Europäische Kommission
Justiz

13. Jahresbericht
der Artikel-29-
Datenschutzgruppe

1830-6462

13. Jahresbericht

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

Berichtsjahr 2009

Angenommen am 14. Juli 2010

Die Datenschutzgruppe wurde gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist das unabhängige Beratungsgremium der Europäischen Union in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

Die Sekretariatsgeschäfte werden wahrgenommen durch die Generaldirektion Justiz, Freiheit und Sicherheit, Direktion C (Grundrechte und Unionsbürgerschaft), der Europäischen Kommission, B-1049 Brüssel, Belgien, Büro LX-46 01/190.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

INHALT

VORWORT DES VORSITZENDEN DER ARTIKEL-29-DATENSCHUTZGRUPPE

Im Jahr 2009 entwickeln sich die neuen Technologien mit atemberaubender Geschwindigkeit und in einer Welt ohne Grenzen. Wir müssen deshalb unseren Rechtsrahmen und unsere Vorgehensweisen an diesen tief greifenden Wandel anpassen und dabei ein hohes Maß an Datenschutz wahren.

Im Rahmen der 31. Internationalen Konferenz der Datenschutzbeauftragten (Madrid, November 2009) haben wir die möglichen Grundlagen für eine weltweite Regelung des Datenschutzes geschaffen, indem wir eine Entschließung über die Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten angenommen haben. Ein historischer Schritt, denn erstmals konnten sich die Datenschutzbehörden auf einen weltweit geltenden Katalog gemeinsamer Grundsätze einigen, der den jüngsten technologischen Entwicklungen Rechnung trägt.

Überlegungen zu den organischen und rechtlichen Folgen dieser Entscheidungen sowie eine rasche, umfassende Sensibilisierung der öffentlichen Hand sind erforderlich, damit Letztere Maßnahmen zur Einführung eines verbindlichen internationalen Rechtsinstruments ergreift.

Gleichzeitig sind Überlegungen auf europäischer Ebene in Bezug auf die Anpassung vorhandener Instrumente eingeleitet worden. Von den im Jahr 2009 gestarteten Initiativen möchte ich insbesondere die der Kommission hervorheben, in deren Rahmen auf Betreiben des Vizepräsidenten Jacques Barrot und der Artikel-29-Datenschutzgruppe eine umfassende öffentliche Anhörung durchgeführt wurde, um Beiträge zu den neuen Herausforderungen im Bereich des Datenschutzes und zur Verbesserung des Rechtsrahmens für den Schutz personenbezogener Daten in der Europäischen Union einzuholen.

Die Artikel-29-Datenschutzgruppe und die Arbeitsgruppe Polizei und Justiz haben auf der Grundlage ihrer Erfahrung und Sachkenntnis eine herausragende Stellungnahme sowohl auf europäischer Ebene als auch zum allgemeinen Datenschutz vorgelegt und dabei insbesondere die Auswirkungen des Inkrafttretens des Vertrags von Lissabon am 1. Dezember berücksichtigt. Die Stellungnahme enthält Vorschläge zur Verbesserung der vorhandenen Instrumente und Verfahren, darunter unter anderem den Willen zur Erarbeitung praktischer Maßnahmen für mehr Transparenz der Rechte des Einzelnen sowie die Einführung von konkreten Handlungsmöglichkeiten zur Ausübung dieser Rechte. Es geht außerdem um eine Verbesserung des Datenschutzes im Bereich der gebräuchlichen und gemeinsamen moralischen Werte in Unternehmen und eine Verbesserung der konkreten Wirksamkeit von Maßnahmen der Datenschutzbeauftragten der Unternehmen, um ihre Einhaltung der geltenden Vorschriften aufzuzeigen.

Zudem wurden Überlegungen zur Unabhängigkeit sowie zum Ausbau der Rolle und der Befugnisse von Datenschutzbehörden gestartet, die die Rolle eines Kontrolleurs übernehmen müssen, der die öffentliche Hand oder sogar die Öffentlichkeit für Fragen sensibilisiert, die schnell zu großen gesellschaftlichen Problemen werden könnten.

Ich hatte die Gelegenheit, meine Besorgnis meinen europäischen Pendants im Februar 2010 in meiner Botschaft zum Mandatsende mitzuteilen. Ich war und bin der Auffassung, dass die Artikel-29-Datenschutzgruppe eine führende Rolle beim Schutz personenbezogener Daten und der Privatsphäre auf europäischer und internationaler Ebene spielen muss. Ich musste jedoch feststellen, dass sie bei der Erfüllung ihrer Aufgaben durch fehlende Eigenmittel stark eingeschränkt ist.

Mit einer Erhöhung der Eigenmittel der Artikel-29-Datenschutzgruppe könnten weitere Anhörungen durchgeführt und mehr Experten befragt werden, um auf die jüngsten technologischen Entwicklungen reagieren zu können und um sich allgemein in wichtigen Fragen durch entsprechende Maßnahmen Gehör verschaffen zu können. Die Zuweisung eines eigenen Budgets an die Artikel-29-Datenschutzgruppe sowie die Einsetzung eines eigenen Sekretariats sind die Voraussetzungen für die Wirksamkeit, Sichtbarkeit und Unabhängigkeit – und somit die Glaubwürdigkeit – der Artikel-29-Datenschutzgruppe in den kommenden Jahren.

Die Arbeit der Artikel-29-Datenschutzgruppe wird des Weiteren durch einen enormen Mangel an Betriebsmitteln und insbesondere an Räumlichkeiten behindert. Zudem fällt es schwer, für jede Sitzung angemessene Dolmetscherdienste bereitzustellen, die allen nationalen Experten eine Teilnahme an der Arbeit der Artikel-29-Datenschutzgruppe ermöglichen. Darüber hinaus benötigt unsere Gruppe bessere Kommunikationsmittel und vor allem eine eigene Website. Durch eine Verbesserung der Kommunikationsmittel würde sicher auch die Sichtbarkeit der Arbeit und der durchgeführten Maßnahmen erhöht.

Somit ist es nunmehr dringend erforderlich, dass den Datenschutzbehörden und der Artikel-29-Datenschutzgruppe die ihrem Auftrag entsprechenden personellen und finanziellen Mittel zugewiesen werden.

Alex Türk

Kapitel 1

FRAGEN, ZU DENEN DIE ARTIKEL-29-DATENSCHUTZGRUPPE STELLUNG GENOMMEN HAT[1]

1 Alle von der Artikel-29-Datenschutzgruppe angenommenen Dokumente können von folgender Website abgerufen werden. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm

1.1. DATENÜBERMITTLUNG IN DRITTLÄNDER

1.1.1. Passagierdaten / PNR

Stellungnahme 8/2009 (WP 167) zum Schutz der von Duty-free-Shops innerhalb von Flug- und Seehäfen erfassten und verarbeiteten Daten von Reisenden.

Das Gemeinschaftsrecht gestattet die Verbrauchsteuerbefreiung bei Einkäufen von Reisenden in Duty-free-Shops innerhalb von Flug- und Seehäfen. Derartige Einkäufe unterliegen jedoch bestimmten Bedingungen. Zur Erfüllung dieser Bedingungen erfassen die meisten Duty-free-Shops in den EU-Mitgliedstaaten beim Kauf ihrer Waren Daten, einschließlich der Daten von Reisenden, und verarbeiten diese.

Die praktische Handhabung der Erfassung und Verarbeitung solcher Passagierdaten in den Duty-free-Shops in ganz Europa ist jedoch von Shop zu Shop sehr unterschiedlich. Den Reisenden werden dabei keinerlei Informationen gegeben über die Erfassung von Daten, einschließlich ihrer personenbezogenen Daten, den Zweck der Erfassung, ihre Rechte und die Nutzung dieser Einzelheiten durch öffentliche Einrichtungen im Falle einer Übermittlung solcher Daten.

Die Europäische Kommission hat die Artikel-29-Datenschutzgruppe gemäß Artikel 30 der Richtlinie 95/46/EG beauftragt, diese Angelegenheit zu untersuchen und die jetzt in den Mitgliedstaaten der EU gängigen Praktiken im Hinblick auf auftauchende Datenschutzfragen zu überprüfen, wenn nötig auch mit Empfehlungen zu einer einheitlichen Anwendung der allgemeinen Datenschutzgrundsätze, wie sie in Duty-free-Shops innerhalb von Flug- oder Seehäfen einzuhalten sind.

Diese Stellungnahme analysiert die rechtlichen und praktischen Fragen im Zusammenhang mit der Erfassung und Verarbeitung von Passagierdaten in Duty-free-Shops und möchte den Geschäftsinhabern und den für die Überwachung der Durchführung des Gemeinschaftsrechts zuständigen Zollbehörden Leitlinien an die Hand geben, um zu einer einheitlicheren Anwendung der geltenden Vorschriften zu kommen.

1.1.2. Standardvertragsklauseln

Stellungnahme 3/2009 (WP 161) über den Entwurf einer Entscheidung der Kommission zu Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter)

Unternehmen und Datenschutzbehörden haben mehrere Jahre lang mit den am 27. Dezember 2001[2] durch die Europäische Kommission angenommenen Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG (vom für die Datenverarbeitung Verantwortlichen zum Datenverarbeiter, Entscheidung 2002/16/EG) gearbeitet.

Obgleich die Standardvertragsklauseln gemäß Entscheidung 2002/16/EG eine solide Grundlage für die Übermittlung personenbezogener Daten darstellen, wird seit mehreren Jahren der Ruf nach einer Aktualisierung immer lauter. Der Hauptgrund für Überlegungen zur Aktualisierung der Standardvertragsklauseln gemäß Entscheidung 2002/16/EG kann vereinfacht mit der Entwicklung des „globalen Outsourcings" erklärt werden. Da Unternehmen ihre Daten immer häufiger nicht nur an einen Auftragsverarbeiter, sondern an „Unterauftragsverarbeiter" übermitteln, die sie manchmal wiederum an „Unter-Unterauftragsverarbeiter" weiterübermitteln, sind die Standardvertragsklauseln gemäß Entscheidung 2002/16/EG kein Instrument für die Bewältigung solch komplexer Weiterleitungsprozesse. Daher erachtet die Europäische Kommission eine Änderung der Standardvertragsklauseln gemäß Entscheidung 2002/16/EG durch eine neue Entscheidung auf der Grundlage von Artikel 26 Absatz 4 der Richtlinie 95/46/EG für erforderlich, um Verträge besser an die aktuellen Geschäftsvorgänge anpassen zu können.

2 ABl. L 6, 10.12002, S.52. Siehe Stellungnahme der Arbeitsgruppe Nr. 7/2001, WP 47, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp47en.pdf

1.1.3. Welt-Anti-Doping-Agentur (WADA)

Zweite Stellungnahme 4/2009 zum Internationalen Standard der Welt-Anti-Doping-Agentur (WADA) zum Schutz der Privatsphäre und personenbezogener Informationen, zu den hiermit in Verbindung stehenden Bestimmungen des WADA-Codes und zu anderen Fragen bezüglich der Privatsphäre im Zusammenhang mit dem Kampf der WADA und (nationaler) Anti-Doping-Organisationen gegen Doping im Sport

In ihrer ersten Stellungnahme zu diesem Thema[3], hat die Arbeitsgruppe die Vereinbarkeit des Entwurfs des *Internationalen Standards zum Schutz der Privatsphäre und personenbezogener Informationen* (der Datenschutzstandard oder Standard) mit dem Schutzniveau untersucht, das die europäischen Datenschutzbestimmungen mindestens verlangen. Wenngleich die Arbeitsgruppe ihre Zustimmung zu einer Reihe von Aspekten des Standards, einschließlich der Bezugnahme auf die Richtlinie 95/46/EG, zum Ausdruck brachte, kam sie dennoch zu dem Schluss, dass der Entwurf nicht mit dem Mindest-Schutzniveau vereinbar war, das die Richtlinie verlangt, und sprach gewisse Empfehlungen aus.

Seitdem wurde der Entwurf des Standards geändert und ist seit dem 1. Januar 2009 in Kraft. Die Welt-Anti-Doping-Agentur (WADA) hat als Antwort auf die vorangegangenen Bitten um Klarstellung zusätzliche Informationen geliefert. Die Arbeitsgruppe ist froh darüber, dass einige ihrer Anmerkungen in den Datenschutzstandard eingefügt wurden[4]. Sie bedauert jedoch, dass ihre anderen Anmerkungen nicht berücksichtigt wurden (siehe Punkt 3.2. unten).

Das Internationale Übereinkommen gegen Doping im Sport der UNESCO aus dem Jahr 2005, das von 25 der 27 EU-Mitgliedstaaten ratifiziert wurde, wurde zur Unterstützung der Arbeit der WADA auf internationaler Ebene abgeschlossen. Das Übereinkommen ändert nicht die Rechte und Pflichten der Unterzeichner in Bezug auf andere, vorher geschlossene Übereinkünfte (Artikel 6). Es fördert die Zusammenarbeit zwischen den Staaten in geeigneten Umständen und grundsätzlich in Übereinstimmung mit innerstaatlichem Recht. Gemäß EU-Recht sind alle Vorschriften eines internationalen Abkommens, die nicht mit dem EU-Recht vereinbar sind, dem EU-Recht untergeordnet. Das Übereinkommen der UNESCO nimmt weder besonderen Bezug auf die Grundrechte im Allgemeinen noch auf die Datenschutzrechte im Besonderen.

Die Arbeitsgruppe kann ihre Anmerkungen nicht auf den Datenschutzstandard beschränken. Da dieser zahlreiche Verweise auf den WADA-Code und die ADAMS-Datenbank (siehe 2.2.) enthält, ist es wichtig, ihn in seinem breiteren Anwendungsbereich zu untersuchen. Deshalb geht die Stellungnahme detaillierter auf die folgenden Punkte ein, nachdem sie die grundlegenden Merkmale des von der WADA entwickelten Systems (Punkt 2) aufgezeigt hat: Aufenthaltsort und Erreichbarkeit (3.1.), unberücksichtigt gebliebene Anmerkungen aus der ersten Stellungnahme (3.2.), Rechtsgrundlagen für die Verarbeitung (3.3.), der Datentransfer zu der ADAMS-Datenbank in Kanada und in andere Staaten außerhalb der EU (3.4.), Zeitraum für die Speicherung der Daten (3.5.) und Sanktionen (3.6.).

Für die Datenverarbeitung Verantwortliche in der EU, wie nationale Anti-Doping- Organisationen (NADO), nationale und internationale Sportfachverbände und Olympische Komitees, können dieser Stellungnahme einige der rechtlichen Grenzen entnehmen, die bezüglich der Verarbeitung der personenbezogenen Daten von Athleten (und von anderen betroffenen Personen) bestehen. Die Arbeitsgruppe betont, dass die für die Datenverarbeitung Verantwortlichen in der EU für die Verarbeitung der Daten in Übereinstimmung mit dem einzelstaatlichen Recht verantwortlich sind

3 Stellungnahme 3/2008 vom 1. August 2008 zum Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code (WP 156) http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp156_en.pdf

4 Die geänderte Bedeutung von „Verarbeitung" und „sensible Daten" (die nicht länger politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit umfasst, deren Bedeutung im Kampf gegen Doping von der Arbeitsgruppe bezweifelt wurde (3.2.)) und die unter Punkt 6.2. bereitgestellte Klarstellung. Des Weiteren hat die Arbeitsgruppe festgestellt, dass Artikel 6 umgeschrieben wurde und nun zusätzlich zu der Einwilligung – ab jetzt Einwilligung in Kenntnis der Sachlage – auch vorsieht, dass „personenbezogene Informationen" nur dort verarbeitet werden, „wo [dies] gesetzlich ausdrücklich zulässig ist". Sie hat weitere Änderungen festgestellt, die entsprechend ihren Bemerkungen erfolgt sind. So wurde z. B. die Anmerkung zu Artikel 9.2. überarbeitet. Die Worte „eindeutig rechtsmissbräuchlich" wurden in Punkt 11.2. unter Bezugnahme auf die Ausübung des Auskunftsrechts und auf das Recht der Teilnehmer gestrichen, Beschwerde gegen eine internationale Anti-Doping-Organisation zu erheben, wie es jetzt in Artikel 11.5. vorgesehen ist.

und deshalb den Welt-Anti-Doping-Code und die Internationalen Standards insoweit unberücksichtigt lassen müssen, als diese dem einzelstaatlichen Recht widersprechen. Die Arbeitsgruppe empfiehlt, dass diese für die Datenverarbeitung Verantwortlichen eine Rechtsberatung in Anspruch nehmen.

1.1.4. Angemessenheit

Stellungnahme 6/2009 (WP 165) zum Umfang des Schutzes personenbezogener Daten in Israel

Am 12. Juli 2007 hat die israelische EU-Mission bei der Kommission den Antrag gestellt, das Verfahren in die Wege zu leiten, damit Israel zu einem Land zu erklärt wird, das im Sinne von Artikel 25 und 26 der Richtlinie ein ausreichendes Datenschutzniveau gewährleistet.

Zur Prüfung der Angemessenheit des israelischen Datenschutzes hat die Kommission bei dem Centre de Recherches Informatique et Droit (nachstehend „CRID" genannt) bei der Universität von Namur einen Bericht in Auftrag gegeben. Das CRID hat in einem sehr ausführlichen Bericht analysiert, inwieweit der israelische Rechtsrahmen die Anforderungen für die Anwendung der Datenschutzbestimmungen für personenbezogene Daten erfüllt, die in dem Arbeitspapier „Übermittlung personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" niedergelegt sind, das die Artikel-29-Arbeitsgruppe am 24. Juli 1998 angenommen hat (Dokument WP 12).

Die Untergruppe Safe Harbor hat den vorgenannten Bericht und die erste Antwort der israelischen Behörden auf den Bericht in einer Sitzung am 18. März 2009 diskutiert. In jener Sitzung wurde der Arbeitsgruppe von der Untergruppe ein Brief zur Stellungnahme vorgelegt, den ihr Vorsitzender an die israelischen Behörden zu schicken gedachte. In diesem Brief wird die in Israel bestehende Regelung zum Datenschutz positiv bewertet; gleichzeitig werden aber auch die Themen hervorgehoben, die einer weiteren Klärung bedürfen.

Am 2. September hat die israelische Rechts-, Informations- und Technologiebehörde (nachstehend „ILITA" genannt) im Namen der israelischen Behörden einen ausführlichen Bericht an die Arbeitsgruppe gesandt, in dem sie zu den Themen Stellung nahmen, die in dem Brief angesprochen worden waren. Dieser Bericht wurde durch die Mitglieder der Untergruppe analysiert. Er war auch Gegenstand einer Sitzung vom 16. September 2009, in der die vorgenannten Behörden gehört wurden. In dieser Sitzung haben die Mitglieder der Untergruppe die israelischen Behörden, die durch den Leiter der ILITA und den Leiter der Justizabteilung dieser Behörde vertreten waren, zur Klärung der Fragen aufgefordert, die nach der vorangegangenen Erörterung des an die Untergruppe gesandten Berichts weiterer Klärung bedurften.

Die Untergruppe informierte die Arbeitsgruppe in der Sitzung am 12. und 13. Oktober 2009 von den Schlussfolgerungen, zu denen sie während der Sitzung vom 16. September gelangt war, und schlug die Annahme der folgenden Stellungnahme unter den in ihr genannten Bedingungen vor. Die Arbeitsgruppe nahm den Vorschlag im Rahmen der erwähnten Sitzung an.

Stellungnahme 7/2009 (WP 166) zum Schutzniveau für personenbezogene Daten im Fürstentum Andorra

Am 21. Mai 2008 hat der Botschafter Andorras bei der Europäischen Union einen Antrag bei der Kommission gestellt, das Verfahren zur Feststellung einzuleiten, dass Andorra ein angemessenes Schutzniveau im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG gewährleistet.

Zur Bewertung der Angemessenheit des Datenschutzniveaus in Andorra hat die Kommission beim Centre de Recherches Informatique et Droit (CRID) der Universität von Namur einen Bericht in Auftrag gegeben. Das CRID hat in einem umfangreichen Bericht analysiert, inwieweit die andorranische Rechtsordnung die Anforderungen an das materielle Recht und die Durchsetzungsmechanismen zum Schutz personenbezogener Daten erfüllt, die in der von der Artikel-29-Arbeitsgruppe am 24. Juli 1998 angenommenen Arbeitsunterlage (Dokument WP12) „Übermittlung personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU" niedergelegt sind.

Der Bericht wurde auf der Sitzung der Untergruppe Safe Harbour vom 18. März 2009 erörtert. In jener

Sitzung bat die Untergruppe die Arbeitsgruppe um Stellungnahme zu einem Brief, den ihr Vorsitzender an die andorranischen Behörden gerichtet hatte, in dem er zunächst die positive Bewertung des in Andorra geltenden Datenschutzsystems zum Ausdruck bringt und anschließend auf bestimmte Punkte hinweist, die unter Umständen weiterer Klarstellung bedürfen.

Am 31. Juli 2009 übermittelten die andorranischen Behörden der Artikel-29-Datenschutzgruppe über die Andorranische Datenschutzagentur (APDA) einen umfangreichen Bericht, in dem sie die Fragen aus dem vorgenannten Schreiben beantworteten. Dieser Bericht wurde von der Untergruppe analysiert und war auch Gegenstand einer Sitzung vom 16. September 2009, in der die vorgenannten Behörden gehört wurden. In dieser Sitzung baten die Mitglieder der Untergruppe die andorranischen Behörden, vertreten durch den Direktor der APDA, den Leiter der Kontrollabteilung und den Leiter der Rechtsabteilung, noch die Punkte zu klären, für die sie nach der Erörterung des Berichts der andorranischen Behörden nach wie vor Klärungsbedarf sahen.

Die Untergruppe informierte die Arbeitsgruppe auf ihrer Sitzung vom 12. und 13. Oktober 2009 über die bei der Sitzung erzielten Schlussfolgerungen und schlug vor, dass sie die vorliegende Stellungnahme zu den darin enthaltenen Bedingungen annimmt; dieser Vorschlag wurde von der Arbeitsgruppe im Rahmen der Sitzung angenommen.

1.1.5. Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung

Arbeitsunterlage 1/2009 (WP 158) über Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung bei grenzübergreifenden zivilrechtlichen Verfahren (pre-trial discovery)

Dieses Arbeitspapier soll den Personen, die nach EU-Recht für die Datenverarbeitung verantwortlich sind, als Leitfaden bei der Bearbeitung von Ersuchen um Übermittlung personenbezogener Daten ins Ausland zwecks Verwendung in einem Zivilprozess dienen. Anlass für die Ausarbeitung dieses Dokuments war die Feststellung der Arbeitsgruppe, dass die Richtlinie 95/46/EG in den Mitgliedstaaten unterschiedlich angewandt wird, was zum Teil auf die Vielfalt der zivilrechtlichen Verfahren in der EU zurückzuführen ist.

Im ersten Abschnitt dieses Papiers legt die Arbeitsgruppe kurz die unterschiedlichen Positionen zu Rechtsstreitigkeiten und insbesondere zu Offenlegungspflichten im Rahmen der vorprozessualen Beweiserhebung (pre-trial discovery) in den angloamerikanischen (u. a. USA und Vereinigtes Königreich) und kontinentaleuropäischen Rechtssystemen dar.

Im Anschluss daran werden Leitlinien für die in der EU für die Datenverarbeitung Verantwortlichen aufgestellt, die die prozessualen Anforderungen eines bei einem ausländischen Gericht anhängigen Rechtsstreits mit den Datenschutzverpflichtungen aufgrund der Richtlinie 95/46/EG in Einklang zu bringen suchen.

1.2. ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

Stellungnahme 1/2009 (WP 159) über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für die elektronische Kommunikation)

Am 13 November 2007 verabschiedete die Kommission einen Vorschlag für eine Richtlinie (der Vorschlag) zur Änderung der Richtlinie 2002/58/EG (Datenschutzrichtlinie für die elektronische Kommunikation) über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Richtlinie 2002/21/EG (Rahmenrichtlinie). Der Vorschlag wurde schließlich am 25. November 2009 vom Europäischen Parlament und vom Rat angenommen.

Die Datenschutzgruppe hatte bereits zwei Stellungnahmen zu den Vorschlägen zur Überprüfung des Rechtsrahmens der EU für

elektronische Kommunikationsnetze und -dienste abgegeben (Stellungnahme 8/2006[5], angenommen am 26. September 2006 und Stellungnahme 2/2008, angenommen am 15. Mai 2008[6]).

Obwohl die Datenschutzgruppe mit Genugtuung feststellt, dass einige ihrer früheren Empfehlungen berücksichtigt wurden, möchte sie auf erhebliche Bedenken im Zusammenhang mit den nach der ersten Lesung im Parlament und im Rat aufgeworfenen Fragen hinweisen.

Stellungnahme 5/2009 (WP 163) zur Nutzung sozialer Online-Netzwerke

Diese Stellungnahme stellt auf die Frage ab, wie das Betreiben sozialer Vernetzungs-Websites (SNS) mit den Bestimmungen des Datenschutzrechts der EU in Einklang zu bringen ist. Sie soll vor allem den Anbietern sozialer Netzwerkdienste (SNS) eine Richtschnur zu den Maßnahmen bieten, die zwecks der Vereinbarkeit mit dem EU-Recht verwirklicht sein müssen.

Die Stellungnahme hält fest, dass es sich bei den Anbietern sozialer Netzwerkdienste und in vielen Fällen auch bei den Drittanbietern von Anwendungs- und Softwaredienstleistungen um „für die Datenverarbeitung Verantwortliche" mit entsprechenden Verpflichtungen gegenüber den Nutzern sozialer Netzwerkdienste handelt. Die Stellungnahme macht klar, dass sich viele Nutzer in einem rein persönlichen Lebensbereich bewegen, indem sie im Rahmen der Besorgung ihrer persönlichen oder familiären Angelegenheiten bzw. ihrer privaten Haushaltsführung Kontakte zu anderen Menschen knüpfen und unterhalten. In diesen Fällen ist nach der Stellungnahme davon auszugehen, dass die „Ausnahmeklausel für Privathaushalte betreffend persönliche oder familiäre Tätigkeiten natürlicher Personen" Anwendung findet und die Vorschriften für die „für die Verarbeitung Verantwortlichen" somit nicht gelten. Die Stellungnahme führt auch Umstände auf, unter denen die Tätigkeiten eines Nutzers eines sozialen Netzwerkdienstes nicht unter die „Ausnahmeklausel für Privathaushalte" fallen. Die Verbreitung und die Verwendung von Informationen, die über soziale Netzwerkdienste verfügbar sind, zu anderweitigen, sekundären und unbefugten Zwecken gehört zu den besorgniserregenden Sicherheitsbedenken der Artikel-29-Datenschutzgruppe. Die Gruppe tritt in ihrer Stellungnahme daher für robuste sicherheits- und datenschutzfreundliche Standardeinstellungen als idealen Ausgangspunkt für alle angebotenen Dienstleistungen ein. Im Mittelpunkt der wachsenden Besorgnis stehen die Zugriffsmöglichkeiten auf Informationen aus Nutzerprofilen. Ebenso behandelt werden Themen wie die Verarbeitung sensibler Daten und Bildmaterialien, die zielgerichtete Werbung und die Direktwerbung über soziale Netzwerkdienste und die Probleme im Zusammenhang mit der Vorratsspeicherung von Daten.

Die Empfehlungen stellen im Kern auf die Verpflichtungen der Anbieter von sozialen Netzwerkdiensten ab, im Einklang mit den Vorschriften der Datenschutzrichtlinie zu handeln und die Rechte der Nutzer aufrechtzuerhalten und zu stärken. Von ganz entscheidender Bedeutung ist, dass die Anbieter von sozialen Netzwerkdiensten ihre Nutzer von Anfang an über ihre Identität aufklären und die gesamte Bandbreite der unterschiedlichen Vorhaben und Zielsetzungen darstellen, die sie mit ihrer Verarbeitung personenbezogener Daten verbinden. Besondere Sorgfalt sollten die Anbieter von sozialen Netzwerkdiensten bei der Verarbeitung personenbezogener Daten von Minderjährigen walten lassen. Die Stellungnahme empfiehlt allen Nutzern, Bilder bzw. Informationen über andere Personen nur mit der konkreten Einwilligung der jeweils betroffenen Person in ein soziales Netzwerksystem hochzuladen, und gibt auch den Anbietern von sozialen Netzwerkdiensten zu bedenken, dass sie in der Pflicht sind, ihre Nutzer im Hinblick auf die Rechte der anderen auf Schutz ihrer Privatsphäre aufzuklären.

1.3. PERSONENBEZOGENE DATEN

Stellungnahme 2/2009 (WP 160) zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen)

Gegenstand der vorliegenden Stellungnahme ist der Schutz der Daten von Kindern. Die Stellungnahme richtet sich hauptsächlich an Zielgruppen, die personenbezogene Daten von Kindern verarbeiten. Im schulischen

[5] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

[6] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf

Kontext sind dies vor allem Lehrer und Schulbehörden. Außerdem wendet sich die Stellungnahme an die nationalen Kontrollstellen für den Datenschutz, die für die Überwachung der Verarbeitung derartiger Daten zuständig sind.

Das Arbeitspapier ist im Zusammenhang mit der allgemeinen Initiative der Europäischen Kommission zu sehen, die diese in ihrer Mitteilung im Hinblick auf eine EU-Kinderrechtsstrategie beschreibt. Durch ihren Beitrag zu diesem allgemeinen Zweck zielt die Mitteilung auf die Stärkung des Grundrechts von Kindern auf den Schutz ihrer personenbezogenen Daten. Die Artikel-29-Datenschutzgruppe hat bereits mehrere Stellungnahmen zu diesem Thema angenommen, und insofern ist das Thema für sie nicht neu. Einige Grundsätze oder Empfehlungen in Bezug auf den Schutz der personenbezogenen Daten von Kindern finden sich in ihren Stellungnahmen zum Verhaltenskodex von FEDMA (Stellungnahme 3/2003), zur Nutzung von Standortdaten (Stellungnahme 5/2005) sowie zu Visumanträgen und biometrischen Identifikatoren (Stellungnahme 3/2007).

Ziel des Arbeitspapiers ist es, das Thema in strukturierter Form zusammenzufassen, die maßgeblichen Grundsätze zu definieren (Teil II) und sie am Beispiel von Schuldaten zu veranschaulichen (Teil III).

Der Bereich der Schuldaten wurde gewählt, weil er zu den wichtigen Bereichen im Leben eines Kindes gehört und in seinem Alltag einen breiten Raum einnimmt. Auch der sensible Charakter vieler Daten, die in Bildungseinrichtungen verarbeitet werden, trägt zur Bedeutung dieses Bereichs bei.

Die Zukunft des Datenschutzes: Gemeinsamer Beitrag (WP 168) zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten.

Am 9. Juli 2009 hat die Kommission ein Konsultationsverfahren zu dem Rechtsrahmen für das Grundrecht auf den Schutz personenbezogener Daten eingeleitet. Gegenstand des Konsultationsverfahrens sind die neuen Herausforderungen für den Schutz personenbezogener Daten, insbesondere angesichts neuer Technologien und angesichts der Globalisierung. Die Kommission erwartet Beiträge zu den Fragen, ob der aktuelle Rechtsrahmen den Herausforderungen gewachsen ist und welche zukünftigen Aktionen erforderlich sind, um die ermittelten Herausforderungen in Angriff zu nehmen. Das vorliegende Dokument enthält die gemeinsame Stellungnahme der Artikel-29-Arbeitsgruppe (WP29) und der Arbeitsgruppe Polizei und Justiz (WPPJ) zu diesem Konsultationsverfahren.

Dieser Beitrag stellt in erster Linie fest, dass die wichtigsten, in der Richtlinie 94/45/EG festgelegten Grundsätze des Datenschutzes nach wie vor gültig sind. Das Datenschutzniveau in der EU kann von einer besseren Anwendung der bestehenden Datenschutzgrundsätze profitieren. Das bedeutet nicht, dass keine Gesetzesänderungen erforderlich sind. Ganz im Gegenteil ist es sinnvoll, die Gelegenheit zu ergreifen, um:

- die Anwendung einiger Grundregeln und Grundsätze des Datenschutzes (wie Einwilligung und Transparenz) zu klären.
- dem Rechtsrahmen durch zusätzliche Grundsätze (wie z. B. „Privacy by Design" und „Rechenschaftspflicht") Neuerungen hinzuzufügen.
- die Wirksamkeit des Systems durch die Modernisierung von Bestimmungen der Richtlinie 95/46/EG zu stärken (z. B. durch eine Einschränkung der bürokratischen Hindernisse).
- die Grundsätze des Datenschutzes in einem umfassenden Rechtsrahmen zusammenzufassen, der auch bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Anwendung findet.

1.4. RECHNUNGSLEGUNG, ABSCHLUSSPRÜFUNG & FINANZIELLE ANGELEGENHEITEN

Beitrag der Artikel-29-Datenschutzgruppe (WP 164) zur öffentlichen Konsultation der GD MARKT zu dem Bericht der Expertengruppe „Kredithistorien"

Die Artikel-29-Arbeitsgruppe begrüßt, dass die Europäische Kommission ihr die Gelegenheit zur

Kommentierung des Berichts der Arbeitsgruppe „Kredithistorien" gegeben hat, zu dem eine öffentliche Konsultation stattfand. Die Artikel-29-Arbeitsgruppe merkt an, dass die Expertengruppe „Kredithistorien" (EGCH) von der Europäischen Kommission das Mandat erhalten hat, Lösungen zur Optimierung der Weiterleitung von Kreditdaten innerhalb der EU zu erarbeiten. Die Arbeitsgruppe erkennt an, dass die EGCH bei der Ausübung dieses Mandats auch das Recht auf Schutz der Privatsphäre sowie sonstige Überlegungen zum Verbraucherschutz diskutiert hat. In diesem Zusammenhang stellt die Arbeitsgruppe fest, dass die EGCH sich gegen die Empfehlung der Einrichtung eines gesamteuropäischen Kreditregisters oder der Anpassung aller nationalen Kreditregister an ein einheitliches bestehendes oder neues Modell entschieden hat und begrüßt dies.

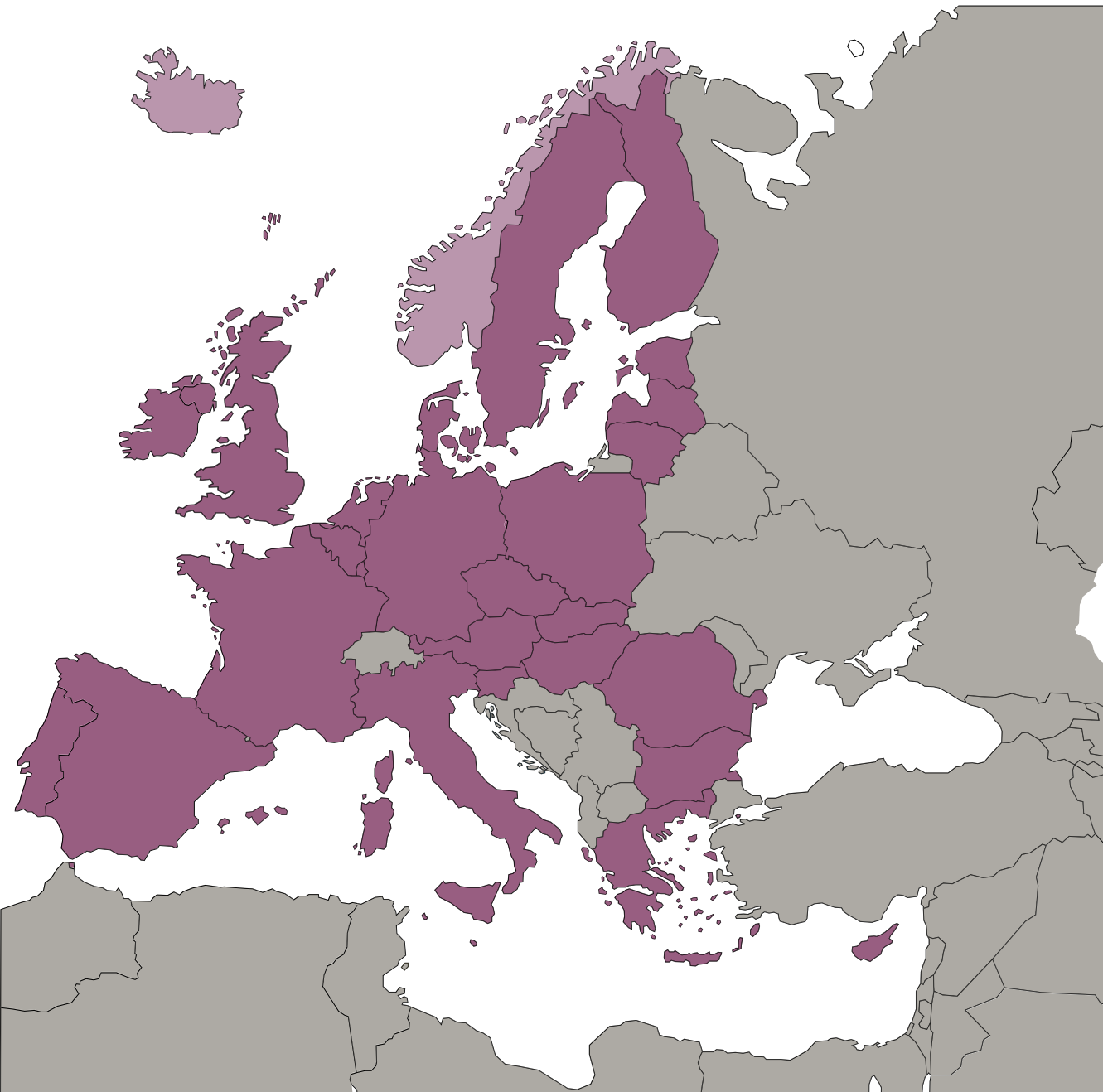
Die Artikel-29-Arbeitsgruppe möchte klarstellen, dass der Ansatz der Datenschutzbehörden der EU/des EWR in dieser Angelegenheit auf der Datenschutzrichtlinie (Richtlinie 95/46/EG) sowie auf den unterschiedlichen Rechtsgrundlagen beruht, die diese Richtlinie in den jeweiligen Mitgliedstaaten umsetzen. Der EGCH-Bericht spricht wichtige Angelegenheiten wie die Harmonisierung von Verordnungen sowie Diskussionen am runden Tisch und die Zusammenarbeit zwischen den Datenschutzbehörden an. Deshalb fordert die Artikel-29-Arbeitsgruppe die Expertengruppe auf, eine klare und eindeutige Position zu beziehen und von allen betroffenen Parteien zu den Angelegenheiten, die regulatorische Maßnahmen erfordern, förmliche Zusagen einzuholen.

Die Empfehlungen der Expertengruppe spiegeln in erster Linie die Anliegen des Finanzsektors wider, da die Mehrheit der Mitglieder der Expertengruppe Finanzinstitute vertritt. Die Mitglieder der Artikel-29-Arbeitsgruppe sind deshalb der Meinung, dass dieser Beitrag und die Reaktionen der Vertreter der Verbraucher auf den Bericht der Expertengruppe ebenfalls berücksichtigt werden sollten.

Der Bericht befürwortet eine weitere Liberalisierung bei der Verarbeitung von Kreditprofilen von Privatpersonen. In den meisten Mitgliedstaaten geht der Trend dahin, eine solche Verarbeitung als Erstellung von „schwarzen Listen" oder Profilen anzusehen. Die wiederkehrenden Verweise auf die „nationalen Datenschutzgesetze" reichen nicht aus, insbesondere da viele Mitgliedstaaten (bislang) noch keine detaillierten und ausgewogenen Bestimmungen zu den Datenschutzaspekten von Kreditinformationen getroffen haben. Außerdem muss der Bericht der Expertengruppe in Bezug auf präzise und besondere Garantien zu den Datenschutzbestimmungen verbessert werden.

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 im Berichtsjahr 2008 beschriebene Projekt der Änderung des österreichischen Datenschutzgesetzes wurde vom Parlament wieder aufgegriffen und am Ende des Jahres 2009 als **Datenschutzgesetz-Novelle 2010** beschlossen[7]. In diesem neuen Gesetzesentwurf[8] wurden die im Entwurf 2008 behandelten Themen nur zum Teil übernommen: Die wesentlichsten Neuerungen betreffen Regelungen über die Videoüberwachung, die Einführung einer Verpflichtung zu einer Meldung eines Verstoßes gegen das Datenschutzgesetz in schwerwiegenden Fällen und die Vereinfachung der Meldung von Datenanwendungen durch den Umstieg auf ein online abzuwickelndes Meldeverfahren. Nicht verwirklicht wurde der ursprünglich im Entwurf enthaltene Vorschlag, eine rechtliche Grundlage für die verpflichtende Einsetzung von Datenschutzbeauftragten zu schaffen.

Über die Details der Novelle und ihre Auswirkungen wird die österreichische Datenschutzkommission im nächsten Jahr berichten, da die Novelle erst am 1.1.2010 in Kraft getreten ist.

Ein neuer Gesetzesentwurf zur Umsetzung der Richtlinie 2006/24/EG (**Vorratsdatenspeicherung**) wurde Ende 2009 zur Begutachtung ausgesendet[9]. Die österreichische Datenschutzkommission hat dazu umfangreich Stellung genommen und zum wiederholten Mal darauf hingewiesen[10], dass bei einem so schwerwiegenden Eingriff in das Grundrecht auf Datenschutz der Zweck der Datenverwendung eindeutig und abschließend definiert sein muss, was eine klare Begrenzung des Begriffs der „schweren Straftaten" bedingt.

Zahlreiche Beschwerden haben im Berichtszeitraum den Bereich der **Kreditinformation** betroffen, weshalb die Datenschutzkommission ihre bereits früher erhobene Forderung nach einer gesetzlichen Regelung der Rahmenbedingungen für die Ermittlung, das Angebot und die Weiterverwendung von Bonitätsinformation mehrfach wiederholt hat. Dies hat dazu geführt, dass das zuständige Bundesministerium beauftragt wurde, bis Jahresende 2010 einen Gesetzentwurf vorzulegen.

In einem weiteren Bereich hat die Datenschutzkommission dringenden legislativen Handlungsbedarf geäußert, nämlich im Bereich des Datenaustausches von Gesundheitsdiensteanbietern (z.B. Krankenanstalten) mit privaten Krankenversicherungsunternehmen. Hier hat die DSK gemeinsam mit den Vertretern der betroffenen Interessensgruppen (Versicherte, Versicherer, Krankenanstalten, Ärzteschaft) eine gründliche Analyse durchgeführt und diese dem zuständigen Bundesministerium für die Erarbeitung eines neuen Gesetzentwurfes zur Verfügung gestellt

B. Rechtsprechung

Das Bestehen eines Rechts auf **Auskunft** über Daten, die im Zuge einer **Videoüberwachung** aufgezeichnet wurden, wurde in einem Fall verneint, in dem

- die regelmäßige Speicherdauer 48 Stunden betrug,
- sich kein Anlass zur Auswertung ereignet hat, und
- mit an Sicherheit grenzender Wahrscheinlichkeit auch andere Personen von der Aufzeichnung und damit von der Auswertung betroffen gewesen wären.

Begründet wurde diese Entscheidung damit, dass die Datenschutzrechte Dritter – nämlich der übrigen Abgebildeten – bei der geschilderten Konstellation als vorrangig gegenüber dem Auskunftsinteresse des Auskunftswerbers anzusehen sei, da dessen Daten nach sehr kurzer Zeit ohnehin gelöscht würden und bis dahin niemandem zur Kenntnis gelangt seien, da kein Anlass zu einer Auswertung (wie z.B. Vandalismus, Angriff auf Menschen etc.) eingetreten ist [11].

[7] http://www.parlament.gv.at/PG/DE/XXIV/I/I_00472/pmh.shtml

[8] Der Entwurf und alle Stellungnahmen sind auf der folgenden Webseite des österreichischen Parlaments abrufbar: http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00062/pmh.shtml

[9] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml

[10] http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00117_I3/imfname_178831.pdf

[11] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20081205_K121385_0007-DSK_2008_00/DSKTE_20081205_K121385_0007-DSK_2008_00.pdf

Wie in der Zwischenzeit auch der Verfassungsgerichtshof bestätigt hat, ist die **Aufbewahrung von (Straf-) Verfahrensakten** über die Verfahrensdauer hinaus auch dann zulässig, wenn der Verdächtige freigesprochen oder das Verfahren eingestellt wird. Dies obwohl es – neben dem Grundsatz, dass Daten nur so lange aufbewahrt werden dürfen, wie sie benötigt werden - keine spezielle gesetzliche Vorschrift über die zulässige Aufbewahrungsdauer von Verfahrensakten gibt. Wesentlicher Grund für die Aufbewahrung von Verfahrensakten nach Verfahrensbeendigung ist die Beweisbarkeit eines Freispruchs oder der Verfahrenseinstellung, aber auch die Nachprüfbarkeit der Rechtsmäßigkeit der Verfahrenshandlungen. Der Gefahr eines allfälligen Missbrauchs von Daten durch Weiterverwendung für einen neuen – vom ursprünglichen Ermittlungszweck verschiedenen – Zweck ist nicht durch die vorzeitige Löschung der Verfahrensakten zu begegnen, sondern muss durch genau definierte und auch technisch und organisatorisch effizient abgesicherte Zugriffsbeschränkungen entgegengetreten werden[12].

C. Wichtige spezifische Themen

E-Voting. Vom 18. Mai bis zum 22. Mai 2009 konnten Studierende in Österreich Ihre Interessenvertretung mit Ihrer Bürgerkarte elektronisch wählen[13]. Im Wahlsystem waren die Identitätsdaten des Wählers und der Inhalt der abgegebenen Stimme getrennt voneinander verschlüsselt. Bei der Stimmauszählung wurden zuerst die Identitätsdaten des Wählers mit dem geheimen Schlüssel des Dienstleisters entschlüsselt. Dabei wurden jene Stimmen aus der elektronischen Urne entfernt, die von nicht stimmberechtigten Personen abgegeben wurden. Sodann wurden die Identitätsdaten vom Datensatz entfernt und gelöscht. Die nach wie vor - mit dem Schlüssel der Wahlkommission - verschlüsselten Inhaltsdaten (Wahlstimmen) wurden dann gemischt und mithilfe der geheimen privaten Schlüssel von 2 Mitgliedern der Wahlkommission entschlüsselt und gezählt. Beim gesamten elektronischen Wahlvorgang wurden als Identitätsdaten keine Namen, sondern ausschließlich die von der Datenschutzkommission anhand des Wählerverzeichnisses ermittelten bereichsspezifischen Personenkennzeichen verwendet. Diese wurden - zwecks Prüfung der Wahlberechtigung - mit den bereichsspezifischen Personenkennzeichen der Studierenden verglichen, die beim Wahlvorgang die Bürgerkarte benutzt hatten.

[12] http://www.ris.bka.gv.at/Dokumente/Dsk/DSKTE_20090121_K121390_0001-DSK_2009_00/DSKTE_20090121_K121390_0001-DSK_2009_00.pdf

[13] http://www.oeh-wahl.gv.at

Belgien

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

Flämischer Überwachungsausschuss für administrative elektronische Datenübermittlung

Der Flämische Überwachungsausschuss für administrative elektronische Datenübermittlung (*Vlaamse toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer* – nachstehend „Überwachungsausschuss" oder „FSC" genannt) genehmigt den Austausch personenbezogener Daten mittels elektronischer Datenübermittlungssysteme zwischen allen Abteilungen der flämischen Verwaltung, den Provinzen, Städten und Gemeinden. Darüber hinaus berät er auf Anfrage oder nach eigenem Ermessen das flämische Parlament, die flämische Regierung sowie andere Behörden und Interessengruppen. In manchen Fällen kann ein Sicherheitsbeamter nur nach positiver Stellungnahme durch den Überwachungsausschuss ernannt werden. Der FSC erstattet dem flämischen Parlament jährlich Bericht. Im Rahmen einer Sitzung vom 17. Dezember 2009 wurden die Mitglieder des FSC vom flämischen Parlament ernannt. Der FSC wurde gemäß dem flämischen Beschluss vom 18. Juli 2008 *über administrative elektronische Datenübermittlung* (dem so genannten „Beschluss zur elektronischen Verwaltung") eingerichtet. Der Vorsitzende sowie zwei Mitglieder des FSC wurden von der Kommission zum Schutz der Privatsphäre (nachstehend „Kommission" oder „belgische Kommission" genannt) ernannt. Drei weitere Mitglieder wurden vom flämischen Parlament ernannt, das von einem beratenden Ausschuss zur Auswahl von Experten unterstützt wurde.

Entwicklungen in der Gesetzgebung zur Kameraüberwachung (Stellungnahmen Nr. 24/2009 und 40/2008)

Seit Inkrafttreten des Gesetzes *zur Regelung von Installation und Einsatz von Überwachungskameras* (nachstehend das „Kameragesetz" genannt) am 10. Juni 2007 sind über 6.000 Meldungen bei der Kommission eingegangen. Ein wichtiges Prinzip des Gesetzes ist, dass nicht jede Kamera gemeldet werden muss, jedoch jeder überwachte Ort. Aufgrund einer Reihe praktischer Probleme, denen sich die Polizei beim Einsatz mobiler Überwachungskameras gegenüber sah, wurde die Kommission im Jahr 2009 vom Senatsausschuss für Interne Angelegenheiten aufgefordert, an der Bewertung des Kameragesetzes teilzunehmen. Diese parlamentarische Maßnahme hatte das Gesetz vom 12. November 2009 *zur Abänderung des Gesetzes vom 21. März 2007 zur Regelung der Installation und des Einsatzes von Überwachungskameras* zur Folge (Belgisches Staatsblatt vom 18. Dezember 2009). Dank des abgeänderten Gesetzes reicht es nun aus, eine Stellungnahme beim betreffenden Gemeinderat zu beantragen. Dieser muss dann wiederum den Leiter der lokalen Polizei konsultieren. Zuvor war es auch erforderlich, eine Stellungnahme des Letzteren zu beantragen. Die abgeänderte Version des Kameragesetzes enthält außerdem ein neues Kapitel, demzufolge eine mobile Kameraüberwachung nur durch die Polizei und im Kontext großer Menschenansammlungen sowie ausschließlich für vorübergehende und zeitlich begrenzte Aufgaben erfolgen darf. Kameras dürfen sowohl an nicht abgesperrten Orten (z. B. während einer Demonstration) als auch an der Öffentlichkeit zugänglichen abgesperrten Orten (z. B. bei einem Rockfestival) eingesetzt werden.

Der Königliche Erlass vom 21. August 2009 *zur Änderung des Königlichen Erlasses vom 10. Februar 2008 zur Festlegung der Art und Weise der Anzeige einer Kameraüberwachung* (Belgisches Staatsblatt vom 25. September 2009) hat außerdem die bestehenden Vorschriften betreffend die Dimensionen des verpflichtenden Hinweisschildes zur Anzeige einer Kameraüberwachung abgeändert.

B. Rechtsprechung

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

C. Wichtige spezifische Themen[14]

Öffentlicher Sektor

Zentrale Datenbank für Fahrzeugdaten (Stellungnahme 06/2009)

[14] Sämtliche Stellungnahmen, Empfehlungen und Genehmigungen der Kommission sind auf ihrer offiziellen Website erhältlich. http://www.privacycommission.be.

Im Jahr 2009 veröffentlichte die Kommission eine positive Stellungnahme zum Entwurf eines Gesetzes *zur Erstellung einer zentralen Datenbank für Fahrzeugdaten*. Hauptzweck dieser Datenbank ist die Nachverfolgung von Fahrzeugeigentümern (über die eingetragenen Fahrzeughalter). In zwei der früheren Jahresberichte der Kommission sind negative Stellungnahmen zu zwei früheren Entwürfen zu finden (Stellungnahmen 42/2006 und 23/2008). Der neue Entwurf berücksichtigt fast alle Anmerkungen der Kommission und enthält umfangreiche Verbesserungen, einschließlich der eindeutigen Ernennung eines für die Datenverarbeitung Verantwortlichen sowie der Integration einer klaren Liste der Zwecke, zu denen die Daten aus der zentralen Datenbank verwendet werden dürfen. Eine Liste möglicher (Kategorien von) Empfänger(n) der Daten wird allgemein beschrieben, und die Genehmigungsbefugnis des Sektoriellen Ausschusses für die Föderalbehörde (der im Rahmen der Kommission eingerichtet wird und teilweise aus Mitgliedern der Kommission besteht) wurde anerkannt. Darüber hinaus wurde dem Ausschuss eine Reihe von Beratungskompetenzen übertragen. Die Kommission wies jedoch überdies auf einige Verbesserungsmöglichkeiten hin. So sollte der Entwurf beispielsweise explizit erwähnen, dass Kennzeichendaten (aus dem aktuellen Fahrzeugregister) in die zentrale Datenbank integriert werden. Es wird empfohlen, besser zu beschreiben, wie die Verwaltungsinstitution für den Sektor[15] sowie alle Datenquellen (z. B. Fahrzeuginspektionszentren und -hersteller) ihrer Pflicht zur Information der betroffenen Personen nachkommen sollen und welche konkreten Maßnahmen zu ergreifen sind, um die für die Informationssicherheit zuständige Person effektiv zu ernennen. Die Kommission schlägt weiterhin vor, dass jeder Dienst bzw. jede Datenquelle, die Zugang zu den Daten hat, die betroffene Person, die Verwaltungsbehörde und den sektoriellen Ausschuss über Sicherheitsverstöße informieren muss. Dieser so genannte „Meldung über einen Sicherheitsverstoß" ist in Belgien neu, existiert jedoch bereits in englischsprachigen Ländern und wird auch (teilweise) in die geplante Änderung von Artikel 4 der „Richtlinie über den elektronischen Geschäftsverkehr" 2002/58/EG[16]. integriert werden.

Allgemeine Genehmigung des Zugangs zum Register für Kennzeichendaten (Beratung FA Nr. 12/2009)

In der Vergangenheit war es für private Verwalter öffentlicher Parkplätze sehr unklar, wie sie Parkgebühren kassieren konnten, was sich in zahlreichen Urteilen zu diesem Thema widerspiegelt. Aus diesem Grund haben es die belgische Kommission und der sektorielle Ausschuss für die Föderalbehörde (der die elektronische Veröffentlichung personenbezogener Daten innerhalb der Föderalbehörden überwacht) stets abgelehnt, privaten Verwaltern von Parkplätzen Zugang zur Identität des Kennzeichenbesitzers in der DIV-Datenbank[17] zu gewähren (Stellungnahme Nr. 37/2003 und Beratung FA Nr. 02/2007). Dank einer Änderung (Gesetz vom 22. Dezember 2008 *zur Festlegung verschiedener Bestimmungen*, Titel 4, Kapitel 2, belgisches Staatsblatt vom 29. Dezember 2008) wurde die Situation nun klargestellt, und Städte und Gemeinden, die Verwalter von Parkplätzen und eigenständige kommunale Unternehmen sind nunmehr befugt, beim DIV eine Anfrage zur Identität eines Kennzeichenbesitzers zu stellen. Hierbei handelt es sich um eine so genannte „allgemeine" Genehmigung, d. h., der sektorielle Ausschuss beschreibt in der Genehmigung die (strengen) Bedingungen, die das DIV sowie die Kategorien der Begünstigten erfüllen müssen. Zudem müssen die Begünstigten einen Standardvertrag unterzeichnen, der sie zur Einhaltung dieser Bedingungen verpflichtet.

Um die Transparenz zu verbessern, werden alle allgemeinen Genehmigungen des sektoriellen Ausschusses sowie die Listen der Begünstigten (in französischer und niederländischer Sprache) auf der Website der Kommission im Bereich „Entscheidungen" veröffentlicht.

[15] Die Generaldirektion für Mobilität und Straßenverkehrssicherheit des belgischen öffentlichen Dienstes für Mobilität und Transport.

[16] Dies ist eine geplante Änderung von Artikel 3 (i) der Richtlinie 2002/58/EG über elektronische Kommunikation, erhältlich unter http://register.consilium.europa.eu/pdf/en/08/st15/st15899.en08.pdf, die vom Europäischen Datenschutzbeauftragten (EDSB) bereits positiv aufgenommen wurde. http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf.

[17] Directie Inschrijving Voertuigen – für die Registrierung von Fahrzeugen und ihren Besitzern zuständiges belgisches Amt

Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Bekämpfung von Doping im Sport (Stellungnahme Nr. 30/2009)

Auf Antrag des zuständigen Ministers veröffentlichte die Kommission im Jahr 2009 eine Stellungnahme zum von der WADA (Welt-Anti-Doping-Agentur) erarbeiteten „Internationalen Standard zum Schutz der Privatsphäre und personenbezogener Informationen". Dieser Internationale Standard beinhaltet ein Mindestmaß an gemeinsamen Vorschriften, das bei der Verarbeitung personenbezogener Daten auf der Grundlage des Welt-Anti-Doping-Codes eingehalten werden muss. Die Kommission hat beobachtet, dass der Internationale Standard nicht immer die Schutzmaßnahmen respektiert, die gemäß den belgischen Datenschutzbestimmungen gegeben sein müssen, und hat einige Anmerkungen ausgesprochen, so z. B. zu den möglichen Gründen für die Verarbeitung sensibler personenbezogener Daten, der Informationspflicht gegenüber den betroffenen Personen, zu Sicherheitsmaßnahmen und Haftungsfragen, zur Dauer der Speicherung der personenbezogenen Daten sowie zur Ausübung der Rechte der betroffenen Personen (Recht auf Zugang, Widerspruch und Berichtigung). Die Kommission betonte außerdem, dass die im Internationalen Standard beschriebenen Mindeststandards die strengeren belgischen Datenschutzvorschriften nicht außer Kraft setzen können.

Auf ein Auskunftsersuchen hin veröffentlichte die Kommission außerdem eine Stellungnahme zu den flämischen Verordnungen zur Bekämpfung von Doping im Sport, insbesondere zur Veröffentlichungspflicht der so genannten Informationen zu „Aufenthaltsort und Erreichbarkeit" bei Dopingkontrollen außerhalb von Wettkämpfen. Im flämischen Erlass vom 13. Juli 2007 *zu medizinisch und ethisch akzeptablen Sportarten* sowie im Erlass der flämischen Regierung vom 28. Juni 2008 zur Umsetzung des erstgenannten Beschlusses ist nicht festgelegt, welche Informationen zu Aufenthaltsort und Erreichbarkeit Spitzensportler bereitstellen müssen. Es wird jedoch Bezug auf den Welt-Anti-Doping-Code genommen. Diese Bezugnahme befindet sich derzeit vor dem Staatsrat in Berufung. Nichtsdestotrotz ist die Kommission der Ansicht, dass die Anforderung von Informationen zu Aufenthaltsort und Erreichbarkeit für vier Stunden täglich angemessen ist. Die Kommission äußerte sich zum Status von Spitzensportlern und machte schließlich einige Anmerkungen zur maximalen Dauer der Speicherung dieser Daten sowie zur Informationspflicht gegenüber der betroffenen Person.

Datenbank für den wallonischen öffentlichen Dienst für Berufsausbildung und Beschäftigung (Stellungnahme Nr. 18/2009)

Im Jahr 2009 veröffentlichte die Kommission eine positive Stellungnahme zum „Jobpass"-System des *„Service public de l'emploi et de la formation professionnelle"* (öffentlicher Dienst für Berufsausbildung und Beschäftigung – nachstehend „Forem" genannt). Forem ist eine wallonische Organisation, die im öffentlichen Interesse agiert und Aufgaben im Rahmen von Partnerschaften gemäß dem Verwaltungsabkommen zwischen der wallonischen Regierung und dem Forem-Vorstand ausführt. Zum einen erhalten die Arbeitslosen im Rahmen des Jobpass-Systems eine Chipkarte, und zum anderen führt das System eine neue Datenbank ein. Ziel der Datenbank und der Chipkarte ist es, die Identifizierung der Arbeitslosen sowie den Austausch ihrer Daten zwischen Forem und seinen Partnern (z. B. Schulungszentren, die nur Zugang zu den für die Ausführung ihrer Aufgaben erforderlichen Informationen haben) zu vereinfachen. Das System erleichtert außerdem den Austausch bestimmter Informationen mit dem Landesamt für Arbeitsbeschaffung (über die Zentrale Datenbank der Sozialen Sicherheit) und hilft Arbeitslosen dabei, Belege für ihre Bemühungen zur Jobsuche zu sammeln: Mit ihrer Chipkarte können sie sich zu Besuchen bei den Organisationen und Partnern von Forem anmelden, ohne einen Arbeitsvermittler hinzuziehen zu müssen. Die Kommission war der Meinung, dass eine solche Verarbeitung von Daten angemessen, relevant und nicht übertrieben sei. Sie verbat jedoch die Nutzung der nationalen Registernummer (die sich auf dem sicheren Teil der Chipkarte befindet), da dies nicht vom sektoriellen Ausschuss des Nationalregisters genehmigt worden war.

Privater Sektor

Direktmarketing (Empfehlung Nr. 04/2009)

Nach Anhörung aller europäischen Datenschutzbehörden sowie auf der Grundlage zahlreicher in den vergangenen Jahren eingegangener Anträge und Beschwerden veröffentlichte die Kommission im Jahr 2008 ein Gesetzesmemorandum zu ihrem Standpunkt in Bezug auf die Praxis im Bereich Direktmarketing. Um

zu einer ausgewogenen Analyse zu gelangen, startete die Kommission zunächst einen Dialog mit den Interessengruppen aus den Bereichen Unternehmen, Verbraucherverbände und Wissenschaft, um so mehr über ihre Interessen, Prioritäten und gegebenenfalls ihre Verhaltensregeln zu erfahren. Schließlich wollte die Kommission auch die Meinungen der Bürger hören und führte deshalb eine öffentliche Umfrage auf ihrer Website durch. Diese Bemühungen mündeten in der Empfehlung Nr. 04/2009 betreffend Direktmarketing und den Schutz personenbezogener Daten. In diesem Dokument liefert die Kommission ihre Interpretation des Datenschutzgesetzes im Hinblick auf Direktmarketing, empfiehlt eine Reihe von Arbeitsweisen, die als bewährte Verfahrensweisen angesehen werden können (und die eine faire und transparente Verarbeitung der Daten begünstigen, ungeachtet ihrer gesetzlichen Verankerung), und spricht einige Empfehlungen an den Gesetzgeber zur Verbesserung der vorhandenen Bestimmungen aus.

Einverständnis
Die Kommission ist der Ansicht, dass das freie, informierte und spezielle Einverständnis der betroffenen Person als Grundlage für die Rechtfertigung von Direktmarketing dienen kann. Dies wird dementsprechend als bewährte Verfahrensweise empfohlen. Die Empfehlung spezifiziert Bedingungen und betont eine Reihe von Fällen, in denen ein Einverständnis absolut erforderlich (z. B. fast immer dann, wenn Direktmarketing über Textnachrichten, per E-Mail, Fax oder über automatische Wählsysteme erfolgt) bzw. praktisch unvermeidlich (z. B. bei Adressenvermittlungen und bei der Erstellung von Profilen) ist.

Legitimes Interesse
Wenngleich es bei weitem nicht offensichtlich ist, dass das Gleichgewicht der Interessen stets gewahrt werden muss (insbesondere bei Adressenvermittlungen und der Erstellung von Profilen), so erkennt die Kommission doch an, dass dieses Prinzip die Grundlage für die Verarbeitung personenbezogener Daten im Fall von Direktmarketing ist. Die Empfehlung legt den Moment zur Bewertung des Interessengleichgewichts sowie die Kriterien und die Methoden zur Bewertung fest. Wird dieses Gleichgewicht gestört, so muss die Verarbeitung unverzüglich gestoppt werden.

Zeitraum für die Speicherung
Zusätzlich zur Verpflichtung, falsche Daten zu berichtigen, empfiehlt die Kommission einen Zeitraum für die Speicherung personenbezogener Daten.

Informationen
Die Kommission betont die Bedeutung korrekter Informationen, insbesondere wenn die Daten nicht direkt von der betroffenen Person erhalten wurden. In diesem Fall empfiehlt die Kommission dringend, dass der für die Datenverarbeitung Verantwortliche aktiv die Datenquelle offen legt. Direktvermarkter können sich im Hinblick auf die Verpflichtung der Information der betroffenen Person nicht auf eine Ausnahmeregelung aufgrund von Unmöglichkeit oder unverhältnismäßigen Anstrengungen berufen. Grund hierfür ist teilweise die Tatsache, dass gerade der Kontakt mit der betreffenden Person das Direktmarketing ausmacht.

Widerspruch
Schließlich erwähnt die Kommission das freie Recht der betroffenen Person, ohne Angabe von Gründen zu widersprechen. Dieser Widerspruch ist für eine Beendigung der Datenverarbeitung ausreichend. Sie erwähnt weiterhin, dass dieses Recht an keine Bedingungen geknüpft sein darf.

Empfehlung an Vermieter und Immobilienmakler zur Verarbeitung personenbezogener Daten potenzieller Mieter (Empfehlung Nr. 01/2009)
In den vergangenen Jahren sind beim Sekretariat der Kommission regelmäßig Fragen von Bürgern zu Mietverträgen und den personenbezogenen Daten eingegangen, die Eigentümer von Mietwohnungen und Immobilienmakler anfordern können. In ihrer Empfehlung legt die Kommission fest, welche Daten angefordert werden dürfen und welche nicht.

