: +353 1 8745405 E-Mail: info@dataprotection.ie Website: www.dataprotection.ie
ITALIEN Professor Francesco PIZZETTI Präsident Garante per la protezione dei dati personali Piazza di Monte Citorio, 121 - I - 00186 ROMA Tel.: +39 06 69677403 Fax: +39 06 06 69677405 E-Mail: garante@garanteprivacy.it Website: http://www.garanteprivacy.it	**LETTLAND** Frau Signe PLUMINA Direktorin Datu valsts inspekcija (Datenschutzbehörde) Kr. Barona Street 5-4 - LV - 1050 RIGA Tel.: +371 722 31 31 Fax: +371 722 35 56 E-Mail: info@dvi.gov.lv Website: http://www.dvi.gov.lv
LITAUEN Frau Ona JAKSTAITE Direktorin Valstybinė duomenų apsaugos inspekcija (Staatliches Datenschutzbehörde) Gedimino Ave 27/2 - LT - 2600 VILNIUS Tel.: + 370 5 279 14 45 Fax: +370 5 261 94 94 E-Mail: ada@ada.lt Website: http://www.ada.lt	**LUXEMBURG** Herr Gérard LOMMEL Präsident Commission nationale pour la Protection des Données (Nationale Datenschutzkommission) 68, rue de Luxembourg - L – 4100 ESCH-SUR-ALZETTE Tel.: +352 26106020 Fax: +352 26106029 E-Mail: info@cnpd.lu Website: http://www.cnpd.lu
MALTA Herr Paul MIFSUD CREMONA Datenschutzbeauftragter 2, Airways House High Street - SIIEMA SLM 16 Tel.: +356 2328 7100 Fax: +356 23287198 E-Mail: commissioner.dataprotection@gov.mt Website: http://www.dataprotection.gov.mt	**NIEDERLANDE** Herr Jacob KOHNSTAMM College Bescherming Persoonsgegevens (CBP) (Niederländische Datenschutzbehörde) Prins Clauslaan 20 Postbus 93374 - NL - 2509 AJ DEN HAAG Tel.: +31 70 381 13 00 Fax: +31 70 381 13 01 E-Mail: info@cbpweb.nl Website: http://www.cbpweb.nl, www.DutchDPA.nl

