Europäische Kommission

14. Bericht der Artikel-29 Datenschutzgruppe

Justiz

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 MO59 02/013.
Website: http://ec.europa.eu/justice/data-protection/

Europe Direct soll Ihnen helfen, Antworten auf Ihre Fragen zur Europäischen Union zu finden.
Gebührenfreie Telefonnummer (*):
00 800 6 7 8 9 10 11

(*) Einige Mobilfunkanbieter gewähren keinen Zugang zu 00 800-Nummern oder berechnen möglicherweise eine Gebühr.

Europäische Kommission – Generaldirektion Justiz
Mehr Informationen über die Europäische Union sind verfügbar über das Internet (http://europa.eu).

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2013

ISSN: 1830-6462
ISBN 978-92-79-29768-7
doi: 10.2838/28425

14. Bericht der Artikel-29-Datenschutzgruppe

Berichtsjahr 2011

Angenommen am 8. Dezember 2011

Table of Contents

VORWORT DES VORSITZENDEN DER ARTIKEL-29-DATENSCHUTZGRUPPE

Die technologischen Entwicklungen der letzten Jahrzehnte gingen mit zahlreichen Vorteilen für die Verbraucher einher und brachten eine ganze neue Online-Kultur und -Terminologie hervor, wie E-Mail, Apps und Twitter, die die Verbraucher übernommen haben und im Alltag verwenden. Diese technologischen Entwicklungen und die enorme quantitative Zunahme webbasierter Dienstleistungen haben dazu geführt, dass die Menge personenbezogener Daten, die gesammelt und verarbeitet werden, unermesslich gestiegen ist. Angesichts der zur gleichen Zeit zunehmenden Globalisierung erfordern diese Entwicklungen eine Aktualisierung der Datenschutzvorschriften.

Im Jahr 2010 konzentrierte die Datenschutzgruppe ihre Arbeit weiterhin auf die Überprüfung des Rechtsrahmens in der Europäischen Union und verabschiedeten spezielle Stellungnahmen diesbezüglich, z. B. zum Konzept der Rechenschaftspflicht oder zum komplexen Thema des anwendbaren Rechts (als Weiterverfolgung des im Dezember 2009 angenommenen Gemeinsamen Beitrags zur Konsultation der Europäischen Kommission (Bericht zur Zukunft des Datenschutzes) der Artikel-29-Datenschutzgruppe und der Arbeitsgruppe Polizei und Justiz).

Die Datenschutzgruppe war sehr erfreut festzustellen, dass viele ihrer Vorschläge weitgehend in die Mitteilung der Europäischen Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union" von November 2010 eingeflossen sind. Darüber hinaus wurde die Datenschutzgruppe von der Kommission gebeten, sie 2011 weiterhin zu Themen wie Zusammenarbeit zwischen Datenschutzbehörden, Meldung, sensible Daten und Einwilligung zu beraten.

Nicht nur in der Europäischen Union, sondern auch im Europarat, der OECD und in den Vereinigten Staaten werden die Datenschutzbestimmungen und Vorschriften über den Schutz der Privatsphäre derzeit einer Prüfung unterzogen. 2010 veröffentlichte die US-Handelsaufsicht (Federal Trade Commission) den vorläufigen Bericht „Protecting Consumer Privacy in an Era of Rapid Change", und das US-Handelsministerium (United States Department of Commerce) veröffentlichte Ende des Jahres das Grünbuch „Commercial Data Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework". Damit bietet sich die Möglichkeit, die Beziehungen zwischen der Europäischen Union und den Vereinigten Staaten zu stärken, um rund um den Globus ein hohes Maß an Datenschutz zu gewährleisten.

Denn das Wichtigste sind letztendlich die Auswirkungen der neuen Datenschutzvorschriften auf die Bürgerinnen und Bürger, d. h. auf die Datensubjekte.

Wie, von wem und aus welchen Gründen Daten gesammelt und verarbeitet werden, muss noch transparenter werden. Es mag politisch wünschenswert erscheinen hervorzuheben, wie wichtig Transparenz ist; allerdings kann sie sich auch als kontraproduktiv erweisen. Studien zufolge kann eine einzelne Person je nach ihren sozialen und beruflichen Aktivitäten heutzutage in 250 bis 1 000 unterschiedlichen Datenbanken registriert sein. Man kann von den Datensubjekten kaum erwarten, dass sie verfolgen, wie und wo ihre Daten gesammelt und verarbeitet werden, ganz zu schweigen davon, dass sie ihre Rechte auf Zugang, Berichtigung und Löschung ihrer personenbezogenen Daten wahrnehmen.

Ein Eckstein des Rahmens für den Schutz personenbezogener Daten ist nach wie vor die Frage der Einwilligung; Es ist jedoch nicht immer angebracht, sich zu sehr auf die Einwilligung als Grundlage für die Verarbeitung zu verlassen, da die Bedingungen für die Erlangung einer Einwilligung nach Aufklärung in der Praxis nicht immer erfüllt werden können. Die Datenverarbeitungsvorgänge in der heutigen (Online-) Welt sind komplex, und der Einzelne ist mit vielzähligen Entscheidungen konfrontiert. Wenn in den Datenschutzbestimmungen eines Unternehmens steht, dass „Informationen auch an andere, sorgfältig ausgewählte Dritte weitergeleitet werden", wird die betroffene Person vollkommen im Dunkeln gelassen, worin sie überhaupt einwilligt.

Man könnte also argumentieren, dass das Grundrecht auf Datenschutz nicht ausreichend gewährleistet werden kann, wenn das Augenmerk zu stark darauf gerichtet ist, dass der Einzelne die für die Ausübung seiner Rechte erforderlichen Maßnahmen selbst ergreift. Die Verantwortung der für die Datenverarbeitung Verantwortlichen, eine tatsächliche Einhaltung der Vorschriften zu gewährleisten, muss deshalb verstärkt werden.

Es wird immer notwendiger und wichtiger, dafür zu sorgen, dass die für die Datenverarbeitung Verantwortlichen wirksame Maßnahmen ergreifen können, um tatsächlichen Datenschutz zu bieten. Es wird für die für die Datenverarbeitung Verantwortlichen immer entscheidender, ihren guten Ruf aufrechtzuerhalten, das Vertrauen der Bürger/-innen und Verbraucher/-innen zu gewährleisten und die rechtlichen und ökonomischen Risiken auf ein Minimum zu beschränken. Die Ernennung von Datenschutzbeauftragten und Durchführung von

Datenschutzfolgenabschätzungen, die die Elemente des sogenannten Grundsatzes der Rechenschaftspflicht darstellen, können einen Beitrag hierzu leisten.

Diesem Grundsatz folgend wären die für die Datenverarbeitung Verantwortlichen gehalten, die Maßnahmen in die Wege zu leiten, die erforderlich sind, um die Umsetzung der wesentlichen gesetzlichen Grundsätze und Verpflichtungen bei der Verarbeitung personenbezogener Daten zu gewährleisten. Zudem müssten sie dies auf Nachfrage nachweisen. Darüber hinaus sollten auch Entwickler neuer Produkte und Dienstleistungen verpflichtet werden, gleich zu Beginn der Entwicklungsphase über den Schutz und die Sicherung personenbezogener Daten im Sinne eines optimalen Schutzes der Privatsphäre nachzudenken.