Die Kommission ist der Ansicht, dass Daten wie Nachname, Vorname, Anschrift, Aufenthaltserlaubnis sowie Geburtsdatum erforderlich sind, um einen Mietvertrag abzuschließen, hält es jedoch für unverhältnismäßig, nach ethnischer Herkunft, Geburtsort und nationaler Registernummer der potenziellen Mieter zu fragen. Familienstand, Telefonnummer sowie Fahrzeugkennzeichen können unter bestimmten Umständen relevant sein. So ist es beispielsweise

verboten, die Kennzeichendaten der Mieter zu verarbeiten, sofern die Mietwohnung nicht über einen Parkplatz verfügt, für den eine Fahrzeugerkennung erforderlich ist, damit der Mieter Zugang zu diesem Parkplatz hat. Ebenso ist der Familienstand nicht relevant bei einem Mieter, der eine Mietwohnung allein bewohnen wird.
Vermieter müssen überprüfen können, ob die Mieter in der Lage sind, die monatliche Miete zu zahlen. Hierzu reichen Informationen über ihr regelmäßiges Einkommen aus. Fragen nach der allgemeinen finanziellen Situation eines Mieters sind nicht erforderlich. Dies bedeutet, dass das Vorzeigen der Gehaltsabrechnung gerechtfertigt ist (Identität des Arbeitgebers, Beruf und andere nicht relevante Daten dürfen hierbei geschwärzt werden, wenn der Mieter dies wünscht), Der Mieter muss dem Vermieter jedoch keine Kopie der Abrechnung aushändigen, da es ausreicht, wenn der Vermieter sehen kann, dass der potenzielle Mieter zahlungsfähig ist. Es ist jedoch akzeptabel, dass ein Immobilienmakler einen Nachweis des Einkommens des potenziellen Mieters aufbewahren will und eine Kopie der Abrechnung anfertigt. Daten aus der zentralen belgischen Kreditdatenbank für Privatpersonen sind Kreditgebern und Organisationen oder Einzelpersonen mit einer ähnlichen Funktion vorbehalten. Sie benötigen diese Daten zur Erfüllung ihrer Pflichten.

Vermieter können Daten zu den Personen anfordern, die in der Mietwohnung leben werden, so z. B. Daten dazu, wie viele Personen dort leben werden und wie alt diese in etwa sind. Auszüge aus dem polizeilichen Führungszeugnis sind gemäß Datenschutzgesetz nicht erlaubt. Die Verarbeitung von Daten zur Gesundheit potenzieller Mieter ist laut Kommission nur unter zwei Bedingungen gestattet. Erstens muss der Mieter sein schriftliches Einverständnis geben, das er jederzeit widerrufen kann. Zweitens müssen die Daten relevant sein: Ein behinderter Mensch, der eine an seine Bedürfnisse angepasste Wohnung mieten möchte, muss möglicherweise Auskunft zu seinem Gesundheitszustand geben.

Neue Technologien

Vorratsspeicherung von Daten (Stellungnahme Nr. 20/2009)

Im Zusammenhang mit der Umsetzung der Richtlinie 2006/24/EG, der so genannten Richtlinie über die Vorratsspeicherung von Daten, in einzelstaatliches Recht, wurde die Kommission gebeten, zu einem Gesetzesentwurf sowie zum Entwurf eines Königlichen Erlasses zur Verpflichtung zur Zusammenarbeit Stellung zu nehmen. Ziel der Richtlinie ist die Harmonisierung der Verpflichtungen von Dienstleistungsanbietern hinsichtlich der Vorratsspeicherung bestimmter Daten sowie die Bereitstellung dieser Daten für befugte Dienste im Rahmen der Untersuchung, Erkennung und strafrechtlichen Verfolgung schwerer Verbrechen. Die Kommission hat in diesem Zusammenhang bereits zwei Mal negative Stellungnahmen veröffentlicht. Im Jahr 2009 wurde jedoch eine positive Stellungnahme zu den angepassten Entwürfen veröffentlicht. Nichtsdestotrotz sind einige Anmerkungen zu berücksichtigen. So muss beispielsweise der Zeitraum für die Vorratsspeicherung der Daten von 24 auf 12 Monate gesenkt und im Gesetzesentwurf festgelegt werden. Das Parlament muss den Gesetzesentwurf und den Entwurf des Erlasses bewerten, und der zuständige Minister muss dem Parlament jährlich Bericht erstatten. Schließlich muss auch die Rolle des Dienstes NTSU-CTIF[18], der direkten Zugang zu den Datenbanken hat, klarer definiert werden. Genauer gesagt müssen sein Platz im Organigramm und ein angemessenes Maß an Sicherheit klargestellt werden.

Funkfrequenzkennzeichnung (Stellungnahme Nr. 27/2009)

In dieser aus eigener Initiative heraus veröffentlichten Stellungnahme legt die Kommission die Bedingungen für eine Verarbeitung personenbezogener Daten durch Radiofrequenzkennzeichnungs-Tags (RFID-Tags) fest. Mit dieser Technologie können auf in Gegenständen eingebauten oder in Lebewesen implantierten Chips gespeicherte Informationen ferngesteuert gespeichert und gelesen werden. Die Kommission hebt zwei Situationen hervor, in denen eine Verarbeitung personenbezogener Daten erfolgt: zum einen die Verbindung personenbezogener Daten mit einem solchen Tag und zum anderen die Platzierung personenbezogener Daten auf einem solchen Tag. In der Stellungnahme listet die Kommission die Prinzipien des Datenschutzgesetzes auf, die der für die Verarbeitung Verantwortliche berücksichtigen muss. So muss die Verarbeitung beispielsweise legitim und verhältnismäßig sein. Das Einverständnis der betroffenen Personen kann eine

[18] Zentraler technischer Überwachungsdienst der föderalen und der lokalen Polizei.

Grundlage für die Verarbeitung sein, jedoch muss auch das Interesse des für die Verarbeitung Verantwortlichen mit den Rechten der betroffenen Person auf Schutz ihrer Privatsphäre abgewogen werden, z. B. durch eine Risikoanalyse. Die betroffene Person muss außerdem ausreichend mittels einer Datenschutzpolitik informiert werden, die leicht zu verstehen ist und mindestens die Identität des für die Verarbeitung Verantwortlichen, den Zweck der Verarbeitung, die verarbeiteten Daten (möglicherweise einschließlich einer Tag-Kontrolle), eine Zusammenfassung der Datenschutzbewertung sowie eine Risikoanalyse umfasst. Schließlich betont die Kommission die Bedeutung angemessener technischer und organisatorischer Sicherheitsmaßnahmen.

Bulgarien

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

1. Im Rahmen ihrer ersten Sitzung des Jahres 2009 verabschiedete die Kommission zum Schutz personenbezogener Daten neue Vorschriften zur Tätigkeit der Kommission zum Schutz personenbezogener Daten. Dies wurde im Amtsblatt vom 2. Februar 2009 bekannt gegeben, wodurch die seit März 2007 geltenden Vorschriften zur Tätigkeit der Kommission außer Kraft gesetzt wurden.

   Das Erfordernis zur Erarbeitung und Verabschiedung der Vorschriften des Jahres 2009 basierte auf den von der Kommission zum Schutz personenbezogener Daten in ihrer Eigenschaft als Kontrollstelle im Bereich der Verarbeitung personenbezogener Daten verabschiedeten neuen Prioritäten. Ziel dieses Rechtsaktes ist die Synchronisierung der Tätigkeit der Verwaltungseinheiten der Kommission durch die Ausübung einer allgemeinen Kontrolle der Einhaltung der Gesetze über den Schutz personenbezogener Daten sowie zur Verarbeitung personenbezogener Daten. Die in den Vorschriften genannten Bestimmungen verliehen der Kommission größere Flexibilität bei der Beschlussfassung, wodurch die Effizienz der Tätigkeiten der Kommission insgesamt gestärkt wurde.

   Diese Vorschriften betonen die im Gesetz über den Schutz personenbezogener Daten festgelegten Befugnisse der Kommission sowie die zugehörigen von der Kommission durchgeführten Verfahren. Es wurden strukturelle Veränderungen in der Verwaltung der Kommission durchgeführt und somit die Referate konsolidiert, die die Kommission bei besonderen Tätigkeiten unterstützen. Auf diese Weise wurde die Expertentätigkeit konsolidiert, was zu besseren Ergebnissen durch die Umsetzung der in der Gesetzgebung definierten Befugnisse der Kommission geführt hat.

2. Die Kommission hat einen Entwurf zur Änderung und Ergänzung des Gesetzes über den Schutz personenbezogener Daten (GSPD) erarbeitet sowie im Februar 2009 öffentliche Diskussionen organisiert und durchgeführt, an denen der Vorsitzende sowie Mitglieder des Ausschusses für innere Sicherheit und öffentliche Ordnung in der Nationalversammlung, Vertreter von Nichtregierungsorganisationen, akademischen Kreisen und den Medien teilgenommen haben. Wegen der Parlamentswahlen im Juni 2009 wurde der Gesetzesentwurf nicht von der 40. Nationalversammlung verabschiedet. Die Arbeit am Entwurf wurde fortgesetzt, und die Empfehlungen aus der öffentlichen Konsultation wurden berücksichtigt.

3. Vertreter der Kommission waren an der Arbeit der abteilungsübergreifenden Arbeitsgruppe zur Vorbereitung eines Gesetzesentwurfs zur Änderung und Ergänzung des Gesetzes über elektronische Kommunikation beteiligt. Die vorgesehenen Änderungen bestimmen die Kommission zum Schutz personenbezogener Daten als Aufsichtsbehörde, um so die Tätigkeit von Unternehmen zu kontrollieren, die öffentliche Netzwerke und/oder Dienste zur elektronischen Kommunikation anbieten, und um die Einhaltung der Vorschriften zu Schutz und Sicherheit der gespeicherten Daten gemäß den Bestimmungen von Art. 7 der Richtlinie 2006/24/EG sicherzustellen. Die Benennung der Kommission als Aufsichtsbehörde erfolgt in Einklang mit der Verpflichtung jedes Mitgliedstaates, gemäß Art. 9 der Richtlinie 2006/24/EG eine öffentliche Stelle zu benennen, die in ihrem Hoheitsgebiet für die Kontrolle der Anwendung der von den Mitgliedstaaten zur Umsetzung von Art. 7 erlassenen Vorschriften bezüglich der Sicherheit der auf Vorrat gespeicherten Daten zuständig ist. Richtlinie 2006/24/EG legt explizit fest, dass diese Stelle die gemäß Art. 28 der Richtlinie 95/46/EG eingerichtete Stelle sein kann. Im Fall der Republik Bulgarien ist diese Stelle die Kommission zum Schutz personenbezogener Daten.

4. Im November 2009 hat der Ministerrat das Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr angenommen und dem Parlament dessen Ratifizierung vorgeschlagen. Das Parlament kam diesem Vorschlag daraufhin

nach, und das Protokoll wurde im Amtsblatt vom 6. Januar 2010 veröffentlicht. Gemäß Art. 1, Absatz 1 des Zusatzprotokolls ist die Kommission die Kontrollstelle.

B. Bedeutende Rechtsprechung

Die Bearbeitung der Beschwerden von Einzelpersonen über spezifische Verletzungen ihrer Rechte stellt einen wesentlichen Teil der Tätigkeiten der Kommission dar. Die Analyse zeigt, dass es in den gegen zentrale Strafverfolgungsbehörden eingelegten Beschwerden hauptsächlich um die Weitergabe personenbezogener Daten an Dritte oder die Verbreitung personenbezogener Daten ohne das Wissen und das Einverständnis der betroffenen Personen geht.

Zahlreiche Beschwerden bezogen sich auch auf die Verweigerung des Zugangs zu personenbezogenen Daten sowie die Weitergabe personenbezogener Daten an Dritte. Die Kommission zum Schutz personenbezogener Daten hat verbindliche Anweisungen für die Gewährung des Zugangs zu personenbezogenen Daten gemäß den Anträgen der Beschwerdeführer veröffentlicht, da die Beschwerden als fundiert eingestuft wurden.

Im Jahr 2009 wurden der Kommission zum Schutz personenbezogener Daten neue Fälle der Verbreitung personenbezogener Daten im Internet vorgelegt. Es wurde festgelegt, dass personenbezogene Daten einer bestimmten Nutzerkategorie als Teil von wissenschaftlichen Abhandlungen, Berichten, Vorlesungen und Analysen zum Zweck der Bereitstellung von Hilfe in Foren verbreitet werden. Abgesehen von den Verstößen gegen das Urheberrecht und verwandte Rechte ist die Kommission zum Schutz personenbezogener Daten der Ansicht, dass die Verbreitung personenbezogener Daten dem Prinzip der Verhältnismäßigkeit sowie der Zweckbeschränkung der verarbeiteten personenbezogenen Daten gemäß Art. 2, Absatz 2, S. 2 und S.3 des Gesetzes zum Schutz personenbezogener Daten widerspricht.

Im Jahr 2009 veröffentlichte die Kommission Stellungnahmen als Reaktion auf Anfragen sowohl von gemäß Art. 3 des GSPD für die Datenverarbeitung Verantwortlichen als auch von Einzelpersonen, die Anfragen zu ihren Rechten stellten. Es wurden Anfragen zur Veröffentlichung personenbezogener Daten von Eigentümern, Vertretern und Mitgliedern von kollektiven Einrichtungen kommerzieller Unternehmen im Handelsregister beantwortet, das von der Registerstelle verwaltet wird. Gemäß Art. 11 des Handelsregistergesetzes ist das Register öffentlich. Jeder hat das Recht auf freien Zugang zum Register, zu den elektronischen Kopien der Dokumente, auf deren Grundlage Einträge, Löschungen und Bekanntmachungen erfolgt sind, sowie zu den elektronischen Kopien der Unternehmensfälle, im Rahmen derer Unternehmer neu registrieren wurden. Darüber hinaus bietet die Stelle freien Zugang zu den Anwendungen des Informationssystems des Handelsregisters, den dazugehörigen Dokumenten sowie den Ablehnungserklärungen. Die Angaben zu den Unternehmen wie z. B. eingetragener Firmensitz, Anschrift der Geschäftsführung und Vertreter des Unternehmens werden nach Eintragung des Unternehmens im Register öffentlich. Verordnung Nr. 1 über die Verwaltung, die Speicherung und den Zugang zum Handelsregister legt die Standardformulare für die Registrierungsanträge fest und gibt ausdrücklich die Umstände an, die eine Registrierung erfordern und die auf den Registrierungs-, Löschungs- oder Veröffentlichungsanträgen anzugeben sind. Die Verordnung regelt die gesetzlichen Verpflichtungen, auf deren Grundlage die Registerstelle die personenbezogenen Daten einer bestimmten Personenkategorie rechtmäßig verarbeitet.

Es wurden Anfragen zu Fällen eingereicht, in denen Angestellte verschiedener Einzelhandelsgeschäfte bei der Durchführung von Zahlungen mit Bank- oder Kreditkarten, die als elektronische Zahlungsinstrumente (EZI) bezeichnet werden, die betroffenen Personen gebeten haben, ein Ausweisdokument – den Personalausweis – vorzuzeigen, um ihre Identität zu überprüfen. Gemäß Artikel 31 Absatz 5 des Gesetzes über Geldüberweisung, Elektronische Zahlungsinstrumente und Zahlungssysteme darf der Händler um Vorlage eines Ausweisdokuments bitten, wenn begründete Zweifel an der Identität des EZI-Inhabers bestehen.

Bezüglich der Umsetzung von Artikel 64 des Justizgesetzes über die Öffentlichkeit und Transparenz von gerichtlichen Vorgängen und die Öffentlichkeit von Gerichtsurteilen sowie in Zusammenhang mit

dem Schutz der Rechte des Einzelnen im Hinblick auf die Verarbeitung personenbezogener Daten äußerte die Kommission ihren Standpunkt, dass bei der Einrichtung und Führung eines öffentlichen Registers für Gerichtsurteile gewisse Maßnahmen ergriffen werden sollten, um die Anonymität der Betroffenen zu wahren. Zusätzlich zur Verwendung von Initialen statt vollständiger Namen der Einzelpersonen sowie der Löschung von Personennummern und Adressen müssen außerdem sämtliche Hinweise zu körperlichen, physiologischen, genetischen, geistigen, psychologischen, wirtschaftlichen, kulturellen und gesellschaftlichen Angaben bzw. sonstige Faktoren, mithilfe derer die Einzelperson trotz der Verwendung von Initialen identifiziert werden könnte, entfernt werden.

C. Wichtige spezifische Themen

Am 30. April 2009 trug die Kommission zum Schutz personenbezogener Daten alle bis dahin nicht registrierten Datenkontrolleure in das Register für Datenkontrolleure und die von ihnen geführten Register ein, die einen Antrag im Zeitraum von 2003 bis 2008 gestellt hatten. Es wurden Identifikationsnummern für 193.351 Datenkontrolleure ausgegeben. Mit diesem Beschluss setzte die Kommission den Datenkontrolleuren eine Frist, die eingereichten Daten zu aktualisieren und so zu gewährleisten, dass die Datenbank auf dem aktuellen Stand ist. Die Verpflichtung zur Aktualisierung der Umstände in den Registern ist eine fortwährende Verpflichtung gemäß dem Gesetz zum Schutz personenbezogener Daten. Das Gesetz sieht Sanktionen für die Verarbeitung nicht registrierter personenbezogener Daten sowie für die unvollständige Aktualisierung ihrer Angaben auf dem in das Register aufzunehmende Registrierungsformular vor. Der Beschluss der Kommission zur Aktualisierung der Informationen bis zum 15. Februar 2010 wurde gefasst, um die Verlässlichkeit der Informationen im öffentlichen Register zu gewährleisten, da dieses Register über die Website der Institution frei zugänglich ist. Den Datenkontrolleuren wird so die Möglichkeit gegeben, ihre Informationen über das Internet – auch ohne elektronische Signatur –, per Post oder persönlich bei der Kommission zu aktualisieren.

Republik Zypern

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

(I) Hinsichtlich der Umsetzung der Richtlinien 95/46/EG und 2002/58/EG gab es keine Entwicklungen in der Gesetzgebung.

(II) Abgeänderte Gesetze

(III) Erlassene Gesetze

B. Bedeutende Rechtsprechung

Als Reaktion auf eine Anfrage des Polizeichefs an den Juristischen Dienst der Republik bezüglich der Rechtmäßigkeit einer gesetzlichen Verordnung zur Erfassung der Fingerabdrücke von Studenten aus Drittländern bei ihrer Ankunft in Zypern veröffentlichte der Generalstaatsanwalt eine Stellungnahme, in der er zu dem Schluss kommt, dass ihm diese Praxis nicht rechtmäßig erscheine. Er schlug daher vor, dass der Kommissar für den Schutz personenbezogener Daten sich weiter mit dieser Frage befassen solle.

Nach Untersuchung aller relevanten, derzeit geltenden gesetzlichen Verordnungen veröffentlichte der Kommissar einen Beschluss, der besagt, dass diese spezielle Verordnung keine rechtliche Grundlage für die Erfassung der erwähnten Fingerabdrücke darstellt/bietet. Infolgedessen wurde ein Verfahren zur Auferlegung von Verwaltungssanktionen gegen die Polizei in die Wege geleitet, jedoch nicht abgeschlossen, weil der Polizeichef zwischenzeitlich die Fingerabdruckdatenbank entsprechend der Stellungnahme und dem Beschluss sowie nach eigenem Ermessen löschen ließ.

Als Reaktion auf Veröffentlichungen in der Tagespresse sowie auf eine Reihe von Anrufen von besorgten Bürgern, die bei unserem Büro eingingen und die Vorgehensweise kommunaler Hilfspolizisten betrafen, falsch parkende Fahrzeuge zu fotografieren, deren Besitzer einen Strafzettel erhalten hatten, nahm unser Büro in Übereinstimmung mit der kommunalen Behörde hierzu Stellung und äußerte die Ansicht, dass diese Vorgehensweise gegen die Datenschutzgesetze verstoße.

Obwohl die kommunale Behörde diese Vorgehensweise entsprechend der genannten Stellungnahme einstellte, reichte sie eine Beschwerde vor dem Obersten Gerichtshof ein. Der Fall ist noch nicht abgeschlossen.

C. Wichtige spezifische Themen

Als Reaktion auf einen vom Kommissar eingereichten Vorschlag verabschiedete der Ministerrat im Oktober 2009 einen Beschluss, dementsprechend alle Ministerien und Regierungsabteilungen/-dienste Datenschutzbeauftragte ernennen sollten, die vom Büro des Kommissars im Umgang mit Fragen des Schutzes interner Daten zu schulen sind.

Nach einer Reihe von Beschwerden, die unserem Büro vorgelegt wurden, veröffentlichte der Kommissar im Jahr 2003 eine Stellungnahme, in der er zu dem Schluss kam, dass die Vorgehensweise der Nationalgarde, medizinische (körperliche oder geistige) Gründe für die Entlassung oder vorübergehende Suspendierung von Soldaten aus dem Dienst auf den Dokumenten zur vorübergehenden Entlassung/Suspendierung aus dem Dienst anzugeben, gegen die Datenschutzgesetzgebung verstößt.

Entsprechend der genannten Stellungnahme stellte Nationalgarde diese Vorgehensweise ein. Im Jahr 2009 veröffentlichte der Verteidigungsminister jedoch einen Beschluss, der besagte, dass die Nationalgarde die beendete Vorgehensweise wieder aufnehmen sollte, und zwar aufgrund der Tatsache, dass die Ausstellung eines Dokuments zur vorübergehenden Entlassung/Suspendierung einen Verwaltungsakt darstellt, der die Verwaltungsbehörde, also die Nationalgarde, dazu verpflichtet, den Soldaten die Gründe für die Entscheidung zu einer vorübergehenden Entlassung/Suspendierung schriftlich mitzuteilen. Der Fall liegt dem Kommissar vor, eine Entscheidung steht noch aus.

Der Verband der Banken von Zypern (ACB) informierte den Kommissar über seine Absicht, ein System/eine Datenbank mit dem Namen „ARTEMIS“ zu entwickeln und einzuführen. Dieses System sollte von einer privaten Organisation verwaltet werden, die dem ACB

Bericht erstattet, um so den Mitgliedsbanken des ACB zu ermöglichen, Informationen über zahlungsunfähige Schuldner auszutauschen und den Kreditstatus potenzieller Kunden zu bewerten.

Der ACB legte unserem Büro einen Entwurf der internen Vorschriften der Organisation zur Einrichtung und Verwaltung des Systems/der Datenbank vor, der entsprechend den Anmerkungen/Empfehlungen des Kommissars finalisiert und angenommen wurde. Die Vorschriften wurden in Kraft gesetzt, und das System ist seit November 2009 in Betrieb.

Ein privates Unternehmen, das einen mit ***Google Street View*** vergleichbaren Dienst anzubieten beabsichtigt, hat um eine Stellungnahme unseres Büros zu diesem Thema gebeten. Der vorgeschlagene Dienst umfasst die Erfassung von Fotos aller öffentlichen Straßen in Zypern sowie die Erstellung einer virtuellen Karte, die Besuchern im Internet für virtuelle Rundgänge zugänglich gemacht wird. Der Dienst könnte potenziell auch von den kommunalen Behörden genutzt werden, um Stellen zu identifizieren, an denen Straßen ausgebessert werden müssen.

Unter Berücksichtigung der von der Artikel-29-Datenschutzgruppe angenommenen relevanten Dokumente informierte unser Büro das Unternehmen, dass – zusätzlich zu weiteren Sicherheitsvorkehrungen – die Fotos so unscharf zu gestalten seien, dass Fahrzeugkennzeichen und Gesichter von Personen nicht zu erkennen sind. Darüber hinaus muss der Dienst den betroffenen Personen eine einfache Möglichkeit bieten, Beschwerden über veröffentlichte personenbezogene Daten einzureichen. Unser Büro prüft derzeit den vorgeschlagenen Dienst.

Tschechische Republik

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

Die grundlegende Rechtsvorschrift im Bereich des Schutzes personenbezogener Daten ist das Gesetz Nr. 101/2000 Coll. über den Schutz personenbezogener Daten und zur Änderung einiger damit zusammenhängender Gesetze, das am 1. Juni 2000 in Kraft getreten ist. Das Amt für den Schutz personenbezogener Daten („ASPD" oder „Amt") wurde auf der Grundlage der Vorschriften dieses Gesetzes errichtet und ist mit weit reichenden Befugnissen ausgestattet; unter anderem kann es bei Gesetzesverstößen Maßnahmen ergreifen und direkt Geldbußen verhängen und ist außerdem unabhängig. Das Gesetz hat die Richtlinie 95/46/EG im Wesentlichen in tschechisches Recht umgesetzt. Mit Wirkung vom 26. Juli 2004 wurde das Gesetz Nr. 101/2000 Coll. durch das Gesetz Nr. 439/2004 Coll. geändert und so mit der oben erwähnten Richtlinie in Einklang gebracht.

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

Im Jahr 2008 wurde ein durch die Notwendigkeit der Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten in nationales Recht erforderliches Änderungsverfahren des Gesetzes Nr. 127 über elektronische Kommunikation abgeschlossen.

Seit 1. April 2009, als das Gesetz zum Schutz personenbezogener Daten durch das Gesetz Nr. 52/2009 Coll. um Definitionen neuer Vergehen ergänzt wurde, ist das Amt verpflichtet, sämtliche Verhaltensweisen strafrechtlich zu verfolgen, die einen Verstoß gegen das Verbot der Veröffentlichung personenbezogener Daten gemäß sonstiger relevanter Verordnungen darstellen. Diese Änderung ging einher mit dem „Maulkorbgesetz", einer Änderung der Strafprozessordnung als Reaktion auf die wiederholte Veröffentlichung großer Mengen personenbezogener Daten aus Strafprozessen, hauptsächlich in Boulevardzeitungen, sowie Daten, die in Zusammenhang mit Minderjährigen stehen. Das Amt empfand es als positiv, dass die Änderung insbesondere die mit unbegrenzter und massenhafter Veröffentlichung personenbezogener Daten (einschließlich der Veröffentlichung in den Medien und im Internet) einhergehenden Gefahren betonte. Leider wurde das ursprüngliche Ziel der Änderung der Strafprozessordnung im Rahmen der sie begleitenden öffentlichen Debatte oder vielmehr im Rahmen einer kritischen Kampagne in den meisten Medien, die sich auf eine vermeintliche Unterdrückung der Meinungsfreiheit konzentrierte, oftmals vernachlässigt: der Schutz der Privatsphäre der Opfer (Geschädigten) von Straftaten.

Gesetz Nr. 111/2009 Coll. über Grundregister verpflichtete das Amt, innerhalb des neu geschaffenen Systems zur elektronischen Verwaltung (eGovernment) die Identifikatoren „Quelle" und „Agenda" für natürliche Personen zu definieren und dafür zu sorgen, dass die Agenda-Identifikatoren natürlicher Personen innerhalb der individuellen elektronischen Agenden übertragen werden. Die neuen Identifikatoren sollten unter anderem das Risiko einer unbefugten Verarbeitung von in Staatsregistern gespeicherten personenbezogenen Daten von Bürgern reduzieren. Das Amt nahm die erwähnte Zuständigkeit unter der Bedingung an, dass die Definition und Übertragung der Identifikatoren unter größtmöglichen Sicherheitsvorkehrungen erfolgt, sowie unter der Bedingung, dass der gesamte Prozess der Erstellung der Identifikatoren streng von der tatsächlichen Verarbeitung personenbezogener Daten durch die Behörden getrennt wird. Die aktuelle Aufsichtsfunktion des Amts im Hinblick auf die Verarbeitung personenbezogener Daten im Rahmen von Staatsregistern und den neu vorgeschlagenen Grundregistern wird hierbei in keiner Weise beeinträchtigt.

B. Bedeutende Rechtsprechung

Im Jahr 2009 betrafen die gesetzgeberischen Aktivitäten des Amts spezifische Gesetze mit Auswirkungen auf Privatsphäre und Datenschutz (im Rahmen des Gesetzgebungsverfahrens der Regierung muss das Amt konsultiert werden). Ein besonderer Schwerpunkt lag hierbei auf der Erarbeitung einer neuen Kodifizierung des Zivilrechts, der Arbeit an neuen elektronischen öffentlichen Verwaltungsregistern sowie auf Verordnungen betreffend die Gesundheitsregister. Die Kommentare und Einwände des Amts wurden teilweise berücksichtigt.

C. Wichtige spezifische Themen

Bei der Umsetzung des nationalen Rechts sowie durch die Erweiterung des EU-/EG-Rechts spielen ***Kontroll- und Prüftätigkeiten***, einschließlich Inspektionen vor Ort, auch weiterhin eine wichtige Rolle. Im Einklang mit Artikel 31 des Gesetzes zum Schutz personenbezogener Daten verfolgt das Amt seine Tätigkeiten entweder auf der Grundlage eines Prüfplans oder auf der Grundlage von Beschwerden. Der Kontrollplan wird vom Präsidenten und den Inspektoren des Amts gemeinsam erstellt – das Dokument ist bindend und seine Erfüllung wird regelmäßig im Rahmen einer Sitzung des Inspektionsausschusses bewertet, der als gemeinsames Beratungsgremium für den Präsidenten und die Inspektoren dient. Die meisten Prüfungen sowie die Inspektionen vor Ort wurden auf der Grundlage von Beschwerden und Anträgen (90 %) durchgeführt und betreffen Verstöße gegen das Gesetz zum Schutz personenbezogener Daten. Die übrigen Prüftätigkeiten basierten auf dem Prüfplan (8 %) sowie auf den Anweisungen des Präsidenten des Amts (2 %). Es ist jedoch darauf hinzuweisen, dass die beiden letztgenannten Kategorien hauptsächlich komplexere Prüfverfahren umfassen.

Ein besonderer Schwerpunkt bei der Erarbeitung des Prüfplans des Jahres 2009 lag auf den folgenden Bereichen:
Informationssysteme der öffentlichen Verwaltung – zur Verarbeitung personenbezogener Daten gingen häufig Anfragen und Konsultationsersuchen ein (die Prüfungen betrafen die Erfassung der Bevölkerungszahlen).
Multinationale Informationssysteme – die Prüfungen gingen meistens von den gemeinsamen Aufsichtsbehörden SIS und EURODAC sowie anderen EU-Initiativen aus (d. h. Verkehrsdaten in Transportsystemen).
Verarbeitung personenbezogener Daten durch den Einsatz von Kameraüberwachungssystemen – die tschechische Datenschutzbehörde hat die im offiziellen Positionspapier der Datenschutzbehörde veröffentlichten Grundprinzipien zum Schutz personenbezogener Daten angewendet.
Informationssysteme im Bereich Justiz – die tschechische Datenschutzbehörde hat die Verarbeitung personenbezogener Daten im Zusammenhang mit Aktivitäten wie Verwaltungssanktionen festgestellt.

In Fällen, in denen bei der Kontrolle ein Verstoß gegen das Gesetz zum Schutz personenbezogener Daten festgestellt wurde, wurden Verwaltungsverfahren hinsichtlich der (illegalen?) Verarbeitung personenbezogener Daten gegen die betreffenden Parteien eingeleitet. In diesen Fällen wurden Bußgelder auferlegt. Die Parteien, gegen die Verfahren eingeleitet wurden, können gegen diese Entscheidung Beschwerde beim Präsidenten des Amts einlegen.

Statistische Daten zu den bearbeiteten Beschwerden des Jahres 2009:

Gesamt	879
davon:	
eingereicht zur Kontrolle	129
eingereicht zur Einleitung von Verfahren	43
weitergeleitet an andere zuständige Behörden	24
eingestellt mit entsprechender Mitteilung	683

Die zuvor genannten Kontrollmaßnahmen umfassen nicht den Bereich der ***unerbetenen Werbenachrichten*** („Marketing-Spam"). Im Jahr 2009 umfasste dieser spezielle Bereich 2.261 Anträge/Beschwerden. 1.678 Anträge/Beschwerden wurden geklärt, 131 Prüfungen wurden durchgeführt und 112 Sanktionen wurden verhängt.

Im höchst vorrangigen Bereich der ***Öffentlichkeitsarbeit und Sensibilisierung*** hat das Amt im Jahr 2009 auch weiterhin die Tradition der Organisation von ausgleichenden Pressekonferenzen fortgeführt. Der Schwerpunkt der Kommunikation mit den Medien lag jedoch auf alltäglichen Diensten und der Bereitstellung von Informationen zu aktuellen Themen auf der Website.

Der jährliche Wettbewerb für Kinder und Teenager „Meine Privatsphäre! Nicht gucken, nicht herumschnüffeln!" („This is my private space! Don't look and don't poke about!") wurde im Jahr 2009 wieder durchgeführt, und das Amt verzeichnete eine stärkere Teilnahme und eine Veränderung der Qualität. Die Preise für die Gewinner wurden traditionell im Rahmen des Internationalen Filmfestivals für Kinder und Teenager in Zlin überreicht. Die Beiträge des Kinderwettbewerbs wurden zu Beginn des neuen Schuljahres im Vorraum des Versammlungssaals des Senats sowie zu anderen Anlässen ausgestellt.

Im Rahmen einer dreijährigen Akkreditierung durch das Ministerium für Bildung, Jugend und Sport war 2009 bereits das dritte Jahr des laufenden Lehrerschulungsprogramms des Amts zum Schutz personenbezogener Daten im Bereich Bildung. Etwa 200 Lehrer nahmen an einem Workshop teil, zu dem das Amt das relevante Fachwissen beisteuerte.

Das Amt hielt es auch für wichtig, Treffen mit älteren Bürgern durchzuführen (in Zusammenarbeit mit der Dritten Medizinischen Fakultät der Karls-Universität). Gerade ihnen muss die Bedeutung des Schutzes personenbezogener Daten regelmäßig erläutert werden. Zudem müssen sie dafür sensibilisiert werden, dass sie ein Recht auf den Schutz ihrer Privatsphäre haben.

Ein Workshop zum Thema DNS-Profile, der auf der Grundlage der Ergebnisse der Prüfungen des Amts initiiert wurde, wurde im Herbst 2009 im Senat unter der Schirmherrschaft des Vizepräsidenten des Senats organisiert. Der Workshop warf eine Reihe von Fragen auf, die eine präzise rechtliche Grundlage erfordern.

Dänemark

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

Das Gesetz über die Verarbeitung personenbezogener Daten (Gesetz Nr. 429 vom 31. Mai 2000) wurde am 31. Mai 2000 verabschiedet und trat am 1. Juli 2000 in Kraft. Die englische Fassung des Gesetzes kann unter folgender Adresse abgerufen werden: http://www.datatilsynet.dk/english/the-act-onprocessing-of-personal-data/

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

Die Richtlinie 2002/58/EG wurde ins nationale dänische Recht übertragen durch:
- die dänische Verfassung;
- das Gesetz über Marketingpraktiken, Paragraph 6 (vgl. Gesetz Nr. 1389 vom 21. Dezember 2005);
- das Gesetz Nr. 429 vom 31. Mai 2000 über die Verarbeitung personenbezogener Daten;
- das Gesetz über die Wettbewerbsbedingungen und den Verbraucherschutz im Telekommunikationsmarkt (vgl. Durchführungsverordnung Nr. 780 vom 28. Juni 2007);
- die Durchführungsverordnung Nr. 714 vom 26. Juni 2008 über die Bereitstellung elektronischer Kommunikationsnetze und Dienstleistungen;
- Kap. 71 der Zivilprozessordnung, vgl. Durchführungsverordnung Nr. 1069 vom 6. November 2008;
- Paragraph 263 des Strafgesetzbuches, vgl. Durchführungsverordnung Nr. 1068 vom 6. November 2008.

Gemäß Artikel 57 des Gesetzes über den Schutz personenbezogener Daten ist die Stellungnahme der dänischen Datenschutzbehörde (DSB) einzuholen, wenn Verordnungen, Rundschreiben oder ähnliche allgemeine Richtlinien für den Schutz der Privatsphäre in Zusammenhang mit der Datenverarbeitung herausgegeben werden. Dies gilt auch für Gesetzesentwürfe. Die DSB hat im Jahr 2008 zu verschiedenen Gesetzen und Regelungen, die Auswirkungen auf den Schutz der Privatsphäre und den Datenschutz haben, Stellung bezogen.

Im Jahr 2009 gab es zwei Änderungen am dänischen Gesetz zum Schutz personenbezogener Daten:
- Ein neuer Abschnitt 72 a des dänischen Gesetzes zum Schutz personenbezogener Daten wurde zur Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit mit Strafsachen verarbeitet werden, verabschiedet.
- Ein neuer Unterabschnitt 3 zu Abschnitt 1 des dänischen Gesetzes zum Schutz personenbezogener Daten wurde verabschiedet. Bis zum Jahr 2009 wurden personenbezogene Daten gemäß dem dänischen Gesetz über die öffentliche Verwaltung manuell zwischen öffentlichen Behörden ausgetauscht. Als Folge dieser Abänderung werden personenbezogene Daten gemäß dem dänischen Gesetz zur Verarbeitung personenbezogener Daten nun manuell zwischen den öffentlichen Behörden offen gelegt.

B. Bedeutende Rechtsprechung

Die DSB hat sich mit zahlreichen Fällen betreffend soziale Online-Netzwerke befasst.

Die sozialen Online-Netzwerke erfassen große Mengen personenbezogener Daten und verfügen über eine gewaltige Menge an Informationen.

Soziale Netzwerke sind ein sich entwickelnder Bereich, und mit den technologischen Entwicklungen und den neuen Privatsphäre-Einstellungen auf den Websites der sozialen Netzwerke ergeben sich fortwährend neue Herausforderungen.

In Dänemark wurde in der Presse umfassend über Facebook berichtet, und viele Bürger haben sich diesbezüglich an die DSB gewandt. Facebook verzeichnet nach eigenen Angaben über 2 Millionen dänische Nutzer.

Die DSB startete im April 2009 einen Dialog mit Facebook und stellte eine Reihe von Fragen – teilweise basierend auf Anfragen dänischer Nutzer – zur Verarbeitung personenbezogener Daten durch Facebook.

Darüber hinaus hat die DSB Facebook um weitere Informationen hinsichtlich eines Austauschs von Daten mit Dritten gebeten, der durch die verschiedenen Anwendungen auf Facebook stattfindet.

Der Dialog zwischen der DSB und Facebook läuft noch. Weitere Informationen und Tipps zu sozialen Netzwerken sowie die Briefe von Facebook sind auf der Website der DSB zu finden: www.datatilsynet.dk.

C. Wichtige spezifische Themen

Videoüberwachung im Allgemeinen
In den Jahren 2008 und 2009 hat sich die DSB mit zahlreichen Fällen betreffend Videoüberwachung befasst. In einigen Fällen ging es um Beschwerden über die unrechtmäßige Veröffentlichung von Daten. In anderen Fällen ergriff die DSB beispielsweise auf der Grundlage von Presseberichten selbst die Initiative. In den meisten dieser Fälle ging es um die unrechtmäßige Veröffentlichung von personenbezogenen Daten aus Videoüberwachungen über das Internet oder die Weitergabe dieser Daten an die Presse.

In den Jahren 2008 und 2009 erstattete die DSB in einigen Fällen Anzeige bei der Polizei aufgrund von Verstößen gegen Kapitel 6a (Videoüberwachung) des dänischen Gesetzes zum Schutz personenbezogener Daten.

Einige dieser Fälle gingen vor Gericht. Manche der Klagen wurden nach der Würdigung des jeweiligen Sachverhalts durch das Gericht abgewiesen. In anderen Fällen, in denen die DSB Anzeige erstattet hatte, haben die betreffenden Unternehmen einen ein festgelegtes Bußgeld akzeptiert.

Im Jahr 2009 hatte die Datenschutzbehörde seltener Anlass zu Anzeigen bei der Polizei aufgrund von Verstößen gegen Kapitel 6a des dänischen Gesetzes zum Schutz personenbezogener Daten als in den vorangegangenen Jahren. Die DSB vermutet, dass dies auf Presseberichte über einige der früheren, bei der Polizei angezeigten Fälle zurückzuführen ist.

Videoüberwachung in Taxis
Im Jahr 2009 konsultierte die dänische Agentur für Straßenverkehrssicherheit und Transport die DSB bezüglich des Entwurfs eines Beschlusses des dänischen Parlaments zur Videoüberwachung in Taxis. Die DSB nahm zu einer Reihe von Fragen des Entwurfs kritisch Stellung.

Im weiteren Verlauf des Jahres 2009 nahm die Datenschutzbehörde Stellung zu einem Gesetzesentwurf, der eine Videoüberwachung in Taxis zur Pflicht macht. Grundlage dieses Gesetzesentwurfs war der Entwurf eines Beschlusses des dänischen Parlaments zur Videoüberwachung in Taxis, zu dem die DSB zuvor bereits kritisch Stellung genommen hatte. Die DSB veröffentlichte außerdem eine Reihe von Kommentaren zum Gesetzesentwurf.

Der Gesetzesentwurf schreibt die Installation von Videoüberwachungsgeräten in Taxis vor, um Raubüberfälle und gewalttätige Angriffe auf Taxifahrer aufzuklären. Des Weiteren soll der Gesetzesentwurf dabei helfen, Raubüberfälle und gewalttätige Angriffe auf Passagiere zu vermeiden und aufzuklären.

Der Gesetzesentwurf soll voraussichtlich im Frühjahr 2010 vorgelegt werden.

Estland

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

Richtlinie 95/46/EG wird durch das estnische Gesetz zum Schutz personenbezogener Daten umgesetzt (die englische Version ist auf der Website der Datenschutzbehörde erhältlich: http://www.aki.ee/eng/?part=html&id=105). Die neue Version des Gesetzes trat am 1. Januar 2008 in Kraft. Seitdem wurden die Gesetze zum Schutz personenbezogener Daten nicht verändert.

Die Richtlinien 2002/58/EG und 2006/24/EG werden durch das Gesetz über die elektronische Kommunikation umgesetzt (eine aktuelle Übersetzung ist noch nicht erhältlich). Die Verpflichtung, Verbindungsdaten zu erfassen und zu speichern, trat im Jahr 2007 in Kraft. Die Vorratsspeicherung von Festnetz-Telefoniedaten und Mobilfunk-Telefoniedaten trat am 1. Januar 2008 in Kraft. Die Vorratsspeicherung der Daten zu Internetverbindungen, E-Mails und Internet-Telefonie trat am 15. März 2009 in Kraft. Daher sind seit 2009 alle estnischen Telekommunikationsanbieter verpflichtet, Verbindungsdaten zu erfassen, was auch im Rahmen der von der Datenschutzinspektion durchgeführten Kontrollverfahren offenkundig wurde.

B. Bedeutende Rechtsprechung

Blogs und soziale Netzwerke

Bei der estnischen Datenschutzinspektion gehen zahlreiche Beschwerden betreffend die Verwendung personenbezogener Daten ohne Einverständniserklärung in Blogs oder sozialen Netzwerken ein. Bei den meisten Fällen ging es um die Löschung von Bildern oder sonstigen personenbezogenen Daten. Gleichzeitig musste die Datenschutzbehörde berücksichtigen, dass der Grund für die Beschwerde in einigen Fällen eine Meinungsverschiedenheit zwischen zwei Personen war, was bedeutete, dass die Daten bzw. Fotos als eine Art Racheakt veröffentlicht wurden. Leider sind solche Fälle mit der zunehmenden Sensibilisierung der Öffentlichkeit für dieses Thema immer öfter an der Tagesordnung. Die Datenschutzbehörde ist der Ansicht, dass diese Fälle vor Zivilgerichten verhandelt und nicht von der Datenschutzbehörde bearbeitet werden sollten.

In manchen Fällen interpretiert die Datenschutzbehörde Blogs als „öffentlichen Journalismus", wodurch diese den gleichen Prinzipien unterliegen wie professioneller Journalismus. Die Veröffentlichung personenbezogener Daten zu journalistischen Zwecken ist im Gesetz zum Schutz personenbezogener Daten folgendermaßen geregelt:

Personenbezogene Daten dürfen ohne das Einverständnis des Datensubjekts zu journalistischen Zwecken in den Medien veröffentlicht werden, wenn das öffentliche Interesse überwiegt und wenn die Prinzipien des ethischen Journalismus' eingehalten werden. Eine Veröffentlichung von Informationen darf die Rechte des Datensubjekts nicht unverhältnismäßig beeinträchtigen.

Das Datensubjekt hat jederzeit das Recht, die Person, die seine personenbezogenen Daten veröffentlicht, aufzufordern, die Veröffentlichung einzustellen, sofern eine solche Veröffentlichung nicht auf einer gesetzlichen Grundlage oder gemäß dem vorgenannten Prinzip erfolgt und eine weitere Veröffentlichung die Rechte des Datensubjekts nicht unverhältnismäßig beeinträchtigt. Die Aufforderung zur Einstellung der Veröffentlichung personenbezogener Daten darf nicht an eine Person gerichtet werden, die personenbezogene Daten zu Datenträgern veröffentlicht, über die die Person, die die personenbezogenen Daten veröffentlicht, zum Zeitpunkt der Aufforderung keine Kontrolle hat.

Webcams und Videoüberwachung

Im Laufe des Jahres 2009 führte die Datenschutzbehörde Prüfungen von Webcams durch. Es gab Fälle, in denen öffentliche Webcams so konfiguriert waren, dass die Kamera die Privatsphäre anderer Personen verletzte (z. B. wenn eine Kamera beweglich war und das Haus einer anderen Person heranzoomen konnte).

Darüber hinaus führt die Datenschutzinspektion als langfristig angelegtes Projekt umfangreiche Prüfungen von Videoüberwachungsanlagen vor Ort durch (z. B. in Kaufhäusern und an Arbeitsstätten). Bisher haben die Ergebnisse dieser Prüfungen gezeigt, dass in manchen Fällen eine einfache Mitteilung nicht ausreichend ist. Das Gesetz zum Schutz personenbezogener Daten besagt:

Überwachungsgeräte, die personenbezogene Daten übermitteln und aufzeichnen, dürfen zum Schutz von Personen oder Eigentum ausschließlich dann verwendet werden, wenn die berechtigten Interessen des Datensubjekts nicht unverhältnismäßig beeinträchtigt werden und wenn die erfassten Daten ausschließlich zum ursprünglichen Zweck ihrer Erfassung verwendet werden. In diesem Fall tritt an die Stelle der Einverständniserklärung des Datensubjekts die hinreichend deutliche Mitteilung über die Verwendung von Überwachungsgeräten sowie die Angabe des Namens und der Kontaktdaten des für die Verarbeitung der Daten Verantwortlichen. Diese Anforderung gilt nicht für die Verwendung von Überwachungsgeräten durch Regierungsbehörden, die sich aus gesetzlich festgelegten Verfahren ergibt oder hieraus abgeleitet ist.

C. Wichtige spezifische Themen

Bereits im dritten Jahr in Folge hat die Datenschutzinspektion vorrangige Themenbereiche festgelegt und Leitlinien zu diesen Fragen veröffentlicht. Die Leitlinien für das Jahr 2009 sind in estnischer Sprache erhältlich:

- Verarbeitung personenbezogener Daten während des Wahlkampfs – http://www.aki.ee/download/1101/erakondadekampaaniad_200309%20(2).rtf
- Verarbeitung personenbezogener Daten durch die Finanzbehörden – http://www.aki.ee/download/1037/AKI%20krediidiasutuste%20juhend.pdf
- Verarbeitung personenbezogener Daten im Bereich genealogische Forschung – http://www.aki.ee/download/1404/Isikuandmete%20töötlemine%20suguvõsa%20uurimiseks%20171109.rtf
- Verarbeitung personenbezogener Daten im Bereich wissenschaftliche Forschung – http://www.aki.ee/download/1469/Isikuandmete%20töötlemine%20teadusuuringus.rtf
- Verwendung nationaler ID-Codes – http://www.aki.ee/download/1102/Isikukoodi%20kasutamise%20juhis.rtf
- Veröffentlichung personenbezogener Daten von Schuldnern von Versorgungsbetrieben – http://www.aki.ee/download/1240/JUHIS%20%20Korterivõlglaste%20avaldamine%20090309.rtf
- Das Recht auf Einsicht in die eigenen Daten – http://www.aki.ee/download/1045/kusi_oma_andmeid_090309.rtf

Darüber hinaus haben wir Leitlinien für Verwalter öffentlicher Informationen erstellt. Die Leitlinien über öffentliche Informationen umfassen die Verwaltung von Dokumentenregistern sowie die Veröffentlichung von Daten auf den Websites öffentlicher Behörden. Die Leitlinien sind in estnischer Sprache erhältlich unter: http://www.aki.ee/est/?part=html&id=125.

Finnland

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

Der Richtlinie des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG) wurde in Finnland durch das Gesetz über personenbezogene Daten (523/1999), das am 1. Juni 1999 in Kraft getreten ist, Gesetzeskraft verliehen. Dieses Gesetz wurde am 1. Dezember 2000 revidiert, als Vorschriften über die Entscheidungsfindung der Kommission und die Festlegung, wie verbindlich diese Entscheidungen in Fragen bezüglich der Übermittlung personenbezogener Daten an Drittländer außerhalb der Europäischen Union gemäß der Datenschutzrichtlinie sind, darin einbezogen wurden.

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

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

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

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

Änderungen
Im Berichtsjahr gab es keine eigentlichen Änderungen am Gesetz über personenbezogene Daten (523/1999).

Die Änderung des Gesetzes über Datenschutz im Bereich elektronische Kommunikation (Laki sähköisen viestinnän tietosuojalain muuttamisesta, 125/2009) trat am 1. Juni 2009 in Kraft. Die Änderung gibt Kommunikationsteilnehmern das Recht, Identifikationsdaten zu verarbeiten, um so eine illegale Nutzung von kostenpflichtigen Diensten der Informationsgesellschaft, Kommunikationsnetzwerken oder Kommunikationsdiensten oder auch Unternehmensspionage gemäß der Definition des Strafgesetzbuches (Rikoslaki 39/1889) zu vermeiden und zu erkennen.

Die illegale Nutzung von Kommunikationsnetzwerken oder Kommunikationsdiensten kann beispielsweise die Installation eines Gerätes, einer Software oder eines Dienstes auf dem Kommunikationsnetzwerk des Kommunikationsteilnehmers, die Öffnung eines illegalen Zugangs zu diesem Kommunikationsnetzwerk oder die Bereitstellung des Dienstes an Dritte oder eine vergleichbare Nutzung des Kommunikationsnetzwerks oder Kommunikationsdienstes sein, wenn diese Nutzung gegen die Nutzungsanweisungen verstößt.

Das zuvor erwähnte Recht gilt nicht für die Identifikation von Daten von Festnetz- oder Mobilfunk-Netzwerkdiensten.

Die vom so genannten LexNokia geforderten Änderungen wurden in die Abschnitte 2 und 21 des Gesetzes zum Schutz der Privatsphäre im Berufsleben (Laki yksityisyyden suojasta työelämässä, 759/2004) integriert und traten am 1. Juni 2009 in Kraft.

Im Berichtsjahr wurden die von der Richtlinie (2006/24/EG) geforderten Änderungen in das Gesetz über Datenschutz im Bereich elektronische Kommunikation (516/2004)

integriert. Die rechtliche Verpflichtung zur Speicherung von Telekommunikations-Identifikationsdaten trat am 15. März 2009 in Kraft.

Im Jahr 2006 beauftragte das finnische Parlament die Regierung mit der Erarbeitung von Gesetzen zum allgemeinen Schutz personenbezogener Daten im Bereich der biometrischen Identifizierung. Laut Justizministerium, das für die Erarbeitung des Gesetzes verantwortlich ist, werden die allgemeinen Vorschriften zur Verarbeitung der biometrischen Identifizierung in Zusammenhang mit der Überprüfung des Gesetzes über personenbezogene Daten (95/46/EG Artikel 8, Paragraph 7) erarbeitet. Diese Überprüfung wird zu einem späteren Zeitpunkt gestartet. Das Gesetz über starke elektronische Identifizierung und elektronische Signaturen (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 617/2009) trat jedoch am 1. September 2009 in Kraft. Es legt strenge Qualitätsverpflichtungen für Anbieter von Identifikationsdiensten fest. Gemäß diesem Gesetz kann auch die biometrische Identifizierung als starke Identifizierung eingesetzt werden.

B. Bedeutende Rechtsprechung

Der Gerichtshof der Europäischen Gemeinschaften (Große Kammer) hat am 16. Dezember 2008 ein Urteil zur Veröffentlichung von Daten zu beruflichem Einkommen verkündet. Der Fall betraf den Anwendungsbereich der Richtlinie 95/46/EG, die Verarbeitung und die Mobilität personenbezogener steuerlicher Daten, den Schutz von Einzelpersonen sowie das Recht auf freie Meinungsäußerung. Das Gericht überließ die Entscheidung hinsichtlich der in Artikel 9 der Richtlinie 95/46/EG genannten Verarbeitung zu journalistischen Zwecken den jeweiligen nationalen Gerichten. Andererseits muss die Datenschutzrichtlinie gemäß dem Urteil auf die Verarbeitung von aus öffentlichen Datenquellen gewonnenen personenbezogenen Daten und die Verwendung zuvor veröffentlichter Listen oder Dienstleistungen angewendet werden. Das Oberste Verwaltungsgericht hat am 23. September 2009 sein Urteil hierzu gesprochen (KHO:2009:82). Das Gericht verwies den Fall zurück an die Datenschutzbehörde und verpflichtete die Datenschutzbehörde, Satamedia die weitere Veröffentlichung der Daten zu untersagen. Die Untersagung umfasste sowohl die Veröffentlichungen als auch den SMS-Dienst. Das Gericht gab in seiner Urteilsbegründung an, das Artikel 2.4 des finnischen Gesetzes über personenbezogene Daten nicht mit der Auslegung des Anwendungsbereichs der Richtlinie durch den EuGH in Einklang steht. Das Gericht fällte diese Entscheidung unter Berücksichtigung des Gleichgewichts zwischen der Meinungsfreiheit und dem Schutz des Privatlebens. Das Gericht betonte, dass dieses Gleichgewicht im Hinblick auf die Meinungsfreiheit erfordert, dass die der Öffentlichkeit bereitgestellten Informationen für die Gesellschaft von Bedeutung sein müssen und nicht ausschließlich der Befriedigung der Neugier dienen dürfen. Im Hinblick auf den journalistischen Zweck betonte das Gericht die Art und Weise, wie diese „Zeitungen" tatsächlich hergestellt werden. Da die Datenbank (das Register) als solches gedruckt werde, könne es nicht nur zu journalistischen Zwecken erstellt werden. Das Gericht entschied, dass Veropörssi keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten habe und der Textnachrichtendienst somit ebenfalls illegal sei. Das Gericht ging nicht auf die Fragen steuerlicher Daten als solche oder die Frage des Gleichgewichts zwischen Meinungsfreiheit und Privatsphäre ein. Der Anbieter des SMS-Dienstes informierte die Datenschutzbehörde am 28. September 2009 darüber, dass der Dienst aufgrund der offensichtlichen Unrechtmäßigkeit am 30. September eingestellt würde. In der Praxis werden finnische Zeitungen auch in Zukunft diese Art personenbezogener Daten über Personen veröffentlichen, die von gesellschaftlicher Bedeutung sind.

Künftige Änderungen des finnischen Gesetzes über personenbezogene Daten hinsichtlich der Widersprüchlichkeit von Artikel 2.4 werden vom Justizministerium erarbeitet, das kürzlich einen künftigen Arbeitsplan veröffentlicht hat, der auch eine Aktualisierung des Gesetzes über personenbezogene Daten umfasst.

In ihrer Entscheidung von 26. November 2009 untersagte die Datenschutzbehörde Satakunnan Markkinapörssi Oy die Verarbeitung von Daten zu Einkünften und Kapitalerträgen sowie zu Vermögenswerten natürlicher Personen in dem Umfang und in der Art und Weise, wie dies in Zusammenhang mit den Steuerdaten von 2001 geschehen war. Darüber hinaus untersagte die Datenschutzbehörde Satakunnan Markkinapörssi

die Weitergabe von erfassten und gespeicherten Daten zu Einkünften und Kapitalerträgen sowie zu Vermögenswerten natürlicher Personen über einen SMS-Dienst oder für sonstige Zwecke. Außerdem untersagte die Datenschutzbehörde Satamedia Oy aufgrund eines Verstoßes gegen das Gesetz über personenbezogene Daten (Henkilötietolaki, 523/1999) die Erfassung, Speicherung und Weitergabe weiterer Daten zu Einkünften und Kapitalerträgen sowie Vermögenswerten von Steuerzahlern, die aus dem Register von Satakunnan Markkinapörssi Oy stammen und in einer Veröffentlichung mit dem Titel „Veropörssi" abgedruckt worden waren. Gemäß der dem Verwaltungsgericht in Helsinki vorgelegten Informationen wurde Berufung gegen die (am 12. Januar 2010 mitgeteilten) Entscheidung der Datenschutzbehörde eingelegt. Die Sache wurde an das Verwaltungsgericht in Turku verwiesen, da sich der Firmensitz des Unternehmens geändert hatte.

Die zuständige Datenschutzbehörde gab ihren Beschluss zu dem vom Büro des Datenschutzombudsmannes eingeleiteten Verfahren zur Authentifizierung von Kunden bei Schnellkrediten per Mobiltelefon bekannt. In ihrem Beschluss entschied die Datenschutzbehörde, dass die Praxis, bei der der Kreditgeber die Antragsteller ausschließlich auf der Grundlage der per Textnachricht übermittelten Daten zu Namen, Sozialversicherungsnummer, Anschrift und Telefonnummer identifiziert und dieser Vorgang als Kreditantrag akzeptiert wird, nicht als hinreichend zuverlässige Praxis angesehen werden kann. Daher untersagte die Behörde dem Verfahrensgegner, der ein in der Branche übliches Authentifizierungsverfahren eingesetzt hatte, personenbezogene Daten auf die zuvor genannte Art und Weise zu verarbeiten. Der Verfahrensgegner legte Berufung gegen den Beschluss der Datenschutzbehörde beim zuständigen Berufungsgericht ein. Zum Teil aufgrund dieses Falles wurde in Finnland der Vorschlag zur Inkraftsetzung eines allgemeinen Gesetzes zur Authentifizierung vorgebracht. Die allgemeine Reform der Gesetzgebung betreffend Verbraucherkredite wurde mit der Änderung von Kapitel 7 des Verbraucherschutzgesetzes (Kuluttajansuojalaki, 38/1978) umgesetzt, das am 1. Februar 2010 in Kraft trat.

C. Wichtige spezifische Themen

Schwerpunkt auf Sondergesetzen

Gemäß Paragraph 10 der finnischen Verfassung muss der Schutz personenbezogener Daten gesetzlich gewährleistet sein. Aufgrund dieser Vorschrift existieren derzeit bis zu 650 Sondergesetze zur Regelung des Schutzes personenbezogener Daten. Im Hinblick auf die Übermittlung von Daten zwischen Behörden ist das allgemeine, neben dem Datenschutzgesetz anzuwendende Gesetz das Gesetz über die Transparenz der Aktivitäten der Regierung.

Als Beispiele für das Prinzip der Rechenschaftspflicht erfordern einige Sondergesetze und -vorschriften die Erstellung einer Datenbilanz. So muss die IKT-Agentur gemäß Unterabsatz 1 von Absatz 2 des Regierungsbeschlusses über IKT-Agenturen (HALTIK) (Valtioneuvoston asetus Hallinnon tietotekniikkakeskuksesta, 810/2007) dem Innenministerium sowie dem Büro des Datenschutzombudsmannes jährlich bis Ende April Bericht über wichtige Fragen zur Verarbeitung von Daten innerhalb ihres Mandates erstatten. Der Beschluss trat am 1. März 2008 in Kraft.

Gemäß Absatz 60 des Gesetzes über das Bevölkerungsinformationssystem und die Identifizierungsdienste des Einwohnermeldeamtes (Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista, 661/2009) muss das Einwohnermeldeamt mindestens einmal jährlich einen detaillierten Bericht über die Verarbeitung von im Register gespeicherten Daten und Vorgänge erstellen. Das Gesetz trat am 1. März 2010 in Kraft.

Durchgeführte Studien

Im Berichtsjahr führte das Büro des Datenschutzombudsmannes zahlreiche Studien durch.

Im Sommer 2009 führte das Büro des Datenschutzombudsmannes eine branchenweite Umfrage zu Markt- und Meinungsumfragen durch. Fragebögen, die an hundert Unternehmen verschickt wurden, skizzierten die in Umfragen angewandten Verfahren und den Umfang der Verarbeitung personenbezogener Daten. Ein besonderer Schwerpunkt lag auf der Einhaltung der Bürgerrechte. Die

Branchenumfrage zeigte, dass einige der Herausgeber von Markt- und Meinungsumfragen die Anforderungen der Datenschutzgesetzgebung kennen und diese bei ihren Tätigkeiten berücksichtigen. Einige der Antworten zeigten jedoch auch eine mangelnde Kenntnis hinsichtlich der Datenschutzanforderungen auf. Zu Forschungszwecken werden die Namen und Kontaktinformationen von Bürgern erfasst, insbesondere aus elektronischen Verzeichnissen und über Auskunftsdienste sowie auch aus offiziellen Registern.

Das Büro des Datenschutzombudsmannes führte eine groß angelegte Prüfung durch, deren Schwerpunkt auf dem nationalen Register der Agenturen für Arbeit und Wirtschaft lag. Die Agenturen für Arbeit und Wirtschaft verteilen sich auf 200 Dienststellen in ganz Finnland. Den Kunden werden Dienste in den Bereichen Arbeitssuche, Karriereplanung, Umschulung und Unternehmertum angeboten. Die Agenturen für Arbeit und Wirtschaft bieten auch Beratung bei der Beantragung von Arbeitslosenunterstützungen und helfen auf verschiedene Art beim Zugang zu einer Beschäftigung. Durch die Prüfung sollte festgestellt werden, ob die Verarbeitung personenbezogener Daten im nationalen Register im Einklang mit der Gesetzgebung erfolgt. Die Prüfung führte zu einer Reihe von Schlussfolgerungen, die dem Ministerium für Beschäftigung und Wirtschaft vorgelegt wurden. Auf der Grundlage der Prüfung nahm das Ministerium einige Änderungen vor und ergriff weitere Maßnahmen.

Da die Datenschutzbehörde in Finnland befugt ist, eine Genehmigung zur Verarbeitung personenbezogener Daten zu erteilen und spezielle Bedingungen für die Verarbeitung festzulegen, führte das Büro des Datenschutzombudsmannes eine Umfrage dazu durch, inwiefern die Genehmigungsempfänger die Entscheidungen und Bedingungen einhalten. Die Umfrage zeigte, dass die Bedingungen der Genehmigungen ordnungsgemäß eingehalten werden.

Frankreich

A. Umsetzung der Richtlinien 95/46/EG und 2002/58/EG sowie sonstige legislative Entwicklungen

Frankreich hat die europäische Richtlinie vom 24. Oktober 1995 durch das Gesetz vom 6. August 2004 in Abänderung des Gesetzes vom 6. Januar 1978 umgesetzt. Eine erste Durchführungsverordnung war am 20. Oktober 2005 verabschiedet worden. Diese war am 25. März 2007 Gegenstand einer Änderung, um die erforderlichen verfahrenstechnischen Änderungen einzubringen.

B. Rechtsprechung

Urteil des Kassationshofs (Cour de cassation) vom 8. Dezember 2009 im Zusammenhang mit Whistleblowing
In einem Urteil vom 8. Dezember 2009 erinnert die in Arbeits- und Sozialsachen zuständige Zivilkammer des Kassationshofes daran, dass der Geltungsbereich des durch die Einzelbewilligung Nr. 4 der CNIL genehmigten Whistleblowings beschränkt sein muss.

Diese Entscheidung stellt nicht das Prinzip des Whistleblowing an sich in Frage und bringt mehr Klarheit in die Auslegungsschwierigkeiten der Gerichte.

Um den Anforderungen des amerikanischen so genannten „Sarbanes Oxley"-Gesetzes gerecht zu werden, hat das Unternehmen Dassault Systèmes einen „Kodex zum Verhalten im Geschäftsleben" mit den Regeln eingeführt, zu deren Einhaltung sich die Arbeitnehmer bei der Ausübung ihrer Berufstätigkeit verpflichten. Dieser Kodex führt insbesondere ein System des Whistleblowing ein, mit dessen Hilfe die Arbeitnehmer jedwede Verfehlung über eine dafür vorgesehene E-Mail-Adresse anzeigen können. Vor der Einrichtung dieses Systems hat das Unternehmen Dassault Systèmes eine Konformitätserklärung zur Einzelbewilligung Nr. 4 abgegeben.

Aus Anlass des aufgrund des Whistleblowing-Systems entstandenen Rechtsstreits erinnert der Kassationshof daran, dass der Geltungsbereich der Einzelbewilligung beschränkt werden muss. Der Kassationshof gibt deutlich zu verstehen, dass sich die Einrichtung eines Whistleblowing-Systems als Gegenstand einer Konformitätserklärung zur Einzelbewilligung ausschließlich auf die Bereiche Buchhaltung, Finanzwesen und Korruptionsbekämpfung zu beschränken hat.

Die CNIL hatte in Artikel 3 ihrer Einzelbewilligung Nr. 4 die Berücksichtigung von Situationen vorgesehen, die zwar nicht unter den Geltungsbereich fallen, aber das „lebenswichtige Interesse der Organisation oder die körperliche oder moralische Unversehrtheit ihrer Arbeitnehmer" betrifft. Der Kassationshof erläutert, dass dieser Artikel nicht derart ausgelegt werden darf, dass er eine Ausweitung des Zwecks der in der Einzelbewilligung vorgesehenen Whistleblowing-Systeme bedeutet. Die Whistleblowing-Systeme, die nicht streng den Bedingungen der Einzelbewilligung Nr. 4 folgen, müssen eine Sondergenehmigung erhalten, die von der CNIL von Fall zu Fall vergeben wird.

Der Kassationshof unterstreicht die Notwendigkeit, dass die Unternehmen die betroffenen Personen entsprechend den Vorschriften des Datenschutzgesetzes informieren müssen. In diesem Zusammenhang erinnert er daran, dass „die im Gesetz vom 6. Januar 1978 vorgesehenen und in die Einzelbewilligung aufgenommenen Informationsmaßnahmen (…) im Dokument zur Einführung des Whistleblowing-Systems genannt werden müssen." Diese Informationen waren in der Rechtssache Dassault unvollständig, da es um Zugangs-, Berichtigungs- und Widerspruchsrechte ging.