POLEN Frau Dr Ewa KULESZA Generalinspektorin Biuro Generalnego Inspektora Ochrony Danych Osobowych (Büro der Generalinspektorin für den Datenschutz) ul. Stawki 2 - PL – 00193 WARSCHAU Tel.: +48 22 860 70 81, 48 22 860 73 12 Fax: +48 22 860 70.90 E-Mail:sekretariat@giodo.gov.pl, dp@giodo.gov.pl Website: http://www.giodo.gov.pl	**PORTUGAL** Herr Luís DA SILVEIRA Präsident Comissão Nacional de Protecção de Dados (Nationale Datenschutzkommission) Rua de São Bento, 148, 3o - P – 1 200-821 LISSABON Codex Tel.: +351 21 392 84 00 Fax: +351 21 397 68 32 E-Mail: geral@cnpd.pt Website: http://www.cnpd.pt
SLOWAKISCHE REPUBLIK Herr Gyula VESZELEI Präsident Úrad na ochranu osobných údajov Slovenskej republiky (Datenschutzbehörde der slowakischen Republik) Odborarska namestie 3 - SK – 81760 BRATISLAVA 15 Tel.: + 421 2 5023 9418 Fax: + 421 2 5023 9441 E-Mail: statny.dozor@pdp.gov.sk or gyula.veszelei@pdp.gov.sk Website: http://www.pdp.gov.sk	**SLOWENIEN** Herr Jože BOGATAJ Hauptinspektor für den Datenschutz Inšpektorat RS za varstvo osebnih podatkov (Datenschutzbehörde der slowenischen Republik) Tivolska 50 - SI-1000 LJUBLJANA Tel. : +386 1 478 52 60 Fax: +386 1 478 53 44 E-Mail: joze.bogataj@gov.si Website: http://www.mp.gov.si
SPANIEN Herr José Luis PIÑAR MAÑAS (Vizevorsitzender) Direktor Agencia Española de Protección de datos (Spanische Datenschutzbehörde) C/ Sagasta, 22 - E - 28004 MADRID Tel.: +34 91 3996219/20 Fax: +34 91 447 10 92 E-Mail: director@agpd.es Website: http://www.agpd.es	**SCHWEDEN** Herr Göran GRÄSLUND Generaldirektor Datainspektionen (Datenschutzaufsichtsrat) Fleminggatan, 14 9. Stock Box 8114 - S - 104 20 STOCKHOLM Tel.: +46 8 657.61.00 - Tel.: 46 8 657 61 57 Fax: +46 8 650 86 13, +46 8 652 86 52 E-Mail: datainspektionen@datainspektionen.se, Goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
VEREINIGTES KÖNIGREICH Herr Richard Thomas Datenschutzbeauftragter The Office of the Information Commissioner (Büro des Datenschutzbeauftragten) Wycliffe House Water Lane WILMSLOW Cheshire SK9 5AF Vereinigtes Königreich Tel.: +44 1625 545 700 (Anrufzentrale) Fax: +44 1625 524 510 E-Mail: pdq@ico.gsi.gov.uk, mail@ico.gsi.gov.uk Website: http://www.informationcommissioner.gov.uk	**EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER** Herr Peter HUSTINX Europäischer Datenschutzbeauftragter Korrespondenzanschrift: 60, rue Wiertz B-1047 Brüssel Büro: Rue Montoyer 63, 6. Stock - B-1047 BRÜSSEL Tel.: + 32 2 283 19 00 Fax: + 32 2 283 19 50 E-Mail: edps@edps.eu.int Website: http://www.edps.eu.int

BEOBACHTER ZUM 25. NOVEMBER 2005

ISLAND Frau Sigrun JOHANNESDOTTIR Direktorin Persónuvernd (Isländische Datenschutzbehörde) Raudararstigur 10 IS - 105 REYKJAVIK Tel.: +354 560 90 10, +354 510 9600 Fax : +354 510 96 06 E-Mail: postur@personuvernd.is Website: http://www.personuvernd.is	**NORWEGEN** Herr Georg APENES Director General Datatilsynet (Datenschutzbehörde) P.B. 8177 Dep N - 0034 OSLO Tel.: +47 22 39 69 00 Fax. +47 22 42 23 50 E-Mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
LIECHTENSTEIN Herr Dr Philipp MITTELBERGER Stabsstelle für Datenschutz Aeulestrasse 51 9490 VADUZ Liechtenstein Tel.: +423 236 60 90, 91 Fax: +423 236 60 99 E-Mail: info@sds.llv.li Website: http://www.sds.llv.li http://www.liechtenstein.li	**BULGARIEN** Herr Ivo STEFANOV Комисията за защита на личните данни (Datenschutzkommission) 1 Bvld Dondukov 1000 SOFIA Bulgarien Tel.: +359 2 940 2046 Fax: E-Mail: kzld@government.bg
RUMÄNIEN Frau Georgeta BASARABESCU Präsidentin Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal (Nationale Datenschutzkontrollbehörde) Eugeniu Carada Str., 3, Sektor 3 BUKAREST Tel.: +40 21 312 49 34 Fax: +40 21 312 71 02 E-Mail: basarabescu@avp.ro	

SEKRETARIAT DER ART. 29 DATENSCHUTZGRUPPE
Philippe RENAUDIERE (Referatsleiter)
Referat Datenschutz
Generaldirektion Justiz, Freiheit und Sicherheit
Europäische Kommission
Postanschrift: Büro: LX46 01/43
BE - 1049 BRÜSSEL
Tel.: +32 2 296 87 50
Fax: +32 2 299 80 94
E-Mail: Philippe.Renaudiere@cec.eu.int
Website: http://europa.eu.int/comm/justice_home/fsj/privacy/

NE-AC-05-001-DE-C

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 92-79-01249-5