Letztendlich kann ein intaktes Datenschutzsystem nur funktionieren, wenn Kontrollen durchgeführt werden und es effektive und solide Durchsetzungsmechanismen gibt. Aus diesem Grund müssen die nationalen Datenschutzbehörden mit ausreichend verstärkten Kompetenzen ausgestattet werden, um ihre Aufgaben angemessen und vollkommen unabhängig erfüllen zu können. Mit anderen Worten, es sollte den Datenschutzbehörden ermöglicht werden, als echte Durchsetzungsinstanzen zu agieren.

Da Daten in stark zunehmendem Maße grenzüberschreitend verarbeitet werden, wird auch eine einheitliche EU-weite Anwendung des Rechtsrahmens, insbesondere in Fällen einer grenzüberschreitenden Aufsicht und Durchsetzung, immer dringlicher. Der Artikel-29-Datenschutzgruppe sollte in diesen Bereichen eine stärkere Rolle zukommen, und die Datenschutzgruppe selbst sollte unabhängiger werden.

Schließlich, um die Balance zwischen den drei Hauptakteuren im europäischen Datenschutzbereich wiederherzustellen, sollten Datensubjekte besser informiert, aber weniger belastet werden, die für die Datenverarbeitung Verantwortlichen sich ihrer Verantwortung stellen und ihrer Rechenschaftspflicht umfassender nachkommen, und die Datenschutzbehörden mehr Kompetenzen haben, um sicherzustellen, dass das Gesetz eingehalten wird, und die Möglichkeit bekommen, über die Landesgrenzen hinweg besser kooperieren zu können.

Jacob Kohnstamm

Kapitel Eins
Fragen, zu denen die Artikel-29-Datenschutzgruppe Stellung genommen hat[1]

[1] Alle von der Artikel-29-Datenschutzgruppe verabschiedeten Dokumente sind auf folgender Website zu finden: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

1. Fragen, zu denen die Artikel-29-Datenschutzgruppe Stellung genommen hat[2]

1.1 DATENÜBERMITTLUNG IN DRITTLÄNDER

1.1.1 Passagierdaten/PNR

Stellungnahme 7/2010 (WP 178) zur Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer

Am 21. September 2010 hat die Kommission ihre Mitteilung über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer vorgelegt. Die Kommission ist der Ansicht, dass die Verwendung von PNR-Daten zu Strafverfolgungszwecken zunimmt und immer häufiger als übliches, notwendiges Mittel für die Vereinfachung der Strafverfolgungsarbeit betrachtet wird.

Daher hat die Kommission beschlossen, eine Reihe allgemeiner Kriterien festzulegen, die die Grundlage für künftige Verhandlungen über PNR-Abkommen mit Drittländern bilden sollen. Die Mitteilung enthält zudem eine Analyse der gegenwärtigen Verwendung von Fluggastdaten sowie eine Liste der Drittländer, mit denen die Kommission in den kommenden Jahren Abkommen zu schließen plant.

Da immer mehr Länder Fluggastdaten anfordern, dürfte sich die Zahl der einschlägigen Abkommen weiter erhöhen. Die Kommission hat daher beschlossen, dass es wünschenswert wäre, einen für alle künftigen PNR-Abkommen maßgeblichen Rahmen festzulegen, um sowohl auf Seiten der Fluggesellschaften als auch bei den Mitgliedstaaten Rechtsunsicherheiten zu vermeiden und unnötigen administrativen Belastungen vorzubeugen, die durch die Notwendigkeit, den unterschiedlichen Vorschriften verschiedener Drittstaaten nachzukommen, entstehen könnten. Die Artikel-29-Datenschutzgruppe begrüßt das sektorübergreifende Konzept der Kommission für die Bearbeitung von Anfragen auf EU-Ebene und für die Sicherstellung hoher Datenschutzstandards unter vollständiger Wahrung der Grundrechte.

Die Datenschutzgruppe weist darauf hin, dass die Frage des Austauschs von Fluggastdaten nicht isoliert betrachtet werden sollte. Das sektorübergreifende Konzept sollte daher auf sämtliche von Drittländern gestellten Anfragen nach Fluggastdaten einschließlich API-Daten, Watchlist-Abgleich und sonstigen Maßnahmen der Vorabkontrolle ausgeweitet werden. Dies heißt, dass die Kommission bei Erhalt einer Anfrage nach Fluggastdaten auch entscheiden sollte, ob bestimmte und auch welche Daten (z. B. API-Daten) ausreichend wären, und ein entsprechendes Abkommen schließen sollte.

Was die Fluggastdaten anbelangt, hat die Datenschutzgruppe die Verhandlungen, die zum Abschluss der PNR-Abkommen mit den Vereinigten Staaten, Kanada und Australien geführt haben, genau verfolgt und diesbezüglich mehrere Stellungnahmen abgegeben, in denen auf verschiedene Datenschutzbelange im Zusammenhang mit den jeweiligen PNR-Systemen hingewiesen wurde. Bisher wurden zahlreiche Einwände der Datenschutzgruppe nicht behandelt. Die gegenwärtige Mitteilung der Kommission ist gleichwohl ein Schritt in die richtige Richtung – auch wenn einige Bedenken bleiben.

FAZIT

Die Datenschutzgruppe stellt mit Zufriedenheit fest, dass die Europäische Kommission klar die Notwendigkeit erkannt hat, dass es dem Thema Datenschutz in künftigen PNR-Abkommen größere Aufmerksamkeit zu schenken gilt, und dass sie rechtsverbindliche Abkommen zu schließen gedenkt, um Rechtssicherheit zu schaffen und Gleichbehandlung sicherzustellen. Die Mitteilung vom 21. September 2010 ist ein Schritt in die richtige Richtung. Der Nutzen eines groß angelegten Profiling anhand von Fluggastdaten muss jedoch auf der Grundlage der vorliegenden wissenschaftlichen Erkenntnisse und der jüngsten Studien gründlich hinterfragt werden

Die Datenschutzgruppe betont erneut, dass es eines sektorübergreifenden Konzepts für sämtliche Passagierdaten bedarf, nicht nur für Fluggastdatensätze. Angesichts der aktuellen Entwicklungen wie der Überprüfung des geltenden

[2] Alle von der Artikel-29-Datenschutzgruppe verabschiedeten Dokumente sind auf folgender Website zu finden: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm#h2-2

Rechtsrahmens der EU für den Datenschutz und der angestrebten Verhandlungen mit den Vereinigten Staaten über ein allgemeines Datenschutzabkommen ist Kohärenz gefragt.

Die Datenschutzgruppe weist darauf hin, dass die in der Mitteilung der Kommission genannten allgemeinen Standards und Kriterien als das Mindestmaß des durch künftige PNR-Abkommen zu gewährleistenden Datenschutzes betrachtet werden sollten. Diese Standards könnten und müssten gleichwohl noch in mehreren Punkten weiterentwickelt werden.

Die Datenschutzgruppe ersucht die Kommission, das Europäische Parlament und den Rat daher dringend, diese Stellungnahme bei der Erörterung von Verhandlungsmandaten und Entwürfen für künftige PNR-Abkommen zu berücksichtigen und die Datenschutzgruppe über die weiteren Entwicklungen auf dem Laufenden zu halten Selbstverständlich steht die Datenschutzgruppe allen EU-Organen erforderlichenfalls zur Verfügung, um ihren Standpunkt zu präzisieren oder näher auszuführen.