Die CNIL wird ihre Einzelbewilligung angesichts des Urteils des Kassationshofs und der im Rahmen jüngst durchgeführter Prüfungen in den Unternehmen gesammelten Eindrücke vermutlich in Kürze abändern.

C. Funktionsweise und Tätigkeiten der CNIL

Die Annahme von Beschlüssen
Während des Geschäftsjahres 2009 ist die CNIL 48 Mal im Rahmen von 35 Vollversammlungen und 13 verwaltungsrechtlichen Sitzungen zusammen gekommen.

Diese Versammlungen haben zur Annahme von **719** Beschlüssen geführt, ein Anstieg um 22,7 % im Vergleich zum Vorjahr.

Im Jahr 2009 hat die CNIL Folgendes angenommen:
- **544** Bewilligungen (**+39 %** im Vergleich zu 2007);
- **5** abgelehnte Bewilligungen;
- **35** Stellungnahmen zur Verarbeitung von sensiblen oder riskanten Daten.

Seit dem Gesetz vom 6. August 2004 verfügt die CNIL über Disziplinargewalt, d. h. sie hat das Recht, Geldbußen bis zu einer Höhe von maximal 150.000 Euro (300.000 Euro bei Wiederholungsfällen) innerhalb des Limits von 5 % des Umsatzes zu verhängen.

Insgesamt hat die CNIL im Jahr 2009:
- 5 Geldbußen
- 4 Verwarnungen;
- 90 Inverzugsetzungen ausgesprochen.

Die Anrufungen
Die CNIL wurde im Jahr 2009 6.482 Mal angerufen.
Im Jahr 2009 sind bei der CNIL 4.265 Beschwerden aufgrund der Nichteinhaltung des Datenschutzgesetzes sowie 2.217 Anträge auf indirekten Zugriff eingegangen, ein leichter Rückgang (-11,8 %) im Vergleich zu 2008 (2.516 Anträge).

Die Zahl der Anmeldungen von Datensammlungen ist 2009 leicht zurückgegangen; sie beläuft sich auf 68.185 Anmeldungen gegenüber 71.990 im Jahr 2008, das entspricht einem Rückgang von **5 %**.

Die Prüfungen
Das Jahr 2009 bestätigt die zunehmende Bedeutung von Prüfungen im Rahmen des Auftrags der CNIL, sowohl im Hinblick auf die Menge der durchgeführten Prüfungen als auch auf die zunehmende Vielfalt der geprüften Sektoren. Die CNIL hat neue Verfahren eingeführt, um auf die Entwicklung der Rechtsprechung im Zusammenhang mit ihrer Tätigkeit reagieren zu können.

Zunächst die Zahlen. Im Jahr 2009 sind **270 Prüfungen** durchgeführt worden, was einer **Zunahme von fast 24 %** entspricht. Die stetige Zunahme der durchgeführten Prüfungen ist kein neues Phänomen und zeugt vom Willen der CNIL, sich voll und ganz im Sinne des Gesetzes aus dem Jahr 2004 für eine Prüfung der Datensammlungen vor Ort zugunsten der Personen, deren Daten verarbeitet werden, einzusetzen.

Der größte Teil der Prüfungen (31 % der durchgeführten Prüfungen) werden im Kontext der **Umsetzung des jährlichen Prüfprogramms** durchgeführt, das vom Plenum angenommen wird. Das Prüfprogramm für das Jahr 2009 wurde weitgehend eingehalten werden.

Die Höhepunkte des Tätigkeitsjahres 2009
a. Die CNIL emanzipiert sich
Im Jahr 2009 kam es zu mehreren parlamentarischen Initiativen zur Überarbeitung des Datenschutzgesetzes.

Insbesondere erwähnenswert ist die Tatsache, dass der Rechtsausschuss des Senats Ende 2008 die Senatoren Anne-Marie Escoffier und Yves Détraigne mit einer **Untersuchung des Schutzes der Privatsphäre in Zeiten der Digitalspeicher** beauftragt hat.

Die Empfehlungen ihres Berichts flossen teilweise in einen Gesetzesvorschlag ein, der im März 2010 vom Senat geprüft worden ist. Dieser Gesetzesvorschlag sieht zunächst eine Stärkung des Rechts auf Löschung von Daten vor, indem die Informationspflicht bezüglich der Dauer der Vorratsdatenspeicherung verschärft und die Wahrnehmung des Rechts auf Datenentfernung, vor allem im Internet, erleichtert wird. Die Staatssekretärin für Zukunftsfragen und die Entwicklung der digitalen Wirtschaft, Nathalie Kosciusko-Morizet, hat zu dieser Frage zudem im November 2009 eine umfassende öffentliche Konsultation zum Recht auf die Entfernung digitaler Daten eingeleitet, um insbesondere bewährte Verfahren zu bestimmen und eine Charta zu deren Umsetzung zu erarbeiten.

Außerdem zielt der Gesetzesvorschlag darauf ab, zur Einrichtung eines IT- und Grundrechtebeauftragten zu verpflichten, wenn eine Behörde oder eine private Stelle personenbezogene Daten verarbeitet und mehr als fünfzig Personen Zugriff auf diese Daten haben oder mit der Verarbeitung beauftragt sind.

Darüber hinaus geht es um die Stärkung der Prüf- und Sanktionsbefugnis der CNIL sowie die Erweiterung ihrer Handlungsmöglichkeiten vor den Gerichten. Und der dem Parlament vorgelegte Text verfolgt schließlich unter anderem das Ziel, die Verpflichtungen der Datenverarbeitungsbeauftragten im Fall von Verletzungen der Integrität oder der Vertraulichkeit

personenbezogener Daten genauer zu bestimmen oder auch das Datenverarbeitungssystem der Polizei zu ändern.

i. Die Strategie zur Öffnung nach außen

Der Défenseur des Droits

Die durch Verfassungsänderung vom 23. Juni 2008 geschaffene Institution des Défenseur des Droits, eine Art Ombudsmann, wird Mitglied der CNIL werden. Er wird persönlich oder durch einen Vertreter am Gremium der Kommission teilnehmen, jedoch mit beratender Stimme (Artikel 9 des Entwurfs zum Organisationsgesetz). Die CNIL wird somit aus 18 Mitgliedern bestehen.

Der Präsident der CNIL begrüßt die baldige Teilnahme des Verteidigers an der CNIL, wodurch der Schutz der Rechte und Freiheiten unserer Mitbürger noch gestärkt wird.

Mehr Anhörungen und internationale Ausrichtung

Um sich nach außen hin zu öffnen und um Regierungsprojekte, Technologien/Dienstleistungsangebote, die derzeit entwickelt werden, und/oder aktuelle und künftige Problemstellungen verständlich zu machen, hat die CNIL im Jahr 2009 während ihren Plenarsitzungen mehr als 20 Anhörungen durchgeführt.

Angehört wurden insbesondere Regierungsmitglieder, so z. B.: Nathalie Kosciuzko-Morizet, Staatssekretärin für Zukunftsfragen und die Entwicklung der digitalen Wirtschaft und Eric Besson, Minister für Immigration, Integration, nationale Identität und solidarische Entwicklung. Unternehmen wie St. Gobain, PSA, Air France, IBM sind ebenfalls von der CNIL angehört worden.

Außerdem empfing die CNIL im Rahmen von Plenarsitzungen, die ausschließlich zu internationalen Themen abgehalten wurden, den Präsidenten der amerikanischen Federal Trade Commission. Des Weiteren empfängt die CNIL im Rahmen der internationalen Zusammenarbeit regelmäßig ausländische Delegationen aus der ganzen Welt, die zu Studienzwecken nach Frankreich und/oder Europa kommen, um ihre Erfahrungen im Bereich des Schutzes personenbezogener Daten sowie der Organisation und der Befugnisse ihrer Kontrollbehörden auszutauschen. Im Jahr 2009 konnte die CNIL Delegationen aus China, Russland (zwei Mal), Indonesien, Armenien und schließlich aus der Türkei empfangen, um sich mit diesen über Probleme auszutauschen, insbesondere im Zusammenhang mit der digitalen Signatur, den Datenverarbeitungssystemen der Polizei, dem Zugang zu Informationen, der Cyber-Kriminalität und dem E-Government.

Der Präsident der CNIL hat sich im Jahr 2009 voll und ganz für die Einleitung und Festigung von Aktionen zur Stärkung dieser positiven Dynamik eingesetzt, und zwar vor allem im Rahmen der AFAPDP (Frankophone Vereinigung der Datenschutzbehörden). Die AFAPDP konnte dank der Unterstützung der Internationalen Organisation der Frankophonie vor allem die 3. frankophone Jahreskonferenz der Datenschutzkommissare durchführen, die im November 2009 in Madrid stattfand. Diese Konferenz bot den 30 Delegationen aus französischsprachigen Ländern und internationalen Gremien eine einzigartige Plattform und diente insbesondere zur Sensibilisierung und zum Erfahrungsaustausch mit französischsprachigen Staaten, in denen es derzeit keine Datenschutzgesetze gibt, sowie zum Aufbau einer Partnerschaft mit dem Iberoamerikanischen Datenschutz-Netzwerk.

ii. Zunehmende Transparenz

Die CNIL war bis zum jetzigen Zeitpunkt nicht befugt, Stellungnahmen zu Gesetzesentwürfen abzugeben.

Die französische Kommission für den Zugang zu Verwaltungsdokumenten, CADA (Commission d'Accès aux Documents Administratifs) war der Auffassung, dass die CNIL keine öffentliche Stellungnahme abgeben kann, „solange diese nur Vorbereitungscharakter hat, d. h. solange der Gesetzes-, Verordnungs- oder Dekretentwurf, auf den sie sich beziehen würde, nicht verabschiedet worden ist." Auch wenn der Entwurf seinen Vorbereitungscharakter verloren hat, kann die Stellungnahme der Kommission, die sich auf „im Ministerrat geprüfte Dokumente" bezieht, d. h. auf Gesetzes-, Verordnungs- und Dekretentwürfe", nicht vorgelegt werden. Somit befanden sich die Parlamentarier in einer paradoxen Situation: Sie mussten von der CNIL geprüfte Fragen diskutieren, durften aber nicht deren Stellungnahme einsehen, von deren Existenz sie allerdings wissen.

*Das Beispiel HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, Hohe Behörde zur Verbreitung von Werken und den Schutz der Rechte im Internet*)*

Eine Wirtschaftstageszeitung hat am 3. November 2008 die Stellungnahme der CNIL vom 29. April 2008 über die Gesetzesvorlage HADOPI veröffentlicht, außerhalb jedes rechtlichen Rahmens und obwohl unsere Kommission nicht befugt war, diese Stellungnahme vorzulegen. Mit dieser Veröffentlichung wurde somit der Standpunkt der CNIL zur Gesetzesvorlage in ihrer ursprünglichen Form bekannt. Nach dieser Stellungnahme wurde der Text vom Parlament umfassend geändert. Die HADOPI konnte beispielsweise gemäß der Gesetzesvorlage Internetdienstleister dazu bringen, die Inhalte zu filtern, was eine Gefährdung der Meinungsfreiheit bedeutete, worauf die CNIL hingewiesen hatte. Der Text, der der Versammlung schließlich vorgelegt wurde, sah dann vor, dass den Internetdienstleistern einzig per Gericht eine Filterung der Inhalte auferlegt werden konnte.

Diese Situation, in der die CNIL über ihre eigenen Stellungnahmen schweigen musste und sie nicht dem Parlament vorlegen durfte, gehört nun der Vergangenheit an. Das Gesetz vom 12. Mail 2009 zur Vereinfachung und Klarstellung des Rechts und zur Erleichterung der Verfahren, das auf eine Initiative von Herrn Jean-Luc Warsmann, Vorsitzender des Rechtsausschusses der Nationalversammlung, zurückgeht, sieht künftig Folgendes vor: **„Auf Antrag des Vorsitzenden eines der ständigen Ausschüsse des Parlaments wird die Stellungnahme der Kommission zu jedwedem Gesetzesentwurf veröffentlicht."**

Die jüngste gesetzgeberische Entwicklung ist somit ein wesentlicher Vorstoß in Bezug auf die Transparenz der Tätigkeiten der Kommission und wird zur einer Verbesserung der Qualität der parlamentarischen Arbeit beitragen.

iii. Die CNIL hat im Februar 2009 neue Mitglieder aufgenommen

Jean-Paul Amoudry, Senator (UC) aus der Haute-Savoie
Jean-François Carrez, Kammervorsitzender am französischen Rechnungshof
Claire Daval, Rechtsanwältin, ordentliche Professorin für öffentliches Recht an der Universität Lille 2
Marie-Hélène Mitjavile, Regierungsrätin
Dominique Richard, Berater

b. Das technologische Fachwissen

Die CNIL unterstützt Unternehmen und Behörden vom Zeitpunkt der Konzeption ihrer Systeme an. Durch ihre Beraterrolle und im Rahmen von Überprüfungen der Dokumente, die die Formalien enthalten, kann die Kommission die Unternehmen oder Behörden zur Änderung ihrer Systeme, zur Verwendung alternativer technologischer Lösungen oder zur Vorsehung von Garantien zum Schutz personenbezogener Daten anhalten.

Die CNIL nimmt in diesem Zusammenhang im Gesundheitsbereich an einer Lenkungsgruppe teil, die mit der Einführung der neuen Identifikationsnummer im Gesundheitswesen, dem Eckstein der künftigen Elektronischen Patientenkarte, beauftragt ist. Die CNIL gehört auch zum Ausschuss, der zum Interoperabilitätsreferenzsystem arbeitet (RGI, Référentiel Général d'Interopérabilité), das am 12. Juni 2009 veröffentlicht worden ist. Es handelt sich hierbei um Empfehlungen zu Normen und Standards, die die Interoperabilität in Informationssystemen der Verwaltung fördern.

Nach den im letzten Jahr durchgeführten Studien über biometrische Geräte zur Venenerkennung des Daumens, eine Biometrie, die keine Spuren hinterlässt, hat die CNIL im Mai 2009 eine Einzelbewilligung für diese Geräte bei deren Verwendung zur Überwachung des Zugangs zu den Räumlichkeiten an Arbeitsplätzen angenommen. Darüber hinaus ist die Venenerkennung der Handfläche zur Bekämpfung des Betrugs bei Prüfungen eingesetzt worden.

Gezielte Werbung

Das Wirtschaftsmodell zahlreicher führender Internet-Unternehmen beruht auf der Bereitstellung von scheinbar „kostenlosen" Diensten für den Internetnutzer, die jedoch überwiegend oder gar ausschließlich über Werbung finanziert werden.

Das gezielte Marketing ist somit zum „Treibstoff" der digitalen Wirtschaft geworden, die nach immer mehr personenbezogenen Daten verlangt.

Diese Entwicklungen lassen vor allem die Entstehung eines systematischen Profils der Internetnutzer ohne deren Wissen befürchten; außerdem besteht die Gefahr des „Verschacherns" der Einzelprofile zwischen den Anbietern von Online-Inhalten und den Werbetreibenden.

In ihrem im März 2009 veröffentlichten Bericht liefert die CNIL einen Überblick über die verschiedenen Online-Werbestrategien, die möglichen Verletzungen der Privatsphäre und die Möglichkeiten, dies zu verhindern.

Nanotechnologien

In ihrer warnenden und beratenden Funktion hat die CNIL im Wesentlichen die Aufgabe, dafür zu sorgen, dass die Entwicklung neuer Technologien weder die menschliche Identität noch die Menschenrechte, die Privatsphäre oder die Bürgerrechte beeinträchtigt.

Die wichtigsten Herausforderungen im Zusammenhang mit dem Wachstum der Nanotechnologien bestehen in der Kontrolle des Unsichtbaren und in der Wahrnehmung der Risiken, die sie insbesondere im Hinblick auf die Rückverfolgbarkeit von Personen und die Achtung der Privatsphäre mit sich bringen.

Wie können wir sicherstellen, dass wir über die Existenz, den Gegenstand und die Wirkungen einer unsichtbaren (oder fast unsichtbaren) und verstreuten Technologie informiert sind? Wie kann man sicherstellen, dass die Entwicklung dieser Technologien nicht auf Kosten einer „Hyper-Rückverfolgbarkeit" von Personen erfolgt, die deren Bewegungsfreiheit in Frage stellt? Denn diese Freiheit besteht nicht, wenn Anonymität nicht garantiert ist!

Angesichts dieser Herausforderungen muss darüber nachgedacht werden, wie dieser Bereich reguliert werden soll und ob der bestehende rechtliche Rahmen weiterentwickelt werden soll. Müssen insbesondere bestimmte Anwendungen der Nanotechnologien verboten werden?

Zudem müssen die Regeln identifiziert werden, die im Bereich des Schutzes der Persönlichkeitsrechte gefördert werden sollen. Die Grundsätze der Unbedenklichkeit, Verhältnismäßigkeit, Sicherheit, Information und Kontrolle der Personen über ihre persönlichen Daten sind Garantien, die bereits in das Planungsstadium der Systeme und Anwendungen im Bereich der Nanotechnologie einbezogen werden sollen.

Aus diesem Grund hat sich die CNIL aktiv an der großen nationalen öffentlichen Debatte über Nanotechnologien beteiligt, um die Menschen und die öffentliche Hand für die Risiken dieser Technologien zu sensibilisieren. Eine ihrer Hauptaktivitäten war das Verfassen eines „Handbuchs der Akteure" in dem ihre Fragestellungen zusammengefasst werden (http://www.cnil.fr/nanos).

Normung und Standards

Die CNIL hat sich im Jahr 2008 der GCSSI angeschlossen, der mit Normung der Sicherheit beauftragten Gruppe der französischen Stelle für Normung, AFNOR (Agence Française de Normalisation), um sich als zentraler Akteur im Bereich der Normung der Schlüsselbereiche des Datenschutzes zu positionieren. Diese Gruppe erarbeitet französische Stellungnahmen zu den ISO-Normungsprojekten.

Die ISO arbeitet derzeit an Normungsprojekten im Bereich des Schutzes der Privatsphäre und des Datenschutzes. Sie arbeitet seit 2005 an dem Normungsprojekt ISO 29100 „Privacy Framework" (Rahmenstandard zum Schutz der Privatsphäre), in dem einheitliche Anforderungen und eine einheitliche Terminologie im Rahmen des Schutzes der Privatsphäre auf internationaler Ebene bestimmt werden. Hierbei handelt es sich um ein Grundlagendokument, das langfristig als Referenz für andere Normen dienen könnte.

Da Struktur und Grundsätze dieses Normungsprojekts weniger streng als die europäischen Standards scheinen und häufig in Widerspruch zu diesen stehen, hat der Präsident der CNIL die Artikel-29-Datenschutzgruppe und die Europäische Kommission im Juni 2009 dringlich in dieser Frage mobilisiert. Die Artikel-29-Datenschutzgruppe hat dieser Frage ihre volle Aufmerksamkeit geschenkt, und die CNIL hat die Erarbeitung von Kommentaren mit ihren europäischen

Pendants sowie mit Kontaktpersonen der AFNOR aus der Industrie sowie aus Institutionen koordiniert.

Im November 2009 hat erstmals ein Vertreter der CNIL an einem der alle zwei Jahre stattfindenden internationalen Treffen der mit der Erarbeitung dieser Norm beauftragten ISO-Gruppe teilgenommen. Die ISO hat zudem ihr Interesse an Beiträgen der Datenschutzbehörden hervorgehoben und den Wunsch geäußert, eine „Verbindung" mit der Artikel-29-Datenschutzgruppe zu formalisieren.

Darüber hinaus hat die ISO beschlossen, einen Lenkungsausschuss zum Thema Privatsphäre (Privacy Steering Committee, PCS) einzurichten, um ihre Tätigkeiten in diesem Bereich besser koordinieren zu können. Die CNIL ist sich der strategischen und transversalen Bedeutung dieses Ausschusses bewusst und hat erwirkt, dass einer ihrer Vertreter auf der Liste der Experten des PSC steht, dessen erste Sitzung im Februar 2010 stattfinden wird.

Kontrolle der elektronischen Abstimmungssysteme
Im Laufe des Jahres 2009 hat die CNIL elektronisch durchgeführte Wahlen von privaten Einrichtungen und Ministerien geprüft. (Arbeitsrichterwahlen und Wahlen der Verband der Krankenpfleger und -schwestern). Diese Prüfungen boten auch eine Gelegenheit zur Prüfung der von den verschiedenen Dienstleistern auf dem Markt angebotenen Wahlsysteme.

Die CNIL prüft die Bedingungen der physischen und logischen Versiegelung der elektronischen Urne, um jede Veränderung der Wahlvorrichtung aufzuspüren und Manipulationen der Wahlgeräte zu verhindern. Sie prüft, ob es Möglichkeiten gibt, sich während des Wahlgangs mit der Wahlvorrichtung zu verbinden oder nicht. Außerdem prüft sie, ob die verschiedenen Programme der verwendeten Wahlvorrichtungen in ihrer Gesamtheit begutachtet worden sind, indem sie insbesondere Dokumente und Dateien kopiert, wie es ihr gesetzlich zusteht. Die Kommission prüft zu guter Letzt die Mittel, die eingesetzt werden, um die Identität der Wähler festzustellen und geheime Wahlen zu gewährleisten.

Dank dieser Prüfungen konnten Unzulänglichkeiten der Schutzmechanismen der Wahlvorrichtungen im Hinblick auf Sicherheit und Vertraulichkeit der Angaben aufgedeckt werden.

Die Kommission hat daraufhin Sanktionen gegen mehrere Einrichtungen verhängt, die elektronische Wahlen durchgeführt haben, weil sie der Auffassung war, dass gewisse wichtige Punkte ihrer Empfehlung nicht befolgt wurden.

c. STIC – kontrolliert und gerügt
Bei der STIC handelt es sich um eine nationale Datenbank, in der Informationen aus kriminalpolizeilichen Ermittlungen gespeichert werden. Die Datenbank hat den Zweck, *„die Feststellung von Verstößen gegen die Strafvorschriften, die Sammlung von Beweisen für diese Verstöße und die Suche nach den Tätern sowie die Nutzung der Daten zur statistischen Forschung zu erleichtern."*

Diese Datenbank ist jedoch auch zu einem Instrument der behördlichen Ermittlung geworden, denn seit dem Gesetz vom 21. Januar 1995 über die Ausrichtung und Programmplanung der Sicherheitspolitik (loi d'orientation et de programmation relative à la sécurité) kann sie auch bei Einstellung, Akkreditierung oder Sicherheitsfreigabe von Personal in den verschiedensten Berufen verwendet werden. Dies gilt beispielsweise für Überwachungs- und Wachpersonal, Personen, die auf Flughäfen arbeiten möchten, kommunale Polizeibeamte, Präfekte, Botschafter, Richter usw. Die Verwendung der STIC im Rahmen von behördlichen Ermittlungen betrifft heute insgesamt vermutlich mehr als eine Million Arbeitsplätze.

Die CNIL hat sich zu den aufeinander folgenden Gesetzen zur Beschreibung dieser Datenbank geäußert und konnte hierbei ihre Beobachtungen mitteilen[19]. Im Rahmen ihrer täglichen Arbeit führt sie auf Anfrage der Betroffenen, die das Recht auf indirekten Zugang betreffen, Prüfungen durch. Außerdem hat sie 2009 die gesamte Datenbank kontrolliert, was eine vollständige Bewertung der Funktionsweise der STIC ermöglichte.

[19] Beratungen Nr. 98-97 vom 24. November 1998, Nr. 00-064 vom 19. Dezember 2000, Nr. 2005-187 vom 8. September 2005.

Zahlreiche Prüfungen vor Ort wurden durchgeführt (in Kommissariaten, regionalen Kriminalpolizeistellen, Gerichten, Präfekturen usw.), um dort zu prüfen, wie Einträge in die Datenbank vorgenommen werden, unter welchen Bedingungen diese aktualisiert wird, wie effektiv diese Aktualisierung ist und wie sich die Zugangsbedingungen sowie die vorhandenen Sicherheitsmaßnahmen darstellen.

Die Ergebnisse sind ziemlich beunruhigend und weisen vor allem darauf hin, dass die Datenbank nicht regelmäßig aktualisiert wird. Offensichtlich wurden im Jahr 2007 nur 21,5 % der Einstellungsbeschlüsse aufgrund unzulänglicher Anklagepunkte oder unzulänglich erwiesener Tatbestände, 31,17 % der Freisprüche, 6,88 % der Tilgungen und 0,47 % der Einstellungen von Verfahren zur Aktualisierung der STIC übertragen.

Die CNIL hat **11 Vorschläge** zur besseren Kontrolle und sichereren Verwendung der STIC unterbreitet, um die Richtigkeit und Aktualisierung der dort gespeicherten und umfassend verwendeten Informationen zu fördern.

d. Datenbanken im Bereich Immigration

Über die politischen Kontroversen hinaus, die das Jahr 2009 in diesem Bereich geprägt haben, haben sich die zur Verwaltung der Daten von Ausländern verwendeten Datenbanken erheblich weiterentwickelt.

Die Datenbank OSCAR

Eine neue Datenbank namens OSCAR, die im Gesetz vom 20. November 2007 über die Kontrolle von Immigration, Integration und Asyl vorgesehen ist, wurde im Jahr 2009 eingerichtet. Hierbei handelt es sich um ein System zur Abgleichung biometrischer Daten, in dem die Fingerabdrücke von Empfängern einer Rückkehrhilfe gespeichert werden, d. h. von Ausländern, die in Frankreich leben und gegen eine finanzielle Hilfe in ihr Herkunftsland zurückkehren möchten. Unsere Kommission hat (insbesondere) gefordert, dass die biometrischen Daten dieser Ausländer aus der Datenbank gelöscht werden, wenn die Rückkehrhilfe abgelehnt worden ist, und dass sie ausschließlich zur Feststellung verwendet werden, ob diese Personen bereits eine solche Hilfe erhalten haben.

RMV2 (Réseau Mondial Visas)

Was Visa-Antragsteller anbelangt, wurde mit einer Neukonzeption für das so genannte RMV2-System, in dem alle Dokumente im Zusammenhang mit Visa-Anträgen gespeichert werden, begonnen. Mit dieser Neukonzeption soll das ***VIS*** (Visa Information System, das die Informationen über Visa-Antragsteller des Schengenraums aus allen europäischen Ländern vereint) umgesetzt werden; gleichzeitig erweitert es den Zugang zu diesen Informationen auf Präfekturen, Zollstellen oder auch bestimmte Polizeibeamte. Es ist gleichfalls vorgesehen, externe Dienstleister hinzuzuziehen, um die Visa-Anträge zu sammeln und im Rahmen der Verarbeitung diese Informationen zu speichern; in diesem Zusammenhang hat unsere Kommission Vorbehalte geäußert, weil diese Dienstleister oder die Behörden der Länder, in denen die Visa ausgestellt werden, diese Informationen unrechtmäßig verwenden könnten.

GIDESE und FNAD (Datenbank über illegale Einwanderer)

2009 sind zwei weitere Datenbanken versuchsweise eingeführt worden: Mit GIDESE soll die Ein- und Ausreise von Ausländern mit Visa in die Ile de la Réunion kontrolliert werden, damit die Behörden in der Lage sind, Personen, die sich dort aufhalten, ausfindig zu machen.

FNAD (Datenbank über illegale Einwanderer) ist ein biometrisches System, in dem Fingerabdrücke und Fotos von Ausländern gespeichert werden, die beim Überqueren der Grenze kontrolliert worden sind und nicht die erforderlichen Einreisebedingungen erfüllten. Das System wurde im Jahr 2007 für 2 Jahre geschaffen und galt lediglich für den Flughafen Roissy; der Versuch wurde vom Ministerium für Immigration um weitere zwei Jahre verlängert. Unsere Kommission hat eine strenge Bewertung dieses Versuchs erwirkt, um den Nutzen dieser Datenbank, die nur die Identifizierung von Personen ermöglicht, die mehrfach gegen die Vorschriften für die Einreise auf französisches Gebiet verstoßen, eindeutig festzustellen, bevor das System auf das gesamte Hoheitsgebiet ausgeweitet wird.

Die Datenverarbeitung in Bezug auf Asylbewerber

Unsere Kommission verfolgt die Entwicklung dieser Datenbanken mit besonderer Aufmerksamkeit; sie müssen Gegenstand besonderer Garantien sein, da

die Dokumente im Rahmen von Asylanträgen sehr sensible Daten enthalten, wie beispielsweise ethnische Herkunft sowie politische und religiöse Anschauung dieser Personen.

Das Ministerium für Immigration hat dieses Jahr die Datenbank DN@ eingerichtet, mit der die Verwaltung der Aufnahmekapazität der Aufnahmeeinrichtungen für Asylbewerber (CADA) verbessert werden soll. In dieser Datenbank werden Informationen gespeichert, die eine personenbezogene Verfolgung derer, die dort aufgenommen worden sind, ermöglicht. Dank der Stellungnahme unserer Kommission werden in der Datenbank DN@ Daten zum sozialen Schutz oder zur Gesundheit der in einer CADA aufgenommenen Personen nicht gespeichert; diese Daten sind für die Verwaltung der Aufnahmekapazitäten dieser Einrichtungen nicht erforderlich. Sie hat ebenfalls gefordert, dass die Empfänger dieser Informationen (insbesondere das OFII, die Asylstellen des Ministeriums für Immigration und die Präfekturen) Gegenstand eines individuellen Benennungs- und Ermächtigungsverfahrens sind, damit nur die direkt für die Aufnahme von Asylbewerbern verantwortlichen Bediensteten Zugang zu den in der DN@ gespeicherten Informationen erhalten.

Nicht nur die Verwaltungsbehörden verwenden Datenbanken mit Informationen über Asylbewerber. Unsere Kommission hat dieses Jahr CIMADE, eine Organisation zur Verteidigung der Rechte von Ausländern, die vor allem im Zusammenhang mit Abschiebegewahrsam tätig ist ermächtigt, zwei Datenverarbeitungssysteme einzuführen, mit denen die Akten der Ausländer, denen die Organisation im Rahmen ihres Bereitschaftsdienstes und in den Schubhaftzentren hilft, verwaltet werden sollen. Die Organisation hat sich im Hinblick auf die Sicherheitsmaßnahmen bezüglich der Funktionsweise dieser Datenbanken (Bedingungen für den Zugang zu Daten, Rückverfolgbarkeit der Vorgänge usw.), im Hinblick auf die Dauer der Speicherung von Informationen, die ein Jahr nicht überschreiten darf, sowie im Hinblick auf die Bedingungen für die Information der Personen und die Ausübung des Rechts auf Widerspruch, Zugriff und Korrektur oder Löschung der sie betreffenden Angaben sehr aufmerksam gezeigt.

Deutschland

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

Am 1. September 2009 traten eine Reihe wichtiger Änderungen des Bundesdatenschutzgesetzes in Kraft. Als Reaktion auf die seit Anfang 2008 anhaltende Welle von Datenschutzskandalen in der Privatwirtschaft wurden insbesondere die Regeln über die Auftragsdatenverarbeitung und die Nutzung von Adressdaten zu Werbezwecken verschärft. Zudem wurden die Sanktionsmöglichkeiten der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich erweitert. Diese erhalten erstmals wirksame Handlungsmöglichkeiten und können strittige Auslegungsfragen gerichtlich klären lassen. Neu ist auch eine Informationspflicht bei Datenschutzpannen: Unternehmen wurden verpflichtet, bei gravierenden Datenschutzverstößen die Betroffenen und die jeweilige Datenschutzaufsichtsbehörde zu informieren. Schließlich hat der Gesetzgeber hat eine besondere Bestimmung zur Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten geschaffen, die auch Papierakten und handschriftliche Aufzeichnungen umfasst. Diese Regelung stellt jedoch keine Vollregelung jeglichen Umgangs mit Beschäftigtendaten dar, die nach den Plänen der Bundesregierung im Jahr 2010 erarbeitet werden soll.

B. Bedeutende Rechtsprechung

Verlängerung der Einstweiligen Anordnungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Mit Beschlüssen vom März und Oktober 2008 (Az. 1 BvR 256/08) schränkte das Bundesverfassungsgericht die Verwendung der Daten vorläufig ein, die aufgrund des „Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ gespeichert werden. So hat es die Straftaten, zu deren Verfolgung die Vorratsdaten genutzt werden dürfen, auf einen Katalog schwerer Delikte beschränkt und die Nutzung der Daten zur Gefahrenabwehr und zu nachrichtendienstlichen Zwecken auf Fälle begrenzt, in denen es eine dringende Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer Gefahr für die Allgemeinheit erforderlich ist. Da die Beschlüsse jeweils auf sechs Monate oder alternativ bis zur Entscheidung des Gerichtes in der Hauptsache beschränkt waren, wurden sie 2009 vom Bundesverfassungsgericht ohne weitere inhaltliche Änderungen entsprechend weiter verlängert. Eine Entscheidung im Hauptsacheverfahren wird 2010 erwartet.

Entscheidung des VG Berlin, die Provider von der Pflicht zur Vorratsdatenspeicherung zu entbinden, vom OVG Berlin-Brandenburg aufgehoben

Mit einer einstweiligen Anordnung untersagte das Berliner Verwaltungsgericht im Oktober 2008 der Regulierungsbehörde (Bundesnetzagentur), Provider mit einem Bußgeld zu belegen, die sich weigerten, der Verpflichtung zur Vorratsdatenspeicherung nachzukommen. Das Gericht begründet seine Entscheidungen damit, dass es keine hinreichende Entschädigungsregelung für die zur Datenspeicherung notwendigen technischen und personellen Investitionen der TK-Anbieter gäbe. Gegen diese Beschlüsse legte die Bundesnetzagentur Rechtsmittel beim zuständigen Oberverwaltungsgericht Berlin-Brandenburg ein. Dieses entschied am 2. Dezember 2009 entgegen der Vorinstanz dahingehend, dass die Zweifel an der Kostenregelung jedenfalls nicht in dem Maße bestünden, dass hierdurch das Interesse an der Einhaltung der auf zwingendem Gemeinschaftsrecht beruhenden Verpflichtung zur Umsetzung der Vorratsdatenspeicherung zurücktreten müsste.

C. Wichtige spezifische Themen

Visa-Warndatei

Die im Jahr 2009 neu gewählte Bundesregierung beabsichtigt, das in der vergangenen Legislaturperiode gescheiterte Gesetzgebungsvorhaben einer Visa-Warndatei in reduzierter Form wieder aufzunehmen. Dabei soll ein zentraler datenschutzrechtlicher Kritikpunkt an dem Gesetzentwurf aus der vergangenen Legislaturperiode Berücksichtigung finden. Die Bundesregierung beabsichtigt, Daten über Einlader, und Verpflichtungsgeber sollen nur dann aufgenommen

werden, wenn sie mit rechtswidrigem Verhalten im Zusammenhang mit dem Visumverfahren oder bei sonstigem Auslandsbezug erkennbar geworden sind.

Datenschutzrechtliche Bedenken bleiben jedoch auch gegen die beabsichtigte Neuregelung bestehen. Insbesondere erscheinen der tatsächliche Bedarf und der langfristige Bestand einer „nationalen Insellösung" vor dem Hintergrund des europäischen Visa-Informationssystems (VIS) fraglich. Zudem besteht noch Klärungsbedarf hinsichtlich der Ausgestaltung der Visa-Warndatei und des Zugriffs auf die gespeicherten Daten.

Anpassung des Gesetzes über das Ausländerzentralregister (AZR-Gesetz)

In Folge des Urteils des EuGH in der Rechtssache ***Huber*** (Urteil vom 16. Dezember 2008, Rs. C-524/06) muss das Gesetz über das Ausländerzentralregister angepasst werden. Die neue gesetzliche Regelung muss sicherstellen, dass in dem Register nur solche Daten von Unionsbürgern gespeichert werden, die für die Anwendung aufenthaltsrechtlicher Vorschriften unabweisbar erforderlich sind.

Des Weiteren ist eine strikte Zweckbindung für die im Ausländerzentralregister gespeicherten Daten zu gewährleisten. Aus datenschutzrechtlicher Sicht kritisch ist daher ein Zugriff von Sicherheitsbehörden auf die Daten von Unionsbürgern im Rahmen einer sog. „gemischten Aufgabenwahrnehmung", soweit nicht sichergestellt wird, dass die abgefragten Daten allein für aufenthaltsrechtliche Zwecke verwandt werden.

Verabschiedung des Gendiagnostikgesetzes

Am 24. April 2009 hat der Deutsche Bundestag ein Gendiagnostikgesetz verabschiedet, das genetische Untersuchungen zu medizinischen Zwecken, zur Klärung der Abstammung sowie im Versicherungsbereich und im Arbeitsleben regelt. Darüber hinaus regelt das Gesetz den Umgang mit genetischen Daten. Zu den wichtigsten Grundprinzipien des Entwurfs zählt das Recht des Einzelnen auf informationelle Selbstbestimmung. Dazu gehören sowohl das Recht, die eigenen genetischen Befunde zu kennen, als auch das Recht, diese nicht zu kennen (Recht auf Nichtwissen).

Eine genetische Untersuchung zu medizinischen Zwecken darf nur von einer Ärztin oder einem Arzt durchgeführt werden. Hierbei ist die Beratung der Patienten besonders wichtig. Bei Untersuchungen, die eine Vorhersage von Erkrankungsrisiken erlauben (prädiktive Gendiagnostik), ist die genetische Beratung vor und nach der Untersuchung verpflichtend.

Eine genetische Untersuchung zur Feststellung der Abstammung ist nur dann zulässig, wenn die Personen, von denen eine genetische Probe untersucht werden soll, in die Untersuchung eingewilligt haben.

Im Arbeitsrecht sind genetische Untersuchungen auf Verlangen des Arbeitgebers grundsätzlich verboten. Auch darf der Arbeitgeber die Ergebnisse einer bereits vorgenommenen genetischen Untersuchung nicht erfragen, entgegennehmen oder verwenden. Allerdings können beim Arbeitsschutz in Ausnahmefällen genetische Untersuchungen im Rahmen arbeitsmedizinischer Vorsorgeuntersuchungen unter eng gefassten Voraussetzungen zugelassen werden.

Versicherungsunternehmen dürfen weder vor noch nach Abschluss des Versicherungsvertrages die Vornahme genetischer Untersuchungen oder die Mitteilung von Ergebnissen aus bereits vorgenommenen genetischen Untersuchungen verlangen oder solche Ergebnisse oder Daten entgegennehmen oder verwenden. Hiervon gibt es eng begrenzte Ausnahmen: Die Ergebnisse bereits vorgenommener genetischer Untersuchungen müssen bei Abschluss einer Lebensversicherung, einer Berufsunfähigkeitsversicherung, einer Erwerbsunfähigkeitsversicherung und einer Pflegeversicherung dann vorgelegt werden, wenn eine Leistung von mehr als 300.000 Euro oder mehr als 30.000 Euro Jahresrente vereinbart wird.

Leider fehlen Regelungen zum Umgang mit genetischen Untersuchungen im Zusammenhang mit Forschungen.

Griechenland

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

Im Jahr 2009 kam es zu einer Reihe gesetzgeberischer Entwicklungen betreffend den nationalen rechtlichen Rahmen zum Schutz personenbezogener Daten. Vor kurzem gab der Minister für Justiz, Transparenz und Menschenrechte der neuen Regierung bekannt, dass die vergangenen Sommer vorgenommenen Änderungen am nationalen Datenschutzgesetz (siehe Punkt 1 unten) sowie am Strafgesetzbuch (siehe Punkt 3 unten) gemäß entsprechenden Stellungnahmen der griechischen Datenschutzbehörde (GDSB) revidiert werden (siehe Stellungnahmen 1/2009 und 2/2009 unten).

1. Änderung des griechischen Datenschutzgesetzes 2472/97 betreffend Videoüberwachungssysteme in öffentlichen Bereichen

Am griechischen Datenschutzgesetz 2472/1997 wurde eine neue Änderung vorgenommen, insbesondere an Artikel 3, d. h. hinsichtlich des Anwendungsbereichs des Gesetzes. Dementsprechend gilt das Gesetz nicht für die Verarbeitung personenbezogener Daten, die von den zuständigen öffentlichen Behörden durch den Einsatz spezieller technischer Geräte zur Aufzeichnung von Bild und Ton in öffentlichen Bereichen mit dem Ziel der Gewährleistung der Sicherheit des Staates, der nationalen Verteidigung, der öffentlichen Sicherheit, dem Schutz von Personen und Eigentum sowie der Verwaltung des Verkehrs erfolgt. Das mithilfe solcher Geräte gesammelte Material wird (sofern es nicht unter Punkt b des vorliegenden Artikels[20] fällt) für einen Zeitraum von 7 Tagen gespeichert und nach Ablauf dieses Zeitraums auf Anordnung der öffentlichen Strafverfolgungsbehörde gelöscht. Jeglicher Verstoß gegen die oben genannten Bestimmungen wird mit Haftstrafen von mindestens einem Jahr geahndet, sofern nicht ein anderes Gesetz eine strengere Strafe vorsieht.

Gemäß dem Bericht zur oben genannten Bestimmung wird die Einführung der vorgenannten Ausnahme angesichts der starken Zunahme der Verbrechensrate sowie der von den Straftätern angewandten Methodik als erforderlich angesehen.

2. Neues Gesetz zur Verpflichtung der Identifizierung der Teilnehmer, Nutzer sowie der technischen Ausrüstung im Bereich Mobiltelefonie

Das neue im August 2009 veröffentlichte Gesetz 3783/2009 beendet die Anonymität von Teilnehmern (und Nutzern) von Prepaid-Mobiltelefonen im Hinblick auf die Gewährleistung der nationalen Sicherheit und die Untersuchung schwerer Verbrechen. Aus den gleichen Gründen führt es, ungeachtet der Vertragsart, die Pflicht zur Registrierung a) der technischen Ausrüstung der Mobiltelefone von Teilnehmern und Nutzern sowie b)

20 Die Bestimmungen dieses Gesetzes gelten nicht für die Verarbeitung personenbezogener Daten, die durchgeführt wird von:
a) einer natürlichen Person im Rahmen einer rein persönlichen Tätigkeit oder Haushaltstätigkeit.
b) öffentlichen Strafverfolgungsbehörden der Justiz und Behörden, die unter deren Aufsicht im Rahmen einer der Justiz zuzuordnenden Tätigkeit oder zu ihren eigenen operativen Zwecken mit dem Ziel agieren, Verbrechen aufzudecken, die als Straftaten oder vorsätzliche Delikte bestraft werden, sowie insbesondere mit dem Ziel der Aufdeckung von Verbrechen gegen das Leben oder die sexuelle Freiheit, Verbrechen betreffend die wirtschaftliche Ausbeutung des Sexuallebens, Verbrechen gegen die persönliche Freiheit, Verbrechen gegen Eigentum und das Recht auf Eigentum, von Verstößen betreffend Drogen, Verschwörungen gegen die öffentliche Ordnung sowie von Verbrechen gegen Minderjährige. Im Hinblick auf das oben Genannte gelten die bestehenden Gesetze bzw. strafprozessualen Bestimmungen. Bei der Ausübung des Versammlungsrechtes der Bürger ist der Einsatz von Geräten zur Aufzeichnung von Bild und Ton bzw. anderer spezieller technischer Mittel gemäß Artikel 11 der Verfassung unter den im nächsten Punkt genannten Bedingungen gestattet.
Die Aufzeichnung von Bild und Ton mithilfe technischer Geräte zum Zwecke der Aufdeckung einer der oben genannten Verbrechen ist auf Anordnung der öffentlichen Strafverfolgungsbehörde sowie unter der Voraussetzung gestattet, dass die öffentliche Ordnung und Sicherheit ernsthaft bedroht sind.
Alleiniger Zweck der vorgenannten Aufzeichnung ist die Verwendung der aufgezeichneten Daten als Beweismittel zum Nachweis von Verbrechen vor einer Untersuchungsbehörde, der öffentlichen Strafverfolgungsbehörde oder einem Gericht. Die Verarbeitung anderer Materialien, die zur Erfüllung des vorgenannten Zweckes der Verifizierung begangener Verbrechen nicht erforderlich sind, ist nicht gestattet, und sämtliches relevantes Material ist auf Anordnung des zuständigen Staatsanwalts zu vernichten.

der Identifikationsdaten der Nutzer ein (d. h. wenn ein Teilnehmer eine Reihe von Mobilfunknummern erwirbt, die von anderen Personen, z. B. Angestellten, verwendet werden).

Insbesondere müssen Anbieter personenbezogene Daten zur Identifizierung aktueller und neuer Teilnehmer und Nutzer erfassen. Hinsichtlich der aktuellen Teilnehmer musste diese Erfassung bis 30. Juni 2010 abgeschlossen sein. Wenn ein Teilnehmer seinem Anbieter bis zum 30. Juli 2010 keine Identifikationsdaten vorgelegt hatte, musste der Anbieter diesen Teilnehmer vom Dienst ausschließen. Anbieter sind verpflichtet, die Daten bis zu einem Jahr nach Kündigung des Vertrages zu speichern. Dem Teilnehmer dürfen hierdurch keine zusätzlichen Kosten entstehen.

Zu den vom Anbieter zu erfassenden Identifikationsdaten gehören der Name, der Name des Vaters, Geburtsort und -datum, eine Kopie des Ausweisdokuments oder Reisepasses sowie die nationale Steuernummer. Für Anbieter, die eine juristische Person sind, sind die Datenkategorien leicht abweichend. Zur Identifizierung der Mobilgeräte sind weitere Daten zu erfassen, so z. B. die IMSI- (International Mobile Subscriber Identity) und IMEI-Nummern (International Mobile Equipment Identity) sowie Zeit und Ort (Cell-ID, Standortkennung) der ersten Aktivierung. Jede verkaufte SIM-Karte (Subscriber Identity Module) muss einem identifizierten Teilnehmer zugeordnet werden können. Die Teilnehmer sind verpflichtet, den Anbieter schriftlich über Änderungen der Nutzung des Prepaid-Mobiltelefons wie z. B. Verlust, Diebstahl oder Übertragung der SIM-Karte an eine andere Person zu informieren.

Der Zugang zu den vom Anbieter gespeicherten Daten wird ausschließlich den Strafverfolgungsbehörden im Rahmen des Gesetzes über die rechtmäßige Überwachung von Kommunikationen gewährt. Aktuellen Schätzungen zufolge gibt es in Griechenland derzeit 13,5 Millionen anonyme Prepaid-Mobiltelefonverträge. Hiervon sind 9 Millionen aktiv. Nur 5 Millionen sind registriert (d. h. der Teilnehmer ist identifiziert).

3. Änderung des griechischen Strafgesetzbuches hinsichtlich der DNS-Analyse und der Einrichtung einer Datenbank für DNS-Profile

Artikel 200[A] der Strafprozessordnung wurde vor kurzem folgendermaßen geändert (Änderungen in Kursivdruck):

1. *„Wenn ernstzunehmende Indizien dafür vorliegen, dass eine Person eine Straftat oder ein Delikt begangen hat, das mit einer Haftstrafe von mindestens drei Monaten bedroht ist, müssen die Strafverfolgungsbehörden eine Zellprobe für einen DNS-Test entnehmen, um die Identität des Täters festzustellen."*

Die Analyse ist auf die zur Feststellung der Identität des Täters erforderlichen Daten beschränkt und erfolgt in einem staatlichen Labor oder dem Labor einer Hochschule.

Der Beschuldigte hat das Recht, zu seiner Verteidigung eine DNS-Analyse zu fordern.

2. Kommt die vorgenannte Analyse zu einem eindeutigen Ergebnis, so ist das Ergebnis der Person mitzuteilen, der die Zellprobe entnommen wurde. Diese Person hat dann das Recht, eine neue Analyse zu beantragen. In diesem Fall gelten die Bestimmungen der Artikel 204 bis 208. Der Untersuchungsbeamte bzw. der Staatsanwalt hat ebenfalls das Recht, eine neue Analyse zu beantragen. Ist das Ergebnis der Analyse negativ, sind Zellprobe und DNS-Profil unverzüglich zu vernichten. Ist das Ergebnis der Analyse jedoch positiv, so ist die Zellprobe unverzüglich zu vernichten. Das DNS-Profil der *Person, die des Verbrechens beschuldigt wird, muss jedoch in einer speziellen, von der Kriminalpolizei bei der Generaldirektion der griechischen Polizei verwalteten Datenbank gespeichert werden. Diese Daten werden gespeichert, damit sie bei der Untersuchung anderer Verbrechen verwendet werden können. Sie sind in jedem Fall nach dem Tod der betreffenden Person zu löschen. Die Verwaltung dieser Datenbank wird von einem stellvertretenden Staatsanwalt oder vom Oberstaatsanwalt beaufsichtigt, der gemäß geltendem Recht vom Obersten Justizrat für eine Dauer von zwei Jahren ernannt wird.*

3. *Die Vernichtung der Zellprobe und des DNS-Profile (siehe Abschnitt 2) muss in Gegenwart des Justizbeamten*

erfolgen, der die Verwaltung der Datenbank beaufsichtigt. Die Person, der die Zellprobe entnommen wurde, wird gebeten, der Vernichtung der Probe beizuwohnen. Die Person darf einen Anwalt und einen Sachverständigen hinzuziehen."

B. Bedeutende Rechtsprechung

Stellungnahme 1/2009 – zur Änderung des griechischen Datenschutzgesetzes im Hinblick auf den Einsatz von Videoüberwachungssystemen an öffentlichen Orten (siehe oben genannte Änderung des Gesetzes 2472/1997)

Unter Berücksichtigung der Verfassung, der Europäischen Menschenrechtskonvention (EMRK) und der Konvention 108 des Europarates sowie nach Durchführung einer vergleichenden Übersicht der relevanten Gesetze in anderen EU-Mitgliedstaaten veröffentlichte die griechische Datenschutzbehörde folgende Stellungnahme:

- Die betreffende Bestimmung schließt den Betrieb von Geräten zur Aufzeichnung von Bild/Ton an öffentlichen Orten aus dem Anwendungsbereich von Gesetz 2472/97 sowie von der Aufsicht der griechischen Datenschutzbehörde praktisch aus. In dieser Hinsicht erfüllt die Bestimmung nicht die Qualitätsanforderungen der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte betreffend Gesetze, die Beschränkungen der Grundrechte mit sich bringen. Insbesondere lassen sich die möglichen Konsequenzen der eingereichten Änderung nur schwer abschätzen, da sie die Bedingungen und Verfahren für die derartige Verarbeitung von Daten, dass die betroffenen Personen angemessen vor einer willkürlichen Verwendung ihrer Daten geschützt sind, nicht spezifiziert. Des Weiteren sollten die Bestimmungen vom gesetzgeberischen Standpunkt her Teil des Gesetzes zur Regelung der öffentlichen Behörden sein, die für die Verarbeitung der Daten verantwortlich sind.
- Der allgemeine Bezug auf den Schutz der öffentlichen Sicherheit erfüllt nicht die Anforderung der Spezifität. Die Gründe für die Verarbeitung der Daten sollten genauer erläutert werden. Eine entsprechend legitime Formulierung könnte beispielsweise die Abschreckung von Verbrechen gegen das Leben, die persönliche Freiheit und gegen Eigentum sein. Sofern ein solcher Zweck nicht spezifiziert ist, kann unmöglich geprüft werden, ob das Prinzip der Verhältnismäßigkeit (gemäß den Formulierungen der griechischen Verfassung und der EMRK) eingehalten wurde, also ob die spezifische Intervention der öffentlichen Hand in das Privatleben (Videoüberwachung öffentlicher Orte) sowie die damit einhergehenden Beschränkungen des Rechts auf den Schutz personenbezogener Daten erforderlich und zur Erreichung des vorgesehenen Zwecks angemessen ist.
- Die Bestimmung spezifiziert keine Gefahrenkriterien (hohe Verbrechensrate in einem Gebiet/in Gebäuden, die besonders geschützt werden müssen) auf deren Grundlage letztlich entschieden werden muss, ob die Installation und der Einsatz von Videoüberwachungsgeräten an öffentlichen Orten erforderlich ist oder nicht. Folglich liegt die Entscheidung betreffend Ort und Zeit der Installation von Videoüberwachungsgeräten im alleinigen Ermessen der zuständigen Behörden. Ein solcher unbeschränkter Ermessensspielraum geht über den erforderlichen Ermessensspielraum hinaus, der gemäß der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte und des griechischen Staatsrates die Beschränkung von Menschenrechten rechtfertigt. In diesem speziellen Fall besteht die Gefahr einer unrechtmäßigen Verletzung nicht nur von Art. 9A der Verfassung, sondern auch anderer Grundrechte (Art. 2 Abs. 1, 5 Abs. 1, 11).
- Außer der zeitlichen Begrenzung der Speicherung dieser Daten werden keine spezifischen Vorschriften für Erfassung, Speicherung, Nutzung und Weiterübermittlung der Daten genannt. Diese Unterlassung führt zu ernsten Bedenken hinsichtlich der Angemessenheit der Änderungen im Hinblick auf die Erfüllung der Qualitätsanforderungen des Europäischen Gerichtshofes für Menschenrechte betreffend Eingriffe in das Privatleben (Art. 8 der EMRK).
- Es werden keine Bestimmungen zu den organisatorischen und technischen Maßnahmen genannt, die für die Gewährleistung der Sicherheit der erfassten und gespeicherten Daten erforderlich sind.
- Es werden keine Bestimmungen für den effektiven Schutz der Rechte der betroffenen Personen genannt, die durch diese Verarbeitung von Daten verletzt werden könnten. Solche Sicherheitsmaßnahmen sind jedoch der Kern des verfassungsmäßigen Rechts auf

den Schutz personenbezogener Daten. (Art. 9A der Verfassung).

- Es wird nicht klar definiert, wer für die Verarbeitung besagter Daten verantwortlich ist. Der allgemeine Bezug auf die „zuständige öffentliche Behörde" schützt den Einzelnen nicht hinreichend vor einer möglichen Verletzung der Bestimmung. Darüber hinaus schafft die Bestimmung das Risiko eines potenziellen Zuständigkeitskonflikts zwischen den verschiedenen beteiligten Behörden.
- Es wird keine Anforderung genannt, derzufolge die Installation von Videoüberwachungsgeräten auf einem vorherigen Verwaltungsakt basieren muss. Dadurch kann die justizielle Prüfung einer solchen Installation nicht sehr effektiv sein. Personen, deren Rechte verletzt wurden (also deren Daten registriert wurden, obwohl sie an keiner kriminellen Aktivität beteiligt waren), haben lediglich die Möglichkeit, eine Schadenersatzklage gegen den Staat einzureichen.
- Nicht zuletzt verstößt auch der Ausschluss eines breiten und sensiblen Bereiches staatlicher Maßnahmen aus dem Kompetenzbereich der griechischen Datenschutzbehörde gegen den Kern von Art. 9A der Verfassung. Man könnte angesichts der Interpretation des Europäischen Gerichtshofes für Menschenrechte argumentieren, dass dies nicht im Einklang mit Art. 8 Abs. 2 der EMRK steht. Der Wortlaut der Artikel 9A und 101A der Verfassung sowie die Diskussion des Parlaments bezüglich der Annahme dieser Bestimmungen im Jahr 2001 zeigen, dass der Gesetzgeber die Schaffung und die Tätigkeit der Datenschutzbehörde als erforderliche institutionelle Garantie für den Schutz personenbezogener Daten erachtet hat. Die Notwendigkeit der Schaffung einer unabhängigen Behörde mit allem erforderlichen technischen Know-how ergibt sich aus der Tatsache, dass die schnell voranschreitenden Entwicklungen im IT-Bereich eine Gefahr für den Schutz der Privatsphäre darstellen. Somit ist die Aufsichtsfunktion der griechischen Datenschutzbehörde im Bereich der Verarbeitung von Daten im öffentlichen und privaten Sektor Teil des Grundrechts auf informationelle Selbstbestimmung.

Zusammenfassend lässt sich feststellen, dass die Änderung lediglich den Einsatz von Geräten zur Aufzeichnung von Bild/Ton an öffentlichen Orten aus dem Anwendungsbereich von Gesetz 2472/97 sowie aus dem Zuständigkeitsbereich der griechischen Datenschutzbehörde ausschließt und somit nicht im Einklang mit Artikel 9A der Verfassung sowie Artikel 8 der EMRK steht.

Stellungnahme 2/2009 – zur Änderung des griechischen Strafgesetzbuches hinsichtlich der DNS-Analyse und der Einrichtung einer Datenbank für DNS-Profile

Die wesentlichen Anmerkungen lauten wie folgt:

- Obwohl die Änderung einige positive Aspekte hat, so erfüllt sie dennoch nicht alle Qualitätsanforderungen hinsichtlich der Menschenrechte und des Schutzes personenbezogener Daten, insbesondere im Fall von DNS-Profilen, die zur Aufklärung von Verbrechen verwendet werden.
- Um das Prinzip der Verhältnismäßigkeit sowie insbesondere den Aspekt der Notwendigkeit zu wahren, sollte im Gesetz festgelegt sein, dass die genetische Analyse nur dann gestattet ist, wenn es keine anderen Möglichkeiten zur Identifizierung des Täters gibt.
- Die Liste der Verbrechen, bei denen die Verwendung eines DNS-Profils als Teil der Untersuchung gestattet ist, wurde erweitert und umfasst nun alle Straftaten und Delikte, die mit Haftstrafen von mindestens drei Monaten bedroht sind.
- Es ist erforderlich, auf der Grundlage der qualitativen Kriterien zwischen der Untersuchung eines tatsächlichen aktuellen Verbrechens und der zukünftigen Untersuchung anderer Verbrechen zu unterscheiden (letzteres wird durch die Einrichtung einer Datenbank mit DNS-Profilen ermöglicht). Um die Verwendung von DNS-Profilen im Hinblick auf die Wahrung des Prinzips der Verhältnismäßigkeit zu beschränken, muss der Gesetzgeber in Erwägung ziehen, entweder die Liste der Verbrechen auf die aktuelle und zukünftige Untersuchung von Straftaten zu beschränken oder die Verwendung von DNS-Profilen zur aktuellen Untersuchung aller Straftaten und Delikte gestatten. Die Speicherung der DNS-Profile für eine zukünftige Verwendung sollte jedoch nur zur Untersuchung schwerer Verbrechen gestattet werden, also z. B. bei Straftaten und/oder Verbrechen, die besondere rechtliche Interessen verletzen, beispielsweise die sexuelle Freiheit (wenngleich letzteres auch in die Kategorie Delikte fallen könnte). Sollte die zweite

Lösung vorgezogen werden, sollte jedes konkrete Urteil nicht nur auf der Grundlage der Schwere des Verbrechens, sondern auch auf der Grundlage anderer Kriterien betreffend den Täter selbst (Vorleben, Persönlichkeit usw.) gefällt werden und auch auf die Wahrscheinlichkeit einer Wiederholungstat eingehen (negative Prognose).

- Die Änderung unterscheidet nicht zwischen der Speicherung von DNS-Profilen verurteilter und freigesprochener Personen oder zwischen Erwachsenen und Minderjährigen. Ferner kann ein solches Profil unbegrenzt gespeichert werden (die einzige zeitliche Begrenzung ist der Tod des Verdächtigen). Die oben genannten Probleme können folgendermaßen angegangen werden: a) die DNS-Profile der Personen, die – aus welchen Gründen auch immer – rechtskräftig freigesprochen wurden, müssen aus der Datenbank für DNS-Profile gelöscht werden; b) die DNS-Profile der Personen, die rechtskräftig verurteilt wurden, dürfen nur für einen begrenzten Zeitraum nach Verbüßung ihrer Strafe gespeichert werden; c) die DNS-Profile von Minderjährigen unter 13 Jahren, bei denen nur Erziehungs- und Rehabilitationsmaßnahmen durchgeführt werden dürfen, dürfen nicht gespeichert werden; und d) die DNS-Profile von Minderjährigen über 13 Jahren, die rechtskräftig verurteilt wurden, dürfen für einen bestimmten Zeitraum gespeichert werden, der deutlich kürzer sein muss als der bei Erwachsenen.
- Es gibt keinen Schutz für nicht identifizierte DNS-Profile.
- Hinsichtlich der Datenbank für DNS-Profile muss ein Gesetz oder ein Präsidialdekret über die Befugnisse und die Struktur der griechischen Polizei Bestimmungen festlegen, die unter anderem Folgendes betreffen: a) den Zweck der Übermittlung und des Online-Zugangs zu den DNS-Profilen, der mit dem Zweck der ursprünglichen gestatteten Speicherung identisch sein sollte; b) die öffentlichen Behörden, die Zugang zur Datenbank haben oder an die eine Übermittlung gestattet ist; c) die Zugangs- und Widerspruchsrechte der betroffenen Personen, einschließlich der Verpflichtung des für die Datenverarbeitung Verantwortlichen, die betroffenen Personen über den Betrieb der Datenbank und die Speicherung ihrer DNS-Profile in dieser Datenbank zu informieren; d) die Lösch- und Sperrverfahren, die in den Fällen greifen, in denen die Daten nicht gelöscht werden; e) die geeigneten Maßnahmen zur Gewährleistung der Sicherheit der Datenbank, der Vermeidung eines unbefugten Zugriffs, der Änderung und Übermittlung der Daten sowie zur Kontrolle jedes Eingriffs.
- Die Änderung setzt die Rolle des Justizrates als verfahrenstechnische Sicherheitsmaßnahme für die Entnahme und Analyse von Zellproben außer Kraft. Hierdurch wird dieses Verfahren auf eine simple Untersuchungsmaßnahme reduziert. Da die Entnahme (und Analyse) von Zellproben jedoch einen erheblichen Eingriff darstellt, der eine Klarstellung und Spezifizierung vager Rechtskonzepte (d. h. ernstzunehmende Indizien, negative Prognose) erfordert, muss es eine justizielle Garantie entweder in Form einer Entscheidung des Justizrates oder zumindest in Form einer Anordnung eines Staatsanwaltes geben, die speziell aus diesem Grund ausgestellt wurde.
- Die Datenbank der DNS-Profile sollte von einem stellvertretenden Staatsanwalt oder einem Oberstaatsanwalt beaufsichtigt werden. Der Staatsanwalt stellt zweifelsohne eine zusätzliche institutionelle Garantie dar. Wenn dies jedoch als Alternative zur Aufsicht durch die Datenschutzbehörde gesehen würde, verstieße dies gegen den Kern von Artikel 9A der Verfassung, der eindeutig besagt, dass die Datenschutzbehörde eine institutionelle Garantie für das Menschenrecht auf den Schutz personenbezogener Daten darstellt.

Zusammenfassend lässt sich sagen, dass die Änderung analog zu den oben genannten Anmerkungen angepasst werden sollte, damit sie die Anforderungen von Artikel 9A der griechischen Verfassung sowie von Artikel 8 der Europäischen Menschenrechtskonvention vollumfänglich erfüllt.

Beschluss 75/2009 – über die Einrichtung einer über das Internet zugänglichen Datenbank der praktizierenden Mitglieder der Ärztekammer Athens

- Im vorliegenden Fall betraf die Anfrage eines Unternehmens die Erfassung der personenbezogenen Daten praktizierender Mitglieder der Ärztekammer (einer Körperschaft des öffentlichen Rechts) von deren Website zur Einrichtung eines neuen Internetportals, um Einzelpersonen eine vereinfachte Suchmaschine für Ärzte zu bieten, sortiert nach Fachgebieten und geografischen sowie sonstigen Kategorien (z. B. Ärzte, die vertraglich an spezielle Krankenkassen

gebunden sind). Die Mitglieder der Ärztekammer wurden vor der Weitergabe ihrer Daten an Dritte bzw. der Veröffentlichung ihrer Daten auf der Website der Kammer informiert, so dass ihre Daten auch zum Zweck der Information der Öffentlichkeit sowie zur Förderung der wissenschaftlichen Zusammenarbeit veröffentlicht werden konnten. Hierbei wurde den Mitgliedern auch ein Widerspruchsrecht eingeräumt.

Die griechische Datenschutzbehörde entschied, dass sich der sekundäre Verarbeitungszweck vom primären unterscheidet (Ärzteregister zur Information der allgemeinen Öffentlichkeit, zur Förderung der wissenschaftlichen Zusammenarbeit usw.), dass die beiden Zwecke jedoch unter der Voraussetzung, dass die Einrichtung und Verwaltung der neuen Datenbank ebenso der Information der Öffentlichkeit dient, durchaus vereinbar sind.

- Die Weiterverwendung von Informationen des öffentlichen Sektors zu Zwecken der kommerziellen Nutzung ist bereits gestattet und ist durchaus mit dem primären Zweck der ursprünglichen Erstellung des Dokuments vereinbar. Die legitimen Interessen der betroffenen Personen, die ihre personenbezogenen Daten zu einem bestimmten Zweck angegeben haben und keine anderweitige, nicht in direktem Zusammenhang mit dem ersten Zweck stehende Verwendung erwarten, wie dies beim sekundären Zweck der kommerziellen Nutzung der Fall wäre, sollten jedoch hinreichend geschützt werden. Die Bestimmungen von Gesetz 3448/2006 über die Weiterverwendung von Informationen des öffentlichen Sektors, das die EU-Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors in nationales Recht umsetzt, gilt auch für die Weiterverwendung von Informationen, die aus öffentlich zugänglichen Quellen abgeleitet sind, da sich die abgeleiteten Informationen in diesem Fall noch immer „im Besitz" des für die Datenverarbeitung Verantwortlichen befinden.

Die Verarbeitung der Daten durch das Unternehmen ist unter folgenden Bedingungen rechtmäßig: Die betroffenen Personen müssen im Voraus schriftlich informiert und ihnen muss das Recht auf Widerspruch gegen die Verarbeitung eingeräumt werden. Die Verarbeitung muss ohne wirtschaftliche Kosten für die betroffenen Personen erfolgen und ihre Namen müssen in alphabetischer aufgelistet werden.