Abschließend möchte die Datenschutzgruppe erneut ihren Wunsch zum Ausdruck bringen, bezüglich der Datenschutzaspekte künftiger Abkommen zu Rate gezogen zu werden, zumal sie das offizielle Datenschutz-Beratungsgremium der EU ist und es sich bei ihren Mitgliedern um Vertreter der nationalen Aufsichtsbehörden handelt, die für die Fluggesellschaften, für die die künftigen Abkommen ja maßgeblich sein werden, zuständig sind. Zudem möchte sie regelmäßig über den aktuellen Stand der Verhandlungen über diese Abkommen informiert werden.

1.1.2. Angemessenheit

Stellungnahme 6/2010 (WP 177) zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Republik Östlich des Uruguay

Am 20. Oktober 2008 übermittelte die Vertretung der Republik Östlich des Uruguay (im Folgenden „Uruguay“) bei der Europäischen Union der Europäischen Kommission ein Schreiben mit dem amtlichen Ersuchen der Regierung Uruguays um Einleitung des Verfahrens zur Klärung der Frage, ob Uruguay ein angemessenes Schutzniveau bezüglich der Übermittlung personenbezogener Daten aus der EU/dem EWR gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG zum Schutz personenbezogener Daten (im Folgenden „die Richtlinie“) aufweist.

Zur Prüfung der Frage, ob Uruguay ein angemessenes Schutzniveau bietet, forderte die Kommission einen Bericht des *Centre de Recherches Informatique et Droit* (CRID) der Universität Namur an. In diesem ausführlichen Bericht wird untersucht, inwieweit das Rechtssystem Uruguays unter dem Aspekt der Beschaffenheit der Gesetzgebung und der Verfügbarkeit von Mechanismen zur Anwendung von Rechtsvorschriften zum Schutz personenbezogener Daten den einschlägigen Anforderungen entspricht. Diese Aspekte waren bereits in der Arbeitsunterlage „Übermittlung von personenbezogenen Daten in Drittländer: Anwendung von Artikel 25 und 26 der EU-Datenschutzrichtlinie“ dargelegt worden, die von der gemäß Artikel 29 der Richtlinie eingesetzten Datenschutzgruppe am 24. Juli 1998 (Dokument WP12) angenommen worden war. Für die uruguayischen Behörden äußerte sich das Kontrollorgan für die Regulierung und Kontrolle personenbezogener Daten (URCDP) mit Zustimmung seines Exekutivrats am 11. Februar 2010 zu den in diesem Bericht aufgeworfenen Fragen.

Der Bericht wurde zusammen mit den Anmerkungen der uruguayischen Behörden von einer eigens hierfür gebildeten Untergruppe der Artikel-29-Datenschutzgruppe geprüft, auf deren Ersuchen hin der Vorsitzende der Datenschutzgruppe die uruguayischen Behörden auf die Aspekte hinwies, die weiterer Klarstellungen bedürfen.

Die uruguayischen Behörden übermittelten der Artikel-29-Datenschutzgruppe einen ausführlichen Bericht des Kontrollorgans URCDP, dem der Exekutivrat des Kontrollorgans am 23. Juni 2010 zugestimmt hatte und der die Antworten auf die in dem Schreiben aufgeworfenen Fragen enthält. Außerdem legten sie verschiedene Unterlagen zum Stand des Datenschutzes in Uruguay vor, einschließlich des Jahresberichts dieses Gremiums für 2009 und des Tätigkeitsberichts für die Zeit bis zum 31. Mai 2010, verschiedener vom Exekutivrat getroffener Entscheidungen sowie maßgeblicher rechtlicher Entscheidungen zum Thema Datenschutz.

Der Bericht wurde den Mitgliedern der Untergruppe im September 2010 erneut vorgelegt, die ihn unter besonderer Berücksichtigung der im Schreiben des Vorsitzenden der Datenschutzgruppe an die uruguayischen Behörden angesprochenen Fragen prüften. Nach Prüfung der zusätzlichen Informationen legte die Untergruppe der Datenschutzgruppe nun den Entwurf ihrer Stellungnahme vor.

Am 12. Oktober 2010 präsentierte die Datenschutzgruppe ihre Stellungnahme, dass die Republik Östlich des Uruguay hinsichtlich des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des

freien Datenverkehrs ein im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 angemessenes Schutzniveau gewährleistet.

Die Datenschutzgruppe weist ferner mit Nachdruck darauf hin, dass sie nach dem Beschluss der Kommission die Entwicklung des Datenschutzes in Uruguay und die Anwendung der in Dokument WP12 und in ihrer Stellungnahme genannten Grundsätze durch die Datenschutzbehörde (URCDP) genau mitverfolgen wird.

1.1.3. Standardvertragsklauseln

Häufig gestellte Fragen (WP 176) zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten des Beschlusses 2010/87/EU der Kommission vom 5. Februar 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG

Am 5. Februar 2010 erließ die Europäische Kommission einen Beschluss mit geänderten Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern, die kein angemessenes Datenschutzniveau gewährleisten (Klauseln für die Verträge zwischen für die Datenverarbeitung Verantwortlichen und Auftragsverarbeitern).

Der neue Beschluss 2010/87/EU regelt die Übermittlung von Daten zwischen im EWR ansässigen für die Datenverarbeitung Verantwortlichen und Auftragsverarbeitern, die außerhalb des EWR niedergelassen sind, und legt die Bedingungen für die Vergabe eines Unterauftrags für die Verarbeitung durch einen außerhalb des EWR niedergelassenen Auftragsverarbeiter an einen ebenfalls außerhalb des EWR niedergelassenen Unterauftragsverarbeiter fest.

Am 12. Juli 2012 verabschiedete die Datenschutzgruppe ein Dokument mit häufig gestellten Fragen zu bestimmten Aspekten im Zusammenhang mit dem Inkrafttreten dieser neuen ab dem 15. Mai geltenden Standardvertragsklauseln. Dieses Dokument gibt den harmonisierten Standpunkt der europäischen Kontrollstellen wieder.

Die Liste der häufig gestellten Fragen ist nicht abschließend und kann bei Bedarf aktualisiert werden.

1.2. Elektronische Kommunikation, Internet und neue Technologien

Stellungnahme 2/2010 (WP 171) zur Werbung auf Basis von Behavioural Targeting

Verhaltensorientierte Werbung bedeutet, das Surfverhalten von Nutzern im Internet zu verfolgen und im Laufe der Zeit Profile anzulegen, die später dazu dienen, ihnen ihren Interessenschwerpunkten entsprechende Werbungen anzubieten. Die Stellungnahme präzisiert den juristischen Rahmen, der auf die verhaltensorientierte Werbung Anwendung findet.

Die Datenschutzgruppe hebt insbesondere hervor, dass die Anbieter von Werbenetzwerken Artikel 5, Abs. 3 der Datenschutzrichtlinie für elektronische Kommunikation unterliegen, demzufolge die Platzierung von Cookies oder ähnlichen Instrumenten auf dem Endgerät des Nutzers oder der Zugriff auf Informationen mithilfe dieser Instrumente nur mit dem Einverständnis des Nutzers gestattet ist.

Von den Anbietern von Werbenetzwerken wird also gefordert, im Vorfeld sog. „Opt-in"-Mechanismen einzurichten, die eine positive Handlung der betroffenen Personen erfordern, mit der ihr Einverständnis signalisiert wird, dass Cookies oder ähnliche Instrumente auf ihren Geräten gespeichert werden und dass ihr Surfverhalten für den Versand personenbezogener Werbungen verfolgt wird.

Die Datenschutzgruppe ist der Auffassung, dass eine einmalige Zustimmung der Nutzer zum Speichern eines Cookies auch die künftige Verwendung dieses Cookies umfasst, und somit auch die Verfolgung ihres Surfverhaltens im Internet.

Da die verhaltensorientierte Werbung auf der Verwendung von Benutzeridentifizierungen basiert, die das Anlegen äußerst detaillierter Nutzerprofile ermöglicht, die in der Mehrzahl der Fälle als personenbezogene Daten gelten, greift ebenfalls die Richtlinie 95/46/EG. Die Datenschutzgruppe legt dar, wie die Anbieter von Online-Werbenetzwerken die durch diese Richtlinie festgelegten Pflichten zu befolgen haben, insbesondere in Bezug auf die Rechte auf Auskunft, Berichtigung, Löschung, Aufbewahrung etc.

Die Stellungnahme analysiert und präzisiert die durch den anzuwendenden Rechtsrahmen festgelegten Pflichten. Allerdings schreibt sie nicht vor, auf welche Weise diese Pflichten technologisch umzusetzen sind. In verschiedenen Bereichen jedoch fordert die Datenschutzgruppe die betreffenden Fachleute zu einem Dialog mit ihr auf, um technische Lösungen und andere Instrumente vorzuschlagen, damit sie sich so schnell wie möglich dem in der Stellungnahme festgelegten Rahmen fügen können.

1.3. Durchsetzung

Bericht 1/2010 (WP 172) über die zweite gemeinsame Durchsetzungsmaßnahme: Erfüllung der nach den innerstaatlichen Rechtsvorschriften über die Vorratsspeicherung von Verkehrsdaten aufgrund der Artikel 6 und 9 der Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation) und der Richtlinie 2006/24/EG (über die Vorratsspeicherung von Daten und zur Änderung der Datenschutzrichtlinie für elektronische Kommunikation) bestehenden Pflichten durch die Telekommunikations-Dienstanbieter und die Internet-Dienstanbieter auf nationaler Ebene

Diese Maßnahme zur Kontrolle der Anwendung der EU-Gesetzgebung durch die Artikel-29-Datenschutzgruppe wurde mit dem Ziel beschlossen, unter Berücksichtigung der von der Datenschutzgruppe in ihren vorherigen Stellungnahmen zu dieser Frage geäußerten Empfehlungen und Bedenken die Einhaltung der durch die Richtlinie 2006/24/EG eingeführten Bestimmungen zu überwachen.

Die Umsetzung der Richtlinie zur Vorratsspeicherung von Daten durch Anbieter elektronischer Kommunikationsdienste und von Internetdiensten ist naturgemäß mit einem erhöhten Risiko verbunden, weshalb geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen sind.

Die Maßnahme basiert auf einem Fragebogen und auf Vor-Ort-Kontrollen, denen die Hauptanbieter und nationalen Internetanbieter unterzogen wurden, um einen Großteil des Marktes zu erfassen, und ergibt ein äußerst uneinheitliches Bild der Durchführungsmaßnahmen, insbesondere in Bezug auf die eingerichteten Sicherheitsvorkehrungen.

Die Artikel-29-Datenschutzgruppe stellt beunruhigt fest, dass die Richtlinie auf nationaler Ebene anscheinend nicht einheitlich umgesetzt wurde. Insbesondere scheint sie von den Mitgliedstaaten so interpretiert worden zu sein, als unterlägen die Grenzen ihres Anwendungsbereichs deren Einschätzung. Ist es nun Ziel der Richtlinie, eine Abweichung von der allgemeinen Verpflichtung zur Löschung von Verkehrsdaten zu erlauben, sobald sie nicht mehr für die Übermittlung einer Mitteilung erforderlich sind, oder aber die Speicherung sämtlicher Daten, die die Anbieter bereits im Rahmen von Artikel 6, Abs. 2 der Richtlinie 2002/58 speichern dürfen, verpflichtend zu gestalten? Die Artikel-29-Datenschutzgruppe unterstützt diese zweite Interpretation, die auch im jüngsten Urteil des EuGH in der Rechtssache *Irland gegen Kommission* (C301/06) zum Ausdruck kommt.

Die Datenschutzgruppe hat folgende Empfehlungen erarbeitet:

Kategorien der auf Vorrat zu speichernden Daten: Die Liste der Verkehrsdaten, die auf Vorrat gespeichert werden müssen, ist als vollständig zu erachten. Folglich kann den Anbietern aufgrund der Richtlinie über die Vorratsdatenspeicherung keine zusätzliche Datenspeicherungspflicht auferlegt werden.

Aufbewahrungsfristen: Um eine größere Harmonisierung zu erreichen, ist es sinnvoll, die Höchstdauer der Datenvorratsspeicherung zu reduzieren und eine einheitliche kürzere Frist festzulegen, die auf alle Anbieter in der EU Anwendung findet, wie dies die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme WP113 vorgeschlagen hat. In einem größeren Zusammenhang geht es darum, dass die allgemeine Sicherheit der Verkehrsdaten „an sich“ von der Kommission neu beurteilt wird.

Technische und organisatorische Sicherheitsmaßnahmen: Es wurden zusätzliche spezifische Maßnahmen (wie die Einrichtung eines stabilen Authentifizierungssystems und die Erstellung eines detaillierten Zugriffsprotokolls) ausführlich beschrieben, und ein Normvorschlag für den Datentransfer an Strafverfolgungsbehörden wurde erarbeitet, um schnellere und zuverlässigere Übertragungen zu ermöglichen, die auch die Voraussetzung für die Erhebung statistischer Informationen und einen verantwortlichen Datenzugriff bieten. In diesem Zusammenhang scheint es, als müsse der Begriff der „schweren Straftat“ auf der Ebene der Mitgliedstaaten geklärt werden, und die Liste der Rechtsträger, die zum Zugriff auf die Daten berechtigt sind, sollte allen betreffenden Parteien übermittelt werden.

1.4. RFID

Stellungnahme 5/2010 (WP 175) zum Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen

Die Datenschutzgruppe analysiert den Vorschlag der Industrie bezüglich der Kommissionsempfehlung zu den Datenschutz-Folgeabschätzungen von RFID-Lösungen.

Die Datenschutzgruppe äußert Vorbehalte zu einem Teil des Vorschlags:

Klassifizierung der Anwendungen. Einige Anwendungen, bei denen die Industrie behauptet, es finde keine Verarbeitung personenbezogener Daten statt, sind falsch klassifiziert und verarbeiten personenbezogene Daten auf der Basis der im RFID-Tag enthaltenen Benutzeridentifikation. Für diese Anwendungen muss eine Folgenabschätzung durchgeführt werden.

Fehlen der Konsultation der betroffenen Parteien in den Verfahren.

Der Fall der Verarbeitung bestimmter Daten, für die genauere Empfehlungen ausgesprochen werden müssen.

Die Datenschutzgruppe ist der Überzeugung, dass die Unternehmen auf der Grundlage der in dieser Stellungnahme formulierten Bemerkungen einen verbesserten Rahmen vorschlagen können, und verpflichtet sich, sämtliche relevanten Mittel umzusetzen, um den Rahmenvorschlag weiter zu verbessern und dessen schnelle Annahme zu bewirken.

1.5. PERSONENBEZOGENE DATEN

Stellungnahme 3/2010 (WP 173) zum Grundsatz der Rechenschaftspflicht

Die Stellungnahme beschreibt die Vorteile, die konkrete interne Maßnahmen und Praktiken von Unternehmen und Verwaltungen für den Datenschutz bringen können. Sofern keine reale Integration in die gemeinsamen Werte und Praktiken einer Organisation und eine explizite Verteilung der Verantwortlichkeiten stattfindet, kann die Einhaltung dieser Prinzipien und Verpflichtungen gefährdet sein, und möglicherweise werden die Zwischenfälle in Bezug auf den Datenschutz fortbestehen.