Beschluss 83/2009 – über die Erfassung, Verwendung und den Handel mit Daten aus der elektronischen Kommunikation und anderen Daten

Als Reaktion auf eine erhebliche Anzahl von Beschwerden führte die griechische Datenschutzbehörde eine Inspektion in den Geschäftsräumen eines Unternehmens durch, das ein Produkt mit dem Namen „Hellas Navigator – Golden Customer Lists" („Navigator für Griechenland – goldene Kundenlisten") anbot. Die griechische Datenschutzbehörde verhängte Verwaltungssanktionen für folgende Vergehen:

- Beschaffung und Verkauf von E-Mail-Adressen. Das Unternehmen nutzte den Larbin-Webcrawler (der ursprünglich für .gr- und .com.gr-Domainnamen eingerichtet wurde) zur Erfassung von Adressen aus dem Internet (insgesamt etwa 160.000 Adressen wurden so aufgespürt). Die Adressenliste wurde an über 400 Kunden verkauft, darunter auch Werbeagenturen, Banken, Politiker und Körperschaften des öffentlichen Rechts.
- Datenerfassung aus Gewerkschaftslisten und Ausstellungsführern (auch E-Mail-Adressen) ohne die vorherige Information der betroffenen Personen.
- Zuordnung von Daten aus in öffentlichen Telefonbüchern veröffentlichten Einträgen zu Geolokationsdaten ohne das Einverständnis der betroffenen Personen.
- Versand von Spam, d. h. E-Mail-Werbung für die Produkte des Unternehmens ohne die vorherige Einwilligung des Empfängers. Die Spam-Mails wurden mithilfe des Turbomailers über 4 verschiedene Anbieter/ADSL-Verbindungen verschickt (die Absenderadressen wurden stets verändert: hnv@otenet.gr, hellasnv@otenet.gr, hnv2@altecnet.gr, hnv1@hol.gr und calino1@ath.forthnet.gr)
- Verkauf von Lizenzrechten an den Daten dieser Datenbank an US-Regierungsbehörden im Jahr 2004 ohne Information und Antrag auf Genehmigung durch die griechische Datenschutzbehörde.

Die griechische Datenschutzbehörde gab eine formelle Warnung hinsichtlich der Nutzung der Daten

aus Telefonbucheinträgen zu anderen Zwecken ohne vorherige Einwilligung der betroffenen Personen aus. Für alle anderen Verstöße verhängte die griechische Datenschutzbehörde ein Bußgeld in Höhe von insgesamt 65.000 Euro und forderte die Löschung aller vom Unternehmen für eigene Zwecke gespeicherten sowie aller im Produkt „Hellas Navigator – Golden Customer Lists" enthaltenen E-Mail-Adressen.

Beschluss 91/2009 – über internetbasierte dreidimensionale, virtuelle Straßennavigationsdienste

Die griechische Datenschutzbehörde entschied, dass die Bereitstellung eines dreidimensionalen, virtuellen Straßennavigationsdienstes durch das Unternehmen „KAPOU S.A. GEOINFORMATICS" insofern als Verarbeitung personenbezogener Daten einzustufen ist, als auf den Bildern identifizierbare Personen, Fahrzeugkennzeichen und Häuser zu sehen sind. Die Verarbeitung entspricht Gesetz 2472/1997, insbesondere auf der Grundlage von Artikel 5, Absatz 2, Punkt e, da die Entwicklung einer wirtschaftlichen Aktivität mit einem Nutzen für die Anwender, die virtuell an bestimmten Orten navigieren können, ein legitimer Zweck ist. Da die betroffenen Personen jedoch direkt oder indirekt auf den Bildern identifiziert werden können und diese keinen vorherigen Kontakt mit dem für die Datenverarbeitung Verantwortlichen hatten, der eine mögliche Verarbeitung ihrer Daten rechtfertigen könnte, darf der Dienst nur unter folgenden Bedingungen bereitgestellt werden: a) Die Gesichter der Personen sowie die Fahrzeugkennzeichen müssen vor der Veröffentlichung des Dienstes unkenntlich gemacht werden; b) der Zeitraum für die Speicherung der Rohdaten, also der scharfen Bilder, wird auf sechs Monate ab dem Datum festgesetzt, an dem das Bild gemacht wurde, außerdem müssen zusätzlich angemessene technische und organisatorische Sicherheitsmaßnahmen ergriffen werden; c) im Hinblick auf potenziell sensible Daten sind zusätzliche Maßnahmen zu ergreifen, insbesondere sollten Daten vorrangig unkenntlich gemacht werden. Des Weiteren muss der für die Datenverarbeitung Verantwortliche vor Veröffentlichung des Dienstes im Internet Zugang (zu den Rohdaten) gewähren und ein Recht auf Widerspruch einräumen. Auf einen solchen Widerspruch hin müssen die Rohdaten unkenntlich gemacht oder gelöscht werden. Nach der Veröffentlichung der Daten im Internet können die betroffenen Personen oder Dritte eine mangelhafte Unkenntlichmachung eines Gesichts oder Fahrzeugkennzeichens melden. Die Unkenntlichmachung des Bildes einer Person kann auch einen größeren Bereich des Bildes außer dem Gesicht umfassen, wenn die betroffene Person dies beantragt (vor oder nach der Veröffentlichung im Internet), da die betroffene Person unter Umständen über ihre Figur identifiziert werden könnte. Nur die betroffenen Personen können die Unkenntlichmachung ihres Hauses beantragen. Schließlich soll die Verpflichtung zur Information der betroffenen Personen nicht nur durch die Markierung der zur Erfassung der Bilder verwendeten Fahrzeuge, sondern auch durch Berichte in der Presse, also den Zeitungen, sowie über die Website des Unternehmens erfüllt werden. Diese Informationen müssen leicht zugänglich sein.

Beschlüsse 56/2009 & 74/2009 über Biometrik

In der zweiten Jahreshälfte 2009 veröffentlichte die griechische Datenschutzbehörde zwei Beschlüsse zur Rechtmäßigkeit der Verarbeitung biometrischer Daten. Beide Beschlüsse basierten auf dem Prinzip der Verhältnismäßigkeit. Insbesondere durch Beschluss 56/2009 gestattete die griechische Datenschutzbehörde einem Anbieter von Zertifizierungsdiensten die Entwicklung eines kartenbasierten biometrischen Fingerabdrucksystems zur Zugangskontrolle in den speziellen zur Erstellung und Pflege kryptographischer Schlüssel verwendeten Bereichen (d. h. private Schlüsse von Zertifizierungsbehörden, die zur Signierung der qualifizierten Zertifikate der Nutzer verwendet werden). Im Gegensatz hierzu verbat die griechische Datenschutzbehörde in Beschluss 74/2009 den Betrieb eines an eine zentrale Datenbank angeschlossenen biometrischen Systems im Bereich der Gesichtsgeometrie, das zur Kontrolle des Zugangs von Angestellten zur den Geschäftsräumen eines mit dem Bankensektor zusammenarbeitenden Dienstleistungsunternehmens eingesetzt werden sollte. In diesem Fall kam die griechische Datenschutzbehörde zu dem Schluss, dass das Unternehmen weniger drastische Maßnahmen zur physikalischen Zugangskontrolle ergreifen könnte, wohingegen in bestimmten Bereichen, in denen wichtige Daten gespeichert werden, strengere Maßnahmen sowie Maßnahmen zur logischen Zugangskontrolle

im technischen System des Unternehmens ergriffen werden können.

Beschluss 9/2009 über organisatorische Maßnahmen in Kliniken

Ein Patient behauptete, dass er einer Klinik ein Röntgenbild zur weiteren Diagnose und Behandlung durch das medizinische Personal der Klinik zur Verfügung gestellt hatte, das zuvor anderswo erstellt worden war. Da die Operation in der Klinik nicht erfolgreich war, forderte er die Klinik nach der Operation auf, das Röntgenbild herauszugeben, um seine medizinische Akte zur weiteren Konsultation und möglichen Behandlung an eine andere Klinik weiterzugeben. Die Klinik reagierte nicht schriftlich auf die Aufforderung des Patienten, sondern teilte ihm lediglich mündlich mit, das Röntgenbild sei verloren gegangen. Nach einer Inspektion in den Geschäftsräumen der Klinik stellte die griechische Datenschutzbehörde fest, dass die Klinik keine vollständigen medizinischen Aufzeichnungen führt, sondern lediglich einige Informationen zur Art der durch die Klinik selbst durchgeführten medizinischen Behandlungen sowie zu verwaltungstechnischen Daten zum Patienten aufbewahrt. Die griechische Datenschutzbehörde bemerkte, dass es gemäß dem Gesetz zum Verhaltenskodex von Ärzten eine rechtliche Verpflichtung gebe, vollständige medizinische Aufzeichnungen zu führen. Die griechische Datenschutzbehörde verhängte ein Bußgeld für die Unterlassung der formellen Antwort auf die Aufforderung des Patienten (d. h. für die Verletzung seines Rechts auf Zugang zu seinen Daten) und für die nicht ergriffenen organisatorischen Maßnahmen, die beweisen könnten, dass die medizinischen Daten aufbewahrt und sicher an den Patienten herausgegeben wurden.

Ungarn

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

Die „Richtlinie zur Vorratsdatenspeicherung" wurde vollständig in ungarisches Recht umgesetzt. Verbindungsdaten von erfolgreichen Anrufen werden ein Jahr lang gespeichert, die von nicht erfolgreichen Anrufen ein halbes Jahr. Der Speicherzeitraum von einem Jahr gilt für Verbindungsdaten, die durch die Nutzung des Internets generiert werden.

Gegen das Gesetz zur Umsetzung der „Richtlinie zur Vorratsdatenspeicherung" wurde Beschwerde vorm Verfassungsgericht eingelegt. Das Gericht hat in dieser Sache jedoch noch keine Entscheidung gefällt.

B. Bedeutende Rechtsprechung

Kameraüberwachung bei Demonstrationen
Viele Bürger beschwerten sich über die Installation von Kameras durch die Polizei zur Überwachung der Teilnehmer von Demonstrationen an öffentlichen Orten. In seiner Stellungnahme betonte der Datenschutzbeauftragte zunächst, dass von öffentlichen Behörden ergriffene Maßnahmen die Nutzung der Grundrechte, unter anderem das Recht auf freie Meinungsäußerung, fördern müssen. Der Einsatz von Kameras durch die Polizei könnte Bürger von der Teilnahme an Demonstrationen abschrecken. Der Einsatz solcher Geräte ist nur dann akzeptabel, wenn ein reales Risiko einer unrechtmäßigen und gewalttätigen Handlung besteht, die die Demonstration gefährden könnte, und wenn zur Wiederherstellung der Ordnung ein Einschreiten der Polizei erforderlich ist.

Von der Polizei beschlagnahmte Computer
In seiner Beschwerde gab ein Bürger an, dass sein Computer von der Polizei im Rahmen eines Strafverfahrens beschlagnahmt worden sei und er ihn über ein halbes Jahr lang nicht zurückbekommen habe. Der Datenschutzbeauftragte war der Ansicht, dass es akzeptabel sei, dass die Polizei IT-Geräte beschlagnahmt, wenn diese zur Begehung eines Verbrechens eingesetzt wurden. Das Strafverfahren darf jedoch keinen Nachteil mit sich bringen, der nicht mit der Durchführung einer ordnungsgemäßen Untersuchung einhergeht. Der Zeitraum von sechs Monaten überschritt offensichtlich das akzeptable Zeitlimit, das die durch ein Strafverfahren verfolgten Zwecke rechtfertigen.

Zugang zu Sprachaufzeichnungen
Zahlreiche Bürger beschwerten sich über abgelehnte Anträge auf Zugang zu von verschiedenen Dienstleistungsanbietern gespeicherten Sprachaufzeichnungen. Die Anträge wurden im Allgemeinen abgelehnt, da für den Antragsteller keine Notwendigkeit bestand, diese Aufzeichnung zu besitzen. Der Datenschutzbeauftragte betonte, dass die betroffenen Personen ein Recht auf Zugang zu den über sie gespeicherten Informationen haben und dass dieser Zugang nur dann beschränkt werden kann, wenn dies ausdrücklich gesetzlich festgelegt ist. Da es keine gesetzliche Beschränkung des Zugangsrechtes gibt, haben die Beschwerdeführer das Recht auf eine Kopie des vom Dienstleistungsanbieter aufgezeichneten Gesprächs. Dieser Ansatz wurde im weiteren Verlauf des Jahres vom Gesetzgeber im Rahmen der Änderung der Verbraucherschutzbestimmungen bestätigt, die die Rechte der betroffenen Personen auf Zugang zu solchen Kopien eindeutig gewährleisten, unter anderem von Gesprächen mit dem Dienstleistungsanbieter.

C. Wichtige spezifische Themen

Im Jahr 2009 nahmen zwei Unternehmen Verhandlungen mit dem Datenschutzbeauftragten auf, um ihn von der Notwendigkeit der so genannten positiven Kreditnehmerliste zu überzeugen. In Ungarn existieren bereits Dateien mit negativen Daten zur Nichterfüllung finanzieller Verpflichtungen, die nicht das Einverständnis der betroffenen Person erfordern. Die Erfassung von Informationen zur Zahlungsfähigkeit erfordert jedoch die Einwilligung der betroffenen Person.

Der Datenschutzbeauftragte ist gegen die Erstellung eines Kreditregisters (Positivliste). Der Datenschutzbeauftragte ist der Ansicht, dass die Kunden unter Druck stehen, ihr Einverständnis zur Verarbeitung zu geben, wodurch die Komponente der „Freiwilligkeit" nicht gewährleistet scheint. Außerdem bestanden Zweifel betreffend die hinreichende Information der betroffenen

Personen. Zahlreiche Finanzinstitutionen unterstützen die Idee der positiven Kreditnehmerliste und haben trotz der Warnungen des Datenschutzbeauftragten eine „Pilotphase" des Projekts gestartet und erfassen Kreditinformationen von zahlreichen interessierten Parteien.

Kameraüberwachung in öffentlichen Verkehrsmitteln
Die Budapester Verkehrsgesellschaft (BKV) leitete eine Konsultation mit dem Datenschutzbeauftragten zur möglichen Installation von Videokameras in BKV-Verkehrsmitteln ein. Der Datenschutzbeauftragte betonte, dass das Einverständnis der Passagiere keine rechtliche Grundlage für die Verarbeitung von Daten sein kann, und da dies der Fall ist, kann die Verarbeitung von Daten aufgrund spezifischer Aspekte des ungarischen Rechts nur dann rechtmäßig sein, wenn es dafür ein Gesetz gibt. Der Gesetzgeber muss ein angemessenes Gleichgewicht zwischen Privatsphäre und öffentlicher Ordnung finden. Die Stellungnahme des Datenschutzbeauftragten wurde vom nationalen ungarischen Institut für Kriminologie unterstützt, das auch Alternativen zur Verbesserung der Sicherheit in öffentlichen Verkehrsmitteln vorschlug.

Irland

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

Beide Richtlinien wurden vollständig in irisches Recht umgesetzt.

Zu den Entwicklungen in der Gesetzgebung, die eine signifikante Auswirkung auf den Datenschutz in Irland haben, zählte im Jahr 2009 die Bekanntmachung des Kommunikationsgesetzes 2009 (Vorratsspeicherung von Daten) im Juli, das die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden (zur Änderung der Richtlinie 2002/58/EG), in Kraft setzte.

B. Bedeutende Rechtsprechung

In den meisten Fällen, in denen Beschwerden im Einklang mit Abschnitt 10 der irischen Datenschutzgesetze von 1988 und 2003 beim Datenschutzbeauftragten eingereicht wurden, kam es zu einer gütlichen Einigung ohne formellen Beschluss oder Vollstreckungsmaßnahme. Eine solche gütliche Einigung kann beispielsweise einen finanziellen Beitrag durch den betreffenden Datenschützer an den Geschädigten oder an eine geeignete wohltätige Einrichtung umfassen. Gegebenenfalls können auch Vollstreckungsmaßnahmen angewendet werden – so zum Beispiel, wenn der Dateninhaber die Zugangsrechte der Geschädigten nicht respektiert. In einigen Fällen werden Dateninhaber auch in Fallstudien im Jahresbericht des Kommissars namentlich erwähnt. Im Laufe des Jahres 2009 war der Datenschutzbeauftragte an Gerichtsverfahren beteiligt, die die Rechte von Personen im Kontext der Datenschutzgesetze von 1988 und 2003 sowie der Rechtsverordnung 535 des Jahres 2003 betrafen. Diese ergaben sich aus einer Reihe kurzfristig angesetzter Inspektionen von Unternehmen aus dem Bereich SMS-Marketing im Jahr 2007 sowie aus der erfolgreichen Abweisung einer Beschwerde gegen die Rechtsgrundlage für die Strafverfahren aus dem Jahr 2008 durch den Obersten Gerichtshof.

C. Wichtige spezifische Themen

Ebenfalls im Jahr 2009 richtete der irische Minister für Justiz, Chancengleichheit und Gesetzesreform eine Gruppe zur Überprüfung der Datenschutzpolitik ein, die Empfehlungen dazu aussprechen sollte, ob die irischen Datenschutzgesetze hinsichtlich der Einführung einer Meldepflicht für mit Bußgeldern belegte Verstöße gegen den Datenschutz geändert werden müssen. Bisher hat die Gruppe ein Konsultationsdokument veröffentlicht, eine öffentliche Aufforderung zur Einreichung von Beiträgen initiiert, eine Konsultation unter den Mitgliedern der Gruppe gestartet und umfassende Schreibtischforschung betrieben.

Italien

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

Der rechtliche Rahmen zur Umsetzung der Richtlinien 95/46/EG, 2002/58/EG und 2006/24/EG wurde im Jahr 2009 nicht wesentlich verändert. Das Parlament hat jedoch einige Maßnahmen ergriffen, die die Datenschutzbehörde dazu veranlasst haben, ihre Sorge hinsichtlich der möglichen negativen Auswirkungen dieser Maßnahmen auf den Schutz personenbezogener Daten zum Ausdruck zu bringen.

Insbesondere Gesetz Nr. 15/2009 zur Steigerung der Produktivität im öffentlichen Sektor führte eine Änderung von Abschnitt 1 des Datenschutzgesetzes (196/2003) ein, da es Folgendes besagt: „Die Informationen zur Ausführung der Tätigkeiten, die eine Rechtspersönlichkeit mit öffentlichen Funktionen betreffen, einschließlich der betreffenden Bewertung der Daten, darf keinen Sicherheitsmaßnahmen im Hinblick auf den Datenschutz unterliegen." Die Datenschutzbehörde lenkte die Aufmerksamkeit der Regierung auf die Zweckmäßigkeit der Übertragung dieser Bestimmung in das Kapitel des Datenschutzgesetzes, das die Verarbeitung von Tätigkeiten öffentlicher Behörden regelt, und stellt überdies die Übereinstimmung sowohl mit der Verfassung als auch mit dem Recht der Gemeinschaft in Frage – da hierdurch bestimmte Informationsgegenstände und ganze Kategorien von betroffenen Personen nicht mehr in den Schutzbereich der Datenschutzgesetzgebung fallen würden.

Artikel 130 und Artikel 162 des Datenschutzgesetzes wurden im Jahr 2009 ebenfalls geändert, um Unternehmen, die vor dem 1. August 2005 mit Hilfe von Informationen aus öffentlichen Telefonverzeichnissen Datenbanken erstellt hatten, zu ermöglichen, diese Daten zu Werbezwecken weiterhin zu verwenden; außerdem wurde ein öffentliches Register eingeführt und der Aufsicht der Datenschutzbehörde unterstellt, über das man Widerspruch einlegen konnte. Es sollte daran erinnert werden, dass die Europäische Kommission der italienischen Regierung am 28. Januar 2010 einen Brief mit einer Informationsabfrage zu den oben genannten Änderungen geschickt hat, da sie der Ansicht war, dass letztere einen Verstoß gegen die Richtlinien 2002/58 und 95/46 darstellt – dies war der erste Schritt im Rahmen eines im Gemeinschaftsrecht festgelegten Vertragsverletzungsverfahrens.

Andererseits sollte hier auch Gesetz Nr. 69/2009 erwähnt werden, das verschiedene Anforderungen zur Förderung der Computerisierung der öffentlichen Verwaltungen sowie der Online-Veröffentlichung von Gerichtsentscheidungen einführte. Die relevanten Datenschutzbestimmungen sind in Artikel 21 dieses Gesetzes zu finden, der die Veröffentlichung der Jahresgehälter, der Lebensläufe, der E-Mail-Adressen sowie der dienstlichen Telefonnummern der leitenden Beamten/Angestellten öffentlicher Verwaltungsbehörden auf den jeweiligen Websites fordert. In Abschnitt 32 sind die für die Veröffentlichung von Verwaltungsbeschlüssen und -instrumenten geltenden Anforderungen genannt, die durch die Veröffentlichung dieser Beschlüsse und Instrumente auf den jeweiligen Websites erfüllt werden. Artikel 36 zielt auf die Förderung der Umsetzung des „öffentlichen Verbindungssystems" ab, um „die vollständige Kompatibilität der Datenbanken und Volkszählungsregister" zu gewährleisten und den Bürgern so bessere Dienste bieten und die Effizienz der öffentlichen Verwaltung verbessern zu können. Artikel 45 ändert schließlich die Zivilprozessordnung und gestattet die Veröffentlichung von Gerichtsentscheidungen auf Internet-Websites.

Ein weiteres wichtiges Gesetz, das im Jahr 2009 in Kraft gesetzt wurde, zielte auf die Umsetzung der Bestimmungen des Vertrags von Prüm durch die Einrichtung der nationalen DNS-Datenbank sowie die Festlegung der relevanten prozeduralen Mechanismen ab (Gesetz Nr. 85/2009). Die nationale DNS-Datenbank wird beim Innenministerium eingerichtet und umfasst DNS-Profile, die im Rahmen von Gerichtsverfahren erfasst wurden, sowie Profile von vermissten Personen und/oder deren Blutsverwandten, von nicht identifizierten Leichen sowie von Einzelpersonen, deren persönliche Freiheit durch gerichtliche Maßnahmen eingeschränkt wurde. Die italienische Datenschutzbehörde wird mit der Beaufsichtigung dieser Datenbank betraut sein. Die meisten Anregungen und Änderungsvorschläge der Datenschutzbehörde wurden aufgegriffen,

insbesondere diejenigen zur Wahrung des Respekts für die Würde der betroffenen Personen und der Verhältnismäßigkeit der Verarbeitungstätigkeiten. Zusätzliche Sicherheitsmaßnahmen werden über eine sekundäre Gesetzgebung festgelegt, die nach der Konsultation und/oder in Übereinkunft mit der italienischen Datenschutzbehörde verabschiedet werden soll. Die Empfehlungen hinsichtlich des übermäßig breiten Anwendungsbereiches der Bestimmungen zur Erfassung von DNS-Proben im Rahmen von Zwangsmaßnahmen sowie die übermäßig langen Fristen für die Vorratsspeicherung der Daten wurden nicht befriedigend umgesetzt.

Schriftliche Anträge an das Parlament – Im Dezember 2009 wurde ein Antrag bezüglich der Zweckmäßigkeit der Verabschiedung von Ad-hoc-Gesetzen zur Regulierung von Meldungen von Missständen (Whistleblowing) im Unternehmenssektor beim Parlament eingereicht. Die Datenschutzbehörde lenkte die Aufmerksamkeit insbesondere auf die Notwendigkeit einer Regulierung der rechtmäßigen Verwendung personenbezogener Daten, die von den Meldern dieser Missstände „in gutem Glauben" angegeben wurden, sowie auf den Zugang der betroffenen Personen zu ihren eigenen, auf diese Art und Weise erfassten Daten.

Parlamentarische Anhörungen – Die Datenschutzbehörde wurde im Jahr 2009 einige Male zu wichtigen Fragen angehört, mit denen sich die zuständigen parlamentarischen Ausschüsse entweder im Rahmen von Untersuchungsmaßnahmen oder einer Debatte zur Verabschiedung von Gesetzen zur Umsetzung des Schutzes personenbezogener Daten befassten. Insbesondere sollte die Anhörung vom 30. Januar 2009 vor dem parlamentarischen Ausschuss für die Sicherheit der Republik erwähnt werden, in der es um den Fall einer Erfassung personenbezogener Daten im Rahmen von Gerichtsverfahren sowie um die Rolle der vom Gericht bestellten Experten und Berater ging. Ebenso erwähnenswert sind die Anhörungen vom 15. Juli 2009 vor dem Ausschuss für Verfassungsangelegenheiten der Abgeordnetenkammer, die im Rahmen einer Informationsinitiative zur Computerisierung der öffentlichen Verwaltungen stattfanden, sowie die Anhörung vom 25. November vor dem Finanzausschuss der Abgeordnetenkammer, die im Rahmen einer Informationsinitiative zu Verbraucherkrediten stattfand und deren besonderer Schwerpunkt auf Kreditvermittlungsagenturen, der Umsetzung des relevanten Verhaltenskodexes und der relevanten Berufspraktiken sowie auf den mit der Aufklärung von Diebstahl und Betrug in diesem Bereich in Zusammenhang stehenden Gesetzen lag.

B. Bedeutende Rechtsprechung

Abhören von Telefonaten

Der **Staatsrat** (die letzte gerichtliche Instanz bei Verwaltungsverfahren) entschied, dass ein Beamter rechtmäßig aus dem Dienst entlassen werden könne, wenn die relevanten Disziplinarverfahren auf Abhörprotokollen aus den Akten des Strafverfahrens basieren, das aus dem gleichen Grund gegen diesen Beamten eingeleitet wurde und im Rahmen dessen er freigesprochen wurde – selbst wenn die betreffenden Protokolle im Strafverfahren nicht zugelassen wurden, da ihre Anfertigung einen Gesetzesverstoß darstellt. Die den Disziplinarverfahren zugrunde liegenden Fakten wurden nicht in Frage gestellt. Dementsprechend musste die Zulässigkeit der Protokolle als irrelevant eingestuft werden (Beschluss Nr. 7703/2009).

Das **Verfassungsgericht** entschied, dass die Vernichtung von Akten, einschließlich derer, die unrechtmäßig erstellte Abhörprotokolle enthalten, stets im Einklang mit den Vorschriften zum Anspruch auf rechtliches Gehör stehen müssen, um somit die Datenschutzanforderungen mit einem ordnungsgemäßen Gerichtsverfahren in Einklang zu bringen (Beschluss Nr. 173/2009).

Der **Kassationshof** befasste sich mit der gleichen Frage und entschied, dass die Vernichtung von Abhörprotokollen in allen Phasen und allen Instanzen von Gerichtsverfahren durch das Gericht anzuordnen ist, das sie als unzulässig eingestuft hat (sofern es eine Meinungsverschiedenheit zur Zulässigkeit dieser Protokolle gab). Die Vernichtung darf jedoch erst dann erfolgen, wenn die gerichtliche Entscheidung rechtskräftig ist (Beschluss Nr. 25590/2009).

Medizinische Daten
HIV-Tests, informiertes Einverständnis, Verbreitung von Daten
Der **Kassationshof** (Abteilung Zivilrechtliche Angelegenheiten) entschied, dass die Grundvoraussetzung für die Durchführung eines HIV-Tests die Information des betreffenden Patienten sowie sein Einverständnis ist, sofern es dem Patienten möglich ist, eine freie, informierte Entscheidung zu treffen. Auf diese Anforderung kann nur dann verzichtet werden, wenn die medizinische Behandlung als überaus dringend eingestuft wird und/oder im öffentlichen Interesse besonders erforderlich ist. Das medizinische Personal muss alle zur Gewährleistung der Vertraulichkeit sowie zur Vermeidung einer Verbreitung von Informationen zum Testergebnis und/oder zum Gesundheitszustand des Patienten erforderlichen Maßnahmen ergreifen. Im betreffenden Fall hatte die Verbreitung dieser Daten zur Schließung des Geschäfts des Patienten geführt, wohingegen der Patient den Test in einem anderen Krankenhaus hätte durchführen lassen, wenn er ordnungsgemäß informiert worden wäre (Beschluss Nr. 2468/2009).

Sonstige Fragen
Veröffentlichung von Informationen über die Mitglieder eines Berufsverbandes. Der Staatsrat bestätigte die Entscheidung, dass der Vorstand eines Berufsverbandes ausschließlich die personenbezogenen Informationen der Verbandsmitglieder veröffentlichen darf, in deren Besitz er gemäß einem Sonderrecht sein darf. Der Verband hatte die zusätzlichen, vom Antragsteller angeforderten personenbezogenen Informationen – z. B. Unternehmensanschriften, Telefon- und Faxnummern sowie E-Mail-Adressen – nicht weitergegeben, da dem Verband diese zusätzlichen Informationen auf streng vertraulicher Basis übermittelt worden waren (Beschluss Nr. 7946/2009).

Bilder als „personenbezogene Daten". Der **Kassationshof** entschied, dass das Bild einer Einzelperson gemäß den Bestimmungen des Datenschutzgesetzes nicht automatisch in die Kategorie „personenbezogene Daten" fällt, auch wenn die Person mithilfe dieses Bildes identifiziert werden kann. Hierzu muss es der betroffenen Person ausdrücklich durch eine Bildunterschrift oder anderweitig (z. B. durch eine Textanmerkung) zugeordnet werden, wodurch diese Person dann identifiziert werden kann. Ist dies nicht der Fall, fällt das Bild nicht in die Kategorie „personenbezogene Daten" (Beschluss Nr. 12997/2009).

Dokumente, die personenbezogene Daten enthalten. Laut **Kassationshof** ist die Erstellung von Dokumenten, die personenbezogene Daten enthalten, im Rahmen von Gerichtsverfahren ohne Einverständnis der betroffenen Person gestattet, wenn dies zur Ausübung des Rechts auf Verteidigung erforderlich ist. Hierbei ist es unerheblich, wie die personenbezogenen Daten erfasst wurden. Dieser Gerichtsbeschluss steht im Einklang mit einem früheren Beschluss der Datenschutzbehörde. Die Ausübung des Rechtes auf Verteidigung unter Verwendung personenbezogener Daten anderer Personen darf jedoch nicht den im Datenschutzgesetz festgelegten Anforderungen von Fairness, Datenrelevanz und Unverhältnismäßigkeit abträglich sein (Beschluss Nr. 3358/2009).

C. Wichtige spezifische Themen

Sensibilisierung der Jugend und soziale Netzwerke
Die italienische Datenschutzbehörde beschloss, anlässlich des Europäischen Datenschutztages (28. Januar) eine Initiative für Schüler zu starten. Die Initiative trug den Titel „Film & Privatsphäre" und lief über vier Tage. Ziel der Initiative war die Sensibilisierung der Jugend für die Bedeutung des Schutzes der Privatsphäre in der heutigen Gesellschaft sowie dafür, dass man lernen muss, wie man seine Privatsphäre schützen kann. Filme mit besonderer Relevanz, die das Thema Privatsphäre aus unterschiedlichen Perspektiven beleuchteten, wurden im Konferenzsaal der italienischen Datenschutzbehörde gezeigt. Jeder Film wurde von einem der vier Mitglieder des Kollegialgremiums der Datenschutzbehörde und durch ein eigens von der italienischen Datenschutzbehörde erarbeitetes Video vorgestellt, um – wieder mithilfe von Filmen – kleinere und größere Eingriffe in unsere Privatsphäre zu beschreiben. Schüler aus Sekundarschulen in Rom wurden zu den Vorführungen sowie zu Diskussion und Meinungsaustausch eingeladen.

Außerdem erstellte die Datenschutzbehörde im Jahr 2009 eine Broschüre, um (insbesondere Jugendlichen) eine Anleitung zu bieten, wie man mit sozialen Netzwerken umgehen und ihr Potenzial sachkundig nutzen sollte.

Die Broschüre mit dem Titel: „Soziale Netzwerke: Vorsicht vor den Nebenwirkungen" wurde in den wichtigsten italienischen Postämtern kostenlos ausgelegt. Ziel der Initiative war die Unterstützung sowohl erfahrener als auch unerfahrener Nutzer, damit diese das volle Potenzial dieser innovativen Kommunikationsinstrumente ohne Gefährdung ihres privaten oder beruflichen Lebens ausschöpfen können.

Datenbanksicherheit

Die Datenschutzbehörde überprüfte und erstellte eine Neufassung (am 25. Juni 2009) eines Beschlusses vom 28. November zur Verbesserung der Sicherheitsmaßnahmen für betroffene Personen in Zusammenhang mit den Tätigkeiten von „Systemverwaltern" – dieser Begriff ist im italienischen Gesetz nicht ausdrücklich definiert. Der neue Text sollte – teilweise zur Erläuterung einiger Anfragen an die Datenschutzbehörde – verschiedene Punkte klarstellen. Die von der Datenschutzbehörde festgelegten Anforderungen betrafen insbesondere die Zugangsprotokollierung (es müssen Systeme zur Protokollierung des Zugangs von Systemverwaltern zu Datenverarbeitungssystemen und elektronischen Datenbanken vorhanden sein, z. B. durch Zeitstempel und Vorgangsbeschreibungen, ohne dabei die von den Systemverwaltern durchgeführten Tätigkeiten nach ihrem Zugang aufzuzeichnen); die Beaufsichtigung der von Systemverwaltern durchgeführten Tätigkeiten durch Datenkontrolleure (zur Überprüfung der Frage, ob die in der Datenschutzgesetzgebung festgelegten organisatorischen, technischen und sicherheitsbezogenen Maßnahmen eingehalten wurden); die Erstellung einer Liste der Systemverwaltern sowie deren Eigenschaften (einschließlich Informationen zur Identifizierung der Systemverwalter und einer Liste der ihnen übertragenen Funktionen), die von jedem Datenkontrolleur in einem internen Dokument zu erstellen ist und der Datenschutzbehörde zur Prüfung vorgelegt werden muss. Die Datenschutzbehörde betonte die Notwendigkeit einer besonderen Sorgfalt beim Umgang mit Erfahrung, Fähigkeiten und Zuverlässigkeit einer Person, die mit den Funktionen eines Systemverwalters betraut wird, insbesondere im Hinblick auf die Gewährleistung der vollumfänglichen Einhaltung der Datenschutzgesetze sowie der entsprechenden Sicherheitsmaßnahmen.

Sensible Daten und medizinische Versorgung

Untersuchungsberichte im Internet. Die italienische Datenschutzbehörde bietet Leitlinien zur Verwendung personenbezogener Daten im Zusammenhang mit dem „Onlinezugang zu Untersuchungsberichten". Die Leitlinien sollen einen spezifischen, einheitlichen Rahmen für den Schutz der Bürger bieten, insbesondere im Hinblick auf die Freiwilligkeit des Onlinezugangs zu Untersuchungsberichten. Den betroffenen Personen muss gestattet werden, frei zu entscheiden, ob auf der Grundlage einer entsprechenden Meldung sowie des Einverständnisses zur Verarbeitung der personenbezogenen Daten im Hinblick auf den besagten Dienst online auf ihre Untersuchungsberichte zugegriffen werden darf oder nicht. In jedem Fall muss den betroffenen Personen weiterhin gestattet werden, diese Untersuchungsberichte bei den jeweiligen Anbietern medizinischer Versorgungsleistungen auch in Papierform zu erhalten. Zur Gewährleistung angemessener Sicherheitsmaßnahmen werden spezifische technische Vorkehrungen festgelegt: Sichere Kommunikationsprotokolle auf der Basis von Verschlüsselungsstandards für elektronische Datenübermittlungen, einschließlich digitaler Zertifizierung der Systeme für die netzwerkbasierten Dienste; angemessene Vorkehrungen zur Vermeidung einer Erfassung der in der elektronischen Datei gespeicherten Informationen, wenn letztere nach einer Online-Konsultation in lokalen und/oder zentralen Speichersystemen (Cache) gespeichert werden; sowie kurzfristige (maximal 45 Tage) Verfügbarkeit des Untersuchungsberichts im Internet.

Leitlinien für die elektronische Patientenakte und Patientendatei. Die Leitlinien schlagen vor, dass die elektronische Patientenakte (EPA) vorzugsweise so erstellt werden sollte, dass keine Vervielfältigung der medizinischen Informationen von den die betroffene Person behandelnden medizinischen Versorgern/Stellen erforderlich ist.

Da die in der EPA enthaltenen medizinischen Daten und Dokumente aus unterschiedlichen Quellen gewonnen werden, müssen angemessene Maßnahmen zur Rückverfolgung der für die Erstellung und Erfassung sowie die Bereitstellung der betreffenden Daten über die EPA verantwortlichen Stellen getroffen werden (auch

im Hinblick auf die Rechenschaftspflicht). Insbesondere sollte angesichts der Tatsache, dass es um separate klinische Aufzeichnungen geht, gewährleistet werden, dass jede Stelle, die solche Aufzeichnungen erstellt/verfasst hat in der Regel allein für besagte Aufzeichnungen verantwortlich ist.

Die betroffene Person muss in der Lage sein, frei zu entscheiden, ob eine elektronische Patientenakte/Patientendatei mit den sie betreffenden medizinischen Informationen erstellt wird oder nicht. Das Einverständnis der betroffenen Person muss auf einer separaten, speziellen Grundlage erteilt werden. Den betroffenen Personen sind angemessene Erklärungen bereitzustellen. Ein teilweises, auf einen bestimmten Umfang beschränktes Einverständnis sollte ebenfalls möglich sein, um den betroffenen Personen zu ermöglichen, ihre Wünsche anzugeben. Spezielle Beschränkungen zu den Zwecken der elektronischen Patientenakte/Patientendatei sind durch die Klarstellung der Tatsache definiert, dass die Verarbeitung personenbezogener Daten über eine elektronische Patientenakte/Patientendatei nur im Hinblick auf Vorbeugung, Diagnose oder Behandlung der betroffenen Person erfolgen. Dementsprechend darf eine elektronische Patientenakte/Patientendatei ausschließlich von praktizierenden Ärzten erstellt werden. Dieser modulare Ansatz ermöglicht beispielsweise die Festlegung, auf welche medizinischen Informationen der EPA der jeweilige Datenkontrolleur in seinem Fachgebiet zugreifen darf – z. B. ein Onkologienetzwerk aus Behandlungseinheiten, die sich auf die Behandlung von Krebs spezialisiert haben. Entsprechend dürfen Mitglieder bestimmter Fachgebiete wie z. B. Apotheker nur auf die Daten (oder Datenmodule) zugreifen, die zur Verschreibung von Medikamenten unerlässlich sind.

Öffentliche Transparenz und Veröffentlichung medizinischer Daten im Internet. Die Datenschutzbehörde ordnete an, dass medizinische Informationen über mehr als 4.500 behinderte Menschen von der Website einer regionalen Institution zu entfernen seien und leitete überdies ein Sanktionsverfahren gegen die zuständige lokale Behörde ein. Es wurde festgestellt, dass die Liste der behinderten Menschen, die einen Zuschuss der Region zum Kauf eines PCs erhalten hatten, im Internet frei abrufbar war – sie enthielt Namen, Behinderungen, Wohnorte und Geburtsdaten. Die Datenschutzbehörde bestätigte, dass die medizinischen Informationen nicht ohne entsprechende Sicherheitsmaßnahmen verbreitet werden dürfen und dass die Anforderungen der öffentlichen Transparenz die Datenschutzverpflichtungen für öffentliche Behörden nicht außer Kraft setzen dürfen – insbesondere gilt dies für die Verpflichtung, im Hinblick auf den jeweils speziellen Zweck keine überflüssigen Informationen zu veröffentlichen.

Nationale und regionale Register für Brustprothesen. Die Datenschutzbehörde erhob Einspruch gegen die Erstellung eines Registers, das die Namen von Frauen mit implantierten Brustprothesen enthalten und in Zusammenhang mit einem Gesetzesvorschlag betreffend Brustoperationen erstellt werden sollte. Es wurde darauf hingewiesen, dass plastische Operationen mithilfe statistischer Codes und Instrumente auch unter Wahrung der Anonymität der operierten Personen überwacht werden können. Die Datenschutzbehörde betonte, dass festgelegt werden müsse, wer zu welchem speziellen Zweck Zugang zu diesem Register haben solle, da der Wortlaut der Gesetzesvorlage überaus vage sei.

Unternehmen

Fusionen und Aufspaltungen – Die Datenschutzbehörde stellte klar, welche Verpflichtungen Unternehmen im Fall einer Fusion (durch Übernahme und/oder Zusammenschluss) oder einer Aufspaltung zur Einhaltung der Datenschutzgesetze erfüllen müssen. Insbesondere müssen die betroffenen Unternehmen ihre Kunden, Angestellten und Lieferanten gegebenenfalls über den (die) Namen des (der) neuen Datenkontrolleurs (Datenkontrolleure) informieren. Hierzu können vereinfachte Mechanismen verwendet werden, wie z. B. die anfängliche Veröffentlichung dieser Informationen auf der Unternehmenswebsite sowie im Anschluss daran die Bereitstellung individueller Informationen für das Personal.

Informationsdienste für Unternehmen – Die Datenschutzbehörde hat verschiedene Informationsdienste für Unternehmen von der Verpflichtung der Bereitstellung von Mitteilungen an alle betroffenen Personen befreit, da festgestellt wurde, dass diese Verpflichtung eine unverhältnismäßige Anstrengung verglichen mit den jeweiligen

Interessen darstellen würde. Die Datenschutzbehörde hat die betreffenden Unternehmen jedoch aufgefordert, effektive alternative Maßnahmen zu ergreifen.

Geldwäschegesetze und Finanzmakler – Es wurde klargestellt, dass Finanzmakler, die demselben Konzern angehören, personenbezogene Daten im Hinblick auf die Meldung „verdächtiger" Transaktionen ohne Einverständnis der betroffenen Person rechtmäßig austauschen und verarbeiten dürfen, solange diese Meldung im Einklang mit den Geldwäschegesetzen erfolgt und ausschließlich der Bekämpfung von Geldwäsche dient.

Unternehmensregister – Die Datenschutzbehörde stellte klar, dass das Datenschutzgesetz den Zugang von Aktionären zu den in Unternehmensregistern enthaltenen personenbezogenen Informationen weder beschränkt noch in Konflikt mit der Transparenz der Unternehmenstätigkeiten steht. Die Aktionäre haben ein Recht, die Adressen und persönlichen Informationen anderer Aktionäre einzusehen, um sie im Hinblick auf die Verteidigung ihrer rechtmäßigen Interessen zu kontaktieren.

Telefonische und elektronische Kommunikation

Telemarketing. Die durch Gesetz 14/2009 (siehe 12. Jahresbericht) eingeführte Möglichkeit der Wiederverwertung (bis 31. Dezember 2009) von Daten aus vor dem 1. August 2005 zu Werbezwecken ohne das Einverständnis der betroffenen Personen erstellten öffentlichen Telefonverzeichnissen veranlasste die Garante, die für die Erstellung und Verwendung solcher Daten geltenden Beschränkungen per Ad-hoc-Beschluss (März 2009) klarzustellen. Insbesondere hatte die Datenschutzbehörde unter anderem gefordert, dass die Datenkontrolleure bei Inanspruchnahme dieser Bestimmung Nachweise dafür vorzulegen haben, dass die Daten tatsächlich aus vor dem 1. August 2005 erstellten Telefonverzeichnissen stammen und ausschließlich zur Kontaktierung der Anschlussinhaber zu Werbezwecken verwendet werden, d. h. es wurde klargestellt, dass es Marketingunternehmen nicht gestattet ist, die Anschlussinhaber zu kontaktieren, um sich ihr Einverständnis für Werbetätigkeiten nach dem 31. Dezember 2009 zu erschleichen. Nach den durch Gesetz 166/2009 (siehe „Entwicklungen in der Gesetzbebung" oben) am Datenschutzgesetz umgesetzten Änderungen zur Verlängerung der Frist für die Verwendung der betreffenden Daten sowie zur Bereitstellung eines für den Bereich Telemarketing geltenden „Widerspruchsregisters" zum 25. Mai 2010 entschied die Datenschutzbehörde, die Umsetzbarkeit der in der oben genannten Entscheidung festgelegten Anforderungen entsprechend zu erweitern. Im gleichen Zusammenhang lehnte die Datenschutzbehörde auch die Vorgehensweise der Verwendung zufällig generierter Telefonnummern zur Kontaktierung von Anschlussinhabern zu Werbezwecken ab, da sie der Ansicht war, dass diese Nummern – trotz ihrer zufälligen Generierung – personenbezogene Daten gemäß dem italienischen Datenschutzgesetz darstellen und als solche für sie die gleichen Sicherheitsbestimmungen wie für andere personenbezogene Daten gelten – einschließlich der Notwendigkeit der Einholung des vorherigen informierten Einverständnisses des Anschlussinhabers im Hinblick auf die Verwendung dieser Daten.

Profilerstellung von Kunden – Den Anbietern von öffentlich zugänglichen elektronischen Kommunikationsdiensten wurden von der Datenschutzbehörde (Beschluss vom 25. Juni 2009) spezielle Verpflichtungen betreffend die Profilerstellung ihrer Kunden auferlegt. Es wurde eine detaillierte Analyse durchgeführt, die zu einer Unterscheidung unterschiedlicher Profilkategorien führte, wodurch die Datenkontrolleure unterschiedliche Vorkehrungen treffen müssen. Insbesondere wurden zwei Szenarien skizziert: 1. Profilerstellung auf der Grundlage „identifizierbarer" persönlicher Informationen, für die das freie, informierte und spezielle Einverständnis der betroffenen Person erforderlich ist; 2. Profilerstellung auf der Grundlage „aggregierter" persönlicher Informationen, also aggregierter Daten, die sich aus identifizierbaren persönlichen Informationen ableiten lassen, für die entweder das Einverständnis der betroffenen Person erforderlich ist oder für die, falls eine solche Einverständniserklärung nicht vorliegt, ein Antrag auf vorherige Überprüfung gemäß Abschnitt 17 des Datenschutzgesetzes vom Datenkontrolleur bei der Datenschutzbehörde gestellt werden muss. In letzterem Fall müssen der Grad der Aggregierung (d. h. die Detailliertheit der aggregierten Daten) sowie die für die Verarbeitung der Daten geltenden technischen Vorkehrungen berücksichtigt werden. Darüber hinaus wurden zusätzliche Verpflichtungen wie z. B. eine Meldepflicht gegenüber der Datenschutzbehörde sowie die Bereitstellung angemessener Informationen für die betroffenen Personen festgelegt.

Journalismus
In zahlreichen Fällen musste die Datenschutzbehörde einschreiten, um die Rechte von Kindern auf Privatsphäre zu schützen. Insbesondere wurde einigen Zeitungen die Veröffentlichung von Namen und Bildern in Zeitungsartikeln und/oder die Bereitstellung von Informationen untersagt, die eine Identifizierung dieser Kinder ermöglichen könnten. In Fällen von Kindesmissbrauch erinnerte die Datenschutzbehörde daran, dass es unbedingt erforderlich sei, sowohl die Privatsphäre der Kinder als auch der anderen beteiligten Personen zu wahren und davon abzusehen, Alter, Geschlecht und Wohnort des Kindes, gegebenenfalls die Beziehung zwischen Kind und Verdächtigem oder den Beruf des Vaters zu veröffentlichen.

Bei der Datenschutzbehörde gingen zahlreiche Anträge auf Löschung von im Internet (z. B. über Google, Emule, YouTube, Foren und Blogs) abrufbaren Daten und Bildern ein. In einigen Fällen könnte die Datenschutzbehörde keine direkten Maßnahmen ergreifen, da der für den Betrieb der Website Verantwortliche nicht in Italien wohnhaft war. In anderen Fällen wiederum wurde der Datenkontrolleur aufgefordert, die unrechtmäßig veröffentlichten Bilder/Daten zu löschen.

Zwei von der Datenschutzbehörde bearbeitete Fälle betrafen Zeitungen und Fernsehsender, die direkt aus Facebook übernommene Bilder bei der Berichterstattung über den Tod zweier Personen verwendet hatten, wenngleich die betreffenden Bilder auch gar nicht die verstorbenen Personen, sondern lediglich Namensvetter zeigten. Die Datenschutzbehörde stufte die Veröffentlichung dieser Bilder als Verstoß gegen die Datenschutzgesetze ein, da die Korrektheit der erfassten Informationen nicht gründlich geprüft und falsche persönliche Informationen verbreitet worden waren. Es sollte betont werden, dass eine zunehmende Anzahl von Beschwerden die Verarbeitung personenbezogener Daten aus Facebook-Profilen betreffen. Thema der meisten ist hierbei der Missbrauch persönlicher Informationen sowie Beleidigungen.

Ein weiterer wichtiger Beschluss in diesem Bereich bestätigte, dass das Filmen und die Verwendung von Bildern von Personen in privaten Räumen ohne das Einverständnis der betroffenen Person gesetzeswidrig ist. Die Datenschutzbehörde untersagte generell die Verbreitung/Veröffentlichung von Bildern, die unter Verletzung der für private Räume geltenden Schutzbestimmungen aufgezeichnet/beschafft wurden, insbesondere im Hinblick auf die Privatsphäre beeinträchtigende Techniken zur Aufzeichnung solcher Bilder, das fehlende Einverständnis der betroffenen Personen sowie die ausschließlich persönliche Natur der auf diesen Bildern dargestellten Tätigkeiten.

Formale Beschwerden
Im Jahr 2009 wurden 360 Beschlüsse zu formalen Beschwerden (die speziell geregelt sind) gefasst. Wie in den vergangenen Jahren, betrafen die meisten Beschwerden Banken, Finanzunternehmen und Kreditvermittlungsagenturen. Die interessantesten Fragen betrafen jedoch das Thema Sprachdaten als personenbezogene Daten, die Wahrnehmung von Datenschutzrechten verstorbener Personen sowie die Veröffentlichung öffentlich zugänglicher Informationen im Internet.

Sprachdaten als personenbezogene Daten. Die Datenschutzbehörde gab einer von einem Verbraucher gegen einen Telefonbetreiber eingereichten Beschwerde statt, der einen Vertrag auf der Grundlage eines „mündlichen Auftrags" in Kraft gesetzt hatte. Die Datenschutzbehörde war der Ansicht, dass die Aufzeichnung des Anrufs dem Antragsteller zur Verfügung gestellt werden müsse und dass eine Bereitstellung eines zusammenfassenden Protokolls der relevanten Inhalte nicht ausreichend sei. Betroffene Personen können ihre in den Datenschutzgesetzen festgelegten Rechte auch betreffend Ton- und Bilddaten geltend machen, da auch diese Daten personenbezogene Daten sind. Dementsprechend ist das Recht auf Zugang zu den im „mündlichen Auftrag" enthaltenen personenbezogenen Daten nur dann erfüllt, wenn die Aufzeichnung des Anrufs zur Verfügung gestellt wird, damit die jeweiligen Sprachdaten bewertet werden können.

Medizinische Aufzeichnungen über Verstorbene. Die Datenschutzbehörde gab einer gegen eine Universitätsklinik eingereichten Beschwerde statt, da die Klinik auf zahlreiche Bitten um persönliche Informationen über die Behandlungen des Partners des Beschwerdeführers nicht reagiert hatte. Die Datenschutzbehörde war der Ansicht, dass der Partner eines Verstorbenen das Recht auf Zugang zur Krankenakte des Verstorbenen habe, um rechtliche Schritte im Hinblick auf das Verhalten von Anbietern medizinischer Versorgungsleistungen zu prüfen. Laut Abschnitt 9(3) des Datenschutzgesetzes kann das Recht auf Zugang

zu personenbezogenen Daten von Verstorbenen „von jeder Partei wahrgenommen werden, die Interesse an diesen Daten hat oder zum Schutze einer betroffenen Person oder aus familiären Gründen, die geschützt werden müssen, handelt" – der Beschwerdeführer hatte klargestellt, dass die betreffenden Daten im Hinblick auf die Einleitung rechtlicher Schritte zur Prüfung von Fehlern und/oder fahrlässigem Verhalten des Anbieters medizinischer Versorgungsleistungen erforderlich seien.

Veröffentlichungen von Beschlüssen einer kommunalen Behörde im Internet. Die Datenschutzbehörde forderte eine Gemeinde auf, die Adresse eines Beschwerdeführers aus einem Beschluss zu löschen, der auf der Website der Gemeinde veröffentlicht und über externe Suchmaschinen abrufbar war. Der Beschwerdeführer gab an, dass die Löschung seiner Adresse aus dem Beschluss nicht mit der Transparenz elektronisch veröffentlichter Instrumente und Aufzeichnungen in Konflikt stehe. Die Datenschutzbehörde betonte die Notwendigkeit einer sorgfältigen Auswahl der auf diese Weise veröffentlichten personenbezogenen Daten, da die Notwendigkeit ihrer Veröffentlichung unter bestimmten Umständen für die beabsichtigten Zwecke gemäß den Prinzipien der Relevanz und Verhältnismäßigkeit nachgewiesen und das Gleichgewicht zwischen dem Recht auf Privatsphäre und der Verpflichtung der Gewährleistung der Öffentlichkeit von Beschlüssen einer lokalen Behörde gewahrt werden muss. Die vollständige Veröffentlichung des betreffenden Beschlusses beeinträchtigte die Rechte des Beschwerdeführers unverhältnismäßig, da sie zur Verbreitung irrelevanter Informationen im Internet führte.

Prüfungen

Auch im Jahr 2009 waren Prüfmaßnahmen wieder ein wesentlicher Bestandteil der Arbeit der Datenschutzbehörde. Auf der Grundlage sechsmonatiger Prüfpläne wurden insgesamt 449 Prüfungen durchgeführt. Bei der Durchführung dieser Prüfmaßnahmen kann die Datenschutzbehörde auf Spezialeinheiten der Finanzpolizei zurückgreifen, deren Aufgabe die Überprüfung der Einhaltung der Anforderungen betreffend Meldungen, Informationsmitteilungen, Sicherheitsmaßnahmen und Umsetzung der von der Garante angenommenen Beschlüsse ist. 45 Prüfungen wurden von der Prüfabteilung der Datenschutzbehörde selbst durchgeführt. Diese betrafen insbesondere öffentliche Behörden, die auf das Informationssystem der Steuerbehörde zugreifen (13), Unternehmen, die Dritten Datenbanken zu Marketingzwecken anbieten (10) und Telefonanbieter im Hinblick auf die Vorratsdatenspeicherung von Verbindungsdaten zum Zwecke der Profilerstellung von Kunden (9). Die von der Finanzpolizei auf Weisung der Datenschutzbehörde (die den Datenkontrolleur sowie den Umfang der Prüfungen vorgibt) durchgeführten Prüfungen betrafen die folgenden Bereiche: private Krankenhäuser (35), öffentliche Krankenhäuser und Pflegeheime (35), öffentliche Verkehrsunternehmen (30), Personaldienstleister (26), Lieferanten von Baumaterial (25), Golfclubs (25), von Gemeinden kontrollierte Abfallentsorgungsunternehmen (20), den Verkauf von Methan (20), den Verkauf von Wasser (20), Fremdenverkehrsorte (20), Wettbüros (15), Skilift-Unternehmen (10), Unternehmen, die Elektrogeräte verkaufen (10), Apotheken (20), Unternehmen die zur Nutzung der Datenbanken mit Bonitäts-/Zahlungsversäumnisdaten (20), andere Einrichtungen gemäß den speziellen Anträgen der Rechtsabteilungen der Datenschutzbehörde (83).

Im Anschluss an die Prüfungen wurden 43 Berichte an die Justizbehörden übermittelt und 368 Verfahren zur Verhängung von Verwaltungssanktionen eingeleitet. Darüber hinaus wurden den zuständigen Rechtsabteilungen der Datenschutzbehörde in etwa 150 Fällen Vorschläge zu Verpflichtungen der Datenkontrolleure vorgelegt, um die Verarbeitung im Einklang mit geltendem Recht zu gestalten.

Im Jahr 2009 wurden 170 Sanktionsverfahren abgeschlossen und Bußgelder in einer Höhe von insgesamt 1.572.432 Euro verhängt.

Bei den Strafsachen wurde in einigen Fällen das Mindestmaß an Sicherheitsvorkehrungen nicht beachtet (24). Außerdem wurden die unrechtmäßige Verarbeitungen von Daten (7), die Bereitstellung falscher Angaben und Informationen gegenüber der Datenschutzbehörde (6) sowie die Nichteinhaltung von Anordnungen/Maßnahmen der Datenschutzbehörde (4) festgestellt.

Lettland

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

Gesetz zum Schutz personenbezogener Daten
Die Richtlinie 95/46/EG wurde durch das Gesetz zum Schutz personenbezogener Daten in nationales Recht umgesetzt, das am 20. April 2000 in Kraft trat. Die letzten Änderungen traten am 1. Juli 2009 in Kraft. Das Gesetz zum Schutz personenbezogener Daten wurde am 12. Juni 2009 geändert. Die wesentlichen Änderungen betrafen Ausnahmen bei der Meldung der Verarbeitung personenbezogener Daten an die staatliche Datenaufsichtsbehörde sowie die Verpflichtung, im Fall eines möglichen Verstoßes gegen das Datenschutzgesetz eine Anfrage bei dem für die Verarbeitung der Daten Verantwortlichen einzureichen, bevor eine Beschwerde bei der Datenaufsichtsbehörde eingereicht wird. Die Änderungen legen außerdem fest, dass die Datenaufsichtsbehörde künftig keine internen und externen Prüfer der Verarbeitung von Daten mehr akkreditieren wird.

Darüber hinaus wurden zwei Entwürfe für zusätzliche Änderungen des Datenschutzgesetzes verfasst:

- betreffend die Ausnahme, im Bereich der Strafverfolgung einen Vertrag zur Datenübermittlung an Drittländer zu schließen, wenn diese die internationale Zusammenarbeit im Bereich nationale Sicherheit oder Strafrecht betrifft;
- betreffend Beschlüsse der Datenaufsichtsbehörde zur Abfangung oder Unterbrechung der Verarbeitung von Daten. Die Änderung besagt, dass die Beschlüsse im Fall einer Berufungsentscheidung nicht anfechtbar sind.

Gesetz über die Datenaufsichtsbehörde
Um die vollständige Unabhängigkeit der lettischen Datenaufsichtsbehörde zu gewährleisten, wurde das Verfahren zum Entwurf eines Gesetzes über die Datenaufsichtsbehörde abgeschlossen. Angesichts der Notwendigkeit einer Überprüfung der für die Arbeit der unabhängigen Datenschutzbehörde erforderlichen Mittel vor dem Hintergrund der wirtschaftlichen Situation in Lettland wurde der Gesetzesentwurf im Jahr 2009 aktualisiert. Die Veröffentlichung des Gesetzes wurde aufgeschoben, bis der Europäische Gerichtshof ein Urteil zur Unabhängigkeit der deutschen Datenschutzbehörde gesprochen hat.

Verordnung betreffend die Übermittlung von Daten an Drittländer
Im Jahr 2009 führte die lettische Datenaufsichtsbehörde ihre Aktivitäten zum Entwurf einer Kabinettsverordnung zu Standard-Anforderungen für Vereinbarungen betreffend die Übermittlung personenbezogener Daten an Drittländer fort. Die Verordnung setzt die in den Entscheidungen 2001/497/EG und 2004/915/EG der Kommission bezüglich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer festgelegten Anforderungen in Bezug auf den Inhalt von Verträgen um. Die Verordnungen werden nach der Änderung von Artikel 28 des Datenschutzgesetzes veröffentlicht. Die Änderung wurde bereits verfasst und beim Parlament eingereicht.

Verordnung über Anforderungen für einen Prüfbericht betreffend die Verarbeitung personenbezogener Daten in staatlichen und lokalen Regierungseinrichtungen
Die Etatkürzungen sowie die Reduzierung der Funktionen und Verwaltungskapazitäten der Datenaufsichtsbehörde führten zu den am 1. Juli 2009 in Kraft getretenen Änderungen des Datenschutzgesetzes. Die Änderungen besagen, dass eine Akkreditierung von Prüfern der Datenverarbeitung künftig nicht mehr erforderlich ist. Stattdessen werden mit den Verordnungen des Ministerkabinetts Anforderungen für Prüfberichte festgelegt. Im Jahr 2009 verfasste die Datenaufsichtsbehörde die Verordnung des Ministerkabinetts (17. November 2009 Nr. 1322) „Anforderungen für einen Prüfbericht betreffend die Verarbeitung personenbezogener Daten in staatlichen und lokalen Regierungseinrichtungen", die am 25. November 2009 in Kraft trat. Die Verordnung besagt, dass der Inhalt von Prüfberichten betreffend die Verarbeitung personenbezogener Daten in staatlichen und lokalen Regierungseinrichtungen der Datenaufsichtsbehörde alle zwei Jahre zu übermitteln ist und eine Risikoanalyse zur Verarbeitung personenbezogener Daten für jeden unterschiedlichen Verarbeitungszweck, die Schlussfolgerungen einschließlich der Risikobewertungen, sowie Verbesserungsvorschläge enthalten muss.

Gesetz über die Informationsfreiheit
Aufgrund von Änderungen des Gesetzes über den Staatshaushalt für 2009, durch die der Etat der Datenaufsichtsbehörde drastisch gekürzt wurde, verfasste die Datenaufsichtsbehörde eine Änderung des Gesetzes über die Informationsfreiheit, die besagt, dass die Aufsicht über das Gesetz über die Informationsfreiheit seit 1. Juli 2010 nicht in den Zuständigkeitsbereich der Datenaufsichtsbehörde fällt.

Gesetz über die Dienste der Informationsgesellschaft
Aufgrund von Änderungen des Gesetzes über den Staatshaushalt für 2009, durch die der Etat der Datenaufsichtsbehörde drastisch gekürzt wurde, verfasste die Datenaufsichtsbehörde eine Änderung des Gesetzes über die Dienste der Informationsgesellschaft. Die Änderungen besagen, dass die Datenaufsichtsbehörde verpflichtet ist, eine Untersuchung einzuleiten, wenn eine Person innerhalb eines Jahres 10 Werbenachrichten vom gleichen Absender erhalten hat. Diese Regelung schließt jedoch Untersuchungen auf Eigeninitiative der Datenaufsichtsbehörde nicht aus.

Vorschriften über die Vorratsspeicherung bei elektronischen Kommunikationsdiensten von Daten zur Durchsetzung von Gesetzen
Die Richtlinien 2002/58/EG und 2006/24/EG werden durch das Gesetz über elektronische Kommunikation in nationales Recht umgesetzt.

Seit 2007 ist die Datenaufsichtsbehörde für die Zusammenfassung der Statistiken über die Vorratsspeicherung jener Daten zuständig, die im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Grundlagen dafür sind Paragraph 19 des Gesetzes über elektronische Kommunikation und Artikel 10 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG. Die Verordnung des lettischen Kabinetts (Nr. 820 vom 4. Dezember 2007) „über Auskunftsersuchen von außergerichtlichen Ermittlungsstellen, den Betroffenen der Ermittlungen, staatlichen Sicherheitsorganen, Staatsanwaltschaften und Gerichten und über die Bereitstellung auf Vorrat gespeicherter Daten durch die Anbieter elektronischer Kommunikationsdienste sowie über die Zusammenfassung der Statistiken über die gewünschten Vorratsdaten und ihre Bereitstellung" gibt den Zeitraum an, für den die Anbieter elektronischer Kommunikationsdienste verpflichtet sind, statistische Daten zu speichern und an die Datenaufsichtsbehörde zu übermitteln Im Jahr 2008 fasste die lettische Datenaufsichtsbehörde die Statistiken erstmals zusammen.

Gemäß Artikel 4 des Gesetzes über elektronische Kommunikation muss der Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation von der Datenaufsichtsbehörde überwacht werden. Im Jahr 2009 sah sich die Datenaufsichtsbehörde einem Problem hinsichtlich der Interpretation der Gesetzgebung zu den Rechten der Datenaufsichtsbehörde auf Zugang zu auf Vorrat gespeicherten Daten gegenüber. Da eine Lösung des Problems erforderlich war, verfasste die Datenaufsichtsbehörde eine Änderung des Gesetzes über elektronische Kommunikation. Diese Änderung wird voraussichtlich im Jahr 2010 in Kraft treten.

B. Bedeutende Rechtsprechung

Im Laufe des Jahres 2009 gingen 140 Beschwerden bei der Datenaufsichtsbehörde ein. Die meisten betrafen die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage sowie die Verarbeitung von Daten, die über den eigentlichen Zweck der Datenverarbeitung hinausgeht (in 20 Fällen erhielten die Beschwerdeführer Anweisungen von der Datenaufsichtsbehörde, wie sie den Verstoß gegen das Datenschutzgesetz direkt mit dem für die Verarbeitung der Daten Verantwortlichen regeln können). Als Ergebnis von Untersuchungen der Datenaufsichtsbehörde wurden in 58 Fällen Verstöße gegen das Gesetz zum Schutz personenbezogener Daten bestätigt. Auf der Grundlage der festgestellten Verstöße wurden in 29 Fällen Verwarnungen ausgesprochen, also in 50 % der gemeldeten Verwaltungsverstöße. Dieser Prozentsatz liegt höher als in den Vorjahren. Im Jahr 2008 wurden in 18 % der Fälle Verwarnungen ausgesprochen, im Jahr 2007 in 10 % der Fälle. 18 weitere Verfahren wurden von der Datenaufsichtsbehörde eingeleitet. Die Datenaufsichtsbehörde verhängte

Bußgelder in einer Höhe von insgesamt 23.800 Lats (etwa 34.000 Euro). Die Beschwerden betrafen zumeist die Verarbeitung von Daten ohne Rechtsgrundlage und Verstöße gegen die Rechte der betroffenen Personen (Artikel 10 und 11 der Richtlinie 95/46/EG) sowie Verstöße gegen das Prinzip der Verhältnismäßigkeit bei der Verarbeitung von Daten.

Am häufigsten ging es bei Verstößen bei der Verarbeitung personenbezogener Daten um Folgendes:

- Veröffentlichungen personenbezogener Daten im Internet;
- Verarbeitung von Daten durch Kreditvermittlungsagenturen sowie Datenübermittlung an Dritte;
- Verwendung personenbezogener Daten durch andere Personen zur Identifizierung bei Verwaltungsverstößen;
- Videoüberwachung;
- Verarbeitung von Daten durch Hausmeisterdienste.

Ein spezieller Fall, der in den Medien große Beachtung fand, war die Videoüberwachung von Umkleidebereichen in einer großen Supermarktkette. Im Jahr 2009 stieg die Zahl der Fälle an, in denen Personen bei einer Überprüfung der Identität durch die Polizei die personenbezogenen Daten einer anderen Person verwendeten.

C. Wichtige spezifische Themen

Auf nationaler Ebene nahm die Datenaufsichtsbehörde an Diskussionen zu verschiedenen Themen teil, zum Beispiel:

- Gesetzesänderungen im Zusammenhang mit den Etatkürzungen (einschließlich der Reduzierung der Funktionen und Verwaltungskapazitäten der Datenaufsichtsbehörde);
- Verarbeitung von Daten zu Bildungszwecken in staatlichen Systemen;
- Einsatz von Körperscannern in Gefängnissen;
- Veröffentlichung von Gerichtsurteilen und Anonymisierung von Daten;
- Verarbeitung von Daten betreffend Verbraucherkredite und die Einziehung von Forderungen; und
- Zugang zu Datenbanken beim Abschluss von Fahrzeugversicherungen (Online-Abschlusssysteme).

Spezifische Fälle (betreffend die wesentlichen Themen, zu denen Beschwerden eingingen):

1. Ein großer Anteil der eingegangenen Beschwerden betraf die Veröffentlichung personenbezogener Daten im Internet ohne das Einverständnis der betroffenen Personen. Die Entscheidungen der Datenaufsichtsbehörde wurden auf der Grundlage von Ausnahmeregelungen zur Verarbeitung personenbezogener Daten ohne Rechtsgrundlage getroffen.
2. Ein großer Anteil der eingegangenen Beschwerden betraf die Kreditvermittlung und die Übermittlung personenbezogener Daten von Schuldnern an Dritte zum Zweck der Einziehung von Forderungen. Die Ausnahmeregelungen betreffen das nicht erteilte Einverständnis der betroffenen Personen zu solchen Datenübermittlungen. In den meisten Fällen wird die Übermittlung personenbezogener Daten als Verarbeitung von Daten ohne Rechtsgrundlage eingestuft und liegt somit außerhalb des zulässigen Bereichs der Datenverarbeitung.
3. Videoüberwachung ohne Rechtsgrundlage oder umfangreiche Verarbeitung von Daten aus Videoüberwachungen. In diesen Fällen wird eine Videoüberwachung zumeist als übermäßige Verarbeitung personenbezogener Daten oder als Verarbeitung von Daten ohne Rechtsgrundlage eingestuft und liegt somit außerhalb des zulässigen Bereichs der Datenverarbeitung.

Vertreter der Datenaufsichtsbehörde nahmen an 7 Workshops mit Vorträgen zu Datenschutz und Spam sowie Fragen zum Bereich Direktwerbung teil. Zielgruppen waren Händler, Verwaltungspersonal von Stadträten, zahlreiche große Unternehmen, Lehrer und Sozialarbeiter in Schulen sowie Studenten und Schüler.

Datenschutzbeauftragte

Im Jahr 2009 organisierte die Datenaufsichtsbehörde vier Untersuchungen von Datenschutzbeauftragten und stellte Bescheinigungen für 17 Datenschutzbeauftragte aus, die sowohl den privaten als auch den Regierungssektor repräsentieren. Die Schulung der Datenschutzbeauftragten wurde im Jahr 2009 vom privaten Sektor durchgeführt.

Entwurf von Empfehlungen und Leitlinien
Im Jahr 2009 verfasste die Datenaufsichtsbehörde die „Empfehlung betreffend die Datenübermittlung an Drittländer". Angesichts der bei der Datenaufsichtsbehörde eingegangenen Anzahl von Fragen zu Artikel 28 des Gesetzes zum Schutz personenbezogener Daten, der die Übermittlung personenbezogener Daten an Drittländer regelt, sprach die Datenaufsichtsbehörde eine Empfehlung zu dieser Frage aus.

Im Hinblick auf die Klarstellung der Meldeverfahren bei der Datenaufsichtsbehörde betreffend die Verarbeitung personenbezogener Daten wurden Leitlinien für alle für die Verarbeitung von Daten Verantwortlichen erstellt. Diese Leitlinien berücksichtigen insbesondere die aktuellen Änderungen des Gesetzes zum Schutz personenbezogener Daten im Hinblick auf Ausnahmen von der Meldepflicht.

Datenschutztag 2009
Am Datenschutztag 2009 organisierte die Datenaufsichtsbehörde Aktivitäten zum Thema Schutz personenbezogener Daten in den Bereichen Fotografie und Verarbeitung personenbezogener Daten durch Fotografen (Amateure und Profis). Eine Diskussion mit dem lettischen Fotografenverband wurde geführt, und ein Vertreter der Datenaufsichtsbehörde nahm an einem Seminar für Fotografen teil, im Rahmen dessen auch ein Vortrag/Workshop zur gesetzlichen Haftung von Fotografen organisiert wurde. Diskutiert wurde beispielsweise die Frage, wie Fotografen bei ihrer alltäglichen Arbeit die Privatsphäre schützen können. Die Datenaufsichtsbehörde präsentierte den Fotografen Leitlinien zum Schutz personenbezogener Daten.

Litauen

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

- Das Gesetz zur Änderung des Gesetzes über den rechtlichen Schutz personenbezogener Daten trat am 1. Januar 2009 in Kraft.

  Der neue Wortlaut legt die Bestimmungen des Gesetzes über den rechtlichen Schutz personenbezogener Daten fest und regelt die Verarbeitung des persönlichen Identifizierungscodes. Gemäß dem neuen Wortlaut müssen Datenkontrolleure, die gesundheitsbezogene Daten zum Zwecke der Gesundheitsvorsorge automatisch verarbeiten und die personenbezogene Daten zu wissenschaftlichen medizinischen Zwecken verarbeiten, der staatlichen Datenschutzbehörde Meldung erstatten, damit diese eine Vorprüfung durchführen kann. Außerdem wurde der Begriff „Videoüberwachung" definiert und Vorschriften zur Verarbeitung personenbezogener Bilddaten sowie zur Verarbeitung personenbezogener Daten für Direktwerbung und Solvenzbewertung wurden verabschiedet. Darüber hinaus wurden Vorschriften zum Status einer für den Datenschutz und die Bearbeitung von Beschwerden verantwortlichen Person oder Abteilung verabschiedet. Der Wortlaut des neuen Gesetzes über den rechtlichen Schutz personenbezogener Daten schreibt die Unabhängigkeit der staatlichen Datenschutzbehörde fest, die als Aufsichtsbehörde für den Datenschutz fungiert und deren Behördenleiter für eine Amtszeit von jeweils 5 Jahren eingesetzt wird.

  Obwohl die neue Version des Gesetzes zum Schutz personenbezogener Daten erst am 1. Januar 2009 in Kraft getreten ist, wird derzeit bereits ein neuer Gesetzesentwurf zur Änderung des Gesetzes zum Schutz personenbezogener Daten vorbereitet. Dieser Entwurf umfasst Änderungen des rechtlichen Status/ der Unabhängigkeit der Datenschutzbehörde sowie der Verarbeitung personenbezogener Daten zum Zweck der Feststellung der Zahlungsfähigkeit.

- Am 16. März 2009 traten die Änderungen der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG in Kraft.

  Das Gesetz legt fest, dass Verbindungsdaten eines Anschlussinhabers oder registrierten Nutzers elektronischer Kommunikationsdienste nicht länger als 6 Monate nach dem Datum der Kommunikation gespeichert werden dürfen. Ausgenommen hiervon sind Fälle, in denen die Rechnung rechtmäßig angefochten wird bzw. die Daten zur Forderungseinziehung erforderlich sind, sowie die in Artikel 77(2) dieses Gesetzes genannten Fälle. Um den Zugang zu den Daten bei schweren oder sehr schweren Verbrechen gemäß den Definitionen des Strafgesetzbuches der Republik Litauen zu gewährleisten, in denen diese Informationen für die Untersuchung, Feststellung und strafrechtliche Verfolgung von Verbrechen erforderlich sind, müssen Anbieter öffentlicher Kommunikationsnetzwerke und/oder öffentlicher Kommunikationsdienste die Informationen für einen Zeitraum von 6 Monaten ab dem Datum der Kommunikation sowie im Einklang mit dem gesetzlich festgelegten Verfahren speichern und diese den zuständigen Behörden kostenlos zusammen mit den durch sie selbst generierten oder verarbeiteten Daten zur Verfügung stellen. Die Pflicht zur Datenspeicherung umfasst auch die Vorratsspeicherung von Daten zu nicht verbundenen Anrufen, die durch die Betreiber öffentlicher Kommunikationsnetzwerke und/ oder öffentlicher Kommunikationsdienste generiert oder verarbeitet und gespeichert (Telefoniedaten) oder aufgezeichnet (Internetdaten) werden.

  Sind die oben genannten Daten für die Geschäftstätigkeit der Behörden, für vorgerichtliche Untersuchungen, für den Staatsanwalt, das Gericht oder den Richter zur Ermittlung und Feststellung von Straftaten oder für von der Regierung bevollmächtigte Institutionen erforderlich, so müssen die Betreiber elektronischer Kommunikationsnetzwerke und/oder -dienste diese Informationen für einen

längeren Zeitraum speichern, jedoch nicht länger als 6 weitere Monate. Für diese Speicherung ist aus staatlichen Mitteln gemäß dem von der Regierung festgelegten Verfahren (Artikel 77(2) des Gesetzes über elektronische Kommunikation der Republik Litauen) eine Entschädigung zu zahlen.

Die Datenschutzbehörde ist für die Überwachung der Umsetzung der Bestimmungen von Kapitel 9 des Gesetzes über elektronische Kommunikation verantwortlich, das auch die Bestimmungen zur Umsetzung der Richtlinie 2006/24/EG umfasst.

- Am 22. Juli 2009 wurde die Regierungsverordnung Nr. 788 zur Änderung der Regierungsverordnung „zur Erteilung der Genehmigung zur Umsetzung des Gesetzes über elektronische Kommunikation" angenommen. Die Datenschutzbehörde wurde als Institution benannt, die für die Sammlung und Bereitstellung von Statistiken für die Europäische Kommission betreffend die Vorratsspeicherung von Daten, die im Zusammenhang mit öffentlich zugänglichen elektronischen Kommunikationsdiensten oder einem öffentlichen Kommunikationsnetzwerk gemäß Artikel 10 der Richtlinie 2006/24/EG stehen, verantwortlich ist.

- Am 22. Juli 2009 wurde die Regierungsverordnung Nr. 789 „zur Genehmigung von Verfahren betreffend die in Artikel 70 des Gesetzes über elektronische Kommunikation vorgesehene Bereitstellung statistischer Daten" angenommen. Diese Verordnung beschreibt die Verfahren, gemäß denen die Strafverfolgungsbehörden der Datenschutzbehörde die in Artikel 10 der Richtlinie 2006/24/EG genannten Daten bereitstellen müssen und wie die Datenschutzbehörde diese an die Europäische Kommission weiterleiten muss.

B. Bedeutende Rechtsprechung

Definition personenbezogener Daten
Die Datenschutzbehörde leitete ein Ordnungswidrigkeitsverfahren gegen ein Unternehmen ein, das personenbezogene Daten (vollständige Namen und Adressen) von einem anderen Unternehmen erhalten und diese dazu verwendet hatte, den betroffenen Personen Angebote zu einem Vertragswechsel zuzuschicken. Die Datenschutzbehörde entschied, dass es keine Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten gebe.

Das Bezirksgericht Kaunas entschied, dass die in Absatz 1 von Artikel 2 des Gesetzes zum Schutz personenbezogener Daten enthaltene Definition personenbezogener Daten nicht den Vor- und Nachnamen sowie die Adresse von natürlichen Personen umfasst und dass das Gesetz zum Schutz personenbezogener Daten somit den gesetzlichen Schutz dieser Daten nicht regelt.

Gegen die Entscheidung des Bezirksgerichts Kaunas wurde Berufung beim Obersten Verwaltungsgericht von Litauen eingelegt. Das Oberste Verwaltungsgericht entschied, dass personenbezogene Daten gemäß der Definition von Absatz 1 von Artikel 2 des Gesetzes zum Schutz personenbezogener Daten alle Informationen über eine natürliche Person als Datensubjekt bezeichnen, durch die die betroffene Person direkt oder indirekt zu identifizieren ist (wie z. B. eine persönliche Identifikationsnummer) oder die durch einen oder mehrere Faktoren, die die körperliche, physiologische, geistige, wirtschaftliche, kulturelle oder soziale Identität dieser Person ausmachen, speziell dieser Person zugeordnet werden können. Darüber hinaus enthält Absatz a von Artikel 2 der Richtlinie 95/46/EG eine parallele Definition. Angesichts dieser Definitionen sind Vor- und Nachname sowie Adresse als personenbezogene Daten einzustufen, da eine Person mithilfe dieser Daten identifiziert werden kann. Das Oberste Verwaltungsgericht bemerkte außerdem, dass der Europäische Gerichtshof diese Daten als personenbezogene Daten einstuft (Entscheidung vom 6. November 2003, Aktenzeichen C-101/2001).

Rechte von betroffenen Personen (Datensubjekten)
Bei der Datenschutzbehörde ging eine Beschwerde betreffend die Erfassung der personenbezogenen Daten einer Person aus dem Immobilienregister ein. Die Datenschutzbehörde entschied, dass das Kriterium für eine rechtmäßige Verarbeitung personenbezogener Daten in Artikel 5, Absatz 1, Unterabsatz 6 des Gesetzes zum Schutz personenbezogener Daten beschrieben sei (personenbezogene Daten dürfen verarbeitet werden, wenn die Verarbeitung zur Verfolgung legitimer Interessen des Datenkontrolleurs oder durch Dritte,

denen die personenbezogenen Daten übermittelt wurden, erforderlich ist, sofern diese Interessen nicht von den Interessen der betroffenen Person außer Kraft gesetzt werden). Obwohl der Datenkontrolleur (eine Bank) verpflichtet war, den Beschwerdeführer über die Bedingungen hinsichtlich seiner Rechte zu informieren, versäumte er dies, d. h. der Datenkontrolleur informierte den Beschwerdeführer nicht über sein Recht auf Zugang zu seinen personenbezogenen Daten im Immobilienregister und informierte ihn überdies auch nicht über sein Recht auf Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten. Aus diesem Grund wies die Datenschutzbehörde den Datenkontrolleur an, dafür Sorge zu tragen, dass Artikel 18, Absatz 2, Unterabsätze 2 und 3 (das Recht, über die Verarbeitung der eigenen personenbezogenen Daten Bescheid zu wissen (darüber informiert zu sein) sowie Artikel 21, Absatz 1 (das Recht auf Widerspruch gegen die Verarbeitung der eigenen personenbezogenen Daten) des Gesetzes zum Schutz personenbezogener Daten (in der bis zum 31. Dezember 2008 geltenden Fassung) künftig eingehalten werden.

Der Datenkontrolleur legte auf der Grundlage der in Artikel 17, Absatz 2, Unterabsatz 5 des Gesetzes zum Schutz personenbezogener Daten genannten Ausnahme (die besagt, dass der Datenkontrolleur der betroffenen Person die Bestimmungen zur Wahrnehmung der in diesem Artikel festgelegten Rechte mitteilen muss, mit Ausnahme der gesetzlich geregelten Fälle, in denen der Schutz der Rechte und Freiheiten der betroffenen oder anderer Personen erforderlich ist) vor Gericht Berufung gegen die Anweisung der Datenschutzbehörde ein.

Das Verwaltungsgericht Wilna entschied, dass der Standpunkt der Datenschutzbehörde unlogisch ist, dass die Verarbeitung der personenbezogenen Daten rechtmäßig ist, gleichzeitig aber ein Verstoß gegen Artikel 18, Absatz 2, Unterabsätze 2 und 3 des Gesetzes zum Schutz personenbezogener Daten (in der bis zum 31. Dezember 2008 geltenden Fassung) vorliegt. Die Ansicht der Datenschutzbehörde, dass der Datenkontrolleur legitime Interessen hinsichtlich der Verarbeitung der personenbezogenen Daten hatte und dass diese Interessen nicht von den Interessen der betroffenen Person außer Kraft gesetzt wurden, berücksichtigt nicht die Verpflichtung des Datenkontrolleurs, die betroffene Person darüber zu informieren, dass ihre personenbezogenen Daten verarbeitet werden. Gemäß Artikel 17, Absatz 2, Unterabsatz 5 des Gesetzes zum Schutz personenbezogener Daten muss der Datenkontrolleur der betroffenen Person die Bestimmungen zur Wahrnehmung der in diesem Artikel festgelegten Rechte mitteilen, **mit Ausnahme der gesetzlich geregelten Fälle**, in denen der Schutz der Rechte und Freiheiten der betroffenen oder anderer Personen erforderlich ist. Das Verwaltungsgericht Wilna kam zu dem Schluss, dass die festgestellten faktischen Umstände die legitimen Interessen des Datenkontrolleurs rechtfertigen und im Einklang mit Artikel 17, Absatz 2, Unterabsatz 5 des Gesetzes zum Schutz personenbezogener Daten stehen. Die Anweisung der Datenschutzbehörde wurde dementsprechend aufgehoben.

Gegen die Entscheidung des Bezirksverwaltungsgerichts Wilna wurde Berufung beim Obersten Verwaltungsgericht von Litauen eingelegt. Das Oberste Verwaltungsgericht stimmte der Argumentation der Datenschutzbehörde zu, derzufolge eine Entscheidung zur Verarbeitung personenbezogener Daten gemäß Artikel 5 des Gesetzes zum Schutz personenbezogener Daten (Kriterium für die rechtmäßige Verarbeitung personenbezogener Daten) nicht unterstellt, dass eine Verarbeitung personenbezogener Daten entsprechend aller in diesem Gesetz genannten Verfahren erfolgt ist. Dementsprechend gab es keine Rechtsgrundlage für die Entscheidung des erstinstanzlichen Gerichts, dass ein Verstoß gegen die Bedingungen zur Regelung der Rechte der betroffenen Personen vorliegt, da die Datenschutzbehörde entschieden hatte, dass ein Kriterium für die rechtmäßige Verarbeitung personenbezogener Daten vorgelegen hatte und eingehalten worden war.

Gemäß Artikel 17, Absatz 2, Unterabsatz 5 des Gesetzes zum Schutz personenbezogener Daten muss der Datenkontrolleur der betroffenen Person die Bestimmungen zur Wahrnehmung der in diesem Artikel festgelegten Rechte mitteilen, mit Ausnahme der **gesetzlich geregelten** Fälle, in denen der Schutz der Rechte und Freiheiten der betroffenen oder anderer Personen erforderlich ist. Aus diesem Grund sollte das Recht des Datenkontrolleurs, die betroffene Person nicht über die Bedingungen für die Wahrnehmung ihrer

Rechte zu informieren, an zwei Bedingungen geknüpft sein: (1) ein solches Recht des Datenkontrolleurs muss gesetzlich geregelt sein und (2) diese Tätigkeiten müssen zur Gewährleistung des Schutzes der Rechte und Freiheiten der betroffenen oder anderer Personen erforderlich sein. Mit anderen Worten: Es reicht nicht aus, dass der Datenkontrolleur diese Ausnahmeregelung nur in Anspruch nehmen will, um zu versuchen, die Rechte und Freiheiten der betroffenen Personen zu schützen. Zusätzlich muss ein solches Recht eines Datenkontrolleurs in einem Rechtsinstrument verankert sein. Das erstinstanzliche Gericht könne nicht entscheiden, dass diese Ausnahmeregelung ohne Angabe des anderen spezifischen Gesetzes angewendet werden müsse, da Artikel 17, Absatz 2, Unterabsatz 5 des Gesetzes zum Schutz personenbezogener Daten eine direktive Rechtsvorschrift ist.

Das Oberste Verwaltungsgericht entschied außerdem, dass der Datenkontrolleur bei der Bereitstellung sämtlicher schriftlicher Erläuterungen im Rahmen der Untersuchung der Beschwerde gegenüber der Datenschutzbehörde nicht auf diese Ausnahme hingewiesen habe und spätere Argumentationen zur Anwendung der Ausnahmeregelung als Absicht interpretiert werden könnten, sich der Verantwortung zu entziehen.

C. Wichtige spezifische Themen

Vorbeugende Maßnahmen

Kapitel 3 des Gesetzes zum Schutz personenbezogener Daten regelt den Bereich Videoüberwachung. Um festzustellen, in welchem Umfang die Rechte von betroffenen Personen bei der Verarbeitung von Bilddaten geschützt werden, führte die Datenschutzbehörde Prüfungen an 92 Tankstellen durch.

33 dieser 92 Tankstellen nutzen keine Videoüberwachung. Verstöße gegen das Gesetz zum Schutz personenbezogener Daten wurden an 57 Tankstellen festgestellt.

Gemäß Artikel 31 des Gesetzes zum Schutz personenbezogener Daten dürfen personenbezogene Daten nur dann automatisch verarbeitet werden, wenn der Datenkontrolleur oder sein Vertreter die Datenschutzbehörde darüber in Kenntnis setzt. Die Datenschutzbehörde war lediglich von zwei der untersuchten Tankstellen über die Videoüberwachung informiert worden. An 55 weiteren Tankstellen wurden die Bilddaten ohne Information der Datenschutzbehörde verarbeitet (11 dieser 55 Tankstellen informierten die Datenschutzbehörde im Laufe der Prüfungen).

Es wurde festgestellt, dass die Tankstellen ihre Verpflichtungen zur Gewährleistung des Rechts der betroffenen Personen auf Information über die Verarbeitung ihrer personenbezogenen Daten nicht ordnungsgemäß einhielten. 47 Tankstellen informieren die betroffenen Personen mit speziellen Hinweisschildern über die Videoüberwachung, bieten jedoch keine Informationen zum Datenkontrolleur und seinen in Artikel 20, Absatz 1 des Gesetzes zum Schutz personenbezogener Daten festgelegten Pflichten. 27 Tankstellen weisen zwar auf die Videoüberwachung hin, jedoch an ungeeigneten Orten, d. h. dass die betroffenen Personen beispielsweise erst beim Eintritt in den überwachten Bereich über die Videoüberwachung informiert werden.

Gemäß Artikel 20, Absatz 3 des Gesetzes zum Schutz personenbezogener Daten muss das Personal im Falle einer Videoüberwachung am Arbeitsplatz sowie in den Geschäftsräumen bzw. auf dem Gründstück des Datenkontrolleurs, in denen bzw. auf dem dessen Personal arbeitet, gemäß dem in Artikel 24, Absatz 1 dieses Gesetzes festgelegten Verfahren schriftlich über die Verarbeitung ihrer Bilddaten informiert werden. Es wurde festgestellt, dass lediglich das Personal von 31 Tankstellen schriftlich über die Verarbeitung seiner Bilddaten informiert worden war.

An 37 Tankstellen wird das Recht der betroffenen Personen auf Zugang zu ihren personenbezogenen Daten respektiert, und die betroffenen Personen werden darüber informiert, wie die Daten verarbeitet werden. 15 hiervon fordern jedoch von den betroffenen Personen einen begründeten Antrag, wenngleich Artikel 25 des Gesetzes zum Schutz personenbezogener Daten besagt, dass betroffene Personen durch Vorlage ihres Ausweisdokuments und eines schriftlichen Antrags beim Datenkontrolleur das Recht auf Zugang haben. Ein begründeter Antrag ist also nicht erforderlich.

Gemäß Artikel 18, Absatz 1 des Gesetzes zum Schutz personenbezogener Daten muss die Verarbeitung von Bilddaten in einem schriftlichen Dokument des Datenkontrolleurs geregelt sein. Dieses Dokument muss Zweck und Umfang der Videoüberwachung, die Dauer der Vorratsspeicherung der Daten, die Bedingungen für den Zugang zu den verarbeiteten Bilddaten, die Bedingungen und Verfahren für die Vernichtung dieser Daten sowie sonstige Voraussetzungen für eine legitime Verarbeitung von Videodaten enthalten. Es wurde festgestellt, dass an 25 Tankstellen kein entsprechendes Dokument vorgelegt werden konnte. An 28 Tankstellen konnte zwar ein entsprechendes Dokument vorgelegt werden, es entsprach jedoch nicht den Anforderungen von Artikel 18, Absatz 1 des Gesetzes zum Schutz personenbezogener Daten.

Die untersuchten Tankstellen wurden über ihre Verstöße gegen das Gesetz zum Schutz personenbezogener Daten aufgeklärt.

Sensibilisierung der Öffentlichkeit

Europäischer Datenschutztag

Am 28. und 29. Januar 2009 wurde der Europäische Datenschutztag gefeiert. Am 28. Januar 2009 wurde ein Treffen mit Vertretern anderer staatlicher Organisationen und Agenturen organisiert, die sich mit verschiedenen Fragen zum Schutz personenbezogener Daten befassten. Die Vertreter des öffentlichen Sektors wurden über den vor kurzem eingeführten Datenschutztag in Europa, seine Ziele und aktuelle Fragen informiert. Außerdem wurde ihnen ein Überblick über die Datenschutzbehörde verschafft.

Im Rahmen des Projekts „Mano teisės" („Meine Rechte") des Zentrums für Menschenrechte wurde eine e-Konferenz organisiert. Die Antworten auf die Fragen zum Schutz personenbezogener Daten, die dem Direktor der Datenschutzbehörde Algirdas Kunèinas betreffend den elektronischen Arbeitsplatz, Videoüberwachung, Direktwerbung, vernichtete Dokumente, die Zuständigkeit der Datenschutzbehörde sowie die Prozentsätze der für die unrechtmäßige Veröffentlichung personenbezogener Daten verhängten Bußgelder gestellt wurden, sind auf der Website abrufbar.

Darüber hinaus beging die Datenschutzbehörde den Europäischen Datenschutztag am 29. Januar 2009 mit einer Gruppe Bibliothekare in der öffentlichen Bibliothek „Adomas Mickevièius" im Bezirk Wilna.

Die Konferenz befasste sich unter anderem mit sensiblen Fragen für Bibliotheken in Bezug auf den Schutz personenbezogener Daten. Auf der Veranstaltung wurden die wichtigsten Fragen zum Schutz personenbezogener Daten von den Vertretern von Bibliotheken in einem breiteren Kontext beleuchtet. Der Schwerpunkt lag hierbei auf einer Sensibilisierung im Bereich des Schutzes der Privatsphäre. Eine Stunde vor Beginn der Konferenz boten die Anwälte der Datenschutzbehörde Angestellten und Nutzern von Bibliotheken Rechtsberatung und Konsultationen zu Fragen bezüglich der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre an.

Zahlreiche Flugblätter und Informationsbroschüren zu den Fragen des Tages wurden gedruckt und verteilt: „Kennen Sie Ihre Rechte als Datensubjekt?", „Schutz personenbezogener Daten und Videoüberwachung", „Schutz personenbezogener Daten für Nutzer von Drahtlosnetzwerken".

Konferenz „Der Schutz der Privatsphäre und personenbezogener Daten in Litauen"

Die Datenschutzbehörde organisierte am 26. November 2009 gemeinsam mit der Aktiengesellschaft „Expozona" eine Konferenz mit dem Titel „Der Schutz der Privatsphäre und personenbezogener Daten in Litauen". Ziel dieser Veranstaltung war die Einführung von Vertretern des öffentlichen und privaten Sektors in das Thema Privatsphäre und Datenschutz im Hinblick auf die Privatsphäre von Angestellten, die Einziehung von Forderungen und Videoüberwachung. Neben Rednern der Datenschutzbehörde nahmen auch Redner von Stromversorgungsunternehmen (UAB „Eastern Distribution Networks"), von Inkassobüros (UAB „Ekskomisarø biuras") sowie von der Kommunalverwaltung der Stadt Wilna an der Veranstaltung teil. Es wurden sieben Vorträge zu den folgenden Themen gehalten:

- Entwickeln wir uns zu einer Gesellschaft im Stile des Buches „1984"? (Privatsphäre und Öffentlichkeit

in der Informationsgesellschaft: Tendenzen und Bedrohungen);
- Auch ein Angestellter hat ein Recht auf Privatsphäre;
- Verarbeitung personenbezogener Daten: Wie kann sie bei der Entwicklung von Kundenbeziehungen helfen?
- Verarbeitung personenbezogener Daten und Probleme bei der Einziehung von Forderungen;
- Gesetzliche Regelung der Videoüberwachung;
- Allgemeine Anforderungen an organisatorische und technische Datenschutzmaßnahmen;
- Videoüberwachungssysteme in der Stadt Wilna: Gegenwart und Zukunft.

Darüber hinaus wurde diskutiert, und die Konferenzteilnehmer konnten Fragen stellen und ihre Meinungen zu den jeweiligen Themen äußern.

Die Datenschutzbehörde veröffentlichte eine Empfehlung zum *„Schutz der Privatsphäre bei Videoüberwachungssystemen. Drahtlose Kommunikationstechnologien"* (16. Dezember 2009). Die Empfehlung erläutert, wie die Privatsphäre auch bei Einsatz von Videoüberwachungskameras, Webcams und anderen Videoüberwachungsgeräten geschützt werden kann, befasst sich mit den Risiken des Einsatzes dieser Geräte und beschreibt mögliche organisatorische und technische Datenschutzmaßnahmen.

Der vollständige Wortlaut dieser Empfehlung ist (nur auf Litauisch) abrufbar unter: http://www.ada.lt/images/cms/File/naujienu/IP%20kamera%20(Galutinis)%2020091216.doc

Die Datenschutzbehörde veröffentlichte am 23. Dezember 2009 eine Empfehlung „zum sicheren Datentransfer über das https-Protokoll". Sie befasst sich unter anderem mit der Einrichtung eines https-Protokolls, der Wirkung eines https-Protokolls sowie mit Arten von SSL-Zertifikaten. Der vollständige Wortlaut dieser Empfehlung ist (nur auf Litauisch) abrufbar unter: http://www.ada.lt/images/cms/File/Inspekcijos%20rekomendacijos/SSL20091228.doc.

Luxemburg

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

Gesetz vom 2. August 2002 über den Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten (Umsetzung der Richtlinie 95/46/EG)

Im Jahr 2009 gab es keine Änderungen an oben genanntem Gesetz.

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

Im Jahr 2009 gab es keine Änderungen an oben genanntem Gesetz.

Verordnungen und abgeleitetes Recht
Die großherzogliche Verordnung vom 13. Februar 2009 zur Einführung des *„Dienstleistungsschecks"* im Bereich der Tagesstätten legt die Einzelheiten zur Schaffung und Nutzung einer Datenbank betreffend diese *„Dienstleistungsschecks"* fest.

Eine Ministerialverordnung vom 10. November 2009 änderte die Bestimmungen der großherzoglichen Verordnung vom 1. August 2007 und gestattete die Entwicklung und Verwendung eines Videoüberwachungssystems in öffentlichen *„Sicherheitsbereichen"* durch die Polizei. Die Ministerialverordnung definiert zu den drei bereits existierenden Sicherheitsbereichen, in denen eine von der Polizei betriebene permanente Videoüberwachung stattfindet, einen weiteren neuen „Sicherheitsbereich".

Die Bedingungen für die Herausgabe von Katasterdokumenten (Grundbuchamt) wurden in den Bestimmungen der großherzoglichen Verordnung vom 9. März 2009 erläutert.

Außerdem hat die Regierung die großherzogliche Verordnung vom 3. Dezember 2009 veröffentlicht, die die Verfahren beschreibt, die zur Feststellung des Todes einer Person angewendet werden müssen, bevor dem Körper dieser Person Stoffe und Proben entnommen werden.

Weitere Entwicklungen in der Gesetzgebung
Im Jahr 2009 beriet die Datenschutzkommission (*„Commission nationale"*) die luxemburgische Regierung zu zahlreichen Themen. Am wichtigsten waren hierbei das Gesetz zur *„Identifizierung natürlicher Personen, zum nationalen Register natürlicher Personen sowie zum Ausweis"*, die oben genannte großherzogliche Verordnung zur Einführung des *„Dienstleistungsschecks"* im Bereich der Tagesstätten, das Gesetz zur Änderung des Gesetzes über die *„Bedingungen, unter denen Richter und Polizeibeamte Zugang zu bestimmten Datenbanken öffentlicher juristischer Personen erhalten können"*, der Entwurf einer großherzoglichen Verordnung zur Regelung der zwischenbehördlichen Zusammenarbeit sowie das Gesetz zum Austausch bestimmter Informationen aus dem Steuerbereich und die Unterzeichnung bilateraler Doppelbesteuerungsabkommen.

Die luxemburgische Datenschutzbehörde beriet darüber hinaus auch den luxemburgischen Verband für Angestellte von Banken und Versicherungen (ALEBA) im Hinblick auf das Problem privater Transaktionen ihrer Angestellten.

B. Bedeutende Rechtsprechung

Zivil- und Strafverfahren
Entscheidung des Bezirksgerichts Luxemburg, 9. Strafkammer, über die Gültigkeit von unter Verletzung des Datenschutzgesetzes von 2002 gesammelten Beweisen (Videoüberwachungsbilder)

Die Anwälte von vier Angeklagten, die beschuldigt wurden, Zigaretten und Alkohol an Tankstellen in ganz Luxemburg gestohlen zu haben, beantragten vor der Streitsache (*„in limine litis"*), dass die als Beweis gegen ihre Mandanten verwendeten Videoaufzeichnungen nicht zugelassen werden dürften, da im Vorfeld keine Genehmigung durch die Datenschutzbehörde erteilt worden war. Daher kamen sie zu dem Schluss, dass diese Beweise als nichtig einzustufen seien und dass das Strafverfahren gegen ihre Mandanten einzustellen sei. Das Gericht entschied unter Berufung auf das „Privateigentum" und die Öffnungszeiten der Tankstellen

sowie auf den allgemeinen Zweck des Gesetzes von 2002 (dessen Absicht nicht der Schutz illegaler Aktivitäten ist), dass die Aufzeichnungen dennoch als Beweismittel verwendet werden können. Es wird darauf hingewiesen, dass sich die Richter in diesem Fall nicht auf eine spezielle Bestimmung des Gesetzes, sondern sich lediglich auf vage rechtliche Konzepte beriefen, die sie aus ihrer eigenen Weltanschauung ableiteten. Diese Konzepte stehen in direktem Gegensatz zu früherer Rechtsprechung. Eine derart voreingenommene Interpretation vermindert eindeutig die vom Gesetz gewährte Sicherheit, und man muss hoffen, dass die Berufungsrichter sich bei ihrer Urteilsfindung zu dieser Frage auf eine ordentliche Rechtsgrundlage des Gesetzes berufen.

C. Wichtige spezifische Themen

Verbindliche Unternehmensregeln (BCR) von eBay genehmigt

Die Datenschutzbehörde, die in diesem Fall zum ersten Mal als leitende Behörde tätig war, genehmigte den Antrag von eBay hinsichtlich der Einhaltung der Datenschutzgesetze durch die verbindlichen Unternehmensregeln sowohl betreffend Kunden- als auch Angestelltendaten.

Nach einer überaus konstruktiven und offenen Zusammenarbeit mit eBay sowie der schnellen Kontaktaufnahme (im Rahmen des Verfahrens zur gegenseitigen Anerkennung) mit den Datenschutzbehörden von 13 anderen Mitgliedstaaten konnte die Datenschutzbehörde das Genehmigungsverfahren hinsichtlich der verbindlichen Unternehmensregeln in weniger als 12 Monaten abschließen.

Google Street View

Google Inc. kontaktierte die Datenschutzbehörde im Hinblick auf die für seinen Dienst „Google Street View" geltenden speziellen nationalen Datenschutzbestimmungen und -anforderungen. Google möchte diesen Dienst in Luxemburg starten.

Die Datenschutzbehörde folgte dem von verschiedenen Datenschutzbehörden im Februar 2009 angenommenen Standpunkt und entschied, dass die erfassten und veröffentlichten Bilder nicht im Konflikt mit den luxemburgischen Datenschutzgesetzen stehen dürfen und dass Google strenge Sicherheitsmaßnahmen einführen und insbesondere gewährleisten müsse, dass die Rechte der betroffenen Personen gewahrt werden.

Insbesondere müsste das Recht auf Widerspruch gegen eine solche Verarbeitung von Daten von Google streng eingehalten und das Widerspruchsverfahren so einfach wie möglich gestaltet werden. Die Datenschutzbehörde entwarf und veröffentlichte einen Musterbrief für alle betroffenen Personen, die Widerspruch gegen die Verarbeitung ihrer Daten einlegen wollen. Die betroffenen Personen müssen Google Inc. diesen Brief lediglich zuschicken.

Im Mai 2009 musste die Datenschutzbehörde die Erfassung von Bildern auf luxemburgischen Gebiet durch den Dienst „Google Street View" einstellen, da bestimmte Bedingungen und Voraussetzungen der Datenschutzbehörde nicht erfüllt worden waren. Insbesondere hatte sich Google nicht an die Verpflichtung gehalten, die genauen Zeiträume, zu denen die Fahrzeuge von Google die Bilder erfassen sollten, über die nationalen Medien oder das Internet zu veröffentlichen.

Nach Erfüllung aller Voraussetzungen durfte Google die Erfassung der Bilder im August 2009 in sieben luxemburgischen Gemeinden fortsetzen. Die Datenschutzbehörde verfolgt derzeit sämtliche Entwicklungen im Hinblick auf diesen Dienst mit zunehmender Aufmerksamkeit.

Untersuchung der wichtigsten luxemburgischen Telekommunikationsunternehmen

Im Laufe des Jahres 2009 führte die Datenschutzbehörde eine umfassende Untersuchung der wichtigsten luxemburgischen Telekommunikationsunternehmen zur *„Einhaltung der rechtlichen Anforderungen hinsichtlich der Vertraulichkeit und der Sicherheitsmaßnahmen für Verbindungsdaten"* durch. Im Rahmen dieser Untersuchung befasste man sich auch mit Fragen zur Vorratsspeicherung von Daten gemäß den von der Artikel-29-Datenschutzgruppe festgelegten Anforderungen der gemeinsamen Vollstreckungsmaßnahmen der Datenschutzbehörden.

Malta

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

Richtlinie 95/46/EG wurde im Rahmen des Datenschutzgesetzes, Kapitel 440 der maltesischen Gesetze, in maltesisches Recht umgesetzt. Das Gesetz trat im Juli 2003 vollständig in Kraft und sah für Meldungen automatischer Datenverarbeitungsprozesse eine Übergangsphase bis Juli 2004 vor. Bestimmte Vorschriften über manuelle Ablagesysteme traten spätestens im Oktober 2007 in Kraft.

Die Richtlinie 2002/58/EG wurde teils im Rahmen des Datenschutzgesetzes durch die Umsetzung der Verordnungen zur Verarbeitung personenbezogener Daten im Bereich elektronischer Kommunikation (gesetzliche Mitteilung 16 aus dem Jahr 2003) und teils im Rahmen des Gesetzes über elektronische Kommunikation durch die Umsetzung der Telekommunikationsverordnungen über personenbezogene Daten und den Schutz der Privatsphäre (gesetzliche Mitteilung 19 aus dem Jahr 2003) in Kraft gesetzt; die ergänzende Gesetzgebung trat im Juli 2003 in Kraft.

Weitere Entwicklungen in der Gesetzgebung

Keine nennenswerten im Berichtsjahr.

B. Bedeutende Rechtsprechung

Keine nennenswerte im Berichtsjahr.

C. Wichtige spezifische Themen

Im Laufe des Jahres 2009 gingen 54 Beschwerden bei der Datenschutzbehörde ein. Dies veranlasste den Datenschutzbeauftragten, jeden Fall auf der Grundlage der ihm per Gesetz übertragenen Befugnisse zu untersuchen und seine jeweilige Entscheidung hinsichtlich des Untersuchungsergebnisses zu kommunizieren. Gegen keine der Entscheidungen wurde Berufung vor dem Berufungsrat für Datenschutz eingelegt. Die meisten Fragen der Beschwerdeführer betreffen die Installation von Überwachungskameras durch Privatpersonen sowie den Versand elektronischer Nachrichten zu Werbezwecken (Direktwerbung), ohne dass hierbei die gesetzlichen Anforderungen erfüllt werden. Im Berichtszeitraum führte der Datenschutzbeauftragte zahlreiche Prüfungen von Verarbeitungen personenbezogener Daten durch Datenkontrolleure durch. Diese Prüfungen wurden auf Anregung des Datenschutzbeauftragten sowie zur Einhaltung der europäischen Verpflichtungen als Teil der Strategie der Datenschutzbehörde zur Bewertung einer bestimmten Branche im Rahmen von Untersuchungen hinsichtlich eingegangener Beschwerden durchgeführt. Die Datenkontrolleure haben auch Anträge auf Vorprüfung betreffend die Einführung biometrischer Systeme am Arbeitsplatz sowie dort, wo die Verarbeitung von Daten ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen mit sich bringt, eingereicht.

Im Berichtsjahr organisierte die Datenschutzbehörde regelmäßige Treffen mit Vertretern aus verschiedenen Branchen mit dem vorrangigen Ziel, die für die jeweilige Branche relevanten datenschutzbezogenen Themen zu diskutieren. Die anhaltenden Bemühungen, mit den Branchen zu kommunizieren, erzeugen ein hohes Maß an positiven Rückmeldungen, die die Datenschutzbehörde zur Entwicklung von Richtlinien und Verhaltensregeln benötigt, die letztlich für alle Branchen maßgeblich sein sollen. Diesbezüglich wurden Treffen mit verschiedenen eingesetzten Behörden und Vertretern aus den Bereichen Bildung, Sozialarbeit, Telekommunikation, Tourismus, Medien, Finanzdienstleistungen und Gesundheit organisiert. Außerdem fanden Diskussionen mit verschiedenen Behörden wie beispielsweise der maltesischen Kommunikationsbehörde, der maltesischen Behörde für Finanzdienstleistungen, der maltesischen Ressourcenbehörde und der maltesischen Verkehrsbehörde statt. Der Datenschutzbeauftragte organisierte auch Treffen mit dem Bürgerbeauftragten, hochrangigen Beamten der maltesischen Polizei sowie Beamten der maltesischen Sicherheitsdienste.

Im Laufe des Jahres hat die Datenschutzbehörde durch die Teilnahme an der Artikel-29-Datenschutzgruppe, der Europäischen Konferenz der Datenschutzbehörden, der Internationalen Konferenz zur Privatsphäre und zum Schutz personenbezogener Daten, an Treffen der

gemeinsamen Aufsichtsbehörden für das Schengener Abkommen, den Zoll, Europol und Eurodac, am Workshop zur Fallbehandlung und an Eurojust (Europarat) sowie an der Arbeit des Büros des Beratungsausschusses der Konvention zum Schutz von Privatpersonen im Hinblick auf die automatische Erfassung personenbezogener Daten ihren Beitrag zu europäischen und internationalen Foren geleistet.

Im Einklang mit der Strategie der Datenschutzbehörde zur Sensibilisierung für das Thema Datenschutz wurden Informationsschreiben an zahlreiche Organisationen und Verfassungsbehörden verschickt, um wichtige Vertreter in die Entwicklung einer Datenschutzkultur einzubeziehen. In der lokalen Presse sowie in Rundfunk und Fernsehen wurden Artikel und Beiträge zu verschiedenen Aspekten des Datenschutzes abgedruckt bzw. ausgestrahlt. Die Bürger werden sich ihrer Rechte immer bewusster. Dies lässt sich an der Anzahl von sowohl telefonischen als auch per E-Mail im Berichtszeitraum bei der Datenschutzbehörde eingegangenen Anfragen ablesen.

Im Hinblick auf die aktuelle Richtlinie des Europäischen Parlaments und des Rates, die unter anderem die Richtlinie 2002/58/EG ändert, nahm die Datenschutzbehörde Diskussionen mit der maltesischen Kommunikationsbehörde auf, um die von der Richtlinie eingeführten Änderungen in die betreffenden nationalen Rechtsinstrumente umzusetzen. Voraussichtlich Anfang des nächsten Jahres werden beide Behörden eine Reihe von Treffen mit Unternehmen organisieren, um Rückmeldungen zu den neuen und geänderten Bestimmungen einzuholen. Diese Konsultation soll positive Ergebnisse liefern und so eine reibungslose und effektive Umsetzung sicherstellen.

Am 28. Januar feierte der Datenschutzbeauftragte zusammen mit den anderen europäischen Datenschutzbehörden den Europäischen Datenschutztag. An diesem Tag verteilte die Datenschutzbehörde Informationsmaterial an Schüler in allen staatlichen, privaten und kirchlichen Schulen. Es ist keine einfache Aufgabe, die Botschaft zu vermitteln und Bürger, insbesondere die jungen, für die Risiken zu sensibilisieren, die mit der Bereitstellung personenbezogener Daten im Internet einhergehen können. Die Datenschutzbehörde war schon immer der festen Überzeugung, dass eine effektive Veränderung der Kultur nur durch andauernde Investitionen in die junge Generation zu erreichen ist. Die Kinder von heute sind unsere Zukunft. Die Veränderung einer Kultur braucht Zeit. Die Konsolidierung aller Elemente des Bereichs Privatsphäre wird jedoch letztlich die gewünschten Ergebnisse liefern. Angesichts der zunehmend verfügbaren Anwendungen zur sozialen Vernetzung verschwimmen die Grenzen der Privatsphäre. Die Datenschutzbehörde hat sich zur Aufgabe gemacht, die Privatsphäre diesbezüglich zu stärken und sich dabei vom Kernkonzept einer vernünftigen Erwartung an den Schutz der Privatsphäre leiten zu lassen.

Nach dem viel zu frühen Tod von Herrn Paul Mifsud Cremona wurde Herr Joseph Ebejer im Februar dieses Jahres formal für eine Amtszeit von fünf Jahren zum Datenschutzbeauftragten ernannt.

Niederlande

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

Die Richtlinie 95/46/EG wurde per *Wet bescherming persoonsgegevens* (Wbp, niederländisches Datenschutzgesetz) in nationales Recht umgesetzt. Das Gesetz vom 6. Juli 2000[21] trat am 1. September 2001 in Kraft und ersetzte damit das alte Datenschutzgesetz *Wet persoonsregistraties* (Wpr) vom 28. Dezember 1988.

Die Richtlinie 2002/58/EG wurde insbesondere durch das geänderte Telekommunikationsgesetz (*Telecommunicatiewet*), das am 19. Mai 2004[22]. in Kraft trat, in niederländisches Recht umgesetzt. Andere Rechtsvorschriften, die diese Richtlinie zum Teil übernommen haben, sind unter anderem das *Wet op de Economische Delicten* (Gesetz über Wirtschaftsvergehen), das den Artikel 13(4) der Richtlinie 2002/58/EG umsetzt.

B. Bedeutende Rechtsprechung

Derzeit findet eine Bewertung des niederländischen Datenschutzgesetzes statt. Angesicht einer möglichen Revision des Gesetzes hat die niederländische Datenschutzbehörde [College bescherming persoonsgegevens (CBP)] die Bedeutung einer Stärkung der Position der Datensubjekte betont. Sie sollten leicht auf Informationen darüber zugreifen können, warum ihre personenbezogenen Daten verarbeitet werden, welche Maßnahmen zur Vermeidung einer illegalen Verwendung dieser Daten ergriffen wurden und wie sie ihre Rechte wahrnehmen können. Zusätzlich sollten leicht zugängliche Beschwerdeverfahren sowie die Möglichkeit von Sammelklagen entwickelt/eingeführt werden.

Hinsichtlich der Position des Datenkontrolleurs vollzieht sich gerade eine Änderung von einer Ex-ante-Kontrolle hin zu einer Ex-post-Kontrolle. Die Datenkontrolleure sollten mehr in die Einhaltung des Gesetzes investieren und stärker für Nichteinhaltungen zur Kasse gebeten werden. Die Datenschutzbehörde unterstützt eine verbesserte Transparenz, eine Voraussetzung für die Meldung von Verstößen gegen das Datenschutzgesetz sowie die Anwendung des Prinzips „Privacy by Design". Letztlich sollte die Position der Aufsichtsbehörde selbst durch die Übertragung zusätzlicher Befugnisse an die Datenschutzbehörde gestärkt werden.

Zusätzlich zu ihrer Arbeit als Beratungsgremium für die Regierung hinsichtlich neuer Datenschutzgesetze behandelt die Datenschutzbehörde im Rahmen ihrer Aufsichtsfunktion Vollstreckungsmaßnahmen vorrangig, um so einen möglichst effektiven Beitrag zur Förderung der Einhaltung des Datenschutzgesetzes zu leisten. Zum Zweck der Festlegung der Prioritäten für das Jahr 2009 wurde eine Risikoanalyse betreffend die Verarbeitung personenbezogener Daten in unterschiedlichen Bereichen der Gesellschaft durchgeführt. Dementsprechend befasste sich die Datenschutzbehörde mit Fällen, bei denen es Anzeichen für schwerwiegende Verstöße gegen das Datenschutzgesetz gab, die struktureller Natur waren, viele Bürger betrafen und bei denen die Datenschutzbehörde die Befugnis hat, Maßnahmen zu ergreifen. Außerdem verfolgte die Datenschutzbehörde im Laufe des Jahres die aktuellen Themen. Die von der Datenschutzbehörde durchgeführten Untersuchungen und Maßnahmen (108 im Jahr 2009) brachten nicht nur Ergebnisse im Hinblick auf die jeweiligen Datenkontrolleure, sondern schienen auch indirekte Auswirkungen zu haben. Die thematischen Leitlinien für das Jahr 2009 umfassten die Verpflichtung zu Information und Transparenz bezüglich der Übermittlung personenbezogener Daten an Dritte.

C. Wichtige spezifische Themen

Das Internet

Nach der Untersuchung eines Internetunternehmens kam die Datenschutzbehörde zu dem Schluss, dass das Unternehmen durch die Erfassung sensibler Daten zu Personen, die Internetplattformen nutzen, und den anschließenden Verkauf der profilierten

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

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

personenbezogenen Daten an Dritte ohne eine klare und vollumfängliche Information der betroffenen Personen gegen das Gesetz verstoßen habe. Zu diesem Zeitpunkt besuchten etwa 2,2 Millionen Menschen die Internetseiten dieses Unternehmens. Das Unternehmen bot ihnen die Möglichkeit, einen Test durchzuführen, z. B. mit dem Titel „Finden Sie heraus, wie alt Sie wirklich sind". Die Untersuchung zeigte, dass das Internetunternehmen unter anderem medizinische Daten erfasst und verarbeitet hatte, obwohl eine solche Tätigkeit prinzipiell gesetzlich verboten ist. Das Internetunternehmen informierte die betroffenen Personen nicht gemäß den gesetzlichen Anforderungen über die Verwendung ihrer Daten.

Eine Website für Schüler, auf der diese ihre Lehrer bewerten können, hat die Privatsphäre der betroffenen Lehrer erheblich verletzt. Nach einer Untersuchung durch die Datenschutzbehörde wurde die Website abgeändert und kann nun nicht mehr über Suchmaschinen gefunden werden.

Die Datenschutzbehörde untersuchte auch zwei Websites für junge Menschen. Das soziale Netzwerk www.zikle.nl wurde aufgefordert, seine Nutzer angemessen über die Zwecke zu informieren, zu denen personenbezogene Daten erfasst und verarbeitet werden, Sicherheitsmaßnahmen umzusetzen und Seiten mit persönlichen Profilen zu verbergen. www.jiggy.nl versuchte seine Nutzer mithilfe eines Spiels dazu zu bewegen, E-Mail-Adressen von anderen Personen zu Werbezwecken (Direktwerbung) anzugeben. Nach der Untersuchung entfernte der Betreiber der Website das Spiel.

Finanzdaten

Nach der Einführung des Instruments eines Warnbriefes im Jahr 2008 entwarf die Datenschutzbehörde im Jahr 2009 ihren ersten eigenen Warnbrief auf Antrag des Nationalen Schulden-Informationssystems [Stichting Landelijk Informatiesysteem Schulden (LIS)], auf den nach einem neuen Entwurf des LIS ein zweiter Warnbrief folgte. Von der Datenschutzbehörde durchgeführte Tests zeigten, dass keiner der Entwürfe die gesetzlichen Anforderungen erfüllte. Im Hinblick auf den zweiten Entwurf kam die Datenschutzbehörde zu dem Schluss, dass der Entwurf weit über seinen ursprünglichen Zweck hinausging, nämlich den der Erfassung überfälliger Zahlungen zur Vermeidung problematischer Schuldeneinträge. Dies könnte dazu führen, dass eine nicht unerhebliche Gruppe von Personen erfasst wird, die nicht in das Register gehört, somit aber trotzdem unter den negativen Folgen der Einstufung als problematischer Kreditnehmer zu leiden hat.

Eine Bank hat die Kontonummern und Adressen junger Menschen an eine Wohltätigkeitsorganisation weitergegeben, ohne die betroffenen Personen darüber zu informieren oder ihr Einverständnis einzuholen. Nach einer Beschwerde untersuchte die Datenschutzbehörde die Angelegenheit. Als Folge dieser Untersuchung änderte die Bank ihre Vorgehensweise.

Im Jahr 2009 befolgte der niederländische Finanzminister einen Rat der Datenschutzbehörde betreffend Gesetzesvorschläge zur Einrichtung eines Rentenregisters. Hintergrund ist, dass jeder Bürger seine Rentenansprüche online einsehen können soll. Da diese Daten zweifellos auch für andere Parteien interessant sind, betonte die Datenschutzbehörde die Notwendigkeit strenger Sicherheitsmaßnahmen.

Medizinische Daten

Im Rahmen einer Untersuchung zweier existierender regionaler, elektronischer Systeme für Patientenakten stellte die Datenschutzbehörde einen Verstoß gegen das Datenschutzgesetz fest. Die Datenschutzbehörde leitete Konformitätsverfahren gegen beide Register ein. Diese Verfahren führten zur Einstellung der unrechtmäßigen Tätigkeiten der Register. Unter anderem wurden alle Patienten persönlich über die Erfassung ihrer Daten in den Registern informiert. Die vorgeschlagenen Gesetze über elektronische Patientenakten bieten noch immer Anlass zur Sorge. Kritische Empfehlungen der Datenschutzbehörde zum ursprünglichen Gesetzesvorschlag aus dem Jahr 2007 hatten eine Anpassung des Entwurfs zur Folge. Änderungen durch die Abgeordnetenkammer haben Krankenversicherern in einigen Fällen jedoch ermöglicht, Zugang zu Patientenakten zu erhalten. Die Datenschutzbehörde riet dem Minister, diese Ausnahme zum allgemeinen Verbot zu entfernen. Der Minister hat angedeutet, dass er diesem Rat folgen wird.

Auch die Informationssicherheit in Krankenhäusern bietet Anlass zur Sorge. Von der Datenschutzbehörde und der niederländischen Inspektion für das Gesundheitswesen [Inspectie voor de Gezondheidszorg (IGZ)] in den Jahren 2007 und 2008 durchgeführte Untersuchungen ergaben, dass keines der 20 untersuchten Krankenhäuser den Standard betreffend die Informationssicherheit erfüllte. Im Jahr 2009 verhängte die Datenschutzbehörde ein Bußgeld aufgrund der Nichteinhaltung der Standards gegen vier Krankenhäuser, die die betreffenden Anforderungen noch immer nicht ordnungsgemäß einhielten.

Untersuchungen der Verfahren einer Reihe von Arbeitsschutzdiensten führten zu dem Ergebnis, dass mindestens ein Dienst systematisch gegen das Gesetz verstieß, indem den Arbeitgebern kranker Angestellter medizinische Daten dieser Angestellten übermittelt wurden, obwohl diese Daten der ärztlichen Schweigepflicht unterliegen. Die Datenschutzbehörde verhängte im Jahr 2009 ein Bußgeld aufgrund der Nichteinhaltung der Gesetze durch diesen Arbeitsschutzdienst. Der Arbeitsschutzdienst stellte daraufhin die Verstöße innerhalb des festgelegten Frist ein. Die Untersuchung dreier weiterer Arbeitsschutzdienste wurde fortgesetzt.

Sonstige Aktivitäten im privaten Sektor

Auch wenn wir uns scheinbar daran gewöhnen, so ist die Videoüberwachung immer noch ein weit verbreitetes Phänomen mit weit reichenden Auswirkungen. Bei der Datenschutzbehörde gehen diesbezüglich zahlreiche Fragen von Bürgern ein. Die Datenschutzbehörde untersuchte den Einsatz von Überwachungskameras auf einem Industriegelände. Die Ergebnisse waren für das für die Überwachung verantwortliche Unternehmen generell positiv. Das Unternehmen versprach, die Kontrollvorschriften zu ändern, um sie in Einklang mit den Anforderungen des Datenschutzgesetzes zu bringen. Da nicht immer eindeutig ist, ob private Unternehmen oder Regierungsbehörden für eine Videoüberwachung verantwortlich sind, hat die Datenschutzbehörde entschieden, neue Leitlinien zu diesem Thema zu entwickeln.

Viel Wirbel gab es um die vorgeschlagene Einführung der so genannten „intelligenten" Stromzähler, die ein sehr detailliertes Bild eines Haushalts und somit auch der Zeiträume, in denen die betroffenen Personen nicht zu Hause sind, bieten. Die Verbraucher müssen in der Lage sein, informierte Entscheidungen hinsichtlich der Häufigkeit und der Menge der erfassten Informationen zu treffen. Der Gesetzesentwurf wurde nach Beratung des Ministers durch die Datenschutzbehörde geändert.

Junge Menschen

Die digitale Verarbeitung personenbezogener Daten im Allgemeinen sowie durch die Regierung im Besonderen erfordert klare Sicherheitsvorkehrungen. Dies gilt besonders im Fall von Informationen über Kinder und junge Menschen. Im Jahr 2008 sprach die Datenschutzbehörde einen äußerst dringlichen Rat zu einem Gesetzesvorschlag aus, der die Schaffung eines Referenzindexes für gefährdete junge Menschen [Verwijsindex Risicojongeren] zur Folge hätte. Die Kritik betraf insbesondere den nicht hinreichend spezifischen Gegenstand des Referenzindexes sowie seine unklaren Kriterien für die Erfassung eines jungen Menschen durch seinen Versorgungsanbieter, was ein fast unvermeidliches Risiko für Willkür mit sich bringt. Obwohl der am 6. Februar 2009 eingereichte Gesetzesvorschlag unter anderem die Kritik der Datenschutzbehörde berücksichtigte, blieb er im Wesentlichen leider unverändert. Im Jahr 2009 wurde die Datenschutzbehörde zu einer Reihe von Vollstreckungsmaßnahmen im Rahmen des neuen Gesetzes um Rat gebeten, und sie warnte erneut vor dem Risiko der Willkür.

Grundschulen stellen Entwicklungsberichte über ihre Schüler für Sekundarschulen aus. Die Datenschutzbehörde hat die Einhaltung der Verpflichtung zur Information der Eltern der Kinder in diese Situation untersucht. Dies ist von größter Bedeutung, da nur so die Möglichkeit gegeben ist, einen Bericht zu korrigieren, der langfristige negative Auswirkungen auf das betroffene Kind haben kann, wenn er falsche oder veraltete Informationen enthält. Mehr als die Hälfte der untersuchten Schulen führte keine Aufzeichnungen darüber, ob die Eltern informiert wurden oder nicht. Nach der Untersuchung veröffentlichte die Datenschutzbehörde Leitlinien für Grundschulen zu diesem Thema.

Polizei und Justizbehörden

Die Sicherstellung der korrekten und transparenten Verwendung personenbezogener Daten ist im Hinblick auf die erweiterten Befugnisse wichtig, die Polizei und Justizbehörden bei der Verarbeitung personenbezogener Daten gewährt wurden. In den Jahren 2007 und 2008 untersuchte die Datenschutzbehörde den internen Austausch personenbezogener Daten innerhalb der Polizei über das interne Informationssystem. Die überwältigende Mehrheit der Polizeibezirke war nicht hinreichend ausgerüstet, um die Anforderungen des Polizei-Datenschutzgesetzes [*Wet politiegegevens*] einzuhalten, das am 1. Januar 2008 in Kraft getreten ist. Eine Nachfolgeuntersuchung im Jahr 2009 in drei regionalen Polizeidienststellen zeigte, dass trotz des unterschiedlichen Kontextes keine der Dienststellen die Anforderungen betreffend Genehmigung und Kontrolle erfüllte.

Nachrichtendienste können ihre Informationen direkt mit den Polizeiakten abgleichen. Im Rahmen der Beratung betreffend den Gesetzesvorschlag zu dieser unabhängigen Form der Konsultation von Polizeidatenbanken bat die Datenschutzbehörde die Regierung um Klarstellung, warum solche groß angelegten Konsultationen erforderlich sind.

Im Jahr 2009 entwickelte die Datenschutzbehörde Leitlinien zur automatischen Nummernschilderkennung (ANPR, automated number plate recognition) durch die Polizei. In diesen Leitlinien erläuterte die Datenschutzbehörde ihre Interpretation der gesetzlichen Standards als Aufsichtsbehörde bei der Ausübung ihrer Befugnisse. Im weiteren Verlauf des Jahres führte die Datenschutzbehörde Untersuchungen der Anwendung der ANPR durch zwei Polizeidienststellen durch und kam zu dem Ergebnis, dass beide Polizeidienststellen bewusst gegen das Polizei-Datenschutzgesetz verstießen und Treffer sowie Nichttreffer in einem Zeitraum von 120 bzw. 10 Tagen verarbeiteten. Ein Nichttreffer bezeichnet ein gescanntes Kennzeichen, das nicht in der Referenzdatei erfasst ist und somit auch nicht von der Polizei gesucht wird. Die Erfassung dieses Kennzeichens muss unverzüglich gelöscht werden. Als Reaktion auf die Veröffentlichung der abschließenden Ergebnisse der Untersuchung erklärten beide Dienststellen Anfang 2010, dass sie diese unrechtmäßige Vorgehensweise einstellen würden.

Passagiere, die beispielsweise mithilfe eines Netzhautscans oder mithilfe von Fingerabdrücken an einem System zur automatischen Grenzüberschreitung teilnehmen wollen, müssen vorab kontrolliert werden. Die Datenschutzbehörde hat den Justizminister aufgefordert, klarzustellen, wo die Untersuchung der Hintergründe dieser Personen beginnen soll.

Polen

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

Revision des Telekommunikationsgesetzes

Das Gesetz vom 24. April 2009 zur Änderung des Telekommunikationsgesetzes trat am 6. Juli 2009 in Kraft. Die Änderungen betrafen unter anderem neue Bestimmungen zur Vorratsspeicherung von Daten, die Anpassung der nationalen Gesetzgebung an die Anforderungen der Richtlinie 2006/24/EG durch die Einführung zahlreicher zusätzlicher Verantwortlichkeiten für Betreiber öffentlicher Telekommunikationsnetzwerke sowie Betreiber öffentlicher Telekommunikationsdienste (so z. B. die Verpflichtung, Verbindungsdaten für einen Zeitraum von 24 Monaten nach dem Anruf auf Vorrat zu speichern und die Daten mit Ausnahme der gemäß anderer gesetzlicher Bestimmungen auf Vorrat gespeicherten Daten nach Ablauf dieses Zeitraums zu vernichten). Die oben genannten Verpflichtungen dürfen nicht so umgesetzt werden, dass sie zu einer Veröffentlichung der Telekommunikationsübertragung führen. Die eingeführte Änderung verpflichtet auch Unternehmer, die Sicherheit personenbezogener Daten durch angemessene technische und organisatorische Maßnahmen sowie außerdem den Zugriff auf diese Daten ausschließlich durch befugtes Personal zu gewährleisten.

Der **Gesetzesentwurf zur Änderung des Gesetzes über den Zugang zu öffentlichen Informationen** legt fest, dass die Daten zum Gesundheitszustand von Personen, die das Amt des Präsidenten und des Premierministers bekleiden, als öffentliche Informationen einzustufen sind. Der Generalinspektor brachte seine negative Einstellung zu den Bestimmungen dieses Entwurfes deutlich zum Ausdruck und betonte, dass die existierenden Bestimmungen der polnischen Verfassung, des Datenschutzgesetzes sowie der Richtlinie 95/46/EG dem Gesetzgeber empfehlen, sich hinsichtlich der Einführung von Bestimmungen zurückzuhalten, die die Veröffentlichung von Daten zum so genannten Gesundheitsstatus als „sensibel" einstufen – selbst wenn es um die Inhaber der höchsten öffentlichen Ämter in Polen geht. Er betonte, dass es – trotz der Tatsache, dass das Recht auf Privatsphäre und auf den Schutz personenbezogener Daten bei Inhabern öffentlicher Ämter im Vergleich zu „gewöhnlichen Bürgern" wesentlich eingeschränkter ist – keine Rechtsgrundlage gebe, die zur Annahme führen könnte, dass diese Rechte in diesem Fall nicht gelten. Die Datenschutzbehörde betonte, dass sich dieser Standpunkt auch in der Erklärung des Ministerkomitees des Europarates vom 12. Februar 2004 über die Freiheit der politischen Debatte in den Medien widerspiegelt.

Angesichts der starken Position des Generalinspektors wurde der oben genannte Entwurf nicht in Kraft gesetzt. Bei etwaigen weiteren Versuchen der Einführung eines solchen Gesetzes ist mit einer starken Reaktion der Datenschutzbehörde zu rechnen.

Die neue vom Ministerium für Inneres und Verwaltung veröffentlichte Verordnung hinsichtlich der **Entwicklung einer Mustervorlage für ein Antragsformular zur Anmeldung des Datenablagesystems** für eine Registrierung durch den Generalinspektor für den Schutz personenbezogener Daten trat am 10. Februar 2009 in Kraft. Die neue, auf Initiative von GIODO entworfene Mustervorlage vereinfacht das Verfahren. Außerdem listet sie die wesentlichen Verantwortlichkeiten des Datenkontrolleurs im Hinblick auf den Schutz der Daten auf. Die Einführung der neuen Vorlage führte zu einem Rückgang der Anzahl falsch ausgefüllter Anmeldeformulare.