Um einen effizienten Datenschutz zu fördern, muss der europäische Rechtsrahmen mit zusätzlichen Instrumenten ausgestattet werden. Diesbezüglich formuliert die Stellungnahme einen konkreten Vorschlag mit dem Ziel, einen Haftungsgrundsatz einzurichten, der von den für die Datenverarbeitung Verantwortlichen fordert, dass sie geeignete und wirksame Maßnahmen ergreifen, um die Einhaltung der in der Richtlinie definierten Grundsätze und Pflichten zu garantieren, und dafür auf Anforderung der Kontrollinstanzen den Nachweis erbringen. Dies wird dazu beitragen, den Datenschutz tatsächlich zu verwirklichen, und die zuständigen Behörden bei ihren Kontroll- und Umsetzungsaufgaben unterstützen.

Darüber hinaus enthält die Stellungnahme Vorschläge, mit denen garantiert werden soll, dass der Haftungsgrundsatz die erforderliche rechtliche Sicherheit bietet, wobei den Datenschutzakteuren ein gewisser Handlungsspielraum gelassen wird (beispielsweise, indem ihnen gestattet wird, konkrete Maßnahmen zu bestimmen, die je nach den mit der Verarbeitung verbundenen Risiken und der Art der zu verarbeitenden Daten zu ergreifen sind). Anschließend werden die Auswirkungen untersucht, die dieser Grundsatz auf andere Bereiche haben könnte, u. a. auf die internationale Datenübertragung, die Anforderungen in Bezug auf die Meldepflicht, auf Sanktionen, und zum Schluss wird die Ausarbeitung von Zertifizierungsprogrammen oder Labels erörtert.

Stellungnahme 8/2010 (WP 179) zum anwendbaren Recht

In dieser Stellungnahme wird der Anwendungsbereich von Artikel 4 der Richtlinie 95/46/EG präzisiert, der bestimmt, welche auf der Grundlage dieser Richtlinie erlassenen einzelstaatlichen Vorschriften auf die Verarbeitung personenbezogener Daten Anwendung finden. Des Weiteren wird auf bestimmte Bereiche eingegangen, in denen Raum für Verbesserungen besteht.

Eine präzisere Bestimmung der Anwendung des EU-Rechts auf die Verarbeitung personenbezogener Daten dient auch dazu, den Anwendungsbereich des EU-Datenschutzrechts sowohl in der EU bzw. im EWR als auch im größeren internationalen Kontext zu klären. Eine klare Vorstellung davon, welches Recht zur Anwendung kommt, wird sowohl den für die Datenverarbeitung Verantwortlichen Rechtssicherheit als auch den Betroffenen und anderen Beteiligten

einen eindeutigen Rechtsrahmen vermitteln. Eine korrekte Auslegung der Vorschriften zum anwendbaren Recht dürfte überdies gewährleisten, dass der durch die Richtlinie 95/46 gebotene weit reichende Schutz personenbezogener Daten keine Rechtslücken oder Schlupflöcher aufweist.

Die Stellungnahme gibt darüber hinaus Auslegungshinweise und Beispiele zu den anderen Bestimmungen des Artikels 4, zu den Sicherheitsanforderungen nach Maßgabe des gemäß Artikel 17 Absatz 3 anwendbaren Rechts sowie zu der Möglichkeit der Datenschutzbehörden, bei einem Verarbeitungsvorgang in ihrem Hoheitsgebiet ihre Untersuchungs- und Eingriffsbefugnisse auch dann auszuüben, wenn das Recht eines anderen Mitgliedstaats anwendbar ist (Artikel 28 Absatz 6).

In der Stellungnahme wird auch angeregt, im Rahmen einer Überarbeitung des allgemeinen Datenschutzrahmens die Richtlinie klarer zu fassen und für eine größere Kohärenz innerhalb des Artikels 4 zu sorgen.

Eine Vereinfachung der Regeln zur Bestimmung des anwendbaren Rechts würde vor diesem Hintergrund auf eine Rückkehr zum Herkunftslandprinzip hinauslaufen: Demnach würden alle Niederlassungen eines für die Datenverarbeitung Verantwortlichen in der EU unabhängig davon, wo diese Niederlassungen jeweils angesiedelt sind, dasselbe Recht anwenden, und zwar das der Hauptniederlassung. Dies wäre jedoch nur dann akzeptabel, wenn das einzelstaatliche Recht, d. h. auch die Sicherheitspflichten, umfassend harmonisiert würde.

Wenn der für die Datenverarbeitung Verantwortliche außerhalb der EU niedergelassen ist, könnten zusätzliche Kriterien herangezogen werden, um eine ausreichende Verbindung zum EU-Gebiet sicherzustellen und gleichzeitig zu vermeiden, dass in Drittländern ansässige Verantwortliche Daten im EU-Gebiet rechtswidrig verarbeiten. Hierfür in Frage kommende Kriterien wären das Anvisieren einzelner Personen (wenn sich die Verarbeitung personenbezogener Daten auf Einzelpersonen in der EU bezieht und die Anwendung des EU-Datenschutzrechts zur Folge hat) oder hilfsweise der begrenzte Rückgriff auf das „equipment"-Kriterium (Verarbeitung personenbezogener Daten durch automatisierte oder nicht automatisierte, im Hoheitsgebiet des betreffenden Mitgliedstaats belegene Mittel) zwecks Erfassung von Grenzfällen (Daten von Drittstaatsangehörigen, für die Datenverarbeitung Verantwortliche ohne Bezug zur EU), wenn es in der EU eine entsprechende Infrastruktur für die Datenverarbeitung gibt.

Fazit

Ziel dieser Stellungnahme ist die Klärung des Anwendungsbereichs der Richtlinie 95/46/EG und insbesondere von Artikel 4 dieser Richtlinie. Zudem soll auf bestimmte Bereiche hingewiesen werden, in denen weitere Verbesserungen möglich sind.

1.6. VERHALTENSKODEX

Stellungnahme 4/2010 (WP 174) zum europäischen Verhaltenskodex von FEDMA zur Verwendung personenbezogener Daten im Direktmarketing

Artikel 27 Absatz 3 der Richtlinie regelt die Verhaltenskodizes der Gemeinschaft wie folgt: *Die Entwürfe für gemeinschaftliche Verhaltensregeln sowie Änderungen oder Verlängerungen bestehender gemeinschaftlicher Verhaltensregeln können der in Artikel 29 genannten Gruppe unterbreitet werden. Die Gruppe nimmt insbesondere dazu Stellung, ob die ihr unterbreiteten Entwürfe mit den zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in Einklang stehen. Sie holt die Stellungnahmen der betroffenen Personen oder ihrer Vertreter ein, falls ihr dies angebracht erscheint. Die Kommission kann dafür Sorge tragen, daß die Verhaltensregeln, zu denen die Gruppe eine positive Stellungnahme abgegeben hat, in geeigneter Weise veröffentlicht werden.*

Um die Anwendung dieser Bestimmung zu erleichtern, hat die Gruppe im September 1998 ein Dokument verabschiedet, in dem das Verfahren für die Unterbreitung gemeinschaftlicher Verhaltensregeln und für die darauf folgende Beurteilung durch die Gruppe gemäß Artikel 27 und 29 der Richtlinie 95/46/EG[3] beschrieben ist. In diesem Dokument sind die wichtigsten Verfahrensschritte zusammengefasst, die in diesem Kontext zu beachten sind.