B. Bedeutende Rechtsprechung

Im Berichtsjahr befasste sich der Generalinspektor mit zahlreichen Fällen, die die Tätigkeit von Kreditinformationsbüros betrafen. Das Oberste Verwaltungsgericht schloss sich in zahlreichen Fällen der Position des Generalinspektors an. Bei einem der wichtigsten Fälle ging es darum, dass die Büros als Datenkontrolleure ihren Kunden Gebühren für den Zugang zu ihren persönlichen Informationen berechneten. Diese Vorgehensweise wurde vom Generalinspektor scharf kritisiert. Gemäß polnischem Recht hat ein Datensubjekt alle sechs Monate das Recht auf Zugang zu seinen Informationen. Dieser Zugang ist kostenfrei zu gewähren. Dieser Ansatz wurde für den oben

genannten Fall durch die Entscheidung des Obersten Verwaltungsgerichtes vom 30. Juli 2009 bestätigt.

Der Generalinspektor befasste sich außerdem mit den Problemen der Erfassung und Verarbeitung biometrischer Daten zum Zweck der Arbeitszeitkontrolle. Der Generalinspektor ist der Ansicht, dass solche Maßnahmen einen übermäßigen Eingriff in die Privatsphäre des Datensubjekts darstellen. In diesen Fällen besteht immer ein großes Risiko einer Verletzung der Privatsphäre. Daher sind andere, weniger einschneidende Methoden anzuwenden. Diese Ansicht wurde vom Obersten Verwaltungsgericht bestätigt, das in seinem Urteil vom 1. Dezember 2009 feststellte, dass bei der Bewertung der Notwendigkeit der Erfassung biometrischer Daten von Angestellten (deren Einverständnis vorausgesetzt) zur Arbeitszeitkontrolle darauf hingewiesen werden muss, dass die wichtigsten Voraussetzungen in diesen Fällen die Einhaltung der Prinzipien der Verhältnismäßigkeit und der Rechtmäßigkeit sind. Das bedeutet, dass das Risiko der Verletzung der Freiheits- und Grundrechte in einem angemessenen Verhältnis zum Zweck der Datenverarbeitung stehen muss. Da das im Datenschutzgesetz genannte Prinzip der Verhältnismäßigkeit ein primäres Kriterium für Entscheidungen betreffend die Verarbeitung biometrischer Daten ist, muss darauf hingewiesen werden, dass die Verwendung dieser Daten zur Arbeitszeitkontrolle im Hinblick auf den durch die Verarbeitung verfolgten Zweck unverhältnismäßig ist. Das Gericht bestätigte die Ansicht, dass die Erfassung biometrischer Daten in diesen Fällen als unverhältnismäßiger Eingriff in die Privatsphäre einzustufen ist und bestätigte somit auch die Position des Generalinspektors.

Im Berichtsjahr befasste sich der Generalinspektor außerdem mit der Frage der Zulässigkeit der Verarbeitung personenbezogener Daten ohne Rechtsgrundlage für eine weitere Verarbeitung im Rahmen der von Banken erstellten Sicherungskopien nach der Löschung von Daten aus dem Datenablagesystem. Eine solche Situation kann nach einer negativen Kreditentscheidung entstehen, wenn die Bank die personenbezogenen Daten des Antragstellers aus dem Ablagesystem löscht, da die im Datenschutzgesetz aufgeführte Rechtsgrundlage mit dieser Entscheidung erlischt. (Verarbeitung von Daten, die im Hinblick auf die zum Abschluss eines Vertrages erforderlichen Tätigkeiten unumgänglich ist). Überdies steht die Verarbeitung von Daten in Sicherungskopien, also wenn sich die Daten nicht mehr im Datenablagesystem befinden, im Widerspruch zum Zweck der Erstellung solcher Kopien (Archivierungszwecke zur Gewährleistung der Betriebssicherheit der Bank). Die oben genannte Position des Generalinspektors wurde durch das Urteil des regionalen Verwaltungsgerichts Warschau vom 16. Januar 2008 bestätigt. Das Oberste Verwaltungsgericht wies die Berufung am 3. Juli 2009 ab.

C. Wichtige spezifische Themen

Im Juni 2009 führte GIODO eine Kontrolle der Verarbeitung personenbezogener Daten durch IT-Systeme bei der Warschauer Behörde für öffentlichen Verkehr (ZTM) durch. Grund für die Kontrolle waren Presseartikel darüber, wie die ZTM Ort und Zeit der Nutzung der öffentlichen Verkehrsmittel erfasste (insbesondere in der Warschauer U-Bahn, in der die Passagiere an jedem Eingang eine elektronisch codierte Fahrkarte scannen lassen müssen, um den Eingang zu öffnen). Die Kontrolle bestätigte die in der Presse beschriebenen Probleme sowie andere Unregelmäßigkeiten hinsichtlich einer unverhältnismäßigen Verarbeitung von Daten, die nicht dem eigentlichen Zweck dient. GIODO informierte die ZTM über die im Rahmen der Kontrolle festgestellten Unregelmäßigkeiten und forderte eine Korrektur. Gegenwärtig führt der Generalinspektor Prüfungen in anderen Städten durch, um den Umfang der Datenverarbeitung anderer öffentlicher Verkehrsunternehmen zu prüfen, die sich für ein Fahrkartensystem entschieden haben, das mit dem der ZTM vergleichbar ist.

Die oben beschriebene Kontrolle der ZTM war der Auslöser für eine größer angelegte Kontrolle anderer öffentlicher Verkehrsunternehmen durch den Generalinspektor.

Soziale Netzwerke. In den ersten beiden Quartalen des Jahres führte der Generalinspektor eine Reihe von Prüfungen von Websites sozialer Netzwerken durch. Im Rahmen der Prüfungen wurde festgestellt, dass der Datenkontrolleur in der Regel der Anbieter der Website ist. Die im Rahmen der Prüfungen dieser Unternehmen

am häufigsten festgestellte Unregelmäßigkeit war der unangemessene Schutz der auf den Benutzerprofilen erfassten Daten. Der Anmeldeprozess und der Bearbeitungsmodus der Profile waren oftmals nur schlecht geschützt (zu kurze Passwörter und Übermittlung nicht geschützter Daten). Im Bereich der Organisation waren Mängel bei der Erfüllung der Informationspflicht, das Fehlen klarer Informationen zur Möglichkeit einer Missbrauchsmeldung sowie unklare Vorschriften zu verzeichnen. Als Folge der vom Generalinspektor ergriffenen Maßnahmen wurde in Zusammenarbeit mit dem Verwalter von „Nasza Klasa" („Unser Klassenkamerad") eine separate Kategorie auf der Website des Portals eingeführt, auf der Informationen zu Datenschutzfragen und Bedrohungen der Privatsphäre zu finden sind. Außerdem wurde eine Option eingeführt, über die die Nutzer den Grad ihrer Datensicherheit selbst einstellen können.

Im Jahr 2009 führte der Generalinspektor eine Kontrolle der Unternehmen durch, die befugt sind, direkt auf das Nationale Informationssystems zuzugreifen, dort Einträge im Schengener Informationssystem (SIS) vorzunehmen und auf SIS-Daten zuzugreifen. Hauptgegenstand der Prüfungen waren die Gerichte. Im Rahmen der Prüfungen wurden zahlreiche Unregelmäßigkeiten festgestellt, so z. B. das Fehlen einer ordnungsmäßigen Dokumentation (z. B. fehlende Sicherheitsrichtlinien) und die Tatsache, dass nicht befugte Personen ohne angemessene Schulung Zugang zu personenbezogenen Daten haben. Nach der Kontrolle und Feststellung der Unregelmäßigkeiten forderte der Generalinspektor den Justizminister auf, sich mit der Sache zu befassen und die Unregelmäßigkeiten zu beheben, insbesondere die Unregelmäßigkeiten, die den Zugang zum SIS betreffen.

Der Generalinspektor führt auch weiterhin Bildungsinitiativen durch, um die Bürger hinsichtlich ihrer Rechte auf Datenschutz und Privatsphäre zu sensibilisieren. Ein weiteres Bildungsprojekt ist ein Pilotprogramm für Gesamtschulen mit dem Titel „Deine Daten – deine Angelegenheit. Effektiver Schutz personenbezogener Daten. Eine Bildungsinitiative für Schüler und Lehrer". Ziel der Bildungsinitiative für Lehrer und Schüler von Gesamtschulen ist die Verbesserung des Wissens in den Bereichen Datenschutz und das Recht auf Schutz der Privatsphäre. Kern des Programms ist die Zusammenarbeit auf der Grundlage einer Partnerschaft zwischen den selbstverwalteten Ausbildungszentren für Lehrer und dem Generalinspektor für den Schutz personenbezogener Daten. Das Pilotprojekt umfasst zwei Phasen. In Phase I werden die Lehrer geschult, wohingegen in Phase II die Datenschutzfragen in die Lehrpläne integriert werden. Den am Programm teilnehmenden Schulen werden die Grundzüge sowie das vom Generalinspektor für Schüler und Lehrer erstellte Material zur Verfügung gestellt. Außerdem wird hinsichtlich der durchgeführten Aktivitäten und des landesweiten Bildungsprogramms ein Bewertungsbericht erstellt.

Am 27. Januar 2009 unterzeichnete der Generalinspektor als Teil der Feierlichkeiten zum 4. Datenschutztag ein Abkommen mit dem polnischen Bankenverband mit dem Titel „Bewährte Verfahrensweisen für die Verarbeitung personenbezogener Daten bei Banken – der Standpunkt der Fachleute", um so die Standards zum Schutz personenbezogener Daten sowie die Einhaltung des Rechts auf Privatsphäre im Rahmen der Tätigkeit von Banken zu verbessern. Dieses Abkommen soll dabei helfen, einen Kodex für die gesamte Bankenbranche zu bewährten Verfahrensweisen im Bereich Datenschutz zu erarbeiten.

Der Generalinspektor für den Schutz personenbezogener Daten entwickelte in Zusammenarbeit mit dem polnischen Episkopat die „Leitlinien zum Schutz personenbezogener Daten im Rahmen der Tätigkeiten der katholischen Kirche in Polen".

Die Leitlinien erläutern die Prinzipien des ordnungsgemäßen Schutzes personenbezogener Daten und sollten dabei helfen, personenbezogene Daten im Rahmen der Tätigkeiten der katholischen Kirche zu schützen, wenngleich die Kontrollbefugnisse des Generalinspektors betreffend die Tätigkeiten der Kirche sehr beschränkt sind.

Portugal

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

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

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

Die Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) wurde per Gesetz 32/2009, das im August 2009 in Kraft trat, in nationales Recht umgesetzt.

B. Bedeutende Rechtsprechung

Das Zentrale Verwaltungsgericht entschied in einem Fall zugunsten der Datenschutzbehörde, in dem die Datenschutzbehörde der Gemeinde Porto nicht gestattete, Alkoholtests bei allen ihren Angestellten von Personen durchführen zu lassen, die keine Fachleute aus dem Bereich Gesundheitswesen sind Die Ergebnisse sollten danach den Vorgesetzten der Angestellten direkt übermittelt werden.

Das Gericht folgte der Argumentation der Datenschutzbehörde und stellte fest, dass es keinen Grund gebe, bei allen Angestellten Alkoholtests durchzuführen, mit Ausnahme bestimmter beruflicher Tätigkeiten, bei denen das Leben der Angestellten oder Dritter in Gefahr sein könnte. Die Tests müssten von Fachleuten aus dem Bereich Gesundheitswesen (Ärzte oder Krankenschwestern) durchgeführt werden, und die Ergebnisse der Tests dürften nicht an die Vorgesetzten übermittelt werden. Diese dürften lediglich den Hinweis „arbeitsfähig" oder „nicht arbeitsfähig" erhalten.

In einem anderen Gerichtsurteil, das sich aus einer Beschwerde gegen die Entscheidung der Datenschutzbehörde ergab, entschied das Verwaltungsgericht ebenfalls zugunsten der Datenschutzbehörde und bestätigte das Verbot der Installation von Videoüberwachungskameras in der Redaktion eines Fernsehsenders, in der Journalisten arbeiten.

C. Wichtige spezifische Themen

Allgemeine Tätigkeit

Im Jahr 2009 hielt die portugiesische Datenschutzbehörde ihr hohes Tätigkeitsniveau aufrecht. Die Anzahl von Meldungen bezüglich der Verarbeitung von Daten belief sich auf mehr als 10.000. Es wurden mehr als 700 Verfahren aufgrund von Beschwerden eingeleitet sowie Untersuchungen auf eigene Initiative der Datenschutzbehörde durchgeführt. Diese Verfahren führten zur Verhängung von 260 Sanktionen in einer Höhe von insgesamt 540.000 Euro.

Außerdem wurden 171 Prüfungen vor Ort durchgeführt, unter anderem auch eine Prüfung der Datenbank des Wählerverzeichnisses. Als Folge dieser Prüfungen wurden entsprechende Empfehlungen ausgesprochen. Die Umsetzung dieser Empfehlungen wurde überwacht. Der Prüfbericht wurde dem Präsidenten der Republik, dem Parlament und der Regierung vorgelegt.

Die Datenschutzbehörde initiierte die Umsetzung eines Online-Meldeverfahrens für bestimmte Datenverarbeitungen und führte den Prozess der Dematerialisierung von Dokumenten sowie die Reform des internen Informationssystems fort, wodurch der Entscheidungsfindungsprozess kurzfristig beschleunigt werden soll.

Leitlinien für Datenkontrolleure

Im Jahr 2009 veröffentlichte die Datenschutzbehörde Leitlinien für Datenkontrolleure zu bestimmten Arten der Verarbeitung von Daten mit folgenden Zielen: Arzneimittelkontrolle, Integritätsgrenzen („Whistleblowing"); Kredittransaktionen und Aufzeichnung von Telefonaten (Call Center).

Diese Überlegungen bieten den Datenkontrolleuren Leitlinien dazu, wie die Datenschutzgesetze besser eingehalten und wie betroffene Personen über ihre Rechte und die für die Verarbeitung der Daten festgelegten Bedingungen informiert werden können.

Im Hinblick auf den Bereich „Whistleblowing" gestattet die Datenschutzbehörde ausschließlich ein vertrauliches System (um Verleumdungen und Diskriminierungen vorzubeugen) für beschränkte Zwecke (Vermeidung und Bekämpfung von Unregelmäßigkeiten in der Buchhaltung, internen Buchprüfungen, Prüfungen, Bekämpfung von Korruption und Finanzverbrechen). Darüber hinaus gestattet sie keine Meldung von Verstößen gegen die gute Unternehmensführung. Hinsichtlich bestimmter Kategorien von Datensubjekten gilt: Meldungen sollten sich hauptsächlich gegen Einzelpersonen richten, die für die Entscheidungsfindung in den oben genannten Bereichen verantwortlich sind. Gemäß dem Verständnis der Datenschutzbehörde sind diese Leitlinien als ergänzende, optionale Mechanismen anzusehen, die den existierenden rechtlichen Methoden zur Meldung von Unregelmäßigkeiten untergeordnet sind; die Angestellten werden vorab eindeutig über die Datenverarbeitung informiert.

Stellungnahmen zu Gesetzesentwürfen
Im Jahr 2009 wurde die Datenschutzbehörde gebeten, Stellung zu 86 Gesetzesentwürfen betreffend Datenschutzfragen auf nationaler oder internationaler Ebene zu nehmen.

Auf EU-Ebene betraf die relevanteste Stellungnahme die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates, die Revision der Verordnung 1049/2001, den Rahmenbeschluss 2005/222/JI des Rates, die Änderungen der Eurodac- und Dublin II-Verordnungen sowie den Entwurf des Ratsbeschlusses zum Zollinformationssystem.

Auf nationaler Ebene nahm die Datenschutzbehörde Stellung zu zahlreichen bilateralen Abkommen zwischen Portugal und anderen Staaten betreffend den Informationsaustausch zu steuerlichen sowie Strafverfolgungszwecken.

Im Laufe des Jahres 2009 nahm die Datenschutzbehörde außerdem Stellung zu Gesetzesentwürfen betreffend die rechtlichen Regelungen im Bereich Sicherheit und Gesundheitsschutz am Arbeitplatz, das Recht auf Information und Einverständniserklärung im Bereich Gesundheit, betreffend Fahrzeugdaten, Wählerverzeichnisse und das Informationssystem im Bereich der Strafverfolgung.

Gemäß der nationalen Gesetzgebung muss die Datenschutzbehörde auch Stellung zu Videoüberwachungsgeräten nehmen, die durch die Strafverfolgungsbehörden auf öffentlichen Straßen installiert werden. Im Jahr 2009 nahm die Datenschutzbehörde drei Mal negativ Stellung zur Installation solcher Systeme und stellte fest, dass die rechtlichen Anforderungen hinsichtlich der Verhältnismäßigkeit nicht erfüllt worden waren. In einem Fall nahm die Datenschutzbehörde einmal generell positiv Stellung beschränkte den Betrieb des Systems jedoch auf die Nachtstunden. Negative Stellungnahmen der Datenschutzbehörde sind verbindlich. Die Bedingungen für eine Genehmigung werden daraufhin vom Innenministerium festgelegt.

DADUS-Projekt
Das von der Datenschutzbehörde für Kinder und Jugendliche im Alter von 10-15 Jahren entwickelte Projekt wird durch die Integration von Fragen zu Datenschutz und Privatsphäre in die Lehrpläne als Teil des Lernprozesses in Schulen durchgeführt.

Im Jahr 2009 haben sich über 2.000 Lehrer für das DADUS-Projekt registriert. Die Website und der Blog des Projekts verzeichneten über 200.000 Aufrufe.

Das Projekt umfasste drei Wettbewerbe zum Thema Privatsphäre: Raptexte, ein Poster und ein Video. Die Teilnahme war sehr gut und die Preise wurden in den Schulen verliehen.

Des Weiteren hat die Datenschutzbehörde ein Abkommen mit der Filmhochschule abgeschlossen, um von ihren Studenten erstelltes audiovisuelles Material im Rahmen des DADUS-Projekts zur Verbesserung der Multimediakomponente zu verwenden. Dies wird als eine der besten Möglichkeiten zur Kommunikation mit jungen Menschen angesehen.

Rumänien

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

Wie in den vergangenen Jahren, so verabschiedete die Aufsichtsbehörde auch im Jahr 2009 Entscheidungen zur Einführung einer standardisierten Vorgehensweise gemäß den EU-Vorschriften:

- Zur Vereinfachung des Genehmigungsverfahrens sowie zur Vermeidung übermäßiger Formalitäten wurde ein Beschluss zur Einführung einer Genehmigungsvorlage für die Übermittlung personenbezogener Daten in andere Länder gefasst.
- Zur Sicherstellung des effektiven Schutzes der Rechte betroffener Personen, insbesondere im Fall bestimmter Datenverarbeitungen, die aufgrund der Art der verarbeiteten Daten, des Zweckes der Verarbeitung, der besonderen Eigenschaften der Kategorien betroffener Personen oder der zur Verarbeitung der Daten eingesetzten Mechanismen spezielle Risiken für die Rechte und Freiheiten der betroffenen Personen bergen, wurde ein Beschluss zur Festlegung der Kategorien von Datenverarbeitungen gefasst, die wahrscheinlich spezielle Risiken für die Rechte und Freiheiten der betroffenen Personen bergen.

Die Aufsichtsbehörde wurde im Rahmen der Erarbeitung von Gesetzesentwürfen betreffend die Verarbeitung personenbezogener Daten sowie von einer Reihe öffentlicher Behörden und Institutionen konsultiert, so z. B. vom Ministerium für Verwaltung und Inneres, dem Ministerium für Kommunikation und Informationstechnologie sowie vom Generalsekretariat der Regierung.

Im Jahr 2009 baten zahlreiche Datenkontrolleure und Einzelpersonen um Rat hinsichtlich der Verarbeitung personenbezogener Daten, was sowohl von einem Interesse am Schutz personenbezogener Daten als auch von einem Bewusstsein für die Auswirkungen der Verarbeitung personenbezogener Daten auf das Privatleben zeugt. Zu den relevantesten Standpunkten gehörte die Schaffung der Positionen des Datenkontrolleurs und des Datenverarbeiters, die Veröffentlichung personenbezogener Daten sowie die Verarbeitung personenbezogener Daten im Rahmen von Ablagesystemen von Kreditbüros.

B. Bedeutende Rechtsprechung

Die Vorgehensweise der Gerichte bei Streitsachen betreffend den Schutz personenbezogener Daten wies auch weiterhin ihren standardisierten Charakter auf. Nachstehend möchten wir einige relevante Situationen beschreiben, in denen Widerspruch gegen die Sanktionen der Aufsichtsbehörde eingelegt wurde:

1. Die Aufsichtsbehörde führte eine Untersuchung bei einem privaten Unternehmen durch, das personenbezogene Daten aus Straßenansichtsdiensten ohne vorherige Anmeldung verarbeitete. Die Verarbeitung hatte bereits im Jahr 2008 begonnen. Im Rahmen der Untersuchung wurde außerdem festgestellt, dass die betroffenen Personen nicht über die Erfassung und spätere Veröffentlichung von Panoramabildern informiert wurden, auf denen natürliche Personen zu sehen sind, und dass der Datenkontrolleur keine Sicherheitsvorkehrungen getroffen hatte, um die personenbezogenen Daten auf den auf der Website veröffentlichten Bildern unkenntlich zu machen.

   Aus diesen Gründen wurde ein Bußgeld verhängt. Der Datenkontrolleur zeigte sich mit dem Ergebnis der Untersuchung unzufrieden und legte Beschwerde dagegen ein.

   Das Gericht entschied, dass der Datenkontrolleur die personenbezogenen Daten verarbeitet hatte, ohne die Datensubjekte angemessen über die Erfassung und Veröffentlichung der Panoramabilder mit personenbezogenen Daten (Gesichter von Personen, Kennzeichen von Fahrzeugen, die zum Zeitpunkt der Erfassung der Bilder gerade vorbeifuhren, sowie Hausnummern und -namen) zu informieren. Gemäß dem Prinzip der Angemessenheit, Relevanz und Verhältnismäßigkeit der Daten im Hinblick auf den Zweck der Verarbeitung hätten diese Bilder technisch so bearbeitet werden müssen, dass eine Identifizierung der abgebildeten Personen nicht möglich ist.

Daher bestätigte das Gericht das von der Aufsichtsbehörde gegen den Datenkontrolleur verhängte Bußgeld.

2. Die Aufsichtsbehörde stellte fest, dass eine Einrichtung des Gesundheitswesens die Verarbeitung personenbezogener Daten nicht gemeldet hatte und einige Patientendaten ohne Einverständnis der Patienten sowie ohne vorherige Information an andere Einrichtungen des Gesundheitswesens übermittelt hatte.

   Für diese Verstöße verhängte die Aufsichtsbehörde Bußgelder.

   Der Datenkontrolleur focht daraufhin die Untersuchungsprotokolle an.

   Das Gericht entschied, dass der Beschwerdeführer (Patient) sich nicht mit der Veröffentlichung der persönlichen Identifikationsnummer seines Sohnes einverstanden erklärt hatte. Diese persönliche Information war daraufhin an alle Arztpraxen des Bezirks übermittelt worden, und der Datenkontrolleur hatte die betroffene Person weder darüber informiert noch die Verarbeitung der personenbezogenen Daten gemeldet.

   Das Gericht bestätigte das von der Aufsichtsbehörde verhängte Bußgeld durch ein unwiderrufliches Urteil.

3. Im Rahmen der Untersuchung einer öffentlichen Behörde durch die Aufsichtsbehörde wurde festgestellt, dass die gesetzlichen Verpflichtungen betreffend die Anwendung von Sicherheitsmaßnahmen und die Vertraulichkeit der Verarbeitung personenbezogener Daten nicht eingehalten wurden.

   Die untersuchte öffentliche Behörde hatte zwei von lokalen Behörden verabschiedete Regulierungsmaßnahmen auf ihrer Website veröffentlicht. Diese enthielten unter anderem Tabellen mit Vornamen, Nachnamen, persönlichen Identifikationsnummern sowie Daten zum Gesundheitszustand (Behinderungen) von Begünstigten bestimmter gesetzlicher Einrichtungen.

   Die Veröffentlichung spezieller personenbezogener Daten (Artikel 7 und 8 von Gesetz Nr. 677/2001), auch wenn diese versehentlich oder aufgrund eines technischen Fehlers erfolgt, stellt einen Verstoß gegen die Bestimmungen von Artikel 20 von Gesetz Nr. 677/2001 dar, da die Ergreifung angemessener technischer und organisatorischer Maßnahmen zur Sicherstellung des Schutzes der personenbezogenen Daten gescheitert ist, sowie außerdem einen Verstoß gegen Anordnung Nr. 52/2002 zur Genehmigung von Mindestsicherheitsstandards betreffend die Verarbeitung personenbezogener Daten.

   Das Gericht bestätigte die von der Aufsichtsbehörde verhängte Sanktion.

C. Wichtige spezifische Themen

Rumäniens Auftrag zur Bewertung des Schutzes personenbezogener Daten im Hinblick auf den Beitritt zum Schengener Durchführungsübereinkommen

Zwischen dem 29. April und dem 1. Mai 2009 wurde in Bukarest eine Bewertung des Schutzes personenbezogener Daten durchgeführt. Diese Bewertung stellte einen wichtigen Teil des Verfahrens zum Beitritt Rumäniens zum Schengen-Raum dar.

Der Bericht der Bewertungsexperten enthält positive Anmerkungen hinsichtlich der Fähigkeit der Aufsichtsbehörde, unabhängig zu handeln, hinsichtlich des hohen Grades der Umsetzung der Gesetzgebung zum Schutz personenbezogener Daten sowie hinsichtlich der effektiven Zusammenarbeit unserer Behörde mit anderen beteiligten Behörden. Wir möchten erwähnen, dass die von der Aufsichtsbehörde in Rumänien in Zusammenarbeit mit der Generalinspektion der rumänischen Polizei sowie auf territorialer Ebene mit der Anwaltsschule „Constantin Brâncuşi" in Tg. Jiu und lokalen Polizeibehörden durchgeführte Informationskampagne besonders geschätzt wurde.

Der Präsident der Aufsichtsbehörde und das an den Debatten beteiligte Personal wurden zur Professionalität und dem hohen Standard ihrer Tätigkeiten sowie zur Organisation der Schengen-Bewertung beglückwünscht.

Die Konferenz der mittel- und osteuropäischen Datenschutzbehörden

Die Aufsichtsbehörde organisierte die Konferenz der mittel- und osteuropäischen Datenschutzbehörden; dieses jährliche Treffen der Datenschutzbehörden dieser Region bietet eine hervorragende Möglichkeit zur Debatte und Analyse spezieller Fragen, die sich im Rahmen der Tätigkeiten der Behörden mit Befugnissen im Bereich des Schutzes des Privatlebens ergeben.

Vertreter von Datenschutzbehörden aus Bulgarien, Kroatien, der Tschechischen Republik, Estland, Ungarn, Polen, der Slowakei und Slowenien sowie Vertreter unserer Aufsichtsbehörde als Organisatoren der Veranstaltung nahmen an diesem 11. Treffen teil. Im Rahmen des Zusammenhangs zwischen dem Recht auf Privatleben, biometrischen Daten, des Geschäftsumfeldes und neuen Technologien wurden generelle Fragen zu den Entwicklungen im Bereich des Schutzes personenbezogener Daten in allen Ländern diskutiert.

Die Veranstaltung, zu der Hochschulprofessoren und Leiter von Polizeieinheiten mit Erfahrung im Bereich Datenschutz ebenso eingeladen wurden wie Datenschutzbeauftragte und -experten aus Mittel- und Osteuropa, bot eine hervorragende Möglichkeit, bewährte Verfahrensweisen im Bereich des Schutzes personenbezogener Daten zu benennen und zu fördern.

Im Hinblick auf die Prüftätigkeiten musste die Aufsichtsbehörde ihre Strategie im Jahr 2009 angesichts der Etatkürzungen ändern, so dass abgesehen von den mit den zuständigen Behörden durchgeführten Untersuchungen betreffend den Beitritt Rumäniens zum Schengen-Raum und der vorläufigen Untersuchungen auf der Grundlage von Sondergesetzen die Bearbeitung von Beschwerden vorrangig behandelt wurde.

Die bei der Aufsichtsbehörde eingegangenen Beschwerden betrafen den Erhalt unerbetener Werbenachrichten, die Meldung personenbezogener Daten von Kreditnehmern an Kreditvermittlungssysteme sowie die illegale Verarbeitung oder Veröffentlichung personenbezogener Daten.

In den Fällen, die auf der Grundlage der eingegangenen Beweise bestätigt werden konnten, wurden Sanktionen verhängt und gegebenenfalls entschieden, dass die Verarbeitung einzustellen oder die ohne Beachtung der Rechte der Datensubjekte verarbeiteten personenbezogenen Daten zu löschen sind.

Die Beschwerden betreffend unerbetene Werbenachrichten betrafen Situationen, in denen die betroffenen Personen solche Nachrichtungen per SMS sowie per Telefon erhalten hatten, ohne vorher ihr ausdrückliches und unmissverständliches Einverständnis gegeben zu haben.

Zusätzlich zu ihrer allgemeinen durch Gesetz Nr. 677/2001 festgelegten Zuständigkeit hält die Aufsichtsbehörde eine Reihe von in Gesetz Nr. 506/2004 genannten Befugnissen betreffend die Verarbeitung personenbezogener Daten und den Schutz des Privatlebens im Bereich elektronische Kommunikation.

Die bei der Aufsichtsbehörde eingegangenen Beschwerden zu möglichen Verletzungen des Rechts auf Privatleben durch die Verarbeitung personenbezogener Daten in Kreditvermittlungssystemen betrafen im Allgemeinen die Übermittlung personenbezogener Daten ohne Beachtung der Rechte und ohne das Einverständnis der betroffenen Personen sowie ohne Beachtung der Bestimmungen der vom Vorstand der Aufsichtsbehörde veröffentlichten Entscheidung zur Verarbeitung personenbezogener Daten in Kreditvermittlungssystemen.

Slowakei

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

Im Jahr 2009 formulierte die Behörde der slowakischen Republik zum Schutz personenbezogener Daten (im Weiteren „Datenschutzbehörde" genannt) einen neuen Wortlaut für einige Bestimmungen des aktuell geltenden Datenschutzgesetzes. Der erarbeitete Entwurf wird das Datenschutzgesetz unter Berücksichtigung von Empfehlungen ändern, die sich aus dem strukturierten Dialog mit Vertretern der Europäischen Kommission, aus Anregungen aus der praktischen Anwendung des Datenschutzgesetzes sowie aus den aktuellen Entwicklungen im Anschluss an die Verabschiedung des Rahmenbeschlusses über den Schutz personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ergeben haben. Der Änderungsentwurf wird der slowakischen Regierung im Oktober 2010 vorgelegt.

B. Bedeutende Rechtsprechung

Im Jahr 2009 war die Datenschutzbehörde an zahlreichen Gerichtsprozessen beteiligt. In zwei Fällen war die Datenschutzbehörde Gegenstand einer gerichtlichen Prüfung ihrer Entscheidung betreffend die Anordnung von Rechtsmitteln gegen den Kontrolleur eines Informationssystems sowie gegen einen Bearbeiter eines Kreditanbieters. Die Anordnung des Rechtsmittels gegen den Kontrolleur erfolgte, um die unrechtmäßige Veröffentlichung der in einem offenen Brief zugestellten Zahlungsaufforderung zu beenden. Durch diese Vorgehensweise stellte der Kontrolleur Daten zur wirtschaftlichen Identität der betroffenen Person ohne Rechtsgrundlage zur Verfügung. Der Kontrolleur reichte bei Gericht Klage gegen die Anordnung ein. Ein endgültiges Urteil wurde 2009 noch nicht gesprochen. In einem ähnlichen Fall befasst sich das Gericht mit einem Antrag des Bearbeiters eines früheren Kontrolleurs, der behauptet, dass die betreffende Entscheidung der Datenschutzbehörde – eine Anordnung zur Ergreifung von Rechtsmitteln, d. h. in diesem Fall die Einhaltung des Umfangs und der Bedingungen für die vom Kontrolleur im Rahmen eines schriftlichen Vertrages festgeschriebene Verarbeitung personenbezogener Daten – unrechtmäßig sei. Auch in diesem Fall wurde noch kein endgültiges Urteil gesprochen.

Im dritten Fall war die Datenschutzbehörde Gegenstand einer gerichtlichen Überprüfung ihrer Entscheidung zur Verhängung eines Bußgeldes gegen einen Kontrolleur. Dieser Kontrolleur hatte insbesondere keine angemessenen Sicherheitsvorkehrungen getroffen. In erster Instanz entschied das Bezirksgericht, dass die Verhängung einer Sanktion im Einklang mit dem Datenschutzgesetz stehe. Der Kontrolleur legte Berufung beim Obersten Gerichtshof ein. Die Sache wurde daraufhin an ein höherinstanzliches Gericht verwiesen. Eine Entscheidung des Obersten Gerichtshofes zu diesem Fall steht noch aus.

C. Wichtige spezifische Themen

Prüfaktivitäten und Bearbeitung von Meldungen
Überwachung des Schutzes personenbezogener Daten in Zahlen
Im Jahr 2009 gingen 108 Meldungen von Datensubjekten und anderen natürlichen Personen bezüglich einer Verletzung des Schutzes ihrer personenbezogenen Daten bei der Datenschutzbehörde ein. 36 weitere Meldungen gingen von anderen Personen ein, die den Verdacht eines Verstoßes gegen das Datenschutzgesetz vorbrachten. Der Oberinspektor der Datenschutzbehörde ordnete von Amts wegen 128 Verfahren gegen die Kontrolleure von Datenablagesystemen an. Im Jahr 2009 leitete die Abteilung für Prüfungen 272 Verfahren ein. Weitere 39 Meldungen aus dem Jahr 2008 waren noch nicht abgeschlossen. Insgesamt bearbeitete die Abteilung für Prüfungen 311 Meldungen.

In diesem Zusammenhang führte die Abteilung für Prüfungen in Zusammenarbeit mit der Unterabteilung für die Untersuchung der Beschwerden 107 Prüfungen durch und stellte 72 „Anträge auf Erläuterungen" an die Kontrolleure und Bearbeiter von Datenablagesystemen. Insgesamt wurden 161 Anordnungen zur Korrektur von im Rahmen der Prüfungen festgestellten Mängeln ausgesprochen, 120 % mehr als im Jahr 2008. Das Recht auf Widerspruch gegen eine ausgesprochene Anordnung wurde nur von vier Kontrolleuren wahrgenommen. Dies entspricht lediglich 2,5 % aller Kontrolleure, die

Gegenstand einer Anordnung der Datenschutzbehörde waren.

Im Jahr 2009 verhängte die Datenschutzbehörde 19 Geldbußen in einer Höhe von insgesamt 27.446,19 EUR**.** 12 Bußgelder wurden pünktlich gezahlt. In drei Fällen laufen noch immer Vollstreckungsmaßnahmen. Im Einklang mit den Verwaltungsverfahren haben die Kontrolleure eine Intervention gegen zwei Entscheidungen der Datenschutzbehörde erwirkt. Zwei Verfahren wurden Ende 2009 eingeleitet. In einem der beiden Fälle wurde dem Kontrolleur eine Erinnerung hinsichtlich der Einleitung des Verwaltungsverfahrens zugestellt.

Im Jahr 2009 betrafen 163 der 272 neuen Meldungen Kontrolleure aus dem privaten Sektor und 55 Meldungen Kontrolleure der öffentlichen Verwaltung, z. B. „sonstige Behörden der öffentlichen Verwaltung". In 31 Fällen untersuchte die Datenschutzbehörde Meldungen betreffend unabhängige Behörden. 18 Fälle betrafen Organisationen der Zivilgesellschaft, Stiftungen, politische Parteien oder Bewegungen sowie eingetragene Kirchen oder Religionsgemeinschaften. In 5 Fällen wurden Untersuchungen bei Verwaltungseinrichtungen durchgeführt.

Von den 108 im Jahr 2009 von Datensubjekten eingereichten Meldungen konnte die Datenschutzbehörde 85 Fälle abschließen, von denen wiederum 66 Fälle innerhalb der grundlegenden gesetzlichen Frist von 60 Tagen abgeschlossen werden konnten. Dies entspricht etwa 78 % aller Fälle. Die Untersuchung anderer Meldungen nahm aus den folgenden Gründen mehr Zeit in Anspruch: Notwendigkeit der Konsultation anderer Institutionen, Notwendigkeit der Kontrolle der Ablagesysteme in den Geschäftsräumen des Kontrolleurs, schwierigere Tatsachenfeststellung oder Antrag auf Zusammenarbeit durch den jeweiligen Antragsteller. Bei insgesamt 47 aller bearbeiteten Meldungen konnten keine Verstöße festgestellt werden.

Wenn ein Beschwerdeführer mit der Bearbeitung seiner Meldung durch die Datenschutzbehörde nicht zufrieden ist, kann er die Meldung binnen der gesetzlichen Frist von 30 Tagen erneut bei der Datenschutzbehörde einreichen. Von den 101 im Jahr 2009 abgeschlossenen Fällen (wovon 85 innerhalb des Jahres 2009 eingeleitet und abgeschlossen wurden und 16 im Jahr 2008 eingeleitet und im Jahr 2009 abgeschlossen wurden) wurden lediglich 7 Meldungen erneut bei der Datenschutzbehörde eingereicht. Sechs hiervon wurden im Einklang mit dem Datenschutzgesetz abgelehnt, da sie keine neuen Fakten enthielten. Eine erneute Einreichung wurde vom Oberinspektor untersucht. Dieser Fall wurde durch die Veröffentlichung einer klarstellenden Stellungnahme abgeschlossen. Eine erneute Einreichung ging erst nach Ablauf der gesetzlichen Frist bei der Datenschutzbehörde ein. Im Laufe des Jahres 2009 reichte die Abteilung für Prüfungen eine Meldung bei den Vollstreckungsbehörden ein.

Landesweite Prüfaktivitäten der Datenschutzbehörde
Prüfungen der Verarbeitung personenbezogener Daten durch Arbeitsvermittlungsagenturen (Headhunter)
Im Laufe des Jahres 2009 führte die Datenschutzbehörde zahlreiche landesweite Prüfungen durch. Eine davon betraf die Verarbeitung personenbezogener Daten durch Arbeitsvermittlungsagenturen (Headhunter).

Arbeitsvermittlungsagenturen verarbeiten nicht nur Identifikationsdaten betroffener Personen, sondern auch Daten zu ihren beruflichen Fähigkeiten und Eigenschaften sowie Angaben zu ihrer Persönlichkeit. Diese Daten werden hauptsächlich über ein Internetportal oder per Briefpost erfasst. Im Rahmen der Prüfungen wurden die folgenden Punkte untersucht:

- Rechtsgrundlage für die Erfassung personenbezogener Daten,
- Einhaltung des festgelegten Umfangs und Zwecks der Datenverarbeitung,
- Meldung zu den Details der Datenverarbeitung,
- Korrektheit, Integrität und Aktualität der verarbeiteten personenbezogenen Daten,
- Pflicht zur Vernichtung personenbezogener Daten, sobald der ursprüngliche Grund für ihre Verarbeitung nicht mehr gegeben ist,
- Ergreifung technischer, organisatorischer und persönlicher Maßnahmen zur Sicherstellung des Schutzes der personenbezogenen Daten, einschließlich Maßnahmen zur Vermeidung des Risikos menschlicher Fehler durch Beratung der zu Zugang und Verarbeitung der personenbezogenen Daten „befugten Personen".

Im Rahmen der Prüfungen wurde festgestellt, dass die Kontrolleure die betroffenen Personen nicht ordnungsgemäß über ihre ihnen gemäß dem Datenschutzgesetz zustehenden Rechte informiert haben. Die Datenschutzbehörde ordnete an, dass alle überprüften Kontrolleure diese Mängel innerhalb eines festgelegten Zeitraums zu korrigieren hätten. In zwei Fällen schlug die Datenschutzbehörde vor, finanzielle Sanktionen im Rahmen von Verwaltungsverfahren zu verhängen.

Prüfungen der Verarbeitung personenbezogener Daten durch Reisebüros
Gemäß dem Prüfplan des Jahres 2009 wurden auch Reisebüros kontrolliert. Bei den Reisebüros untersuchte die Abteilung für Prüfungen ähnliche Fragen wie bei den Arbeitsvermittlungsagenturen und prüfte darüber hinaus, ob der Inhalt der Verträge mit den Datenkontrolleuren im Einklang mit dem Datenschutzgesetz steht.
Die Prüfungen ergaben, dass die kontrollierten Reisebüros für den betreffenden Zweck angemessene personenbezogene Daten verarbeiteten, diese vorschriftsgemäß vernichteten und zum Schutz der personenbezogenen Daten angemessene technische, organisatorische und persönliche Maßnahmen ergriffen haben, mit Ausnahme eines Falles. In besagtem Fall wurde festgestellt, dass die Datenkontrolleure die betroffenen Personen nicht angemessen über ihre ihnen gemäß dem Datenschutzgesetz zustehenden Rechte informierten.

Alle Kontrolleure erfassten Daten betroffener Personen mit Hilfe von Datenverarbeitern. In zwei Fällen wurde festgestellt, dass die Verträge nicht im Einklang mit den Bestimmungen des Datenschutzgesetzes standen, da sie im Hinblick auf die Datenverarbeiter keine Liste/keine Angabe des Umfangs der Verarbeitung der personenbezogenen Daten und keine Bedingungen für die Verarbeitung enthielten. Die Datenschutzbehörde forderte die Kontrolleure auf, die festgestellten Mängel zu beseitigen. Diesen Aufforderungen kamen die Kontrolleure vollumfänglich nach.

Besondere Prüftätigkeiten
Im Hinblick auf den Beitritt der Slowakischen Republik zum Schengen-Raum führte die Abteilung für Prüfungen im Jahr 2009 weitere Prüfungen bei ausgewählten Botschaften der Slowakischen Republik im Ausland sowie bei relevanten Behörden in der Slowakischen Republik durch. Ziel der Prüfungen war die Untersuchung der Einhaltung des Datenschutzgesetzes durch die Kontrolleure von Ablagesystemen, der Anwendung der korrekten Verfahren bei der Ausstellung von Schengen-Visa sowie die Erfüllung der im Schengen-Katalog genannten Anforderungen (Empfehlungen und bewährte Verfahrensweisen) im Hinblick auf die Ausstellung von Visa.

Im März 2009 wurden Prüfungen bei den Konsulatsabteilungen der Botschaften der Slowakischen Republik in London und Dublin durchgeführt.

Im dritten Quartal des Jahres 2009 wurden Prüfungen in den folgenden Abteilungen des Büros der Grenz- und Ausländerpolizei (BGAP) des Innenministeriums der Slowakischen Republik durchgeführt: Grenzkontrolleinheit Bratislava Ružinov – Flughafen, Einheit für die Koordination des Betriebs der Informationssysteme der BGAP, Grenzkontrolleinheit Vyšné Nemecké, Grenzkontrolleinheit Košice – Flughafen und Grenzkontrolleinheit Poprad – Flughafen und Direktion der Grenzpolizei Sobrance. Im November 2009 wurde eine Kontrolle bei der Migrationsbehörde des Innenministeriums der Slowakischen Republik sowie beim Asylbewerberzentrum Rohovce durchgeführt, die sich mit der Verarbeitung der personenbezogenen Daten von Asylbewerbern befasste.

Zusammenarbeit der Abteilung für Prüfungen mit den ausländischen Datenschutzbehörden
Im Frühjahr und Herbst 2009 nahm die Abteilung für Prüfungen an internationalen Workshops für Inspektoren der Behörden zum Schutz personenbezogener Daten teil. Im Rahmen des XIX. Workshops in Prag im März 2009 stellte die Abteilung für Prüfungen ihren Beitrag zum Thema „Die Verarbeitung personenbezogener Daten im Gesundheitswesen" vor. Im Rahmen des Arbeitstreffens der Inspektoren in Limassol im Oktober 2009 präsentierte die Datenschutzbehörde ihre aus den Prüfungen gewonnenen Erfahrungen hinsichtlich der Verarbeitung personenbezogener Daten durch Arbeitgeber, einschließlich der Vervielfältigung und Erfassung offizieller Dokumente.

Im November 2009 nahmen die Angestellten der Datenschutzbehörde an der frankophonen Konferenz zum Thema Privatsphäre und Schutz personenbezogener Daten in Madrid teil, die vom Verband der frankophonen Datenschutzbehörden organisiert wurde. Ganz oben auf der Agenda der Konferenz standen der Schutz personenbezogener Daten in der digitalen Welt und der Schutz der Privatsphäre von Kindern. Nach der Konferenz nahmen die Vertreter der Datenschutzbehörde an der Generalversammlung des Verbandes der frankophonen Datenschutzbehörden teil.

Grenzübergreifende Übermittlung personenbezogener Daten

Im Jahr 2009 erteilte die Datenschutzbehörde acht Genehmigungen zur grenzübergreifenden Übermittlung personenbezogener Daten an Länder, in denen es kein angemessenes Datenschutzniveau gibt. Im Fall eines multinationalen Unternehmens wurden Genehmigungen zur Übermittlung personenbezogener Daten unter der Bedingung der Einhaltung der Safe Harbour-Prinzipien durch den Empfänger der Daten erteilt. In den anderen Fällen erfolgte die Erteilung der Genehmigung durch die Anwendung der Standardvertragsklauseln über Datenverarbeiter in Drittländern in den jeweiligen Verträgen betreffend die Übermittlung personenbezogener Daten. Es gab auch Fälle, in denen der Datenkontrolleur – ein multinationales Unternehmen – sowohl die Safe Harbour-Prinzipien einhielt als auch die Standardvertragsklauseln über Datenverarbeiter in Drittländern anwendete und dennoch keinen angemessenen Datenschutz gewährleisten konnte. Bei den Daten, die grenzübergreifend übermittelt werden, handelt es sich meistens um personenbezogene Daten von Angestellten und Kunden internationaler Unternehmen.

Im Laufe des Jahres 2009 gab die Abteilung für Auswärtige Beziehungen 48 schriftliche Stellungnahmen zu Fragen aus, die von Kontrolleuren von Informationsablagesystemen oder von Anwaltskanzleien, die die Kontrolleure von Informationsablagesystemen vertreten, eingereicht wurden. Die Fragen betrafen zumeist die Übermittlung persönlicher Beschäftigungsdaten, die Personalverwaltung, den Bereich Whistleblowing sowie die Verarbeitung der personenbezogenen Daten der Kunden des Kontrolleurs.

Die Fragen zielten auf eine Klarstellung der Bedingungen für die grenzübergreifende Übermittlung personenbezogener Daten zwischen folgenden Teilnehmern ab:

- Kontrolleure und Datenverarbeiter in EU-Ländern,
- Kontrolleure und Datenverarbeiter in Indien und der Republik Korea,
- Kontrolleure und Datenverarbeiter mit Sitz in EU-Ländern, die diese Daten an ein Drittland weiterübermitteln, das keinen angemessenen Datenschutz bietet,
- Grenzübergreifende Übermittlung von Daten zum Zweck des Whistleblowings.

Internationale Zusammenarbeit

Die Aufgaben auf internationaler Ebene ergaben sich hauptsächlich aus der Mitgliedschaft der Slowakischen Republik in der Europäischen Union sowie in Arbeitsgruppen, die unter der Schirmherrschaft und im Rahmen von Rechtsakten der Europäischen Gemeinschaften eingerichtet wurden. Besondere Verpflichtungen ergaben sich aus folgenden Mitgliedschaften der Slowakischen Republik: Europol, Schengener Informationssystem, Zollinformationssystem, Arbeitsgruppe für polizeiliche und justizielle Zusammenarbeit, Koordinationsgruppe Eurodac und Arbeitsgruppe Schengen-Bewertung (SCHEVAL). Gemäß dem von der Europäischen Kommission und dem Ständigen Ausschuss zur Bewertung der Schengen-Staaten erarbeiteten Arbeitsprogramm für 2009 führte die Expertengruppe SCH-EVAL folgende Maßnahmen durch:

- Eine Prüfung der Umsetzung der Grundprinzipien für die Verarbeitung personenbezogener Daten im SIS durch „alte Schengen-Staaten" (Deutschland, Frankreich, Belgien, die Niederlande und Luxemburg),
- Eine Prüfung der Bereitschaft zur die Umsetzung des Schengen-Besitzstandes im Bereich des Schutzes personenbezogener Daten in den Bewerberländern – Bulgarien und Rumänien.

Die in den Bewertungsberichten genannten Ergebnisse und Empfehlungen zeigten einerseits die Grenzen der praktischen Anwendung des SIS-Übereinkommens und andererseits einen verantwortungsvollen Ansatz der bewerteten Bewerberländer, die bemüht sind, die für den Beitritt zum Schengen-Raum erforderlichen Kriterien zu erfüllen. Die endgültigen Bewertungsberichte

wurden der Arbeitsgruppe SIS / SIRENE und dem Rat zur Genehmigung vorgelegt.

Im Rahmen von bilateralen und regionalen Treffen zur Diskussion spezifischer Fragen der Zusammenarbeit sowie zum Austausch bewährter Verfahrensweisen waren die wichtigsten Veranstaltungen folgende:

- Teilnahme am 11. Treffen der mittel- und osteuropäischen Datenschutzbehörden (Datenschutzbehörden der EWG-Staaten) im Mai 2009,
- Treffen mit dem Europäischen Datenschutzbeauftragten Peter Hustinx in den Räumen der Datenschutzbehörde im September 2009. Herr Hustinx wurde gründlich über die Tätigkeiten der Datenschutzbehörde informiert und diskutierte mit den Angestellten der Datenschutzbehörde Herausforderungen und neue Prioritäten im Bereich Datenschutz in der Europäischen Union sowie Möglichkeiten zur Erreichung der bestmöglichen Synergie der Anstrengungen der Datenschutzbehörden im Bereich Datenschutz. Herr Hustinx besuchte auch den Nationalrat der Slowakischen Republik. Dort traf er sich mit Mitgliedern des parlamentarischen Ausschusses für Menschenrechte, Minderheiten und den Status von Frauen. Zum Anlass seines Besuches in der Slowakei wurde eine Sonderpressekonferenz organisiert.
- Ein umfassender Austausch bewährter Verfahrensweisen im Bereich der Strategie gegenüber Massenmedien, Sensibilisierung sowie Möglichkeiten zur Zusammenarbeit mit der Datenschutzbehörde der Tschechischen Republik in Bratislava im Oktober 2009.

Slowenien

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

In Slowenien ist der rechtliche und institutionelle Rahmen im Bereich Datenschutz (sowie im Hinblick auf den Zugang zu öffentlichen Informationen) bereits seit Jahren umgesetzt und steht im Einklang mit dem Besitzstand der Gemeinschaft (*acquis communautaire*).

Im Einklang mit der Sonderbestimmung von Art. 48 des Gesetzes zum Schutz personenbezogener Daten[23] (GSPD) hat der Datenschutzbeauftragte zahlreiche vorläufige Stellungnahmen zu Gesetzesentwürfen hinsichtlich deren Einhaltung des Datenschutzgesetzes ausgegeben. Zu den wichtigsten Errungenschaften des Datenschutzbeauftragten gehören die Ende 2009 verabschiedeten Änderungen und Ergänzungen des Gesetzes über elektronische Kommunikation[24] (GEK). Die Änderungen umfassen die Bestimmung betreffend die Anonymisierung von Telefonnummern in Einzelverbindungsnachweisen für Anschlussinhaber gemäß den Vorgaben der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG). Die Empfehlungen der Artikel-29-Datenschutzgruppe (WP 113) hinsichtlich der Richtlinie über die Vorratsdatenspeicherung (2006/24/EG) wurden ebenfalls berücksichtigt. Der Zeitraum für die Vorratsspeicherung von Daten ist nunmehr auf acht Monate gekürzt und darf nicht mehr als 14 Monate betragen. Das geänderte GEK beschränkt auch den Zeitraum der Vorratsspeicherung bereitgestellter auf Vorrat gespeicherter Daten und limitiert die Registrierung bereitgestellter auf Vorrat gespeicherter Daten von einem unbegrenzten Zeitraum auf einen Zeitraum von 10 Jahren. Eine der wichtigsten Änderungen des GEK ist die Bestimmung betreffend die Weitergabe von Verbindungs- und Standortdaten an die Polizei zum Zwecke des Schutzes von Leib und Leben sowie betreffend die Kompetenz des Datenschutzbeauftragten zur Überwachung der Bestimmungen über das rechtmäßige Abfangen von Kommunikationen.

[23] Amtsblatt der Republik Slowenien, Nr. 94/2007

[24] Amtsblatt der Republik Slowenien, Nr. 13/2007

Die weiteren wesentlichen Gesetze, mit denen sich der Datenschutzbeauftragte im Jahr 2009 befasste, betreffen allgemeine Verwaltungsverfahren, Strafverfahren, Ausländer, Ausweise, die Staatsgrenzen, das Bankenwesen, auswärtige Angelegenheiten, das Gesundheitswesen, die Polizei, das Rote Kreuz, das Familiengesetz, Geldwäsche, die Unterbindung der Finanzierung von Terroristen und Archive.

B. Bedeutende Rechtsprechung

Wie in den vergangenen Jahren, befasste sich der Datenschutzbeauftragte im Jahr 2009 mit zahlreichen Fällen die in den nationalen Medien große Beachtung fanden.

Politische Parteien

Der Datenschutzbeauftragte leitete aufgrund des Verdachts einer unrechtmäßigen Erfassung und Vorratsspeicherung personenbezogener Daten zu Wahlkampfzwecken ein Prüfverfahren gegen zwei politische Parteien in Slowenien ein. Die Beschwerden wurden von einer Reihe slowenischer Bürger/eingetragener Wähler, die im Ausland leben, vorgebracht, die Werbematerial (Direktwerbung) von zwei politischen Parteien erhielten, ohne den Parteien zuvor ihr Einverständnis gegeben zu haben, ihre Kontaktdaten zu Werbezwecken zu verwenden. Im Laufe des Verfahrens konnten die politischen Parteien keine Rechtsgrundlage für die Erfassung der Kontaktdaten der Bürger benennen. Aufgrund des festgestellten Verstoßes verhängte der Datenschutzbeauftragte ein Bußgeld von jeweils 4.170 € gegen die Parteien. Die haftbaren Personen der Parteien wurden ebenfalls mit einer Geldbuße von jeweils 830 € belegt.

Präsident des Bezirksgerichts

Gegen den Präsidenten des Bezirksgerichtes wurde aufgrund zweier Fälle unrechtmäßiger Verarbeitung personenbezogener Daten eine Geldbuße in Höhe von 1.660 € verhängt. Im Rahmen des Verstoßverfahrens wurde festgestellt, dass die betreffende Person Daten zu Anrufen von Diensttelefonen (Verbindungsdaten) zweier Angestellter erfasst und weiterverarbeitet hatte. Der Zweck der Verarbeitung dieser Verbindungsdaten war nicht definiert oder rechtmäßig und die Weiterverarbeitung dieser Daten stand

nicht im Einklang mit dem Gesetz. Die Entscheidung des Datenschutzbeauftragten ist noch nicht endgültig. Gemäß den Bestimmungen des Gesetzes über die Gerichte führte das höherinstanzliche Gericht ebenfalls eine Prüfung der Arbeit der Verwaltung bei oben genanntem Bezirksgericht durch.

Da dieser Fall weit verbreitete Probleme im Bereich Privatsphäre am Arbeitsplatz betraf, brachte der Datenschutzbeauftragte erneut seine Ansicht zum Ausdruck, dass dieser Bereich einen verbesserten rechtlichen Rahmen benötige, da praktisch ein Drittel aller Fälle, die in den Zuständigkeitsbereich des Datenschutzbeauftragten fallen, die Privatsphäre am Arbeitsplatz betrifft.

Unrechtmäßiger Austausch personenbezogener Daten zwischen zwei Versicherungsunternehmen

Der Datenschutzbeauftragte verhängte für die unrechtmäßige Verarbeitung personenbezogener Daten Bußgelder gegen zwei Versicherungsunternehmen sowie die jeweils haftbaren Personen. Im Rahmen des Verfahrens stellte der Datenschutzbeauftragte fest, dass die personenbezogenen Daten von 2.382 Personen ohne Rechtsgrundlage sowie ohne das Einverständnis der betroffenen Personen ausgetauscht worden waren.

Gegen das Versicherungsunternehmen, das die personenbezogenen Daten bereitgestellt hatte, wurde ein Bußgeld für die unrechtmäßige Bereitstellung personenbezogener Daten sowie für die unzureichende Rückverfolgbarkeit der bereitgestellten Daten verhängt. Der Datenschutzbeauftragte hatte unwiderlegbare Beweise dafür, dass die Daten von 26 Personen unrechtmäßig verarbeitet worden waren. Gegen das Unternehmen wurde ein Bußgeld in Höhe von 112.590 € verhängt. Gegen die haftbaren Person wurde ein Bußgeld in Höhe von 20.000 € verhängt. Das Unternehmen legte Berufung gegen diese Entscheidung ein. Gegen das andere Versicherungsunternehmen wurde für den unrechtmäßigen Erwerb personenbezogener Daten ein Bußgeld in Höhe von 108.420 € verhängt. Gegen die haftbaren Person wurde ein Bußgeld in Höhe von jeweils 20.000 € verhängt. Dieses Unternehmen nutzte die gesetzlich mögliche Option und zahlte die Hälfte des Bußgeldes sofort.

Die Bußgelder in diesen Fällen waren die höchsten, die der Datenschutzbeauftragte bisher verhängt hatte. Der Datenschutzbeauftragte betonte, dass in zukünftigen Fällen des unrechtmäßigen Austauschs personenbezogener Daten zwischen Datenkontrolleuren, die im Besitz sensibler personenbezogener Daten oder großer Datenbanken sind, mit strengen Sanktionen zu rechnen ist.

Datenschutz bei Banken

Der Datenschutzbeauftragte führte eine systematische Prüfung der Sicherheit personenbezogener Daten in der Bankenbranche durch (sechs der größten Banken). Hierbei wurde die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten bei der Übermittlung der Kreditdaten von Kunden zwischen Banken im Rahmen des neuen SISBON-Systems sowie die Rechtmäßigkeit der Zugriffe auf die Bankkontodaten der Kunden untersucht. Der Datenschutzbeauftragte stellte fest, dass im Rahmen des Datenaustauschs zwischen Banken nicht unrechtmäßig auf Daten zugegriffen worden war. In zwei der geprüften Banken wurde jedoch ein unbefugter Zugriff auf die Daten einiger bekannter Kunden (Politiker) festgestellt. Gegen die Angestellten, die unbefugt auf die Daten der Bankkonten der Kunden zugegriffen hatten, wurde gemäß dem allgemeinen Strafgesetzbuch ein Bußgeld verhängt.

Auf der Website des Datenschutzbeauftragten veröffentlichte E-Mail-Adressen und Fragen von Journalisten

Der Datenschutzbeauftragte veröffentlichte auf seiner Website eine E-Mail von einem Journalisten, die journalistische Fragen sowie die dienstliche E-Mail-Adresse des Journalisten enthielt. Die E-Mail-Adresse des Journalisten wurde auch an eine Reihe von Empfängern der Mailingliste des Datenschutzbeauftragten verschickt. Der Journalist legte Beschwerde ein. Der Datenschutzbeauftragte konnte jedoch keinen Verstoß gegen das Datenschutzgesetz feststellen und leitete kein Untersuchungsverfahren ein. Die Begründung des Datenschutzbeauftragten lautete, dass die E-Mail an die dienstliche E-Mail-Adresse des Datenschutzbeauftragten geschickt wurde, die eingerichtet worden war, um E-Mails mit Fragen zur Arbeit des Datenschutzbeauftragten von natürlichen und juristischen Personen zu empfangen. Vorname, Nachname sowie dienstliche E-Mail-Adresse des Journalisten stellten in diesem Fall keine geschützten

personenbezogenen Daten dar, da der Journalist in seiner öffentlichen Funktion als Journalist handelte und sein Name auch auf der offiziellen Webseite der Medien veröffentlicht war. Die Veröffentlichung seiner E-Mail-Adresse stellte somit keine Beeinträchtigung seiner Privatsphäre und Würde dar. Die in der E-Mail enthaltenen Fragen betrafen die öffentliche Natur der Arbeit des Datenschutzbeauftragten. Darüber hinaus waren die Inhalte der Kommunikation zur Veröffentlichung bestimmt. Aus diesem Grund konnten die Fragen des Journalisten nicht als geschützte personenbezogene Mitteilungen, sondern vielmehr als öffentliche Information eingestuft werden.

Veröffentlichung eines Gerichtsurteils in der Zeitung
In einer slowenischen Tageszeitung wurde ein Teil eines Gerichtsurteils mit personenbezogenen Daten des Klägers veröffentlicht. Der Datenschutzbeauftragte stufte dies als Verstoß gegen das Gesetz zum Schutz personenbezogener Daten ein und verhängte gegen die Zeitung sowie die haftbare Person ein Bußgeld. Der Fall ist von großer Bedeutung, da der Datenschutzbeauftragte der Ansicht war, dass die in einem Gerichtsurteil enthaltenen personenbezogenen Daten als nicht-öffentlich einzustufen und damit zu schützen sind. Das Gerichtsurteil darf somit nur in anonymisierter Form veröffentlicht werden. Der Datenschutzbeauftragte war außerdem der Ansicht, dass im Fall eines Konflikts zwischen dem Recht auf Meinungsfreiheit und dem zugehörigen verfassungsmäßigen Prinzip der Öffentlichkeit von Prozessen sowie dem Recht auf Datenschutz in diesem Fall das Recht auf Datenschutz nicht-öffentlicher Informationen vorrangig ist. Das öffentliche Interesse umfasst nicht alles, woran die Öffentlichkeit interessiert ist, und die bloße Neugier der Öffentlichkeit darf keine Beeinträchtigung des verfassungsmäßigen Rechts auf Datenschutz mit sich bringen.

C. Wichtige spezifische Themen

Zusätzlich zu seiner Funktion als Aufsichts- und Vollstreckungsbehörde führte der Datenschutzbeauftragte auch weitere Tätigkeiten im Hinblick auf die Bestimmungen des Gesetzes zum Schutz personenbezogener Daten durch.

Da **biometrische Messungen** nur mit Genehmigung des Datenschutzbeauftragten durchgeführt werden können, gingen im Jahr 2009 insgesamt nur 10 Anträge auf solche Messungen ein (verglichen mit 16 im Jahr 2008 und 40 im Jahr 2007). Im Verhältnis war ein Rückgang der Anzahl an ausgegebenen Entscheidungen zu verzeichnen – 6 Entscheidungen (4 genehmigt, 2 abgelehnt) im Vergleich zu 17 Entscheidungen im Jahr 2008 und 35 im Jahr 2007.

Die Situation bei der Erteilung von Genehmigungen zur **Zusammenschaltung von Ablagesystemen** zeigte sich im Jahr 2009 unverändert: In den Jahren 2009 und 2008 wurden acht Entscheidungen bezüglich der Verknüpfung von Ablagesystemen getroffen (sieben im Jahr 2007).

Im Jahr 2009 gingen beim Datenschutzbeauftragten als zuständige Stelle für die Bearbeitung von Beschwerden von Datensubjekten hinsichtlich des **Rechts auf Information** 71 Beschwerden ein.

Bis zum Ende des Jahres 2009 wurden mehr als 11.000 Kontrolleure von Ablagesystemen für personenbezogene Daten in dem vom Datenschutzbeauftragten verwalteten **öffentlichen Register** eingetragen und auf seiner Website veröffentlicht. Die Zahlen zeigen eine Zunahme um etwa 1.000 neue Einträge pro Jahr.

Im Rahmen seiner **Prüfaktivitäten** (seit Dezember 2009 gibt es neun beim Datenschutzbeauftragten beschäftigte staatliche Datenschutzinspektoren), gingen beim Datenschutzbeauftragten im Jahr 2009 624 Anträge und Beschwerden betreffend vermutete Verstöße gegen die Bestimmungen des Gesetzes zum Schutz personenbezogener Daten ein, davon 219 (256 im Jahr 2008) aus dem privaten Sektor und 405 (379 im Jahr 2008) aus dem öffentlichen Sektor. Verglichen mit den vorherigen Jahren (635 Fälle im Jahr 2008, 406 Fälle im Jahr 2007 und 231 Fälle im Jahr 2006) war eine Abmilderung des starken Anstiegs der Fälle von 76 % im Jahr 2007 und 56 % im Jahr 2008 zu verzeichnen. Ähnlich wie in den vorangegangenen Jahren betrafen die meisten Beschwerden die unrechtmäßige oder unverhältnismäßige Erfassung personenbezogener Daten, die Weitergabe personenbezogener Daten an nicht befugte Nutzer, die illegale Videoüberwachung, den unzureichenden Schutz personenbezogener Daten, die unrechtmäßige Veröffentlichung personenbezogener Daten usw. In 163

Fällen wurden Verwaltungsverfahren eingeleitet (279 Fälle im Jahr 2008 und 133 Fälle im Jahr 2007).

Im Jahr 2009 führten die Anträge auf **schriftliche Stellungnahmen** und Klarstellungen zu 596 schriftlichen Antworten und 1471 Kurzantworten des Datenschutzbeauftragten (sowie mehreren Hundert Antworten per Telefon). Angesichts der Zahl von 853 Fällen im Jahr 2008 und 1.144 Fällen im Jahr 2007, spiegeln diese Zahlen deutlich das nachhaltig hohe Niveau des öffentlichen Bewusstseins für das Recht auf Privatsphäre wider, das einem modernen Gesetz zum Schutz personenbezogener Daten sowie außerdem der transparenten Arbeit und den intensiven Öffentlichkeitskampagnen des Datenschutzbeauftragten zu verdanken ist.

Zusätzlich zur Veröffentlichung nicht bindender Stellungnahmen in Form von schriftlichen Erläuterungen auf seiner Website sowie zur Veröffentlichung einer Reihe von Broschüren zu Datenschutzfragen veröffentlichte der Datenschutzbeauftragte auch im Jahr 2009 **Leitlinien** zu speziellen Datenschutzfragen. Ziel der Leitlinien des Datenschutzbeauftragten ist die Bereitstellung praktischer Anweisungen und Informationen für die Öffentlichkeit, Datensubjekte und Datenkontrolleure in Form von häufig gestellten Fragen und Antworten im Hinblick auf die Einhaltung der rechtlichen Bestimmungen des Gesetzes zum Schutz personenbezogener Daten und/oder anderer Gesetze. Im vergangenen Jahr bearbeitete der Datenschutzbeauftragte Leitlinien zum Verhaltenskodex betreffend die Erfassung personenbezogener Daten, den Schutz personenbezogener Daten im Hinblick auf die Medien, die Information und Sensibilisierung von Verbrauchern, die Erkennung von Datendiebstahl, den Datenschutz von Kindern in Schulen, die Vorbeugung und den Schutz vor Belästigungen im Internet (Cyber-Mobbing) und die Sozialwissenschaft.

Im Rahmen des dritten Europäischen **Datenschutztages**, der im Jahr 2009 zum fünften Mal begangen wurde, organisierte der Datenschutzbeauftragte ein Rundtischgespräch zum Thema „Privatsphäre am Arbeitsplatz". Zum dritten Mal zeichnete der Datenschutzbeauftragte Personen aus dem öffentlichen und privaten Sektor für vorbildliches Verhalten im Bereich Datenschutz aus. Die Preise für herausragende Leistungen im Bereich Datenschutz wurden an das Unternehmen Cetis d. d. sowie das Verteidigungsministerium der Republik Slowenien verliehen. Außerdem wurden zum ersten Mal Auszeichnungen an Unternehmen verliehen, die im Rahmen eines ISO/IEC27001-Zertifikates für Informationssicherheit ein hohes Maß an Sicherheit personenbezogener Daten bieten.

Internationale Zusammenarbeit

Ständige Zusammenarbeit in den Gremien der Europäischen Union und des Europarates

Der Datenschutzbeauftragte arbeitet als nationale Regulierungsbehörde im Bereich Datenschutz permanent mit den zuständigen Stellen der Europäischen Union und des Europarates im Bereich Datenschutz zusammen. Der Datenschutzbeauftragte ist gemäß den Bestimmungen der Richtlinie 95/46/EG zur internationalen Zusammenarbeit verpflichtet.

Im Jahr 2009 nahm der Datenschutzbeauftragte aktiv an fünf Arbeitsgruppen auf EU-Ebene teil, die sich mit der Kontrolle des Datenschutzes in der EU in verschiedenen Bereichen befassen. Hierzu gehören die Artikel-29-Datenschutzgruppe, die Gemeinsame Kontrollinstanz von Europol, die Gemeinsame Kontrollinstanz von Schengen und die Arbeitsgruppe Zollinformationssystem sowie die Koordinationstreffen des Europäischen Datenschutzbeauftragten mit den nationalen Behörden zum Schutz personenbezogener Daten unter Kontrolle von EURODAC.

Im Jahr 2009 wurde der Datenschutzbeauftragte als stellvertretender Vorsitzender der gemeinsamen Kontrollinstanz von Europol gewählt und nahm im Rahmen der polizeilichen und justiziellen Zusammenarbeit regelmäßig an Treffen der Arbeitsgruppe für Polizei und Justiz teil.

Mit dem Beitritt Sloweniens zum Schengen-Raum wurde der Datenschutzbeauftragte zur unabhängigen Stelle für die Beaufsichtigung von Datenübermittlungen zum Zweck des Übereinkommens. Seine Kompetenzen wurden um die Beaufsichtigungsbefugnisse von Artikel 128 des Schengener Übereinkommens erweitert. Im Jahr 2009 gingen 55 Anträge auf Zugang zu personenbezogenen Daten ein. Keiner der Anträge wurde abgelehnt. Beim Datenschutzbeauftragten gingen keine

Beschwerden hinsichtlich der Wahrnehmung des Rechts von Einzelpersonen auf Zugang zu ihren Daten im SIS auf erster Ebene ein.

Im Jahr 2009 nahm der Datenschutzbeauftragte im Rahmen von SCHEVAL an der Arbeit der Kontrollgruppe zur Schengen-Bewertung hinsichtlich des Beitritts von Bulgarien und Rumänien zum Schengen-Raum Teil.

Im Kontext des Europarates nahm ein Vertreter des Datenschutzbeauftragten an der Arbeit des Beratungsausschusses des Europarates zur Kontrolle des Übereinkommens zum Schutze der Menschen bei der automatischen Verarbeitung personenbezogener Daten (T-PD) teil. In diesem Jahr arbeitete der Rat hauptsächlich am Entwurf einer Empfehlung betreffend den Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten im Rahmen von Profilerstellungen.

Der Datenschutzbeauftragte nahm außerdem aktiv an der Untergruppe Internet und Informationstechnologie im Rahmen der Arbeitsgruppe Datenschutz teil. Die Arbeitsgruppe verabschiedete im Jahr 2009 zwei wichtige Dokumente, nämlich die Empfehlung zum Datenschutz und elektronischem Müll sowie den Bericht und die Leitlinien zum Thema Straßenbenutzungsgebühren – „Sofia-Memorandum". Das Sofia-Memorandum wurde auf Empfehlung des slowenischen Datenschutzbeauftragten initiiert. Die internationale Arbeitsgruppe IWGDPT setzt ihre Arbeit in den Bereichen Deep Packet Inspection, Geolokationsdaten, Websites für soziale Netzwerke sowie in anderen Bereichen fort.

Sonstige internationale Zusammenarbeit
Die Vertreter des Datenschutzbeauftragten haben an den folgenden wichtigen **internationalen Veranstaltungen** teilgenommen:

Konferenz in Barcelona „Hochrangiges Treffen zum gemeinsamen Vorschlag für einen Entwurf internationaler Standards im Bereich Privatsphäre und Datenschutz".
Frühlingskonferenz zum Schutz personenbezogener Daten, Edinburgh
2. European Privacy Open Space und „re:publica", Berlin
Datenschutzkonferenz 2009, Brüssel
11. Treffen der mittel- und osteuropäischen Datenschutzbeauftragten, Rumänien
Treffen des Open Society Institute zum Thema Informationsfreiheit, Budapest
Stärkung des Datenschutzes in Israel, Tel Aviv (Partnerschaftsprojekt)
Internationale Konferenz der Datenschutzbeauftragten, Oslo
10. Workshop zur Fallbearbeitung, Limassol
3. Privacy Open Space-Konferenz, Wien
31. Internationale Konferenz für Datenschutz und Privatsphäre, Madrid

Grundlage für die Arbeit des Datenschutzbeauftragten war eine **bilaterale Zusammenarbeit**, hauptsächlich mit Ungarn, Serbien und Montenegro.

All diese Anstrengungen und Errungenschaften haben zu dem hohen Ansehen des Datenschutzbeauftragten in Bezug auf Reputation, Vertrauen der Öffentlichkeit sowie Bewusstsein der Öffentlichkeit über seine Tätigkeiten geführt. Dies spiegelt sich auch in den Ergebnissen öffentlicher Meinungsumfragen wider. Den aktuellen Ergebnissen (Januar 2010) der vom öffentlichen slowenischen Meinungsforschungszentrum durchgeführten Umfrage zum Vertrauen der Öffentlichkeit in den Datenschutzbeauftragten zufolge genießt dieser offensichtlich ein zunehmendes Vertrauen. Von allen Institutionen, zu denen Meinungsumfragen durchgeführt wurden, ist lediglich die offizielle Währung, der Euro, noch vertrauenswürdiger als der Datenschutzbeauftragte. Mit einem hohen Maß an Vertrauen der Öffentlichkeit (53,1 %) lag der Datenschutzbeauftragte noch vor allen anderen Institutionen, so zum Beispiel vor dem Militär, dem Präsidenten der Republik, dem Ombudsmann, den Schulen und der Polizei. Außerdem erwähnenswert ist die Tatsache, dass der Datenschutzbeauftragte von allen in der Umfrage genannten Institutionen die geringste Misstrauensquote verzeichnet.

Im Mai 2009 wählte die Nationalversammlung der Republik Slowenien auf Vorschlag des Präsidenten der Republik Frau Nataša Pirc Musar für weitere fünf Jahre mit überwältigender Mehrheit zur Datenschutzbeauftragten.

Spanien

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

Im Laufe des Jahres 2009 wurden die folgenden Verordnungen zum Datenschutz angenommen:

1. Gesetz 25/2009 vom 22. Dezember zur Änderung zahlreicher Gesetze im Hinblick auf die Anpassung an Gesetz 17/2009 über den freien Zugang zu Dienstleistungen sowie deren Erbringung.
   Dieses Gesetz ändert unter anderem das Gesetz zum Schutz der privaten Sicherheit und liberalisiert den Verkauf, die Bereitstellung, die Durchführung sowie die Verwaltung zahlreicher Sicherheitsdienste, einschließlich Systemen zur Videoüberwachung. Vor dem Inkrafttreten dieses Gesetzes war die Installation solcher Geräte gemäß dem Datenschutzgesetz nur dann gestattet, wenn sie durch vom Innenministerium akkreditierte Unternehmen erfolgte. Darüber hinaus musste der Installationsvertrag der Polizei gemeldet werden. Diese formalen Anforderungen gelten jetzt nicht mehr.

2. Gesetz 29/2009 vom 30. Dezember zur Änderung der Verordnungen betreffend unlauteren Wettbewerb und Werbung im Hinblick auf die Verbesserung der Rechte von Verbrauchern und Nutzern.

   Unbeschadet der Bestimmungen der Datenschutzvorschriften sowie der Vorschriften für Dienstleistungen der Informationsgesellschaft und Telekommunikation, legt dieses Gesetz fest, dass wiederholte unaufgeforderte Nachrichten zu Werbezwecken (Direktwerbung), die per elektronischer Post oder mithilfe ähnlicher Mittel zugestellt werden, als unlauteres Verhalten eingestuft werden. Ausgenommen hiervon sind Situationen, in denen dies im Hinblick auf die Erfüllung einer vertraglichen Verpflichtung gesetzlich gerechtfertigt ist.

Darüber hinaus hat die spanische Datenschutzbehörde (AEPD, Agencia Española de Protección de Datos) ihre Arbeit hin zu größerer rechtlicher Sicherheit und einem nationalen Rechtssystem im Einklang mit dem Datenschutzgesetz fortgeführt. Die Rechtsabteilung veröffentlichte gemäß den Anforderungen des Datenschutzgesetzes über 100 Berichte über die Annahme allgemeiner Bestimmungen, wie zum Beispiel:

- Entwurf für das Gesetz zur Vorbeugung von Geldwäsche sowie der Finanzierung von Terroristen, das bereits zweimal verschoben worden war.
- Entwurf für das Gesetz über die sexuelle und reproduktive Gesundheit und Abtreibung.
- Entwurf für den Königlichen Beschluss über die MindestdatenmengeMindestdatensätze, die in klinischen Berichten im Nationalen Gesundheitssystem zu erfassen sind.

Entwurf von Bestimmungen zur Änderung von Gesetz 11/2007 vom 22. Juni über den elektronischen Zugriff von Bürgern auf öffentliche Dienste zur Umsetzung der Richtlinie 2006/123/EG in spanisches Recht.

B. Bedeutende Rechtsprechung

Vor der Analyse der einzelnen Urteile der spanischen Gerichte ist es wichtig, zu erwähnen, dass eine nicht unerhebliche Anzahl von Urteilen betreffend das Recht auf Löschung aus den Taufbüchern der katholischen Kirche gefällt wurden. Alle entsprechenden Urteile standen im Einklang mit Urteil 4646/2008 des Obersten Gerichtshofes vom 19. September, das im 12. Jahresbericht der Artikel-29-Datenschutzgruppe detailliert erläutert ist. Aus diesem Grund wurden die folgenden Analysen unter Berücksichtigung dieser Urteile durchgeführt.

Nationaler Gerichtshof

Im Jahr 2009 fällte der Nationale Gerichtshof Urteile zu 240 Berufungen im Hinblick auf die Aufhebung von Beschlüssen der spanischen Datenschutzbehörde. 162 davon wurden in vollem Umfang abgewiesen (68 %). Hinsichtlich der zugelassenen Berufungen (17 teilweise und 61 in vollem Umfang) sollte erwähnt werden, dass viele hiervon auf unterschiedlichen Interpretationen von Beweisen basierten und nicht auf der Anwendung der Gesetze. Bemerkenswert sind folgende Urteile:

- Das Urteil vom 17. März, das sich zum ersten Mal mit einer Klage gegen einen Beschluss befasste, der eine Übermittlung personenbezogener Daten an ein Drittland nicht gestattete.

- Das Urteil vom 22. April, das besagt, dass die Aufzeichnung einer Person ohne deren Einverständnis in einer auf CD gespeicherten Videodatei, die als Beweis in einem Prozess verwendet werden soll, außerhalb des Anwendungsbereichs des Datenschutzgesetzes liegt, da solche Daten nicht Teil eines Ablagesystems sind und die Integration dieser Daten in ein Ablagesystem nicht beabsichtigt ist.
- Das Urteil vom 9. Juli, das besagt, dass die Veröffentlichung von Bildern eines Terroropfers mit irreversiblen Gehirnschäden in einer Zeitung unverhältnismäßig war und dass das Recht auf Datenschutz in diesem Fall Vorrang vor dem Recht auf Informationsfreiheit hat.
- Das Urteil vom 9. Oktober, das klarstellte, dass von Staatsanwälten verwaltete Ablagesysteme den Bestimmungen des Datenschutzgesetzes und somit der Aufsichtsbefugnis der spanischen Datenschutzbehörde unterliegen.
- Das Urteil vom 26. November, das die von der spanischen Datenschutzbehörde verhängten Bußgelder gegen ein Unternehmen bestätigte, welches die personenbezogenen Daten eines Minderjährigen ohne das Einverständnis seiner Eltern verarbeitet hatte, um ihm im Rahmen einer Direktwerbekampagne eine Kreditkarte anzubieten.

Oberster Gerichtshof

Der Oberste Gerichtshof bestätigte die Kriterien der spanischen Datenschutzbehörde in 16 seiner 19 Urteile zu Beschlüssen der Datenschutzbehörde; nachstehend einige Beispiele:

- Das Urteil vom 28. April, das besagt, dass für ein auf einem in den Vereinigten Staaten befindlichen Server gespeichertes Ablagesystem spanisches Recht gilt; die Daten des Ablagesystems werden zur Durchführung einer Werbekampagne eines spanischen Unternehmens verarbeitet, die sich an spanische Bürger richtet.
- Das Urteil vom 17. November, das bestätigt, dass die Ausnahmeregelung zur Genehmigung der Übermittlung personenbezogener Daten an Gerichte nur dann gilt, wenn die Gerichte die Übermittlung dieser Daten direkt beantragen.

Beschlüsse der spanischen Datenschutzbehörde

Die Anzahl der im Jahr 2009 bei der Datenschutzbehörde gemeldeten Verstöße führte zu einem Anstieg der durchgeführten Maßnahmen um 75 % und belief sich auf über 4.100 (wobei zumeist die Bereiche Telekommunikation, Finanzinstitutionen und Videoüberwachung geprüft wurden). Hinsichtlich der Verhängung von Sanktionen gegen private Organisationen, Telekommunikations- und Finanzinstitutionen konnte jedoch ein Rückgang um 10,34 % beziehungsweise 21,26 % verzeichnet werden, obwohl diese Bereiche bei den eingeleiteten Verfahren die Plätze eins und drei belegten. Andererseits kletterte der Bereich der privaten Videoüberwachung aus Sicherheitsgründen mit einer Zunahme von 229,55 % im Vergleich zum Vorjahr auf den zweiten Platz. Darüber hinaus war angesichts der im Jahr 2009 entstandenen Wirtschaftskrise eine exponentielle Zunahme der Maßnahmen zu verzeichnen, die sich aus Klagen wegen Verzug ableiteten oder damit in Zusammenhang standen. Die Zahl der Beschlüsse, die einen Verstoß der öffentlichen Verwaltung gegen das Datenschutzgesetz darstellen, erhöhte sich um etwa 12,5 %.

Es wurden Sanktionen in einer Höhe von insgesamt 24.872.979,72 Euro verhängt. Wenngleich diese Zahl im Vergleich zum Vorjahr eine Zunahme um 12,99 % bedeutet, so liegt sie jedoch im Bereich der im Jahr 2006 verhängten Sanktionen. Der wesentliche Unterschied liegt darin, dass die Anzahl der im Jahr 2009 abgeschlossenen Strafverfahren um 235 % höher liegt als im Jahr 2006. Gerade diese deutliche Zunahme der Strafverfahren und nicht die Summe der verhängten Sanktionen erklärt den Betrag der verhängten Sanktionen. Die stärkste Zunahme ist bei den kleineren Sanktionen zu verzeichnen (44,76 %), während die Zahl der Sanktionen aufgrund schwerer Verstöße gleich geblieben und die Zahl der Sanktionen aufgrund sehr schwerer Verstöße um fast 6 % zurück gegangen ist. Im Hinblick auf die insgesamt verhängten Sanktionen ist in 40,72 % der Fälle ein deutlicher Rückgang der Haftungssumme derer, die einen Verstoß begangen hatten, zu verzeichnen. Nach Analyse der präsentierten Daten ist die Schlussfolgerung angebracht, dass die quantitative Zunahme der Sanktionen, eine Folge der vorherigen Zunahme der Anzahl an Beschwerden, nicht von der Tatsache ablenken darf, dass die Bestimmungen des Datenschutzgesetzes besser eingehalten werden

(die Zunahme der Verstöße beruht hierbei auf formalen Gründen) und die Zahl der sehr schweren Verstöße sowie die Haftungssumme im Falle von Verstößen zurückgegangen sind.

Die folgenden Beschlüsse sind in jedem Fall erwähnenswert:

- Beschluss PS/00053/2009 vom 13. Januar. Die Datenschutzbehörde des Vereinigten Königreichs meldete der spanischen Datenschutzbehörde, dass ein spanisches Unternehmen bei britischen Bürgern unerwünschte Werbeanrufe (Kaltakquise) durchführte. Das Unternehmen konnte seine Datenquelle nicht belegen. Es bestand weder ein Vertragsverhältnis mit den betroffenen Personen, noch wurden diese um ihr Einverständnis gebeten. Aus diesem Grund verhängte die Datenschutzbehörde wegen eines schweren Verstoßes gegen das Datenschutzgesetz ein Bußgeld in Höhe von 60.001 Euro.
- Beschluss PS/00593/2008 vom 20. April. Über ein P2P-Datenaustauschprogramm konnte auf eine Datenbank mit medizinischen Daten von über 140 Arbeitern zugegriffen werden. Der Datenkontrolleur, ein auf die Vermeidung berufsbedingter Risiken spezialisiertes Unternehmen, versuchte die Schuld hierfür einem ehemaligen Angestellten zu geben. Die Datenschutzbehörde verhängte wegen fehlender angemessener Sicherheitsvorkehrungen und somit eines sehr schweren Verstoßes gegen das Datenschutzgesetz ein Bußgeld in Höhe von 60.001 Euro.
- Beschluss PS/00183/2009 vom 14. September. Ein Onlineshop für Konzertkarten bot demjenigen Nutzer zwei Konzertkarten an, der es schafft, eine bestimmte Werbeanzeige am häufigsten weiterzuleiten. Die Datenschutzbehörde stellte fest, dass der Shop unerwünschte Werbenachrichten verschickte und verhängte wegen eines schweren Verstoßes gegen das Gesetz über Dienstleistungen der Informationsgesellschaft ein Bußgeld in Höhe von 30.001 Euro.
- Beschluss PS/00233/2009 vom 20. Oktober. Ein Telekommunikationsunternehmen verkaufte nicht eingezogene Forderungen von Kunden an dritte Unternehmen. Die Datenbank umfasste nicht vorhandene, unsichere und strittige Forderungen, die sogar in die Kreditgeschichte einiger betroffener Personen aufgenommen wurden. Die Datenschutzbehörde verhängte wegen eines schweren Verstoßes gegen das Datenschutzgesetz ein Bußgeld in Höhe von 420.000 Euro.
- Der vollständige Text der von der spanischen Datenschutzbehörde verabschiedeten Beschlüsse ist (in spanischer Sprache) erhältlich unter https://www.agpd.es/.

C. Wichtige spezifische Themen

Maßnahmen zur Vereinfachung der Einhaltung der Gesetze: eine Garantie für die Bürger. Die Politik der Datenschutzbehörde zur Sensibilisierung der Öffentlichkeit wurde in der Überzeugung bestärkt, dass eine Förderung der Umsetzung der Gesetze mehr Garantien für die Bürger mit sich bringt. Dementsprechend fand im Januar 2009 die zweite öffentliche jährliche Sitzung statt, der etwa 700 Teilnehmer beiwohnten. Darüber hinaus wurden der Katalog der praktischen Leitlinien erweitert und neue Auflagen mit Empfehlungen für Internetnutzer, für den Bereich Videoüberwachung und Datenschutz am Arbeitsplatz sowie (in englischer Sprache) Leitlinien zu Videoüberwachung und den Rechten von Jungen und Mädchen sowie den Pflichten von Vätern und Müttern veröffentlicht.

Die Beratungsstelle ist auch weiterhin eine sehr nützliche Einrichtung für die Informationspolitik der Datenschutzbehörde. Dies zeigt sich Jahr für Jahr in der Zunahme der Beratungen. Die Rechtsabteilung bearbeitete insgesamt 679 Anfragen. 359 davon (54 %) kamen aus der öffentlichen Verwaltung, 313 (die übrigen 46 %) aus dem privaten Sektor.

Diese Maßnahmen liefern fortwährend Ergebnisse. Im Jahr 2009 wurden etwa 400.000 Dateien im Allgemeinen Datenschutzregister (RGPD) registriert. Dies entspricht einer Zunahme von über 50 % verglichen mit dem Jahr 2008. Insgesamt sind nun 1.647.756 Dateien registriert. Einen Beitrag zu dieser Zunahme lieferte das vereinfachte Meldesystem NOTA, das Meldungen per Internet ermöglicht. Diese Möglichkeit wird in fast 90 % aller manuellen Meldungen genutzt. Darüber hinaus wird die Verwendung digitaler Zertifikate immer besser ange-

nommen. Dieses Format wird mittlerweile bei jeder fünften Meldung verwendet.

Die stärkste Zunahme von Registrierungen ist mit 63 % im privaten Sektor zu verzeichnen, wohingegen im öffentlichen Sektor eine Zunahme von Dateien lokaler Verwaltungen von fast 50 % zu verzeichnen ist. Die im RGPD registrierten Daten von Gemeinden repräsentieren fast 96 % der spanischen Bevölkerung.

Das Angebot neuer Möglichkeiten zur Einhaltung der Gesetze hat zu einer deutlichen Verbesserung des EVALÚA-Programms, einem Onlinetest zur Selbsteinschätzung der Einhaltung des Datenschutzgesetzes für Unternehmen und lokale Behörden, geführt. Dieses Programm beantwortet kostenfrei die häufigsten Fragen der für die Verarbeitung personenbezogener Daten Verantwortlichen.

Das Internet. Neue Dienste, neue Herausforderungen. Die Gegenleistung für die kostenlose Nutzung von Internetdiensten durch deren Nutzer ist die einseitige Festlegung von Nutzungsbedingungen durch den Dienstleistungsanbieter. Aus diesem Grund sollten aktive Strategien zur Herstellung von Beziehungen zu den Anbietern dieser Dienstleistungen vorrangig behandelt werden. In diesem Zusammenhang hat die Datenschutzbehörde Empfehlungen aus einer in Zusammenarbeit mit INTECO durchgeführten Studie an Facebook und Tuenti weitergeleitet. Diese Empfehlungen fordern eine Verbesserung der Datenschutzbestimmungen, damit diese eindeutige und verständliche Informationen bieten, und bestehen auf der Notwendigkeit der Festlegung von Standard-Datenschutzbestimmungen und auf der Löschung sämtlicher Inhalte eines Profils im Fall einer Abmeldung.

Im Jahr 2009 wurden 156 Verfahren zu Vorverfahren eingeleitet, die spezielle über das Internet angebotene Dienstleistungen betrafen. Neu hierbei war, dass 18 dieser Verfahren infolge von 31 Beschwerden von Nutzern der sozialen Netzwerke Facebook und Tuenti eingeleitet wurden. Im Großteil der Fälle ging es um die Verbreitung von Fotos Dritter ohne deren Einverständnis.

Der Großteil der anderen Beschwerden betraf ebenfalls die unerlaubte Verbreitung personenbezogener Daten über das Internet: 37 hiervon betrafen Foren oder Blogs, 13 so genannte Videohosting-Dienste (hauptsächlich Youtube) und 38 betrafen sonstige Websites wie zum Beispiel Unternehmenswebsites, Urteilssammlungen und persönliche Websites. Weitere 28 Beschwerden betrafen Werbewebsites, Online-Datingdienste oder E-Mail-Dienste. In den meisten Fällen ging es um die unerlaubte Verbreitung von Daten.

In 10 Fällen ging es um verschiedene Vorfälle im Zusammenhang mit Onlineshopping beziehungsweise elektronischem Handel. Schließlich sind auch fünf eingeleitete Vorverfahren in Bezug auf Internetsuchmaschinen sowie die Speicherung persönlicher Informationen in Verzeichnissen oder Personensuchmaschinen erwähnenswert.

Minderjährige. Notwendiger Schutz angesichts der zunehmenden Präsenz im Internet. Die Nutzung sozialer Netzwerke ist im Hinblick auf die soziale Entwicklung von Minderjährigen zum Alltag geworden. Diese Netzwerke bieten ihnen neue Möglichkeiten der Kontaktaufnahme. Das Risiko besteht hierbei zumeist darin, dass sie diese Netzwerke ohne eine grundlegende Aufklärung darüber nutzen, wie sie ihre Informationen wirklich kontrollieren können.

Die Datenschutzbestimmungen gestatten es Minderjährigen unter 14 Jahren nicht, sich ohne das Einverständnis der Eltern als Mitglied eines sozialen Netzwerkes zu registrieren. Die Datenschutzbehörde sieht die Einhaltung dieser Verpflichtung als Priorität. In den mit den Verantwortlichen von Tuenti und Facebook durchgeführten Treffen war die Zugangskontrolle für Minderjährige eine ständige Forderung.

Als Reaktion auf die Forderungen der Datenschutzbehörde präsentierte Tuenti ein System zur Altersüberprüfung, dass die Profile auffälliger Nutzer analysiert und die Profile der Nutzer löscht, die jünger als 14 Jahre sind. Ebenso sollen die Überprüfung bestehender Profile verbessert werden und Systeme zur Verifizierung der auffälligen Profile entwickelt werden. Außerdem wurden Informationen über die Änderung der Datenschutzbestimmungen veröffentlicht, im Rahmen derer nunmehr als Standardwert für Nutzer unter 18 Jahren automatisch die maximale

Sicherheitsstufe eingestellt ist. Ebenso forderte die Datenschutzbehörde die Verantwortlichen von Facebook auf, die Altersbegrenzung für Nutzer in Spanien auf 14 Jahre anzuheben.

Es ist jedoch erforderlich, angemessene Information zum Thema Datenschutz und Privatsphäre in Schulbücher zu integrieren. Außerdem müssen die öffentliche Verwaltung und Schulen den Schülern Technologien zur Verfügung stellen, die den Zugang zu Internetdiensten für Kinder unter 14 Jahren beschränken. In diesem Zusammenhang erweist sich ein elektronisches Ausweisdokument als eines der effizientesten Instrumente zur Altersüberprüfung im Internet. Die Datenschutzbehörde hält es für besonders wichtig, dass angemessene Initiativen gestartet werden, damit Jugendlichen über 14 Jahren die digitalen Möglichkeiten zur Verfügung stehen, ihr Alter zu belegen und ihr Einverständnis zur Verarbeitung ihrer Daten zu geben

Videoüberwachung: ein Leben mit Garantien. Die Videoüberwachung aus Sicherheitsgründen ist zur allgegenwärtigen Realität geworden. Jedes Jahr ist eine deutliche Zunahme der Dateien aus Videoüberwachungen zu verzeichnen. So belief sich die Zunahme der aus dem privaten Sektor im Allgemeinen Datenschutzregister erfassten Dateien im Jahr 2009 auf etwa 240 % (eine Zunahme um mehr als 37.000 Dateien). Im öffentlichen Sektor war eine Zunahme um 60 % zu verzeichnen (eine Zunahme um 578 Dateien).

Die Umfrage der CIS aus dem Jahr 2009 zeigt, dass 68,7 % der Bürger für die Installation von Videoüberwachungsgeräten sind, während 10 % dagegen sind. Immer mehr Menschen reichen jedoch auch Beschwerden betreffend Verstöße gegen das Datenschutzgesetz durch Videoüberwachungsgeräte ein. In diesem Bereich hat sich die Zahl der abgeschlossenen Sanktionsverfahren um 230 % erhöht.

Im Hinblick auf Kameras, die die Übertragung von Bildern über das Internet ermöglichen, führte die die Datenschutzbehörde eine sektorweite Kontrolle durch und stellte fest, dass die gefilmten Personen auf den meisten Bildern identifiziert werden konnten. Der am häufigsten festgestellte Mangel ist die Tatsache, dass die Kontrollmechanismen für den Zugang zu den Bildern oftmals vom Hersteller her deaktiviert oder sich nur mithilfe eines Benutzernamens und eines Passwortes aktivieren lassen mit einem Standardpasswort und Benutzernamen voreingestellt sind. Die mangelnde Sorgfalt bei der Zugangskontrolle führt dazu, dass Dritte aufgrund einer fehlenden Verschlüsselung der von der Kamera erfassten Daten auf diese zugreifen können. Es wurde ein Katalog von Empfehlungen bereitgestellt, der auch die Notwendigkeit einer Kontrolle des Zugangs zu den Bildern durch die Vergabe von Benutzernamen und Passwörtern umfasst. Infolge der Prüfungen wurden sieben Strafverfahren eingeleitet und abgeschlossen.

Arbeitsumfeld: das Gleichgewicht zwischen Rechten und Pflichten. Das breite Spektrum der Verarbeitung personenbezogener Daten im Bereich Beschäftigung hat die Datenschutzbehörde dazu veranlasst, Leitlinien zum Datenschutz in Unternehmen zu erarbeiten, die praktische Fragen beantworten sollen, denen sich Unternehmen häufig gegenübersehen. Sie schlagen Kriterien zur Einhaltung der Gesetze zum Schutz personenbezogener Daten vor. Die Leitlinien umfassen spezifische Empfehlungen betreffend die Verarbeitung von besonders geschützten Daten, insbesondere von Daten aus dem Gesundheitswesen und Daten über die Mitgliedschaft in einer Gewerkschaft sowie die Garantien, die im Hinblick auf die Vermeidung berufsbedingter Gefahren gewährt werden müssen.

Sie umfassen überdies auch Empfehlungen, die sicherstellen sollen, dass interne Meldeverfahren („Whistleblowing") in Unternehmen unter gleichzeitiger Gewährleistung des Schutzes der Angestellten umgesetzt wird. Im Kapitel über die Kontrollen des Arbeitgebers sind die Vorschriften für biometrische Kontrollen, die Videoüberwachung am Arbeitsplatz bzw. den Einsatz von durch den Arbeitgeber bereitgestellten technischen Werkzeugen sowie für die Kontrolle der Abwesenheit vom Arbeitsplatz beschrieben.

Internationale Datenflüsse. Flexibilität und Globalisierung. Internationale Datenübermittlungen aus Spanien gehen mittlerweile in alle Welt – ein Zeichen für die Globalisierung. Die Anzahl der Genehmigungen hat um 25 % zugenommen. Trotz eines Rückgangs der Anzahl der Übermittlungen sind die USA das Hauptzielland. Ein starkes Wachstum von 100 % konnte

hinsichtlich der lateinamerikanischen Länder verzeichnet werden (132 Genehmigungen), wohingegen die Genehmigungen für Asien konstant blieben (115). Auf dem afrikanischen Kontinent lag der Schwerpunkt der internationalen Übermittlungen auf Marokko (19) und der Republik Südafrika (3). Auch Australien scheint sich als neues Zielland zu etablieren.

Die Suche nach flexibleren Verfahren zur Genehmigung internationaler Übermittlungen hatte im Jahr 2009 Fortschritte zu verzeichnen. Die Datenschutzbehörde genehmigte die erste Übermittlung auf der Grundlage verbindlicher Unternehmensregeln (BCR) und nahm über ein koordiniertes Verfahren an 10 Anträgen dieser Art von Garantien teil, die bei anderen Behörden in der Europäischen Union eingereicht wurden.

Zusammenfassend lässt sich eine konstante Zunahme der internationalen Datenflüsse feststellen. Der Schwerpunkt in diesem Bereich liegt auf einer Delokalisierung der Dienstleistungen und flexibleren Genehmigungsverfahren. Hieraus lässt sich ableiten, dass wir dringend verbindliche Standards benötigen, um den Schutz der Privatsphäre in einer globalisierten Welt zu garantieren.

2009: Madrid, Welthauptstadt des Datenschutzes. Die Madrid-Resolution: ein gemeinsamer Nenner für eine globale Regulierung. Im Jahr 2009 organisierte die Datenschutzbehörde die 31. Internationale Konferenz der Datenschutzbehörden – das weltweit größte Forum für Privatsphäre und eine gemeinsame Plattform für die Datenschutzbehörden und Schützer der Privatsphäre aus aller Welt sowie für Vertreter öffentlicher und privater Gremien und der Zivilgesellschaft –, die Madrid vom 2. bis 6. November zur Welthauptstadt des Datenschutzes machte. Über 1.000 Menschen aus 83 Ländern nahmen teil.

Diese Konferenz, die von Ihren Hoheiten dem Prinzen und der Prinzessin von Asturien eröffnet wurde, fand im Kongresspalast von Madrid statt und stand unter dem Motto „Privatsphäre: Heute ist morgen". Fast einhundert Redner nahmen an über 20 Sitzungen teil, darunter der spanische Innenminister, Alfredo Pérez Rubalcaba, die Ministerin für Heimatschutz der Vereinigten Staaten, Janet Napolitano, Martin Cooper (der Erfinder des Mobiltelefons), Vinton Cerf (der Miterfinder der TCP/IP-Internetprotokolle) sowie der marokkanische Minister für Industrie, Handel und neue Technologien, Ahmed Reda Chami. Die größte Errungenschaft dieser Veranstaltung war jedoch der im Bereich Privatsphäre erzielte Fortschritt auf dem Weg hin zu einem allgemein gültigen und verbindlichen Rechtsinstrument, das die Rechte und Freiheiten der Menschen in einer globalisierten Welt besser schützen und auf einem breitest möglichen institutionellen und sozialen Konsens aufbauen soll.

Durch die Annahme dieser „Madrid-Resolution" wurde ein großer Schritt hin zu einem „Gemeinsamen Vorschlag für einen Entwurf internationaler Standards zum Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten" unternommen. Dieser Vorschlag zielt zum einen darauf ab, das Recht auf Datenschutz und Privatsphäre mit Hilfe eines Regulierungsmodells international zu fördern, das ein hohes Maß an Schutz bietet und gleichzeitig in jedem Land umgesetzt werden kann. Des Weiteren soll er die Übermittlung personenbezogener Daten auf internationaler Ebene erleichtern und gleichzeitig dabei helfen, bestehende Hindernisse zu überwinden.

Trotz der Tatsache, dass es sich hierbei nicht um ein internationales Abkommen oder eine rechtlich verbindliche Regelung handelt, hat dieser Vorschlag als Referenztext nicht nur durch die breite Teilnahme der internationalen Gemeinschaft im Bereich Datenschutz und Privatsphäre an seiner Erarbeitung einen hohen Stellenwert, sondern auch aufgrund der Tatsache, dass er Elemente enthält, die in allen derzeit geltenden Datenschutzsystemen zu finden sind, und dass er von allen Behörden unterstützt wird, die an der internationalen Konferenz teilgenommen haben. Aus diesem Grund wird die Bewerbung und Verbreitung dieses Textes bei privaten Gremien, Experten sowie nationalen und internationalen öffentlichen Organisationen eine der Prioritäten der Datenschutzbehörde für das Jahr 2010 sein.

Schweden

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

In Schweden wurde die ***Richtlinie 95/46/EG*** durch das ***Gesetz zum Schutz personenbezogener Daten*** (Personal Data Act, PDA, 1998:204) umgesetzt, das am 24. Oktober 1998 in Kraft trat. Das Gesetz zum Schutz personenbezogener Daten wird durch die ***Datenschutzverordnung*** ergänzt, die am gleichen Tag in Kraft trat. Das Gesetz findet wie die Richtlinie auf die automatisierte ebenso wie auf die manuelle Datenverarbeitung Anwendung. Dieses Gesetz gilt zwar grundsätzlich für die Verarbeitung personenbezogener Daten in allen Bereichen der Gesellschaft, jedoch gibt es in bestimmten Bereichen mehrere spezielle Gesetze und Beschlüsse für die Datenverarbeitung, entweder anstelle des Gesetzes zum Schutz personenbezogener Daten oder ergänzend hierzu. Auch beim Entwurf dieser speziellen Gesetze und Beschlüsse wurde der Richtlinie Rechnung getragen.

Die ***Richtlinie 2002/58/EG*** wurde mit Inkrafttreten des ***Gesetzes über die elektronische Kommunikation*** ECA (2003:389) am 25. Juli 2003 in schwedisches Recht umgesetzt. Kapitel 6 dieses Gesetzes enthält Datenschutzregeln für den Sektor der elektronischen Kommunikation. Die Einhaltung der Datenschutzbestimmungen des ECA-Gesetzes wird von der Überwachungsbehörde für das Post- und Telekommunikationswesen kontrolliert (PTS). Artikel 13 der EG-Richtlinie über unerbetene E-Mails wurde durch die Änderungen des ***Gesetzes zu Marketingpraktiken*** (1995:450) umgesetzt. Diese Änderungen traten am 1. April 2004 in Kraft. Das Gesetz zu Marketingpraktiken untersteht der Aufsicht der Verbraucheragentur (Konsumentverket).

Die ***Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums*** (***Ipred***) wurde durch verschiedene Änderungen an nationalen Gesetzen, die am 1. April 2009 in Kraft getreten sind, in schwedisches Recht umgesetzt. Die Änderungen vereinfachen die Untersuchung von Verdachtsfällen betreffend den illegalen Datenaustausch. Eine Besonderheit des Gesetzes ist, dass sich Organisationen, die geistiges Eigentum schützen, an ein Gericht wenden und Internetanbieter auffordern können, Informationen zum Nutzer einer betreffenden IP-Adresse herauszugeben, wenn ein Verdacht auf illegalen Datenaustausch vorliegt. Einige Prozesse wurden bereits durchgeführt, ein Fall ist vor dem Berufungsgericht Svea noch anhängig.

Seit dem 1. Dezember 2009 hat der schwedische Nachrichtendienst „Radioanstalt der Verteidigung" (Försvarets Radioanstalt, FRA) im Rahmen des am selben Tag in Kraft getretenen ***Gesetzes über Signalüberwachung*** schrittweise mit der Erfassung von Geheimdienstinformationen per Kabel begonnen. Dieses neue Gesetz ermöglicht dem FRA, sowohl durch die Luft, also zum Beispiel über Funksignale, als auch per Kabel übermittelte Geheimdienstinformationen zu erfassen. Vor der Inkraftsetzung dieses Gesetzes konnten per Kabel übermittelte Geheimdienstinformationen nicht erfasst werden. Ein zunehmender Anteil internationaler Verbindungen, die interessante Informationen enthalten, wird mittlerweile per Kabel übermittelt. Aus diesem Grund war die Einführung einer technologieneutralen Gesetzgebung erforderlich. Die Datenschutzbehörde ist für die Überwachung der Verarbeitung der personenbezogenen Daten durch den FRA verantwortlich. Am 12. März 2009 beschloss die Regierung, der Datenschutzbehörde die Sonderaufgabe der Überwachung der Tätigkeiten im Hinblick auf die Privatsphäre zu übertragen. Die Datenschutzbehörde wird von einem Beratungsgremium unterstützt, das sich aus Mitgliedern des schwedischen Parlaments (Riksdag) zusammensetzt. Im Dezember 2010 wird die Datenschutzbehörde ihre Ergebnisse der Regierung vorlegen.

Die ***dritte EG-Richtlinie über Geldwäsche*** wurde im Jahr 2008 in schwedisches Recht umgesetzt und trat im März 2009 in Kraft.

Wie bereits im vergangenen Jahr berichtet wurde, wurde im Jahr 2006 ein Untersuchungsausschuss eingerichtet. Dem Ausschuss wurde die Aufgabe übertragen, das Monopol des schwedischen Apothekenverbandes (Apoteket AB) für den Verkauf von Pharmaprodukten aufzuheben und anderen Betreibern zu ermöglichen, solche Produkte zu verkaufen. Eine der in diesem Zusammenhang zu bearbeitenden Fragen war die der Registrierung von Rezepten. Im Juli 2009 trat das ***Gesetz***

über Apothekendaten in Kraft, und das Monopol des Apothekenverbandes wurde aufgehoben.

Die ***EG-Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden,*** ist noch immer nicht in schwedisches Recht umgesetzt worden. Derzeit liegen keine Informationen vor, wann die Regierung dem schwedischen Parlament (Riksdag) einen Gesetzesentwurf vorlegen wird.

Ende November 2009 unterzeichnete Schweden das ***EU-Telekommunikationspaket***, das Vorschriften zur Stärkung der Verbraucherrechte im Hinblick auf Telefon- und Internetbetreiber umfasst. Es ist nun Aufgabe der Regierung, einen Gesetzesentwurf zum Telekommunikationspaket vorzulegen, das bis spätestens Frühjahr 2011 umgesetzt werden soll.

Im Mai 2009 legt ein Untersuchungsausschuss einen Bericht zum Thema ***Schutz der Privatsphäre im Berufsleben*** vor. Der Ausschuss schlägt ein neues Gesetz vor, das Bestimmungen zur Klarstellung und Stärkung des Schutzes von Angestellten umfassen soll. Das vorgeschlagene Gesetz betrifft ausschließlich Maßnahmen, die Arbeitgeber im Hinblick auf ihre Angestellten ergreifen. Das vorgeschlagene Gesetz befasst sich unter anderem mit medizinischen Untersuchungen und verschiedenen Formen der Überwachung. Der Gesetzesvorschlag wurde zur Begutachtung an verschiedene Interessengruppen der allgemeinen Öffentlichkeit weitergeleitet, unter anderem auch an die Datenschutzbehörde. Die Regierung hat noch nicht entschieden, ob sie einen entsprechenden Gesetzesentwurf vorlegen wird.

Der Bereich Videoüberwachung war Gegenstand einer Überprüfung und eines Berichts durch einen Untersuchungsausschuss. Im Oktober 2009 wurde der Regierung ein neues ***Gesetz zur Videoüberwachung*** vorgelegt. Aktuell ist der Bereich Videoüberwachung durch zwei unterschiedliche Gesetze geregelt, deren Anwendungsbereich vom Gegenstand der Videoüberwachung abhängt. Viele, die eine Videoüberwachung nutzen möchten, halten diese Situation für kompliziert. Dementsprechend umfasst der Vorschlag des Untersuchungsausschusses im Wesentlichen die Einführung eines einzigen Gesetzes zur Regelung aller Arten von Videoüberwachung. In diesem Zusammenhang wird auch vorgeschlagen, dass der Datenschutzbehörde die zentrale Verantwortung für die Überwachung der Anwendung des neuen Gesetzes übertragen wird. Das neue Gesetz soll im Januar 2011 in Kraft treten.

Die Regierung hat einen Gesetzesentwurf mit Vorschlägen zu ***Änderungen des verfassungsrechtlichen Gesetzes*** vorgelegt. Eine der vorgeschlagenen neuen Bestimmungen soll den Schutz vor erheblichen Eingriffen in die Privatsphäre von Menschen durch eine Überwachung oder Erfassung persönlicher Umstände gewährleisten. Die vorgeschlagenen Änderungen sollen im Januar 2011 in Kraft treten.

Wie bereits im vergangenen Jahr berichtet wurde, gibt es im Bereich der Kreditinformationen Probleme aufgrund der Tatsache, dass diese Informationen wegen des verfassungsrechtlichen Schutzes von Informationen und Erklärungen (eine im Jahr 2003 eingeführte Änderung des Grundrechtes auf freie Entfaltung) im Internet veröffentlicht werden. Die Änderung hat es ermöglicht, Kreditinformationen auf Websites zu veröffentlichen, ohne dabei die strengen Regeln des ***Kreditinformationsgesetzes*** einhalten zu müssen. Dies führte zu Verletzungen der Privatsphäre und zahlreichen Beschwerden. Die Datenschutzbehörde hat die Regierung mehrfach schriftlich über diese Probleme in Kenntnis gesetzt. Der Justizminister hat angekündigt, dass im Frühjahr 2010 ein entsprechender Gesetzesentwurf vorgelegt werden wird.

Im Dezember 2009 setzte die Regierung einen Untersuchungsausschuss zur Erarbeitung eines Vorschlags für eine neue Organisation der ***Anti-Doping-Maßnahmen*** ein. Eine der Aufgaben ist die Untersuchung der Möglichkeiten zur Schaffung einer unabhängigen nationalen Anti-Doping-Organisation, für die der Staat und die zentrale Sportorganisation gemeinsam verantwortlich sein sollen. Auch die Möglichkeit zur Beteiligung anderer Interessengruppen, mit denen im Rahmen von Anti-Doping-Maßnahmen zusammengearbeitet werden könnte, sollte untersucht werden. Der

Untersuchungsausschuss wird der Regierung im Oktober 2010 einen Bericht vorlegen.

B. Bedeutende Rechtsprechung

Die Entscheidung des Obersten schwedischen Verwaltungsgerichts betreffend IP-Adressen

Im Jahr 2009 konnte ein Fall zur Frage, ob IP-Adressen als personenbezogene Daten einzustufen sind, endgültig abgeschlossen werden. Eine private Organisation hatte zum Zweck der Gewährleistung urheberrechtlicher Interessen eine spezielle Software zur Aufspürung von Internetnutzern verwendet, die an einem Datenaustausch beteiligt waren. Im Jahr 2005 stellte die Datenschutzbehörde fest, dass die Erfassung und Verarbeitung von IP-Adressen in diesem Fall eine Verarbeitung personenbezogener Daten darstellt. Gegen die Entscheidung der Datenschutzbehörde wurde beim Bezirksverwaltungsgericht sowie beim entsprechenden Berufungsgericht Berufung eingelegt. Beide Gerichte bestätigten die Entscheidung der Datenschutzbehörde. Als Reaktion auf eine Berufung vor dem Obersten Verwaltungsgericht entschied das Gericht im April 2009, die Berufung abzuweisen. Die Entscheidung des Verwaltungsgerichtes ist somit weiterhin rechtskräftig und die Ansicht der Datenschutzbehörde, dass IP-Adressen als personenbezogene Daten einzustufen sind, weiterhin gültig.

Im letztjährigen Bericht skizzierte die Datenschutzbehörde einen Fall betreffend ***auf RFID-Techniken basierende Fahrkartensysteme mit so genannten „Smart Cards"***. In den Jahren 2006 und 2008 führte die Datenschutzbehörde Prüfungen öffentlicher Verkehrsunternehmen durch, die neue (auf RFID-Techniken basierende) Fahrkartensysteme mit so genannten „Smart Cards" nutzen, die elektronische Spuren hinterlassen. Die Datenschutzbehörde entschied, dass die durch die Nutzung der elektronischen Karten durch die Passagiere erfassten personenbezogenen Daten nur 60 Tage lang gespeichert werden dürften und danach eine Identifizierung nicht mehr möglich sein sollte. Eines der untersuchten Verkehrsunternehmen legte Berufung gegen die Entscheidung der Datenschutzbehörde ein und argumentierte, dass Informationen zu Reisenden als offizielle Dokumente einzustufen sind und somit gemäß dem Archivgesetz in Ermangelung spezieller Vorschriften zur Löschung gespeichert werden müssten. Das Bezirksverwaltungsgericht hob die Entscheidung der Datenschutzbehörde im Januar 2009 auf und legte den Fall zur Neuprüfung vor. Aufgrund der Einschätzung, dass das Archivgesetz anzuwenden sei, kam die Datenschutzbehörde zu dem Schluss, dass keine Verpflichtung zur Löschung oder Anonymisierung der Informationen vorliegt. Die Datenschutzbehörde blieb jedoch bei der Ansicht, dass detaillierte Informationen zur Nutzung öffentlicher Verkehrsmittel nicht für einen unbegrenzten Zeitraum gespeichert werden sollten. Daher wandte sich die Datenschutzbehörde im Juni 2009 schriftlich an die Regierung und legte die Notwendigkeit für neue Gesetze in dieser Hinsicht dar.

Im vergangenen Jahr berichtete die Datenschutzbehörde auch über das Thema ***Videoüberwachung an Schulen***. Hintergrund war ein im Jahr 2008 an Schulen verschickter Internet-Fragebogen. Das Ergebnis zeigte, dass das Ausmaß der Videoüberwachung an Schulen verglichen mit dem Jahr 2005, in dem eine vergleichbare Untersuchung durchgeführt worden war, um 150 % zugenommen hatte. Daraufhin untersuchte die Datenschutzbehörde sieben Schulen und stellte fest, dass die Videoüberwachung von Schülern während der Schulzeit gegen das Datenschutzgesetz verstößt. Die Untersuchungen zeigten auch, dass die Kenntnisse in Bezug auf die Datenschutzgesetze mangelhaft sind. Aus diesem Grund gab die Datenschutzbehörde eine Checkliste heraus, damit die Schulen einfacher entscheiden können, wann eine Videoüberwachung erlaubt ist. Gegen die Entscheidungen der Datenschutzbehörde vom Oktober 2008 wurde Berufung vor dem Bezirksverwaltungsgericht eingelegt, das im September 2009 ein Urteil in diesem Fall sprach. Die Berufungen wurden abgewiesen und die Entscheidungen der Datenschutzbehörde bestätigt. Gegen zwei der fünf Entscheidungen wurde jedoch Berufung beim zuständigen Berufungsgericht eingelegt. Die Verfahren sind anhängig. Im Laufe des Jahres 2009 führte die Datenschutzbehörde vier neue Untersuchungen an Schulen durch und stellte fest, dass es im Hinblick auf die Verarbeitung von Daten noch immer eine Reihe von Mängeln gibt und dass die Kenntnisse der Schulen hinsichtlich der Frage, wie lange personenbezogene Daten von Schülern gespeichert werden dürfen, noch immer unzureichend oder nicht vorhanden sind. Es konnten

keine Verfahren zur Löschung von Daten festgestellt werden, die nicht mehr benötigt werden.

C. Wichtige spezifische Themen

Der Pirate Bay-Prozess
Im Februar 2009 begann am Stockholmer Bezirksgericht der Prozess gegen die vier Verantwortlichen für die beliebte Website zum Datenaustausch „Pirate Bay". Im April sprach das Gericht sein Urteil. Die vier Gründer von „Pirate Bay" wurden zu einer Haftstrafe von einem Jahr und einem Bußgeld in Höhe von 3.000.000 EUR verurteilt, für das sie als Gesamtschuldner haften. Medien aus der ganzen Welt verfolgten den Prozess und kommentierten das Urteil. The Guardian schrieb: „Das hinter der Anklage stehende Konsortium aus Medien- und Musikunternehmen wird ob dieses Sieges jahrelang frohlocken. Es ist sicherlich ein Meilenstein, jedoch wirft das Urteil mehr Fragen auf als es beantwortet." Gegen das Urteil wurde Berufung beim Berufungsgericht von Svea (Svea hovrätt) eingelegt. Das Verfahren ist dort anhängig.

Im Frühjahr 2009 lud die Datenschutzbehörde Vertreter einiger der größten ***Websites für soziale Netzwerke*** in Schweden ein. Ziel war die Erarbeitung von Empfehlungen von Nutzungsbedingungen sowie die Bearbeitung von Beschwerden. Im November wurde das Ergebnis dieser Zusammenarbeit präsentiert: ***„Sicherheit für deine Seite – Leitlinien für Nutzungsbedingungen von Websites für junge Menschen".***

Im Laufe des Jahres 2009 bearbeitete die Datenschutzbehörde zahlreiche Fälle betreffend die ***Veröffentlichung personenbezogener Daten im Internet***. Drei dieser Fälle befassten sich mit Websites, auf denen beispielsweise Namen und Adressen von Personen veröffentlicht wurden, die wegen unterschiedlicher ***Sexualstraftaten*** verurteilt worden waren. Die Datenschutzbehörde brachte diese Fälle bei der Polizei zur Anzeige. Bei der Datenschutzbehörde ging eine Beschwerde über eine Website ein, auf der ***Einzelpersonen Unternehmen*** und manchmal auch andere Einzelpersonen ***bewerten und kommentieren*** konnten. Die Datenschutzbehörde stellte fest, dass die Website selbst im gewissen Maße hierfür verantwortlich war und dass die Verarbeitung der Daten nicht im Einklang mit dem Gesetz zum Schutz personenbezogener Daten stand. Der Fall ist mittlerweile abgeschlossen, da die Informationen von der Website gelöscht wurden. Im August 2009 gab die Polizei in Skåne in Südschweden bekannt, dass sie beabsichtige, ***Fotos aus Überwachungskameras im Internet zu veröffentlichen***, um so Hinweise aus der Öffentlichkeit im Hinblick auf die Identifizierung von Personen zu erhalten, die eines Verbrechens verdächtigt werden. Seitdem wurden beispielsweise Fotos von Untersuchungen betreffend Körperverletzung, Betrug und Diebstahl veröffentlicht. Die Veröffentlichung hat große Aufmerksamkeit erregt. Aus diesem Grund bat die nationale Polizeibehörde die Datenschutzbehörde um eine Stellungnahme zur Veröffentlichung. Die Datenschutzbehörde antwortete, dass eine solche Veröffentlichung nur in Ausnahmefällen erfolgen sollte und dass die Voraussetzungen für eine solche Veröffentlichung gesetzlich geregelt sein sollten. Die Stellungnahme der Datenschutzbehörde wurde daher auch dem Justizministerium übermittelt.

Ein neuer Bericht über die Privatsphäre (***Privatsphäre 2009***) wurde erstellt, der, ebenso wie der letztjährige Bericht, eine umfassende Untersuchung der neuen Gesetzgebung, Vorschläge, Entscheidungen und Techniken umfasst, die den Bereich der Privatsphäre im laufenden Jahr betrafen.

Das Treffen der nordischen Datenschutzbeauftragten
Im Mai 2009 veranstaltete die Datenschutzbehörde das halbjährlich stattfindende Treffen der nordischen Datenschutzbeauftragten. Das Treffen fand in Stockholm statt, die Teilnehmer kamen aus Dänemark, Finnland, Island, Norwegen und Schweden.

Vereinigtes Königreich

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

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

Die Richtlinie 2002/58/EG wurde als Verordnungen über Datenschutz und elektronische Kommunikation in britisches Recht umgesetzt und am 11. Dezember 2003 rechtswirksam.

Die endgültige Übergangszeit endete am 23. Oktober 2007, womit die vor 1998 manuell erstellten Aufzeichnungen nun den gesetzlichen Bestimmungen des Datenschutzgesetzes unterliegen.

B. Bedeutende Rechtsprechung

Vorratsspeicherung von Polizeiakten
Im Jahr 2008 stellte der Datenschutzbeauftragte fünf Polizeidienststellen Vollstreckungsbescheide zu, in denen er sie dazu aufforderte, alte Verurteilungen aus Strafverfahren aus dem nationalen Datenverarbeitungssystem der Polizei (PNC, police national computer) zu löschen.

Diese Maßnahme wurde infolge unserer Untersuchung im Rahmen von Beschwerden von fünf Personen ergriffen, die einmalig verurteilt oder von der Polizei verwarnt und danach wegen keiner weiteren Verstöße verurteilt wurden.

In jedem Fall wandte sich der Datenschutzbeauftragte schriftlich an die zuständige Polizeidienststelle und forderte sie auf, die Informationen aus dem PNC zu löschen oder den Zugriff auf diese Daten zu beschränken. In letzterem Fall würden die Daten auch weiterhin im PNC gespeichert bleiben, jedoch dürften nur Polizeibeamte auf diese Informationen zugreifen. Die Polizeidienststellen erklärten sich damit einverstanden, den Zugriff auf die Informationen zu beschränken, diese jedoch nicht zu löschen.

Als Reaktion hierauf stellte der Datenschutzbeauftragte den Hauptkommissaren der betreffenden Polizeidienststellen Vollstreckungsbescheide zu. In diesen Bescheiden wurde die Löschung der Informationen zur Verurteilung der betreffenden Einzelpersonen gefordert.

Die Hauptkommissare legten Berufung beim Informationsgericht (Information Tribunal) ein, um die Vollstreckungsbescheide des Datenschutzbeauftragten außer Kraft zu setzen. Anders gesagt wollten die Kommissare sicherstellen, dass sie die Informationen zu den betreffenden Verurteilungen im PNC speichern konnten.

Der Gerichtshof bestätigte die Vollstreckungsbescheide des Datenschutzbeauftragten und forderte die Hauptkommissare auf, die entsprechenden Informationen zu den fünf betroffenen Personen zu löschen.

Eine Berufung der fünf Hauptkommissare beim Berufungsgericht wurde zugelassen. Das Gericht entschied, dass die Polizeidienststellen die Informationen nicht löschen müssten und dass die Vorratsspeicherung der Akten keinen Verstoß gegen das Datenschutzgesetz darstelle. Das Urteil kann eingesehen werden unter: www.bailii.org/ew/cases/EWCA/Civ/2009/1079.html

Die Datenschutzbehörde ist der Ansicht, dass dieses Urteil wichtige Fragen aufwirft, und zwar nicht nur für die Betroffenen, sondern auch für andere Personen, über die Angaben zu nicht schwerwiegenden und veralteten Verurteilungen gespeichert sind, sowie Fragen dazu, wie das Datenschutzgesetz in der Praxis zu interpretieren ist. Es wirft außerdem ernste Fragen zur Anwendbarkeit von Art. 8 der Europäischen Menschenrechtskonvention im Hinblick auf die von der Polizei gespeicherten Daten von Verurteilungen auf. Die Datenschutzbehörde hat beim Obersten Gerichtshof die Zulassung eines Rechtsmittels eingelegt und hofft, damit erfolgreich zu sein, damit diese Fragen vom Obersten Gerichtshof untersucht werden können.

C. Wichtige spezifische Themen

Januar
Am Europäischen Datenschutztag starteten wir die Aktion „Versprechen zu persönlichen Informationen" („Personal Information Promise"). Dieses Versprechen ist ein eindeutiges Bekenntnis der Führungspersonen von Unternehmen dazu, dass der Wert persönlicher Informationen anerkannt wird und angemessene Vorkehrungen zu ihrem Schutz ergriffen werden. Bis Ende 2009 hatten etwa 1.000 Organisationen dieses Versprechen unterzeichnet.

Wir stellten einen Verstoß gegen das Datenschutzgesetz beim Innenministerium fest. Ein Auftragnehmer hatte einen unverschlüsselten Memorystick verloren, auf dem sensible personenbezogene Daten des Jahres 2008 zu Tausenden Personen gespeichert waren. Unter anderem waren dort Daten zu Freiheitsstrafen der betroffenen Personen sowie Daten zu früheren Verurteilungen wegen Straftaten gespeichert.

März
Wir haben eine versteckte Datenbank mit personenbezogenen Daten zu 3.213 Arbeitern der Baubranche beschlagnahmt und dem Eigentümer dieser Datenbank, Herrn Ian Kerr, firmierend als „The Consulting Association" einen Vollstreckungsbescheid zugestellt. Die Daten wurden von über 40 Baufirmen zur Prüfung der Eignung von Personen im Hinblick auf ihre Beschäftigung verwendet. Gegen Ian Kerr wurde in der Folge ein Bußgeld in Höhe von 5000 £ zuzüglich der Gerichtskosten verhängt. 14 Baufirmen wurden wegen Verstößen gegen das Datenschutzgesetz Vollstreckungsbescheide zugestellt. Einige Unternehmen hatten Tausende Pfund bezahlt, um auf unlauterem Wege personenbezogene Daten zu Bauarbeitern zu erlangen.

Wir veranstalteten unsere zweite Konferenz der Datenschutzbeauftragten in Manchester, der etwa 300 Delegierte beiwohnten. Auf dieser Veranstaltung wurde die zunehmende Beachtung diskutiert, die der Bereich Datenschutz aufgrund aktueller Fälle von Datenverlusten erfahren hat. Darüber hinaus wurden Ideen und Erfahrungen dazu ausgetauscht, wie mit den Herausforderungen umgegangen werden sollte, denen sich Datenschutzbeauftragte gegenübersehen.

April
Im Jahr 2008 beauftragten wir RAND Europa, eine Überprüfung der Europäischen Datenschutzrichtlinie durchzuführen. Im Rahmen des Projekts wurden die Stärken und Schwächen der europäischen Datenschutzvorkehrungen sowie implizit auch des Datenschutzgesetzes des Vereinigten Königreichs untersucht. Der Entwurf des endgültigen Berichts wurde auf der von der Datenschutzbehörde im April 2009 in Edinburgh organisierten Konferenz der Europäischen Datenschutzbeauftragten präsentiert und im Mai veröffentlicht.

Juni
Wir haben einen Verhaltenskodex für Meldungen von Verletzungen der Privatsphäre veröffentlicht. Dieser Kodex soll Unternehmen dabei helfen, eindeutige Meldungen von Verletzungen der Privatsphäre zu verfassen und sicherstellen, dass persönliche Informationen fair und transparent erfasst werden.

Außerdem begrüßten wir unseren neuen Datenschutzkommissar, Christopher Graham, der nach Ablauf der Amtszeit von Richard Thomas zu uns gestoßen ist.

Oktober
Unsere Meldegebühr erhöhte sich für einige Großunternehmen von 35 £ auf 500 £. Betroffen sind Unternehmen mit einem Umsatz von mindestens 25,9 Millionen £ sowie mindestens 250 Angestellten. Die neue Gebühr gilt auch für öffentliche Behörden mit mindestens 250 Angestellten.

November
Der Gesetzentwurf „Gerichtsmediziner und Justiz" erhielt die königliche Zustimmung und wurde somit zum Gesetz. Dementsprechend haben wir die Befugnis, Regierungsbehörden ohne deren Einverständnis nach Zustellung eines Feststellungsbescheides zu überprüfen. Unsere neuen Prüfbefugnisse sollen im April 2010 in Kraft treten.

Wir haben Leitlinien zum Datenschutz veröffentlicht, die eine eindeutige Anleitung zur praktischen Anwendung des Gesetzes bieten und die von den entsprechenden Interessengruppen gut aufgenommen wurden.

Dezember

Auf unserer am 9. Dezember in Manchester organisierten Konferenz haben wir eine öffentliche Konsultation zu unserem Entwurf für einen Verhaltenskodex betreffend persönliche Informationen im Internet gestartet. Der Entwurf beinhaltet eindeutige, umfassende Empfehlungen hinsichtlich der korrekten Bearbeitung personenbezogener Daten sowie dazu, wie die betroffenen Personen ein angemessenes Maß an Auswahlmöglichkeiten und Kontrolle hierüber gewährt werden kann. Unternehmen mit einer Internetpräsenz sollte er dabei helfen, durch die Annahme bewährter Verfahrensweisen rechtlichen Unsicherheiten entgegenzuwirken. Die endgültige Fassung des Verhaltenskodexes soll im Mai 2010 veröffentlicht werden.

Weitere Informationen zu unseren Tätigkeiten im Lauf des Jahres 2009 sind den auf unserer Website www.ico.gov.uk veröffentlichten Jahresberichten für 2008/09 sowie 2009/10 zu entnehmen.

Kapitel 3

AKTIVITÄTEN DER EUROPÄISCHEN UNION UND DER GEMEINSCHAFT

3.1. EUROPÄISCHE KOMMISSION

Konferenz[25]: „Personenbezogene Daten – größere Nutzung, größerer Schutz?" 19.-20. Mai 2009.

Die Europäische Kommission organisierte eine Konferenz über die neuen Herausforderungen im Hinblick auf die Nutzung und den Schutz personenbezogener Daten.

Wie sollten personenbezogene Daten in einer globalisierten Welt geschützt werden, in der die Mobilität stetig wächst, moderne Informations- und Kommunikationstechnologien den Alltag bestimmen und neue Strategien entwickelt werden? Welche Daten werden von Behörden und privaten Unternehmen herangezogen und ausgetauscht? Wie steht es in Zeiten von verteiltem Rechnen in „Rechnerwolken („Cloud Computing")" um die Wirksamkeit der geltenden Vorschriften für die internationale Übermittlung personenbezogener Daten? Welche Erwartungen haben Bürger, Unternehmen und die Gesellschaft als Ganzes? Um diese und andere Themen zu erörtern, organisierte die Europäische Kommission am 19. und 20. Mai 2009 in Brüssel eine Konferenz zu der Nutzung, dem Schutz und dem Austausch personenbezogener Daten in der EU.

Interessierte Bürger, Unternehmer, Vertreter von Verbraucherverbänden und der Wissenschaft, Datenschutzbeauftragte und Behördenvertreter aus der EU und Drittländern waren eingeladen, an der Konferenz teilzunehmen. Als Redner trat unter anderem der für Justiz, Freiheit und Sicherheit zuständige Kommissionsvizepräsident Jacques Barrot auf.

Die Konferenz bot den Teilnehmern Gelegenheit, sich über die neuen Herausforderungen im Bereich des Datenschutzes und die Notwendigkeit einer effektiven Strategie für das Informationsmanagement in der EU auszutauschen. Die Konferenz war eingebunden in die öffentliche Konsultation der Kommission zu der Frage, wie das Grundrecht auf Schutz personenbezogener Daten ausgeweitet und wirksam durchgesetzt werden kann, insbesondere im Raum der Freiheit, der Sicherheit und des Rechts.