Im Juni 2003 verabschiedete die Arbeitsgruppe eine Stellungnahme zum europäischen Verhaltenskodex des Fachverbands FEDMA zur Verwendung personenbezogener Daten im Direktmarketing; der Kodex steht im Einklang mit Artikel 27 der Datenschutzrichtlinie und bietet gemessen an der Richtlinie genügend Mehrwert, da er alle speziellen Datenschutzfragen und -probleme im Direktmarketingbereich ausreichend behandelt und hinreichend klare

[3] Künftige Arbeit im Hinblick auf Verhaltensregeln: Arbeitsunterlage über das Verfahren für die Prüfung der Verhaltensregeln der Gemeinschaft durch die Datenschutzgruppe, angenommen am 10. September 1998, WP 13.

Lösungen für diese Fragen und Probleme bietet[4]. Die Datenschutzgruppe gelangte zu der Schlussfolgerung, dass der Kodex somit die Auflagen von Artikel 27 der Richtlinie erfüllt.

Die Datenschutzgruppe betonte jedoch, dass ein allgemeiner Kodex wie dieser per definitionem nicht alle der Online-Kommunikation inhärenten speziellen Probleme lösen kann, und forderte die FEDMA deshalb auf, einen Anhang zum Kodex auszuarbeiten, der sich mit diesen Problemen befasst. Dieser Anhang sollte insbesondere auf den Schutz von Kindern abstellen, deren Rechte bei der Online-Kommunikation besonders leicht verletzt werden können; dies wird auch in der Stellungnahme des Europäischen Verbraucherverbandes BEUC betont, den die Datenschutzgruppe zum Inhalt des Kodex befragt hat.

In einem Schreiben vom 16. Dezember 2005 legte die FEDMA der Datenschutzgruppe einen Anhang zum Europäischen Ehrenkodex für die Verwendung personenbezogener Daten im Direktmarketing (nachstehend: „Anhang") vor. Der FEDMA zufolge soll der Anhang bestimmte Probleme im Zusammenhang mit dem Online-Marketing abdecken. Analog zum FEDMA-Kodex ist auch dieser Anhang weder dazu bestimmt, geltende nationale Bestimmungen einzuschränken bzw. zu ersetzen, noch dazu, in Bereiche vorzudringen, die zurzeit nicht durch die EU-Gesetzgebung erfasst sind. Der Anhang soll grenzüberschreitend tätigen Marketingunternehmen als Leitfaden für ihre Online-Marketingaktivitäten dienen.

Im Juni 2010 übermittelte die FEDMA eine endgültige Version des Anhangs zum Online-Marketing, die nunmehr in Einklang mit Richtlinie 95/46/EG steht und hinreichenden Mehrwert bietet.

FAZIT

Die Arbeitsgruppe begrüßt, dass der Anhang des europäischen Verhaltenskodex der FEDMA zur Verwendung personenbezogener Daten im Direktmarketing mit der Richtlinie 95/46/EG und der derzeit anwendbaren Richtlinie 2002/58/EG sowie mit den nationalen Rechtsvorschriften in Einklang steht[5]. Der Anhang behandelt eine Reihe wichtiger Themen speziell im Online-Bereich (wie Mitglieder-werben-Mitglieder-Kampagnen, Schutz von Kindern, Möglichkeit der Abmeldung aus einem Verteiler) und liefert somit gegenüber den Richtlinien hinreichenden Mehrwert, indem er klare Lösungen für die Fragen bietet, die sich im Bereich Online-Marketing stellen. Damit erfüllt er auch die in Artikel 27 der Richtlinie 95/46/EG gestellten Anforderungen. Allerdings kann die Umsetzung der Richtlinie 2002/58/EG (geändert durch die Richtlinie 2009/136/EG) in nationale Rechtsvorschriften der Mitgliedstaaten eine Überarbeitung des Anhangs erforderlich machen, damit er mit den neuen Bestimmungen in Einklang steht; dies gilt insbesondere für Cookies und Spyware. Die Datenschutzgruppe empfiehlt der FEDMA, die bis zum 25. Mai 2011 erforderlichen Änderungen am Anhang des Verhaltenskodex zu prüfen, damit weiterhin Einklang mit dem rechtlichen Rahmen gemäß der Richtlinie 2002/58/EG, geändert durch die Richtlinie 2009/136/EG, sowie den nationalen Umsetzungsvorschriften besteht.

Um sicherzustellen, dass die nationalen Datenschutzbehörden in angemessener Weise über das Funktionieren des Kodex in der Praxis informiert werden, legt das FEDMA-Datenschutzkomitee der Datenschutzgruppe einen jährlichen Bericht über die Anwendung des Kodex vor. Sollte dieser Bericht Fragen aufwerfen, wird die Datenschutzgruppe mit der FEDMA Kontakt aufnehmen, um die in Rede stehenden Sachverhalte zu klären.

Die Datenschutzgruppe ermutigt die FEDMA, die Verbreitung dieses Online-Marketing-Anhangs zum Verhaltenskodex im Direktmarketingbereich aktiv voranzutreiben und sicherzustellen, dass die Datensubjekte ausreichend über die Existenz des Anhangs und seinen Inhalt informiert sind. Es wäre wünschenswert, dass die FEDMA ihre Arbeit in diesem Bereich fortsetzt und so das Schutzniveau des Einzelnen weiter anhebt. Die Datenschutzgruppe wird den jährlichen Berichten des FEDMA-Datenschutzkomitees über die Anwendung des Kodex besondere Aufmerksamkeit widmen.

4 Stellungnahme 3/2003, Dokument WP 77, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp77_en.pdf

5 Die nationalen Rechtsvorschriften können zusätzliche Anforderungen enthalten.

Kapitel Zwei

Die wichtigsten Entwicklungen in den Mitgliedstaaten

2. Die wichtigsten Entwicklungen in den Mitgliedstaaten

ÖSTERREICH

A. Neue Entwicklungen und Aktivitäten

Mit 1. Jänner 2010 ist die **Datenschutzgesetz-Novelle 2010** in Kraft getreten. Die wesentlichsten Neuerungen betreffen Regelungen über die Videoüberwachung, die Einführung einer Verpflichtung zur Meldung eines Verstoßes gegen das Datenschutzgesetz in schwerwiegenden Fällen („data breach notification") und die Vereinfachung der Meldung von Datenanwendungen durch den Umstieg auf ein online abzuwickelndes Meldeverfahren.

Noch nicht anwendbar waren im Berichtszeitraum die Bestimmungen zum vereinfachten Meldeverfahren, da zum einen die technischen Voraussetzungen noch nicht vorlagen, zum anderen diese Bestimmungen erst anwendbar werden, wenn eine neue Datenverarbeitungsregister-Verordnung erlassen wurde und in Kraft getreten ist. Eine solche Verordnung ist bis spätestens 1. Jänner 2012 zu erlassen.

Allgemein kann dazu festgehalten werden, dass durch die explizite Regelung der Videoüberwachung im Datenschutzgesetz das Bewusstsein in der Bevölkerung gestiegen ist, dass es sich bei Videoüberwachungen um Datenanwendungen handelt, und daher die diesbezügliche Zahl der Meldungen an die Datenschutzkommission gestiegen ist.