[25] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

Workshop zum wirtschaftlichen Nutzen von Technologien zum Schutz der Privatsphäre (PET) – 12. November 2009[26]

Die europäische Kommission hat eine Studie zum wirtschaftlichen Nutzen von Technologien zum Schutz der Privatsphäre (PET) in Auftrag gegeben. Im Rahmen des Workshops wurde der Zwischenbericht[27] zu dieser von London Economics durchgeführten Studie präsentiert. Außerdem wurde einem breiten Spektrum von Interessengruppen die Möglichkeit geboten, ihre Erfahrungen mit PET auszutauschen. Man hoffte, dass die Teilnehmer praktische Beispiele dafür liefern würden, ob PET funktionieren oder nicht und wie sie zum Nutzen aller eingesetzt werden könnten. Dieser Workshop richtete sich an Interessengruppen im Bereich PET (Entwickler, Anwender, öffentliche Behörden, Nutzer/Verbraucher). Um ein praktisches Arbeitsumfeld zu bieten, war die Teilnahme am Workshop auf 50 Experten begrenzt.

Öffentliche Konsultation zum rechtlichen Rahmen für das Grundrecht auf Schutz personenbezogener Daten[28]

Die Konsultation zum rechtlichen Rahmen für das Grundrecht auf Schutz personenbezogener Daten war der Öffentlichkeit vom 09.07.2009 bis 31.12.2009 zugänglich. Ziel der Konsultation war, Meinungen zu den neuen Herausforderungen im Bereich des Schutzes personenbezogener Daten einzuholen, um einen effektiven und umfassenden rechtlichen Rahmen zum Schutz der personenbezogenen Daten von Einzelpersonen in der EU zu gewährleisten. Die wesentlichen Themen lauteten wie folgt: a) Meinungen zu den neuen Herausforderungen betreffend den Schutz personenbezogener Daten präsentieren, insbesondere angesichts der neuen Technologien und der Globalisierung, b) Meinungen zur Frage einholen, ob der aktuell geltende Rechtsrahmen diesen Herausforderungen gerecht wird und c) Diskussion der Frage, welche Maßnahmen in der Zukunft erforderlich sind, um besagten Herausforderungen gerecht zu werden. Auf diese öffentliche Konsultation gingen 168 Antworten von Bürgern, Unternehmen

[26] http://ec.europa.eu/justice_home/news/events/events_2009_en.htm

[27] http://ec.europa.eu/justice_home/news/events/workshop_pets_2009/report_en.pdf

[28] http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm

(eingetragenen sowie nicht eingetragenen) und öffentlichen Behörden ein.

Datenschutzrichtlinie für elektronische Kommunikation

Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) wurde im Rahmen der Überprüfung des Telekom-Reformpaketes überarbeitet. Dieses Paket umfasst fünf EU-Richtlinien (Rahmenrichtlinie, Zugangsrichtlinie, Genehmigungsrichtlinie, Universaldienstrichtlinie und die Datenschutzrichtlinie für elektronische Kommunikation). Eine neue Verordnung zur Einrichtung des Gremiums Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK) ist Teil des Telekom-Reformpaketes.

Der Schutz der Privatsphäre sowie der personenbezogenen Daten wird durch die neuen Vorschriften zur Einführung der Pflicht zur Meldung von Verstößen gegen das Datenschutzgesetz gestärkt – dies ist das erste Gesetz dieser Art in der EU. Dies bedeutet, dass die Anbieter von Kommunikationsdienstleistungen verpflichtet werden, die Behörden und ihre Kunden über Sicherheitsverstöße zu informieren, die ihre personenbezogenen Daten betreffen. So soll ein zusätzlicher Anreiz für einen besseren Schutz personenbezogener Daten durch die Anbieter von Kommunikationsnetzwerken und -diensten geschaffen werden.

Darüber hinaus werden auch die Vorschriften betreffend Privatsphäre und Datenschutz gestärkt, so zum Beispiel im Hinblick auf die Verwendung von „Cookies" oder ähnlicher Instrumente. Die Internetnutzer werden besser über „Cookies" sowie darüber informiert, was mit ihrem personenbezogenen Daten passiert. In der Praxis soll die Kontrolle persönlicher Informationen durch die Nutzer vereinfacht werden. Des Weiteren erhalten Internet-Diensteanbieter das Recht, Unternehmen und ihre Kunden auf dem Rechtsweg vor Spammern zu schützen.

Die revidierte Datenschutzrichtlinie für elektronische Kommunikation muss bis Mai 2011 in nationales Recht umgesetzt sein.

3.2. EUROPÄISCHER GERICHTSHOF

Beschluss des Gerichtshofs (Achte Kammer) vom 19. Februar 2009 (Vorabentscheidungsersuchen des Obersten Gerichtshofes (Österreich) – LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH/Tele2 Telecommunication GmbH) (Rechtssache C-557/07)[29]

Urteilstenor:
Das Gemeinschaftsrecht, insbesondere Art. 8 Abs. 3 der Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums in Verbindung mit Art. 15 Abs. 1 der 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 (Datenschutzrichtlinie für elektronische Kommunikation), hindert die Mitgliedstaaten nicht daran, eine Verpflichtung zur Weitergabe personenbezogener Verkehrsdaten an private Dritte zum Zweck der zivilgerichtlichen Verfolgung von Urheberrechtsverstößen aufzustellen Die Mitgliedstaaten sind aber gemeinschaftsrechtlich verpflichtet, darauf zu achten, dass ihrer Umsetzung der Richtlinien 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, 2002/58 und 2004/48 eine Auslegung derselben zugrunde liegt, die es erlaubt, die verschiedenen beteiligten Grundrechte miteinander zum Ausgleich zu bringen. Außerdem müssen die Behörden und Gerichte der Mitgliedstaaten bei der Durchführung der Maßnahmen zur Umsetzung dieser Richtlinien nicht nur ihr nationales Recht im Einklang mit Letzteren auslegen, sondern auch darauf achten, dass sie sich nicht auf eine Auslegung dieser Richtlinien stützen, die mit den Grundrechten oder den anderen

[29] Abl. C 113 vom 16.05.2009, S.14.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:113:0014:0014:DE:PDF

allgemeinen Grundsätzen des Gemeinschaftsrechts wie etwa dem Grundsatz der Verhältnismäßigkeit kollidiert.

Ein Access-Provider, der den Nutzern nur den Zugang zum Internet verschafft, ohne weitere Dienste wie insbesondere E-Mail, FTP oder File-Sharing anzubieten oder eine rechtliche oder faktische Kontrolle über den genutzten Dienst auszuüben, ist „Vermittler" im Sinne des Art. 8 Abs. 3 der Richtlinie 2001/29.

Urteil des Gerichtshofs (Dritte Kammer) vom 7. Mai 2009 (Vorabentscheidungsersuchen des Raad van State — Niederlande) — College van burgemeester en wethouders van Rotterdam/M. E. E. Rijkeboer (Rechtssache C-553/07)[30]

Urteilstenor:
Nach Art. 12 Buchst. a 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 sind die Mitgliedstaaten verpflichtet, ein Recht auf Auskunft über die Empfänger oder Kategorien der Empfänger der Daten sowie den Inhalt der übermittelten Information vorzusehen, das nicht nur für die Gegenwart, sondern auch für die Vergangenheit gilt. Es ist Sache der Mitgliedstaaten, eine Frist für die Aufbewahrung dieser Information sowie einen darauf abgestimmten Zugang zu ihr festzulegen, die einen gerechten Ausgleich bilden zwischen dem Interesse der betroffenen Person am Schutz ihres Privatlebens, insbesondere mit Hilfe der in der Richtlinie 95/46 vorgesehenen Rechte und Rechtsbehelfe, auf der einen Seite und der Belastung, die die Pflicht zur Aufbewahrung der betreffenden Information für den für die Verarbeitung Verantwortlichen darstellt, auf der anderen Seite.

Eine Regelung, die die Aufbewahrung der Information über die Empfänger oder Kategorien der Empfänger der Daten und den Inhalt der übermittelten Daten und dementsprechend den Zugang zu dieser Information auf die Dauer eines Jahres begrenzt, während die Basisdaten viel länger aufbewahrt werden, stellt keinen gerechten Ausgleich zwischen dem hier in Rede stehenden Interesse und der fraglichen Verpflichtung dar, sofern nicht nachgewiesen wird, dass eine längere Aufbewahrung der betreffenden Information den für die Verarbeitung Verantwortlichen über Gebühr belasten würde. Dies zu prüfen, ist Sache des nationalen Gerichts.

3.3. DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

Einleitung

Aufgabe des Europäischen Datenschutzbeauftragten (EDSB) ist es, sicherzustellen, dass die Rechte und Freiheiten von natürlichen Personen sowie insbesondere deren Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, von den Organe und Einrichtungen der Gemeinschaft nicht verletzt werden.

Die Hauptaktivitäten des Europäischen Datenschutzbeauftragten umfassen, wie in der Verordnung (EG) Nr. 45/2001[31] („die Verordnung") festgelegt, Folgendes:

- Überwachung und Sicherstellung der Einhaltung der Bestimmungen der Verordnung durch die Organe und Einrichtungen der Gemeinschaft bei der Verarbeitung personenbezogener Daten (Überwachung);
- Beratung der Organe und Einrichtungen der Gemeinschaft zu allen Fragen der Verarbeitung personenbezogener Daten. Dies umfasst die Beratung zu Gesetzesvorschlägen sowie die Überwachung neuer Entwicklungen, die Auswirkungen auf den Schutz personenbezogener Daten haben (Beratung);
- Zusammenarbeit mit nationalen Datenschutzbehörden und Aufsichtsbehörden als „dritte Säule" der EU im Hinblick auf eine Verbesserung der Einheitlichkeit des Schutzes personenbezogener Daten (Zusammenarbeit).

Überwachung

Die Überwachungsaufgaben reichen von der Beratung und Unterstützung der Datenschutzbeauftragten (DSB) über vorherige Überprüfung bedenklicher Verarbeitungsvorgänge bis zur Abwicklung von

[30] Abl. C 153 vom 04.07.2009, S.10.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:153:0010:0010:DE:PDF

[31] Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8, 12.01.2001, S. 1

Anfragen, einschließlich Vor-Ort-Untersuchungen und Bearbeitung von Beschwerden. Weitere Beratungsdienste für die EU-Verwaltung können auch in Form von Konsultationen zu Verwaltungsmaßnahmen oder in Form von Veröffentlichungen thematischer Leitlinien bereitgestellt werden.

In allen EU-Institutionen und -Organen muss es mindestens einen Datenschutzbeauftragten geben. Im Jahr 2009 stieg die Zahl der **Datenschutzbeamten** auf 45. Eine regelmäßige Interaktion zwischen ihnen und ihren Netzwerken ist eine wichtige Voraussetzung für effektive Prüfungen.

Die vorherige Überprüfung hochriskanter Datenverarbeitungen war auch im Jahr 2009 eine der wichtigsten Aufgaben. Der Europäische Datenschutzbeauftragte veröffentlichte 110 Stellungnahmen zu vorherigen Überprüfungen in den Bereichen Gesundheitsdaten, Personalbewertung, Personalbeschaffung, Zeiterfassung, Aufzeichnung von Telefonaten, Instrumente zur Messung von Leistungen und Sicherheitsüberprüfungen. Diese Stellungnahmen sind auf der Website des Datenschutzbeauftragten veröffentlicht, ihre Umsetzung wird systematisch überprüft.

Die Umsetzung der Verordnung durch die Organe und Institutionen wird außerdem durch die regelmäßige Erfassung von Leistungsindikatoren bei allen EU-Institutionen und -Organen **systematisch überprüft**. Nach den im Frühjahr 2009 durchgeführten Prüfungen veröffentlichte der Europäische Datenschutzbeauftragte einen Bericht, dem zu entnehmen war, dass die EU-Institutionen gute Fortschritte hinsichtlich der Erfüllung der Datenschutzbestimmungen gemacht haben, während die meisten Agenturen jedoch hinsichtlich der Einhaltung schlechter abschnitten.

Der Europäische Datenschutzbeauftragte führt außerdem vier Vor-Ort-**Überprüfungen** in verschiedenen Organen und Einrichtungen durch. Diesen Überprüfungen folgt eine systematische Nachprüfung. In der näheren Zukunft werden solche Überprüfungen häufiger durchgeführt werden. Im Juli 2009 verabschiedete der Europäische Datenschutzbeauftragte ein Handbuch für Prüfverfahren und veröffentlichte die wesentlichen Elemente dieses Verfahrens auf seiner Website.

Im Jahr 2009 stieg die Zahl der insgesamt eingereichten **Beschwerden** auf 111 an. Hiervon waren jedoch nur 42 zulässig. Viele unzulässige Beschwerden betrafen Fragen auf nationaler Ebene, für die der Europäische Datenschutzbeauftragte nicht zuständig ist. Die meisten zulässigen Beschwerden betrafen vermutete Verletzungen der Vertraulichkeit, die unverhältnismäßige Erfassung von Daten oder die unrechtmäßige Nutzung von Daten durch den Datenkontrolleur. In acht Fällen stellte der Europäische Datenschutzbeauftragte fest, dass gegen die Datenschutzbestimmungen verstoßen worden war.

Es wurde auch weiterhin in Bezug auf **Verwaltungsmaßnahmen** beraten, die die Organe und Institutionen der Gemeinschaft in Bezug auf die Verarbeitung personenbezogener Daten in Betracht zogen. Es ergab sich eine Vielzahl von Fragen, darunter die Übermittlung von Daten an Drittländer oder internationale Organisationen, die Datenverarbeitung im Fall einer Pandemie, der Datenschutz beim Internen Auditdienst sowie die Umsetzung der Bestimmungen der Verordnung (EG) Nr. 45/2001.

Der Europäische Datenschutzbeauftragte verabschiedete **Leitlinien** zur Verarbeitung personenbezogener Daten im Bereich der Personalbeschaffung sowie zur Verarbeitung von Gesundheitsdaten am Arbeitsplatz. Im Jahr 2009 führte der Europäische Datenschutzbeauftragte eine öffentliche Konsultation zu den Videoüberwachungsrichtlinien durch und hob dadurch unter anderem die Prinzipien „Privacy by Design" sowie Rechenschaftspflicht als wesentliche Prinzipien in diesem Zusammenhang hervor.

Beratung

Eine Reihe wichtiger Ereignisse half dabei, einem neuen rechtlichen **Rahmen im Bereich Datenschutz** einen Schritt näher zu kommen. Die Erreichung dieses Ziels wird auf der Agenda des Europäischen Datenschutzbeauftragten für die kommenden Jahre ganz oben stehen.

Ende des Jahres 2008 wurde auf EU-Ebene eine Rahmenentscheidung zum Datenschutz im Bereich der Zusammenarbeit von Polizei und Justiz verabschiedet. Wenngleich dieser Schritt noch nicht alle Erwartungen vollumfänglich erfüllen konnte, so war es doch ein wichtiger Schritt in die richtige Richtung.

Im Jahr 2009 stellte die Verabschiedung der revidierten Datenschutzrichtlinie für elektronische Kommunikation als Teil eines größeren Paketes eine weitere wesentliche Entwicklung dar. Dies war auch ein erster Schritt hin zur Modernisierung des rechtlichen Rahmens im Bereich Datenschutz.

Die Inkraftsetzung des Vertrags von Lissabon am 1. Dezember 2009 führte nicht nur dazu, dass die Charta der Grundrechte für alle Organe und Institutionen sowie für alle Mitgliedstaaten verbindlich wurde, wenn sie im Bereich des EU-Rechts agieren, sondern auch zur Einführung einer allgemeinen Basis für einen umfassenden rechtlichen Rahmen in Artikel 16 des Römischen Vertrages.

Im Jahr 2009 startete die Kommission außerdem eine öffentliche Konsultation zur Zukunft des rechtlichen Rahmens im Bereich Datenschutz. Der Europäische Datenschutzbeauftragte arbeitete eng mit Kollegen zusammen, um einen angemessenen Beitrag zu dieser Konsultation sicherzustellen, und betonte zu unterschiedlichen Anlässen die Notwendigkeit eines umfassenderen und effektiveren Datenschutzes in der Europäischen Union.

Der Europäische Datenschutzbeauftragte führte die Umsetzung seiner allgemeinen **Beratungspolitik** fort und veröffentlichte eine Rekordzahl von Stellungnahmen zu Gesetzesvorschlägen in unterschiedlichen Bereichen. Diese Politik umfasst auch einen proaktiven Ansatz, der eine regelmäßige Bestandsaufnahme der zur Konsultation einzureichenden Gesetzesvorschläge sowie die Verfügbarkeit informeller Kommentare in der Vorbereitungsphase der Gesetzesvorschläge umfasst. Die meisten Stellungnahmen des Europäischen Datenschutzbeauftragten wurden mit dem Parlament und dem Rat weiter diskutiert.

Im Jahr 2009 verfolgte der Europäische Datenschutzbeauftragte die Entwicklungen des **Stockholm-Programms** sowie dessen Vision für die nächsten fünf Jahre im Bereich Justiz und Inneres mit besonderem Interesse. Der Europäische Datenschutzbeauftragte beriet zur Entwicklung des Programms und nahm an den vorbereitenden Arbeiten für das Europäische Informationsmodell Teil.

Sonstige Tätigkeiten in diesem Bereich betrafen die Überprüfung der Eurodac- und Dublin-Verordnungen, die Einrichtung einer Agentur für das operative Management eines großen IT-Systems sowie einen kohärenten Ansatz für Prüfungen in diesem Bereich.

Im Kontext der **Privatsphäre in der elektronischen Kommunikation und der Technologie** war der Europäische Datenschutzbeauftragte zusätzlich zu oben genannten allgemeinen Überprüfung auch an Überprüfungen zu Fragen bezüglich der Richtlinie über die Vorratsspeicherung von Daten, die Nutzung von RFID-Tags oder intelligenten Transportsysteme sowie des RISEPTIS-Berichts mit dem Titel „Vertrauen in der Informationsgesellschaft" beteiligt.

Im Kontext der **Globalisierung** war der Europäische Datenschutzbeauftragte an der Entwicklung globaler Standards, dem transatlantischen Dialog betreffend Datenschutz und Daten aus dem Bereich der Strafverfolgung sowie an Fragen im Bereich von Beschränkungen in Bezug auf mutmaßliche Terroristen und bestimmte Drittländer beteiligt.

Weitere Bereiche, die für den Europäischen Datenschutzbeauftragten von besonderem Interesse waren, waren die Bereiche **Gesundheitswesen** – einschließlich der grenzüberschreitenden medizinischen Versorgung, den elektronischen Gesundheitsdiensten sowie der Kontrolle von Arzneimitteln – und der **öffentliche Zugang zu Dokumenten** – wie zum Beispiel die Revision der Verordnung (EG) Nr. 1049/2001 über den Zugang der Öffentlichkeit zu Dokumenten sowie verschiedene Gerichtsverfahren zum Zusammenhang zwischen öffentlichem Datenzugang und Datenschutz.

Zusammenarbeit

Die wesentliche Plattform für die Zusammenarbeit zwischen den Datenschutzbehörden in Europa ist die **Artikel-29-Datenschutzgruppe**. Der Europäische Datenschutzbeauftragte nimmt an den Aktivitäten der Datenschutzgruppe teil, die eine zentrale Rolle bei der einheitlichen Anwendung der Datenschutzrichtlinie spielt.

Der EDSB und die Arbeitsgruppe haben zusammengearbeitet, um eine gute Synergie zu einer Reihe von Themen zu erreichen. Der Schwerpunkt lag hierbei auf der Umsetzung der Datenschutzrichtlinie sowie auf Herausforderungen durch die Nutzung neuer Technologien. Der EDSB unterstützte außerdem Initiativen zur Erleichterung internationaler Datenflüsse.

Besonders erwähnenswert ist der gemeinsame Beitrag zur „Zukunft der Privatsphäre" als Reaktion auf die Konsultation der Europäischen Kommission zum rechtlichen Rahmen der EU im Bereich Datenschutz sowie auf die Konsultation der Kommission zu den Auswirkungen von „Körperscannern" im Bereich der Flugsicherheit.

Eine der wichtigsten Aufgaben des Europäischen Datenschutzbeauftragten in Bezug auf die Zusammenarbeit betrifft **Eurodac**, in deren Rahmen die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte für die Überwachung des Datenschutzes verantwortlich zeichnen. Der Koordinierungsausschuss zur Eurodac-Überwachung – der sich aus den Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten zusammensetzt – trat drei Mal zusammen. Der Schwerpunkt lag hierbei auf der Umsetzung des vom Ausschuss im Dezember 2007 verabschiedeten Arbeitsprogramms.

Eines der wesentlichen Ergebnisse war die Annahme eines zweiten Prüfberichtes im Juni 2009, dessen Schwerpunkt auf zwei Themen lag: dem Recht auf Information für Asylbewerber und den Methoden zur Schätzung des Alters junger Asylbewerber.

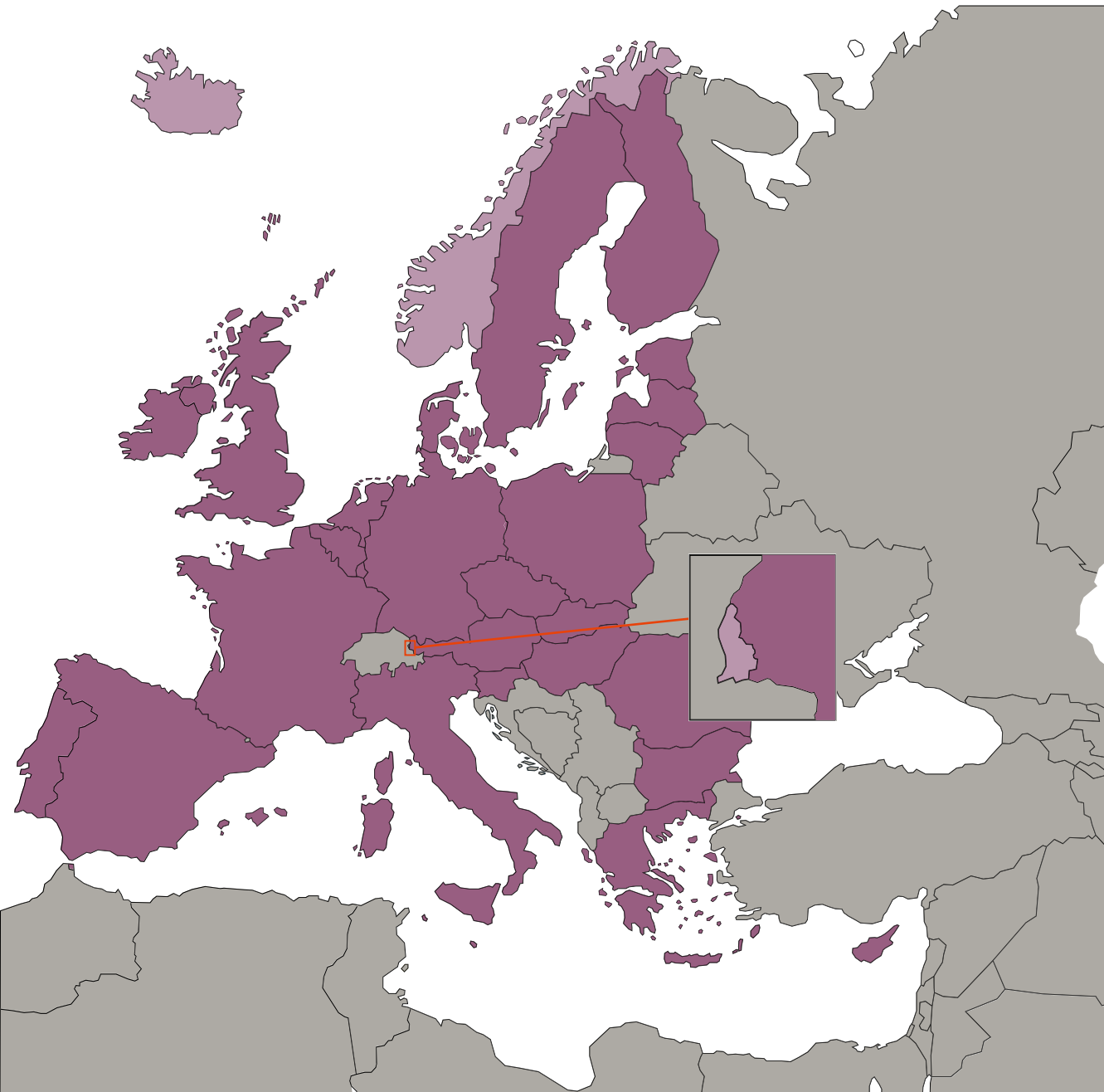
Der EDSB führte seine enge Zusammenarbeit mit den Datenschutzbehörden im Rahmen der ehemaligen „dritten Säule" – des Bereichs der **Zusammenarbeit zwischen Polizei und Justiz** – sowie mit der Arbeitsgruppe Polizei und Justiz fort. Im Jahr 2009 umfasste diese Zusammenarbeit einen Beitrag zur Debatte zum Stockholm-Programm sowie die Bewertung der Auswirkungen des Rahmenbeschlusses des Rates zum Datenschutz.

Der Zusammenarbeit in anderen **internationalen Foren**, insbesondere im Rahmen der 31. Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Madrid, auf der eine Reihe globaler Standards festgelegt wurden, wurde auch weiterhin Beachtung geschenkt.

Der EDSB organisierte im Rahmen der auf der 28. Internationalen Konferenz der Datenschutzbeauftragten im November 2006 gestarteten „Londoner Initiative" außerdem einen Workshop mit dem Titel „Auf Sicherheitsverstöße reagieren", um so für den Bereich Datenschutz zu sensibilisieren und die diesbezügliche Arbeit effektiver zu gestalten.

Kapitel 4

DIE WICHTIGSTEN ENTWICKLUNGEN IM EUROPÄISCHEN WIRTSCHAFTSRAUM



Island

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

Im Jahr 2009 wurde eine Reihe von Rechtsakten und Verwaltungsvorschriften im Zusammenhang mit dem Datenschutz erlassen, die die Richtlinie 95/46/EG (jedoch nicht die Richtlinie 2002/58/EG) betrafen. Die wichtigsten davon waren folgende:

1. Gesetz Nr. 37/2009 zur Änderung des Gesetzes über die Arbeitslosenversicherung, Nr. 54/2006. – Durch Gesetz Nr. 37/2009 wurden die Befugnisse der Direktion für Arbeit hinsichtlich der Erfassung von Daten erweitert. Die Direktion für Arbeit war befugt, Daten zu erfassen, die zur Umsetzung von Gesetz Nr. 54/2006 erforderlich waren. Gleiches galt für Daten von Steuerbehörden, Sozial- und Krankenversicherungsbehörden, der Datensammelstelle für Kinderbeihilfe sowie der Rentenkasse. Durch Gesetz Nr. 37/2009 erhielt die Direktion für Arbeit außerdem Befugnis, Daten von Schulen auf oberer Sekundar- und Hochschulebene zu erfassen. Diesbezüglich erhielt die Direktion für Arbeit Listen der in diesen Schulen angemeldeten Schüler, da die Anmeldung an einer Schule Auswirkungen auf das Recht auf Arbeitslosenhilfe haben kann.

2. Gesetz Nr. 48/2009 zur Änderung des Gesetzes über Biobanken, Nr. 110/2000. – Das Gesetz über Biobanken enthält Bestimmungen zum Schutz personenbezogener Daten im Hinblick auf die Entnahme, Lagerung, Aufbewahrung und Verwendung biologischer Proben. Ursprünglich mussten alle biologischen Proben separat von persönlichen Identifikatoren aufbewahrt werden. Gesetz Nr. 48/2009 hat dies geändert. Nunmehr wird zwischen wissenschaftlichen und klinischen Proben unterschieden. Erstere sind ohne persönliche Identifikatoren aufzubewahren, und die Verbindung der Proben mit den persönlichen Identifikatoren muss im Einklang mit den Vorschriften der Datenschutzbehörde erfolgen (aktuelle Vorschrift Nr. 918/2001). Letztere Proben dürfen zwar mit persönlichen Identifikatoren markiert werden, müssen jedoch so aufbewahrt werden, dass sie nicht verloren gehen, beschädigt werden und unbefugte Personen nicht auf sie zugreifen können. Ziel des Gesetzes Nr. 48/2009 war die Beseitigung der Gefahr einer fälschlichen Identifizierung klinischer Proben, die die Sicherheit von Patienten bedrohen könnte.

3. Das Gesetz über Patientenakten, Nr. 55/2009. – Das Gesetz umfasst die Verpflichtung zur Aufbewahrung von Patientenakten. Ziel des Gesetzes ist die Einführung von Vorschriften für Patientenakten, um Patienten jederzeit die bestmögliche medizinische Versorgung bieten und gleichzeitig den Schutz ihrer gesundheitsbezogenen Daten gewährleisten zu können. Patientenakten sind so weit wie möglich in elektronischer Form anzulegen. Das Gesetz ermöglicht Einrichtungen des Gesundheitswesens und selbstständigen Ärzten, ihre Gesundheitsinformationssysteme, die die Patientenakten enthalten, miteinander zu verbinden oder ein gemeinsames Gesundheitsinformationssystem zu betreiben. Die Patienten haben das Recht, den Austausch ihrer Daten in verbundenen Gesundheitsinformationssystemen zu untersagen. Darüber hinaus können die Patienten den Zugang zu ihren Daten in einem gemeinsamen Gesundheitsinformationssystem außerhalb der medizinischen Versorgungseinrichtungen bzw. der Praxis des betreffenden Arztes, bei denen bzw. dem die Patientenakten angelegt ist, vollständig oder teilweise verbieten. Die Patienten können bei der Behandlung entscheiden, dass Daten über die Behandlung ausschließlich der Person, die den Dateneintrag vornimmt, dem Kontrolleur der Patientenakten sowie gegebenenfalls weiteren angegebenen Ärzten zugänglich sind. Wird es im Hinblick auf die Behandlung als erforderlich eingestuft, dass andere Ärzte Zugang zu den betreffenden Gesundheitsdaten erhalten, muss der Patient darüber informiert werden. Darüber hinaus muss der Patient eingehend aufgeklärt werden, dass eine Verweigerung des erforderlichen Zugriffs auf die Patientenakte unter Umständen als Ablehnung der Behandlung eingestuft werden kann. Die Einhaltung der Bestimmungen des Gesetzes soll in erster Instanz von den für die Gesundheitsinformationssysteme Verantwortlichen sowie in zweiter Instanz vom Ärztlichen Direktor des Gesundheitswesens („Medical Director of Health“) und der Datenschutzbehörde überwacht werden. Sollte im Rahmen der Überwachung festgestellt werden,

dass mit großer Wahrscheinlichkeit eine Verletzung des Rechts auf Privatsphäre eines Patienten vorliegt, so ist dies bei der Polizei zur Anzeige zu bringen.

4. Gesetz Nr. 146/2009 zur Änderung des Gesetzes über eine Untersuchung der Ereignisse und der Gründe, die im Jahr 2008 zum Niedergang der isländischen Banken geführt haben sowie damit in Zusammenhang stehender Ereignisse, Nr. 142/2008. – Gesetz Nr. 146/2009 führt Verfahrensklauseln ein, die das isländische Parlament (Althing) bei der Reaktion auf den Bericht des vom Parlament gemäß Gesetz Nr. 142/2008 eingerichteten Sonderuntersuchungsausschusses befolgen muss. Das Gesetz beinhaltet Bestimmungen zu den im Rahmen der Tätigkeiten des Ausschusses erstellten Datenbanken. Diese Datenbanken enthalten umfassende Daten zu Einzelpersonen. Einige dieser Daten (hauptsächlich Daten zu Unternehmern, Politikern und leitenden Beamten) wurden in dem im April 2010 veröffentlichten Bericht des Untersuchungsausschusses veröffentlicht, da man davon ausging, dass diese Daten Hinweise auf die Gründe für den Niedergang der isländischen Banken liefern könnten. Der großen Masse der Daten wird jedoch kein solch großer Wert beigemessen, dass ihre Veröffentlichung erforderlich wäre. Aus diesem Grund umfasst Gesetz Nr. 146/2009 Bestimmungen zum Schutz dieser Daten, um einen unberechtigten Zugriff zu verhindern. Gemäß dem Gesetz ist ein Zugriff auf diese Daten zu Forschungszwecken als legitim einzustufen. Die Verarbeitung dieser Daten zu Forschungszwecken darf jedoch nicht die Veröffentlichung persönlich identifizierbarer Daten umfassen.

B. Bedeutende Rechtsprechung

Keine nennenswerte.

C. Wichtige spezifische Themen

Eine der wichtigsten Tätigkeiten im Bereich Datenschutz im Jahr 2009 war ein von der Nationalbank Islands durchgeführtes Forschungsprojekt, in dessen Rahmen umfassende Daten zu den Finanzen von Vertretern verschiedenster Bereiche, wie zum Beispiel Banken oder sonstigen Finanzinstitutionen, der Direktion für Arbeit, der Rentenkasse sowie der Sozialversicherungsverwaltung miteinander verknüpft wurden. Der Zweck der Verknüpfung bestand darin, einen besseren Einblick in die Auswirkungen der Finanzkrise in Island auf den Einzelnen und auf Familien zu erhalten und so besser auf die Krise reagieren zu können. Die Datenschutzbehörde erteilte die Genehmigung zur Verknüpfung dieser Daten unter der Voraussetzung der Anwendung technischer und organisatorischer Sicherheitsmaßnahmen, zum Beispiel der Anonymisierung der Daten. Wurden Daten nicht verarbeitet, so wurde der Computer, auf dem die Daten gespeichert waren, bei der Datenschutzbehörde aufbewahrt. Wie in der Genehmigung festgelegt, wurde die Festplatte, auf der alle Daten gespeichert waren, Anfang 2010 vernichtet.

Am 28. April veröffentlichte die Datenschutzbehörde einen Beschluss über die Verwendung von Daten in der zentralen isländischen Datenbank für Arzneimittelverschreibungen, die gemäß geltendem Recht seit 2003 von der Gesundheitsdirektion verwaltet wird. Das Gesetz, insbesondere Artikel 27 des Gesetzes Nr. 93/1994 über die Verschreibung von Arzneimitteln, geändert durch Gesetz Nr. 89/2003, legt fest, zu welchen Zwecken die Datenbank genutzt werden darf. Hauptsächlich sind dies verwaltungstechnische Zwecke, unter anderem die Untersuchung von vermutetem Missbrauch suchterregender Arzneimittel. Eine Person hatte um die Verschreibung eines solchen Arzneimittels gebeten. Der Arzt, an den sich diese Person gewandt hatte, erkundigte sich bei der Gesundheitsdirektion über den Arzneimittelkonsum dieser Person und erhielt als Antwort, dass diese Person in der Vergangenheit suchterregende Arzneimittel missbraucht hatte. Die Person wurde erst danach über die Verwendung ihrer Daten in der Datenbank informiert und reicht eine Beschwerde bei der Datenschutzbehörde ein. Im oben genannten Beschluss stellte die Datenschutzbehörde fest, dass die Übermittlung der Informationen an den Beschwerdeführer nicht im Einklang mit Artikel 27 des Gesetzes über die Verschreibung von Arzneimitteln stand und dass die Gesundheitsdirektion die Informationen somit unrechtmäßig an den Arzt weitergegeben hatte.

Am 16. Dezember 2009 veröffentlichte die Datenschutzbehörde einen Beschluss über die von der Direktion für Arbeit durchgeführte Verarbeitung von Daten in IP-Adressen. Personen, die Arbeitslosenhilfe

erhalten möchten, übermitteln der Direktion jeden Monat eine elektronische Meldung zur Bestätigung, dass sie noch immer arbeitslos sind. Gemäß der Interpretation der Arbeitslosengesetze durch die Direktion müssen Arbeitslose in Island bleiben, wenn sie Arbeitslosenhilfe erhalten wollen, damit sie kurzfristig Beschäftigungsverhältnisse eingehen können. Die IP-Adresse einer an die Direktion übermittelten elektronischen Meldung enthielt Informationen, anhand derer nachvollzogen werden konnte, dass die betroffene Person sich nicht in Island befand. Die Direktion informierte die betroffene Person in einem Brief darüber, dass Informationen über den Auslandsaufenthalt der betroffenen Person vorlägen, machte jedoch keine Angaben dazu, wie sie diese Informationen erhalten hatte. Die betroffene Person legte Beschwerde bei der Datenschutzbehörde ein, die in oben genanntem Beschluss feststellte, dass die Direktion für Arbeit korrekterweise auf ihrer Website hätte darauf hinweisen müssen, dass IP-Adressen erfasst werden und dass die in diesen Adressen enthaltenen Daten unter anderem zur Feststellung verarbeitet werden, ob sich eine Person außerhalb Islands aufhält.

Liechtenstein

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

Eine der Aufgaben der Datenschutzstelle (DSS) ist es, zu gesetzlichen Vorlagen und Erlässen, die für den Datenschutz erheblich sind, Stellung zu nehmen und die Übereinstimmung mit den Bestimmungen der Richtlinie 95/46/EG zu überprüfen. Im Jahr 2009 wurde die DSS zu insgesamt 34 Gesetzesvorhaben in verschiedenen Stadien des Gesetzgebungsverfahrens ersucht, eine Stellungnahme abzugeben. Im Rahmen der Gesetzesvorhaben soll insbesondere auf Folgende näher eingegangen werden, da sie wichtige datenschutzrechtliche Aspekte tangieren:

Bereits im letzten Jahresbericht war ausführlich über die zwei Teilrevisionen des Datenschutzgesetzes (DSG) berichtet worden. Die eine Revision trat bereits zum 1. Januar 2009[32], die andere zum 1. Juli 2009[33] in Kraft. Parallel dazu wurde die Datenschutzverordnung (DSV) angepasst, die ebenfalls mit Juli in Kraft trat.[34] In der DSV wurde insbesondere die Institution eines betrieblichen oder behördlichen Datenschutzverantwortlichen neu geschaffen.[35] Mit der Funktion eines internen Datenschutzverantwortlichen soll die Eigenverantwortung der Inhaber der Datensammlungen unterstützt und verstärkt werden. Ausserdem wird die Einrichtung der Stelle eines Datenschutzverantwortlichen auch als Wettbewerbsvorteil für Unternehmen angesehen. Private Personen oder Behörden, die einen internen Datenschutzverantwortlichen benennen, erfahren gewisse Erleichterungen. So entfällt zum Beispiel unter gewissen Voraussetzungen die Pflicht zur Anmeldung der Datensammlungen. Für private Personen entfällt sogar die Pflicht, ein Bearbeitungsreglement für automatisierte Datensammlungen zu erstellen. Um die gesetzlich vorgesehenen Vorteile auch nützen zu können, müssen die intern ernannten Datenschutzverantwortlichen bei der DSS gemeldet werden, die diese dann in einer öffentlich verfügbaren Liste publizieren muss.

In der Praxis machten sich vor allem die Neuerungen zur verstärkten Unabhängigkeit der DSS[36], zum Datentransfer ins Ausland und zur Videoüberwachung bemerkbar. Im Zusammenhang mit dem grenzüberschreitenden Datentransfer ist insbesondere die für bestimmte Fälle neu eingeführte Genehmigungspflicht für einzelvertragliche Datenschutzvereinbarungen und für verbindliche unternehmensinterne Datenschutzregelungen zu nennen.[37] Sofern im betroffenen Ausland eine Gesetzgebung fehlt, die einen angemessenen Datenschutz gewährleistet, müssen diese Vereinbarungen zuvor von der Regierung genehmigt werden. Im Rahmen des Genehmigungsverfahrens hat die DSS eine Stellungnahme abzugeben. Diese gibt darüber Auskunft, ob die Garantien oder einheitlichen Datenschutzregelungen einen angemessenen Schutz im Sinne des liechtensteinischen DSG gewährleisten. Die Regierung ist bei Erteilung der Genehmigung grundsätzlich an die Stellungnahme der DSS gebunden.

Die Einführung einer allgemeinen Rechtsgrundlage für die Videoüberwachung im öffentlich zugänglichen Raum[38] hat die Ressourcen der DSS im Berichtsjahr stark eingebunden. Der Betrieb einer Videoüberwachung im öffentlichen Bereich unterliegt seit 1. Juli 2009 der Genehmigungspflicht durch die DSS. Generell muss die Genehmigung vor Inbetriebnahme eingeholt werden. Für bestehende Überwachungen wurde daher eine Übergangsfrist bis Jahresende vorgesehen. Für das Genehmigungsverfahren mussten im Vorfeld über das Internet verfügbare Antragsformulare, Ausfüllhilfen, eine ausführliche Wegleitung erarbeitet und die Öffentlichkeit entsprechend informiert werden. Zu beachten ist, dass die Genehmigungspflicht nur besteht, wenn mittels der gewonnenen Daten Personen bestimmbar sind, die Daten bearbeitet werden und es sich um öffentlich zugängliche Bereiche handelt. Umgekehrt bedeutet dies, dass beispielsweise Bildaufzeichnungen für den rein privaten oder familiären Bereich, Bildübertragungen

[32] LGBl. 2008 Nr. 273.

[33] LGBl. 2009 Nr. 46.

[34] LGBl. 2009 Nr. 209.

[35] Art. 4a, 13a, 23 Abs. 2 DSV.

[36] S. dazu ausführlich den Beitrag Liechtensteins im 12. Jahresbericht der Artikel 29 Datenschutzgruppe, S. 132 sowie den Tätigkeitsbericht des Datenschutzbeauftragten des Fürstentums Liechtenstein, 2008, 10.1.

[37] Art. 8 Abs. 3 DSG in Verbindung mit Art. 6 DSV.

[38] Art. 6a DSG in Verbindung mit Art. 27 DSV.

ausschließlich in Echtzeit oder Aufnahmen von Webcams, die keine Personenidentifikation ermöglichen, nicht genehmigungspflichtig sind.

Ein wesentliches Gesetzesvorhaben betraf die Revision des Kommunikationsgesetzes (KomG), welches im Berichtsjahr noch nicht abgeschlossen wurde:
Liechtenstein hatte bereits 2006 die Vorratsdatenspeicherung von Verkehrsdaten im KomG eingeführt, obwohl die Richtlinie 2006/24/EG bis dato noch nicht Bestandteil des EWR-Abkommens ist und somit auch keine Umsetzungspflicht besteht. Diese Regelungen waren von verschiedenen Seiten immer wieder kritisiert worden. Dabei wird die Speicherung der Verkehrsdaten für die Dauer von sechs Monaten – in Übereinstimmung mit der Art. 29 Datenschutzgruppe - als erheblichen Eingriff in die Freiheitsrechte der Bürger und deren Privatsphäre angesehen. Die Regierung hat diese Kritik nunmehr zum Anlass genommen, die einschlägigen Regelungen im Interesse einer bürger- und grundrechtsfreundlichen Ausgestaltung nochmals zu überarbeiten und für den Zugriff auf bzw. die Verwertung von auf Vorrat gespeicherten Daten strenge Voraussetzungen zu normieren.[39] Ausserdem ist eine umfassende Kontrolle des Datenschutzes und der Datensicherheit durch die DSS vorgesehen.

B. Bedeutende Rechtsprechung

Keine nennenswerte.

C. Wichtige spezifische Themen

Die bereits im Vorjahr intensiven Arbeiten zur Vorbereitung eines Beitritts Liechtensteins zu den Abkommen von Schengen und Dublin wurden fortgesetzt und intensiviert.[40] So hatte sich die DSS bereits mit Rechtsakten der Weiterentwicklung des Schengenbesitzstandes zu befassen, wie etwa der Umsetzung der sogenannten Schwedischen Initiative (Rahmenbeschluss 2006/960/JI). Zur Vorbereitung auf die Datenschutz-Evaluation konnten auch Erkenntnisse anderer Schengen-Staaten genutzt werden. Im Berichtsjahr wurde zudem eine Probe-Bewertung im Bereich Datenschutz durchgeführt, durch die positive Erfahrungen gewonnen werden konnten. Dabei wurde das Hauptaugenmerk auf die Unhabhängigkeit und Struktur der Datenschutzstelle, deren gesetzlichen Aufgaben und Prüfbefugnisse sowie die Rechte der Bürger gelegt. Im Zentrum der Vorbereitungen stand aber auch die Beantwortung eines Fragebogens, in dem die Rahmenbedingungen zur „Schengen-Reife" darzulegen sind und die Erstellung von Dokumentationen.

Wenngleich Liechtenstein noch keinen Zugriff auf die Daten hat, konnte durch die Teilnahme als Beobachter an Sitzungen der unterschiedlichen Gremien, wie der Gemeinsamen Kontrollinstanz Schengen, wertvolle Erkenntnisse über die Funktions- und Arbeitsweise von Schengen gewonnen werden.

Zu den zentralen Aufgaben der Datenschutzstelle gehören weiters die Information und Sensibilisierung der Öffentlichkeit für Datenschutz. Zur Information der Öffentlichkeit wird nach wie vor die Internetseite der DSS am meisten genutzt. Wesentlich zur Information der Öffentlichkeit trägt auch der Newsletter bei, in dem monatlich über ein aktuelles Thema berichtet wird.

Auf der Internetseite führte die Datenschutzstelle im Berichtsjahr erstmals eine Online-Umfrage durch. Insgesamt wurden zum Thema Datenschutz vier Fragenblöcke zu den Bereichen Allgemeines – Information – Vertrauen – Verhalten gestellt. Seitens der Medien konnte ein erhebliches Interesse an den Ergebnissen der Umfrage festgestellt werden. Ein Ergebnis dieser Umfrage besteht darin, dass eine überwiegende Anzahl an Teilnehmern sich nicht ausreichend über ihre Datenschutzrechte informiert fühlt. Internet und Datenschutz war ein Thema, zu welchem sich die Teilnehmer mehr Informationen wünschten. Dies wurde aufgegriffen und eine Schulung für Mitarbeiter der liechtensteinischen Landesverwaltung durchgeführt.

Anlässlich des Europäischen Datenschutztages am 28. Januar lud die DSS in Zusammenarbeit mit dem Institut für Wirtschaftsinformatik der Hochschule Liechtenstein zu einer öffentlichen Veranstaltung unter dem Titel „Denn sie wissen nicht, was sie tun?! - Soziale Netzwerke

[39] Bericht und Antrag Nr. 110/2009, S. 113.

[40] Vgl. Tätigkeitsbericht 2008, 10.1.

unter der Lupe" ein.[41] Ziel der Veranstaltung war es, auf das Thema Datenschutz aufmerksam zu machen und die Öffentlichkeit zu sensibilisieren.

Zur Klärung einiger Rechtsfragen gab die Datenschutzstelle zwei Rechtsgutachten in Auftrag: Diese betrafen die Ausnahmen der ärztlichen Schweigepflicht sowie das Spannungsfeld Amtsgeheimnis – Amtshilfe unter besonderer Berücksichtigung der Auslegungsmethoden *lex specialis* und *lex posterior*. Das letztgenannte Gutachten enthält wichtige Erkenntnisse, die noch auszuwerten sind.

[41] http://www.llv.li/amtsstellen/llv-dss-datenschutztag/llv-dss-datenschutztag-archiv.htm.

Norwegen

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

Am 9. Januar verabschiedete das norwegische Parlament (Storting) eine Änderung des Gesetzes zum Schutz personenbezogener Daten. Abschnitt 26 wurde durch ein neues Gesetz zur Regulierung des Bereichs Direktwerbung ersetzt, dass den Verbraucherbeauftragten ermächtigt, in Fällen unrechtmäßiger oder unethischer Werbung im Interesse der Öffentlichkeit zu handeln. Im alten Abschnitt 26 hatte diese Befugnis bei der Datenschutzbehörde gelegen.

Anfang 2009 wurde ein Abkommen zwischen der Datenschutzbehörde und der nationalen Steuerbehörde geschlossen, dass der Datenschutzbehörde ermöglicht, verhängte Bußgelder einzuziehen und in Zukunft Bußgelder zu verhängen.

Wie im letzten Jahresbericht erwähnt, hat das Parlament ein neues Gesundheitsforschungsgesetz verabschiedet. Das Gesetz trat am 1. Juli 2009 in Kraft. Die Datenschutzbehörde ist demzufolge nicht mehr für die Erteilung einer Genehmigung für Forschungsprojekte im Bereich Gesundheit zuständig. Die Datenschutzbehörde ist jedoch immer noch befugt, Prüfungen der Datenkontrolleure durchzuführen, um sicherzustellen, dass die Bestimmungen des Gesundheitsforschungsgesetzes eingehalten werden.

Den Vorschriften zum Schutz personenbezogener Daten wurde ein neues Kapitel 9 zur Regelung der „Kontrolle von E-Mail-Postfächern etc." hinzugefügt. Diese Regelung stellt eine Kodifizierung der offiziellen Vorgehensweise der norwegischen Datenschutzbehörde in diesem Bereich dar. Der wichtigste Aspekt ist, dass Arbeitgeber ein spezielles Protokoll einhalten müssen, um E-Mail-Postfächer sowie persönliche Daten in Computernetzwerken einsehen zu dürfen. Die Regelung legt eindeutig fest, dass es einen Bereich des „Arbeitsraumes" von Angestellten geben muss, der vor Überwachung und Protokollierung geschützt ist.

Das Gesetz zum Schutz personenbezogener Daten soll revidiert werden, und die Datenschutzbehörde hat einige kleinere Änderungen vorgeschlagen, um das Gesetz in Einklang mit der technologischen sowie gesellschaftlichen Entwicklung zu bringen.

B. Bedeutende Rechtsprechung

Keine nennenswerte.

C. Wichtige spezifische Themen

Richtlinie über die Vorratsspeicherung von Daten
Das Jahr 2009 wurde beherrscht von der Debatte um die Richtlinie über die Vorratsspeicherung von Daten. Die Datenschutzbehörde betonte, dass die Richtlinie einen Bruch mit der aktuellen Tradition der Registrierung und Speicherung von Kommunikationsdaten darstelle. Unserer Ansicht steht die Richtlinie im Widerspruch zu zentralen rechtlichen Prinzipien, Freiheiten und Menschenrechten. Die Umsetzung der Richtlinie in norwegisches Recht bedeutet, dass große Datenmengen zu Kommunikation und Bewegungen norwegischer Bürger für einen langen Zeitraum gespeichert würden. Eine der wesentlichen politischen Frage lautet, ob das Parlament sein Vorbehaltsrecht im Rahmen des EWR-Abkommens wahrnehmen sollte.

Im Rahmen der Debatte um die Richtlinie behaupten die Befürworter, dass die Privatsphäre durch die Speicherung der Daten nicht beeinträchtigt werde, weil es klare und strenge Bedingungen für die Verwendung der Informationen gebe. Im Entwurf einer Konsultation zur Umsetzung der Richtlinie in Norwegen wird betont, dass die Polizei nur bei konkreten Verdachtsfällen auf die Daten zugreifen darf und dass ein solcher Zugriff von einem Gericht genehmigt werden muss.

Der Schutz der Privatsphäre sollte in der westlichen Tradition nicht nur vor einer Weiterverwendung erfasster Informationen, sondern auch vor einer unverhältnismäßigen Erfassung persönlicher Informationen schützen. Eine systematische Speicherung nur für den Fall, dass die gespeicherten Informationen im Rahmen einer späteren Untersuchung eventuell benötigt werden, könnte die Unschuldsvermutung gefährden, die ein wichtiges Prinzip des norwegischen Rechtssystems ist.

Schwerwiegende Mängel im Krebsregister
Im Rahmen eines Treffens von Vertretern des Krebsregisters und der norwegischen Datenschutzbehörde wurde festgestellt, dass das Krebsregister selbst an der Rechtsgrundlage für die Erfassung von Informationen gesunder Frauen, die an einem Mammographieprogramm teilgenommen haben, zweifelte.

Die Datenschutzbehörde untersuchte die Sache und stellte fest, dass das Krebsregister seit 2002 Informationen zu etwa 600.000 Frauen ohne deren Einverständnis gemäß den rechtlichen Anforderungen für Krebsregister verarbeitet hatte.

Vorschlag zur Einrichtung eines nationalen Registers für Herz- und Gefäßkrankheiten
Das Gesundheitsministerium schlug die Einrichtung eines nationalen Registers für Herz- und Gefäßkrankheiten vor. Das Register soll direkt identifizierbare und verpflichtende Informationen enthalten. Das bedeutet, dass das Register direkt identifizierbare Informationen enthalten wird, die nicht auf der Grundlage des Einverständnisses der betroffenen Patienten erfasst wurden. Überdies besteht nicht die Möglichkeit, Widerspruch gegen die Erfassung einzulegen.

Das besagte Register ist nur eine von zahlreichen zentralen Datenbanken und soll ein „Muster" für ähnliche Register anderer Krankheitsgruppen sein. Aus diesem Grund betont die Datenschutzbehörde die Wichtigkeit einer sorgfältigen Erwägung der Rechtsgrundlage für die Einrichtung solcher Register. Die Datenschutzbehörde betont, dass die wesentliche Rechtsgrundlage für eine Erfassung von Daten das Einverständnis der betroffenen Person sein sollte, insbesondere wenn die im Register gespeicherten Daten direkt identifizierbar sind. Daten, die ohne ein solches Einverständnis erfasst wurden, müssen daher anonymisiert oder anderweitig besonders geschützt werden.

Vorschläge für neue Ausnahmeregelungen zur Schweigepflicht von medizinischem Personal
Das Gesundheitsministerium hat im Berichtsjahr eine neue Bestimmung für das Gesetz über medizinisches Personal (Art. 29 b.) vorgeschlagen, um eine Ausnahmeregelung von der ärztlichen Schweigepflicht zum Zweck der Qualitätssicherung, Verwaltung, Planung oder dem Management von medizinischen Versorgungsleistungen zu erwirken.

Die Datenschutzbehörde macht sich Sorgen um die ständig neu eingeführten Ausnahmeregelungen betreffend die Schweigepflicht von medizinischem Personal. Der Vorschlag des Ministeriums beinhaltet ein sehr umfassendes Mandat, das die Schweigepflicht von medizinischem Personal erheblich untergraben könnte. Dies bedeutet, dass Patienten Gefahr laufen, die Kontrolle über ihre gesundheitsbezogenen Informationen zu verlieren.

Prüfung – elektronische Fahrkartensysteme
Im Frühjahr 2009 führte die Datenschutzbehörde drei Prüfungen bei öffentlichen Verkehrsunternehmen durch. Zentrales Thema der Prüfungen war die Verarbeitung personenbezogener Daten im Rahmen elektronischer Fahrkartensysteme, d. h. durch elektronische Fahrausweise.

Es ist wichtig, dass die Öffentlichkeit auch in Zukunft ihre Reisefreiheit in der Gesellschaft nutzen kann, ohne dabei elektronische Spuren zu hinterlassen, über die die Reiseroute sowie das Datum der Reise nachvollziehbar sind. Die Bewertung durch die Datenschutzbehörde ist eine Grundvoraussetzung für die Gewährleistung der Freizügigkeit sowie für den Schutz der Privatsphäre.

Es ist wichtig, dass Reisende öffentliche Verkehrsmittel nutzen können, ohne dass hierbei Informationen zu ihren Bewegungen erfasst werden. Im Fall persönlicher elektronischer Fahrkarten wurde im Wesentlichen festgestellt, dass das Verkehrsunternehmen mehr Informationen erfasste und speicherte als eigentlich erforderlich war. Die Datenschutzbehörde hat die Unternehmen aufgefordert, Informationen, über die Reiseroute und Reisezeit identifiziert werden können, unverzüglich bzw. binnen kurzer Zeit nach der Zahlung der Reise zu löschen.

Kapitel 5

MITGLIEDER UND BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE IM JAHR 2009

Österreich	**Belgien**
Frau Waltraut Kotschy Österreichische Datenschutzkommission Ballhausplatz 1 - AT - 1014 Wien Tel: +43 1 531 15 / 2525 Fax: +43 1 531 15 / 2690 E-mail: dsk@dsk.gv.at Website: http://www.dsk.gv.at/	Herr Willem Debeuckelaere Kommission des Schutzes des Privatlebens (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute, 139 - BE - 1000 Bruxelles Tel: +32(0)2/213.85.40 Fax : +32(0)2/213.85.65 E-mail: commission@privacycommission.be Website: http://www.privacycommission.be/
Bulgarien	**Zypern**
Herr Krassimir Dimitrov Kommission für Schutz persönlicher Daten (Комисия за защита на личните данни) 1 Dondukov - BG - 1000 Sofia Tel: +359 2 915 3501 Fax: +359 2 915 3525E- mail: kzld@government.bg kzld@cpdp.bg Website: http://www.cdpd.bg	Frau Goulla Frangou Kommissionsmitgliedes für Schutz persönlicher Daten (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2nd floor - CY - 1082 Nicosia (P.O. Box 23378 - CY - 1682 Nicosia) Tel: +357 22 818 456 Fax: +357 22 304 565 E-mail: commissioner@dataprotection.gov.cy Website: http://www.dataprotection.gov.cy
Tschechische Republik	**Dänemark**
Herr Igor Nemec Büro für Schutz persönlicher Daten (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Praha 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-mail: posta@uoou.cz Website: http://www.uoou.cz/	Frau Janni Christoffersen Datenschutzagentur (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk

Estland	**Finnland**
Herr Viljar Peep Estnisches Datenschutzinspektorat (Andmekaitse Inspektsioon) Väike - Ameerika 19 - EE - 10129 Tallinn Tel: +372 6274 135 Fax: +372 6274 137 E-mail: info@dp.gov.ee Website: http://www.dp.gov.ee	Herr Reijo Aarnio Büro des Datenschutzombudsmannes (Tietosuojavaltuutetun toimisto) Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki (P.O. Box 315) Tel: +358 10 36 166700 Fax: +358 10 36 166735 E-mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
Frankreich	**Deutschland**
Herr Alex Türk Vorsitzender Nationale Kommission der Informatik und der Freiheiten (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 Herr Georges de La Loyère Nationale Kommission der Informatik und der Freiheiten (Commission Nationale de l'Informatique et des Libertés - CNIL) Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02 Tel: +33 1 53 73 22 22 Fax: +33 1 53 73 22 00 E-mail: laloyere@cnil.fr Website: http://www.cnil.fr	Herr Peter Schaar Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Husarenstraße 30 - DE -53117 Bonn Tel: +49 (0)1888 7799-0 Fax: +49 (0)1888 7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.bfdi.bund.de Herr Alexander Dix (Vertreter der Bundesländer) Berliner Beauftragter für Datenschutz und Informationsfreiheit An der Urania 4-10 – DE – 10787 Berlin Tel: +49 30 13 889 0 Fax: +49 30 215 50 50 E-mail: mailbox@datenschutz-berlin.de Website: http://www.datenschutz-berlin.de
Griechenland	**Ungarn**
Herr Christos Yeraris Hellenische Datenschutzbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Strasse 1-3 GR - 115 23 Athen Tel: +30 210 6475608 Fax: +30 210 6475789 E-mail: christosyeraris@dpa.gr Website: http://www.dpa.gr	Herr András Jóri Datenschutzbeauftragte von Ungarn (Adatvédelmi Biztos) Nador u. 22 - HU - 1051 Budapest Tel: +36 1 475 7186 Fax: +36 1 269 3541 E-mail: adatved@obh.hu Website: http://abiweb.obh.hu/abi/

Irland	**Italien**
Herr Billy Hawkes Kommissionsmitglied des Datenschutzes (An Coimisinéir Cosanta Sonraí) Canal House, Station Rd, Portarlington, IE -Co.Laois Tel: +353 57 868 4800 Fax: +353 57 868 4757 E-mail: info@dataprotection.ie Website: http://www.dataprotection.ie	Herr Francesco Pizzetti Italienische Datenschutzaufsichtsbehörde (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Roma Tel: +39 06.69677.1 Fax: +39 06.69677.785 E-mail: garante@garanteprivacy.it, f.pizzetti@garanteprivacy.it Website: http://www.garanteprivacy.it
Lettland	**Litauen**
Frau Signe Plumina Staats Datenschutz Inspektorat (Datu valsts inspekcija) Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia Tel: +371 6722 31 31 Fax: +371 6722 35 56 E-mail: signe.plumina@dvi.gov.lv, info@dvi.gov.lv Website: http://www.dvi.gov.lv	Herr Algirdas Kunčinas Staatsdatenschutzinspektorat (Valstybinė duomenų apsaugos inspekcija) A.Juozapaviciaus str. 6 / Slucko str. 2, LT-01102 Vilnius Tel: +370 5 279 14 45 Fax: + 370 5 261 94 94 E-mail: ada@ada.lt Website: http://www.ada.lt
Luxemburg	**Malta**
Herr Gérard Lommel Nationale Kommission für den Datenschutz (Commission nationale pour la Protection des Données - CNPD) 41, avenue de la Gare - L - 1611 Luxembourg Tel: +352 26 10 60 -1 Fax: +352 26 10 60 – 29 E-mail: info@cnpd.lu Website: http://www.cnpd.lu	Herr Joseph Ebejer Kommissionsmitgliedes des Datenschutzes Büro des Kommissionsmitgliedes des Datenschutzes (Office of the Data Protection Commissioner) 2, Airways House High Street Sliema SLM 1549 MALTA Tel: +356 2328 7100 Fax: +356 23287198 E-mail: joseph.ebejer@gov.mt Website: http://www.dataprotection.gov.mt

Niederlande	**Polen**
Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ Den Haag Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl	Herr Michał Serzycki Generalinspektor für Schutz persönlicher Daten (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 70 86 Fax: +48 22 860 70 90 E-mail: Sekretariat@giodo.gov.pl Website: http://www.giodo.gov.pl
Portugal	**Rumänien**
Herr Luís Novais Lingnau da Silveira Nationale Kommission von Datenschutz (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lisboa Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-mail: geral@cnpd.pt Website: http://www.cnpd.pt	Frau Georgeta Basarabescu Nationale Aufsichtsbehörde für persönliche Datenverarbeitung (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Olari Street no. 32, Sector 2, RO - Bucharest Tel: +40 21 252 5599 Fax: +40 21 252 5757 E-mail: georgeta.basarabescu@dataprotection.ro international@dataprotection.ro Website: www.dataprotection.ro
Slowakei	**Slowenien**
Herr Gyula Veszelei Büro für den persönlichen Datenschutz der Slowakische Republik (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441 E-mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	Frau Natasa Pirc Musar Kommissionsmitglied der Informationen (Informacijski pooblaščenec) Vosnjakova 1, SI - 1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78 E-mail: gp.ip@ip-rs.si Website: http://www.ip-rs.si

Spanien	**Schweden**
Herr Artemi Rallo Lombarte Spanische Agentur des Datenschutzes (Agencia Española de Protección de Datos) C/ Jorge Juan, 6 ES - 28001 Madrid Tel: +34 91 399 6219/20 Fax: + +34 91 445 56 99 E-mail: director@agpd.es Website: http://www.agpd.es	Herr Göran Gräslund Dateninspektionsbehörde (Datainspektionen) Fleminggatan, 14 (Box 8114) - SE - 104 20 Stockholm Tel: +46 8 657 61 57 Fax: +46 8 652 86 52 E-mail: datainspektionen@datainspektionen.se, goran.graslund@datainspektionen.se Website: http://www.datainspektionen.se
Vereinigtes Königreich	**European Data Protection Supervisor**
Herr Christopher Graham Büro des Kommissionsmitgliedes der Informationen (Information Commissioner's Office) Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-mail: Fuellen Sie bitte das Online-Kontaktformular auf unserer Website aus Website: http://www.ico.gov.uk	Herr Peter Hustinx Europäischer Datenschutzbeauftragter (EDPS) (European Data Protection Supervisor – EDPS) Postal address: 60, rue Wiertz, BE - 1047 Brussels Office: rue Montoyer, 63, BE - 1047 Brussels Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE IM JAHR 2009

Island	**Norwegen**
Frau Sigrun Johannesdottir Datenschutzbehörde (Persónuvernd) Raudararstigur 10 - IS - 105 Reykjavik Tel: +354 510 9600 Fax: +354 510 9606 E-mail: postur@personuvernd.is Website: http://www.personuvernd.is	Herr Georg Apenes Dateninspektorat (Datatilsynet) P.O.Box 8177 Dep - NO - 0034 Oslo Tel: +47 22 396900 Fax: +47 22 422350 E-mail: postkasse@datatilsynet.no Website: http://www.datatilsynet.no
Liechtenstein	**Republik Kroatien**
Herr Philipp Mittelberger Datenschutzbeauftragter Datenschutzstelle (DSS) Kirchstrasse 8, Postfach 684 –FL -9490 Vaduz Tel: +423 236 6090 Fax: +423 236 6099 E-mail: info@dss.llv.li Website: http://www.dss.llv.li	Herr Franjo LACKO Direktor Kroatische Datenschutzaufsichtsbehörde (Agencija za zaštitu osobnih podataka - AZOP) Republike Austrije 25, 10000 Zagreb Tel. +385 1 4609 000 Fax +385 1 4609 099 E-mail: azop@azop.hr or info@azop.hr website: http://www.azop.hr/default.asp
die ehemalige jugoslawische Republik Mazedonien	
Frau Marijana Marusic Datenschutzdirektion (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3244 760 Fax: +389 2 3244 766 E-mail: info@dzlp.gov.mk Website: www.dzlp.mk,	

Sekretariat der Artikel-29-Datenschutzgruppe

Frau Marie-Hélène Boulanger
Geschäftsführende Referatsleiterin
Referat Datenschutz
Generaldirektion Justiz, Freiheit und Sicherheit
Europäische Kommission
Büro: LX46 1/02 - BE - 1049 Brussels
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E-mail: Marie-Helene.Boulanger@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

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 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 den Gemeinschaft Empfehlungen zu Angelegenheiten auszusprechen, die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft betreffen.

DS-AA-11-001-DE-C doi:10.2838/3722

ISBN 978-92-79-19983-7