Mit einer **Novelle zur Standard- und Musterverordnung** des Bundeskanzlers wurden aber auch einige Videoüberwachungen von der Meldepflicht an die Datenschutzkommission ausgenommen. Dies betrifft Videoüberwachungen durch Banken, Juweliere, Antiquitätenhändler, Gold- und Silberschmiede, Trafiken und Tankstellen sowie Videoüberwachungen durch Besitzer bebauter Privatgrundstücke („Einfamilienhäuser").

Die Datenschutzkommission hat zum Entwurf einer **Verwaltungsgerichtsbarkeits-Novelle 2010** kritisch Stellung genommen. Diese Novelle sieht vor, dass bestimmte weisungsfreie Verwaltungsbehörden (darunter auch die Datenschutzkommission) aufgelöst werden und deren rechtsprechende Tätigkeit auf neu zu schaffende Verwaltungsgerichte übergehen soll. Die Datenschutzkommission hat insbesondere darauf hingewiesen, dass die Tätigkeiten aufgrund des Art. 28 der Richtlinie 95/46/EG einer neuen Behörde übertragen werden müssten, da diese Tätigkeiten nicht von den Verwaltungsgerichten wahrgenommen werden können. Letztere könnten nur für rechtsförmliche Entscheidungen zuständig gemacht werden.

Die Datenschutzkommission hat im Jahr 2010 im Rahmen ihrer Arbeit für die **Bewusstseinsbildung** zum Datenschutz die **Broschüre „Du bestimmst"** herausgegeben, die sich primär an Jugendliche wendet und sie über die datenschutzrechtlichen Risiken bei der Benutzung neuer Technologien (insbesondere Internet und soziale Netzwerke) informiert. Die Broschüre erfreut sich vor allem an Schulen großer Beliebtheit und wird immer wieder bei der Datenschutzkommission angefordert.

Die Veranstaltung zum **Europäischen Datenschutztag 2010** wurde gemeinsam mit Datenschutzrat und Bundeskanzleramt abgehalten und war vor allem den rechtlichen Neuerungen im Datenschutz aufgrund des Vertrags von Lissabon gewidmet.

Organisation	Österreichische Datenschutzkommission
Vorsitz und/oder Gremium	Vorsitz: Dr. Anton Spenling. Geschäftsführendes Mitglied: Dr. Eva Souhrada-Kirchmayer. Gremiumsmitglieder: Dr. Anton Spenling, Dr. Eva Souhrada-Kirchmayer, Mag. Helmut Hutterer, Dr. Claudia Rosenmayr-Klemenz, Dr. Klaus Heissenberger, Mag. Daniela Zimmer.
Budget	Kein eigenes Budget. Die Ressourcen der Kommission werden aus dem Budget des Bundeskanzleramts gedeckt.
Personal	20 Vollzeitstellen (18 Vollzeit- und vier Teilzeitbeschäftigte)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	61 formale Entscheidungen (Beschwerden), zehn formale Stellungnahmen, 22 Genehmigungen (Datenübermittlung in Drittländer, Forschung und Begutachtungen), fünf formale Empfehlungen.
Vorabprüfungen	7 569
Anträge betroffener Personen	3 977 (Meldungen, die Vorabprüfungen unterliegen).
Beschwerden betroffener Personen	Schriftlich: 913 (ohne Beschwerden). Telefonisch: ca. 22 500.
Vom Parlament bzw. der Regierung angeforderte Beratung	Beschwerden, denen eine formale Entscheidungen folgte: 94. Beschwerden, denen eine Klärung oder Empfehlung folgte: 298.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Diese Aufgabe fällt in die Zuständigkeit zweier anderer Institutionen: des *Datenschutzrats* und der Rechtsabteilung der Regierung im Bundeskanzleramt.
Prüfmaßnahmen	Von der E-Government-Registerbehörde, die Teil der österreichischen Datenschutzkommission ist, wurden 5 757 000 Personenkennzeichen vergeben. Die Behörde ist für das im Rahmen des österreichischen E-Government verwendete bereichsspezifische Identitätsmanagement und dessen Kontrolle zuständig.
Prüfungen, Untersuchungen	
Sanktionsmaßnahmen	
Sanktionen	14: Die meisten Fälle stehen in Zusammenhang mit Videoüberwachung.
Geldbußen	

Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Keine. Das österreichische Recht sieht keine Datenschutzbeauftragten vor.

B. Rechtsprechung

Die Datenschutzkommission hat einer Beschwerde stattgegeben, die gegen eine **Radarüberwachung durch eine Gemeinde** gerichtet war. Die Radaranlage war zur Verkehrsüberwachung eingesetzt worden, was von der Datenschutzkommission als hoheitliches Handeln qualifiziert wurde. Im konkreten Fall bestand aber keine gesetzliche Zuständigkeit der Gemeinde für derartige verkehrspolizeiliche Maßnahmen; es hätte vielmehr in diesem Fall einer Übertragung dieser Befugnisse durch eine Landes-Verordnung bedurft, die aber nicht gegeben war. Der Bescheid wurde von der Gemeinde (neuerlich) beim Verwaltungsgerichtshof bekämpft, der jedoch die Beschwerde abwies.

Eine Beschwerde einer Studentin gegen die **Wahlkommission bei der HochschülerInnenschaft an der Universität Wien** wegen Verletzung im Recht auf Geheimhaltung personenbezogener Daten im Zuge der Teilnahme an der elektronischen Hochschülerschaftswahl **(E-Voting**) wurde abgewiesen. Im Wahlsystem waren die Identitätsdaten und die Wahlstimme getrennt voneinander verschlüsselt. Wie von der Datenschutzkommission dargelegt wurde, waren umfangreiche technische Vorkehrungen getroffen worden, die eine Zusammenführung dieser Daten verhinderten. Im Übrigen entsprach das E-Voting auch der gesetzlichen Grundlage im Hochschülerinnen- und Hochschülerschaftsgesetz.

Von einem Beschwerdeführer wurde Beschwerde gegen das **„Parlament** Republik Österreich“ erhoben. Der Beschwerdeführer behauptete eine Verletzung im Recht auf Auskunft dadurch, dass seinem Auskunftsbegehren an einen Abgeordneten des österreichischen Nationalrates, der auch Mitglied eines **Untersuchungsausschusses** war, nicht nachgekommen worden war. Da auch die Tätigkeit in einem parlamentarischen Untersuchungsausschuss der „Gesetzgebung“ zuzurechnen ist, war die Datenschutzkommission nicht zuständig und die Beschwerde daher zurückzuweisen.

Google Street View wurde Anfang 2010 bei der Datenschutzkommission registriert. Als im Frühjahr 2010 bekannt wurde, dass Google Inc. bei den Street View-Fahrten auch **WLAN (WiFi)** Daten ermittelt hatte und noch dazu dabei Inhaltsdaten von E-Mails dgl. aufgezeichnet hatte, wurde von der Datenschutzkommission ein Prüfverfahren gegen Google Inc. eingeleitet. Google hat daraufhin die Inhaltsdaten gelöscht.

Das geschäftsführende Mitglied der Datenschutzkommission erließ einen Mandatsbescheid wegen Verdachts der Gefährdung schutzwürdiger Geheimhaltungsinteressen und untersagte Google die Weiterverwendung aller Street View-Daten. Unklar war insbesondere, wie die Ermittlung von WLAN-Daten, die ja von der Meldung an die Datenschutzkommission nicht erfasst war, mit Street View zusammenhängt. Dieser Bescheid wurde bei der Datenschutzkommission von Google Inc. beansprucht. Inzwischen erklärte Google auch, dass bei den Street View-Fahrten keine WLAN-Daten mehr erhoben werden. Da sich im Ermittlungsverfahren herausstellte, dass die Erhebung der WLAN-Daten zu einem anderen Zweck erfolgte als die Anwendung "Google Street View" und daher nicht der Datenanwendung "Street View" zuzuordnen war, wurde der Mandatsbescheid aufgehoben.

Gleichzeitig wurde ein „Verfahren zur Überprüfung der Registrierung" eingeleitet Dies ist zulässig, wenn Umstände bekannt werden, die den Verdacht der Mangelhaftigkeit einer Registrierung begründen. Inzwischen wurde Google Street View nach Verbesserungen der Meldung registriert; gleichzeitig wurden durch die Datenschutzkommission mehrere Empfehlungen an Google Inc. ausgesprochen. Ein Prüfverfahren bezüglich der Verwendung von WLAN–Daten durch Google Inc. blieb noch offen.

BELGIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Case Handling Workshop 2010

Im März 2010 hat die belgische Datenschutzbehörde im Le Square in Brüssel den 21. Workshop zur Fallbearbeitung ausgerichtet. Folgende Themen wurde von den Teilnehmern – hauptsächlich Rechtsexperten der europäischen Datenschutzbehörden – erörtert: wissenschaftliche Forschung, Direktmarketing und Mobilität.

Die belgische Datenschutzbehörde beteiligte sich an den Diskussionen zur wissenschaftlichen Forschung mit der Präsentation „Striking the balance between scientific freedom and data protection", die folgende Themen behandelte: Legitimität der Aufbewahrung und Speicherung personenbezogener Daten in öffentlichen und privaten Archiven, mögliche Bedingungen für den Archivzugriff, anonyme/verschlüsselte/unverschlüsselte personenbezogene Daten.

'Privacy and Scientific Research: from Obstruction to Construction'

Am 22. und 23. November 2012 organisierte die belgische Datenschutzbehörde eine internationale Konferenz mit dem Titel „**Privacy and Scientific Research: from Obstruction to Construction**" zu Aspekten der Privatsphäre und des Datenschutzes in der wissenschaftlichen Forschung. Die Veranstaltung fand im Rahmen der belgischen EU-Ratspräsidentschaft statt und sollte dazu dienen, einen Dialog zwischen den Datenschutzbehörden, nationalen und internationalen Universitäten und Wissenschaftlern über bewährte Verfahrensweisen in der medizinischen wie auch historischen Forschung herzustellen. Am 22. November wurden Seminare abgehalten, um die Teilnehmer über relevante Datenschutzvorschriften und spezifische medizinische und historische Themen zu informieren. Ziel war es, die erforderlichen Hintergrundinformationen für die Diskussions-Workshops am 23. November zu vermitteln, die in eine Reihe von Schlussfolgerungen mündeten. Weitere Informationen zur Konferenz, ihren Ergebnissen und den Folgeaktivitäten sind der Website (http://www.privacyandresearch.be) zu entnehmen.

Zentrale Themen – Empfehlungen und Stellungnahmen

2010 veröffentlichte die belgische Datenschutzbehörde offizielle Dokumente zu folgenden Themen: E-Ticketing (Empfehlung Nr. 01/2010), Trusted Third Parties (Empfehlung Nr. 02/2010), Mobile-Mapping-Technologie (Empfehlung Nr. 05/2010), Dopingbekämpfung (Stellungnahme Nr. 08/2010), Aufhebung des Bankgeheimnisses (Stellungnahmen Nr. 10 und 11/2010), Bekämpfung von Scheinehen (Stellungnahme Nr. 12/2010) und die Weitergabe elektronischer Kommunikationsdaten an Geheim- und Sicherheitsdienste (Stellungnahme Nr. 23/2010). Diese Dokumente bzw. allgemein alle 2010 verabschiedeten Stellungnahmen, Empfehlungen und Genehmigungen können in Französisch und Niederländisch auf der Web-site der belgischen Datenschutzbehörde im Bereich „Decisions" abgerufen werden: (http://www.privacycommission.be/en/decisions).

„Ich entscheide": Sensibilisierungs-Website für junge Menschen zum Thema Privatsphäre

In Anbetracht der besonderen Gefährdung, der junge Menschen aufgrund ihrer häufigen Nutzung neuer Technologien ausgesetzt sind, und nach Beratung mit verschiedenen Akteuren hat die belgische Datenschutzbehörde begonnen, eine spezielle Website zu entwickeln, die sich an vier Zielgruppen richtet (Kinder, Jugendliche, Eltern und Mitarbeiter/-innen von Bildungseinrichtungen) und im Januar 2010 online ging. Ziel der Website (in Französisch http://www.jedecide.be und Niederländisch http://www.ikbeslis.be) ist es, die Nutzung neuer Technologien durch junge Menschen zu fördern und ihnen gleichzeitig die Vor- und Nachteile dieser Technologien bewusst zu machen.

Organisation	Belgische Datenschutzbehörde
Vorsitz und/oder Gremium	Willem Debeuckelaere Zusammensetzung der Datenschutzkommission auf http://www.privacycommission.be

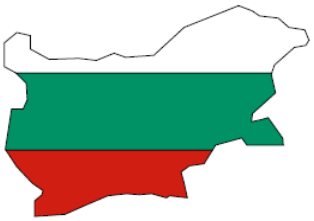
Budget	Staatliche Gelder für 2010: 5 516 000 EUR. Eigene Einnahmen: 60 000 EUR, besondere Vereinbarung mit der belgischen Abgeordnetenkammer über die Zuteilung von weiteren 354 112,37 EUR für die Organisation einer wissenschaftlichen Konferenz, dem Workshop für Fallbearbeitungen und Schengen-Kontrollen.
Personal	56
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Kommission: 25 Stellungnahmen, 1 Empfehlung, 1 Empfehlung zur Weiterverarbeitung Sektorielle Ausschüsse: 32 Stellungnahmen, 209 Einzelgenehmigungen, 4 allgemeine Genehmigungen, 121 Vereinigungen/Verbände mit allgemeinen Genehmigungen.
Meldungen	Gesamt: 11 269 Meldungen über 11 269 neue Verarbeitungsaktivitäten, 261 Änderungen bestehender Verarbeitungsaktivitäten, 73 Berichtigung bestehender Verarbeitungsaktivitäten, 376 Beendigungen bestehender Verarbeitungsaktivitäten.
Vorabprüfungen	k. A.
Anträge betroffener Personen	Eingegangen: 2 399 Informationsanforderungen ans Back Office und 3 008 ans Front Office; bearbeitet: 1 983 Informationsanforderungen im Back Office und 3 008 im Front Office.
Beschwerden betroffener Personen	Eingegangen: 348; bearbeitet: 190
Vom Parlament bzw. der Regierung angeforderte Beratung	87
Prüfmaßnahmen	Eröffnete Fälle: 85 Bearbeitete Fälle: 47
Prüfungen, Untersuchungen	
Sanktionsmaßnahmen	k. A.
Sanktionen	k. A.
Geldbußen	
Datenschutzbeauftragte (DPO)	Die Funktion des Datenschutzbeauftragten wurde mit Artikel 17 des belgischen Datenschutzgesetzes vorgesehen, aber es gibt noch keinen königlichen Erlass zur Umsetzung dieses Artikels. Dieses Dokument wird derzeit im Justizministerium erörtert.

B. Informationen zur Rechtsprechung

Eine Entscheidung des Genter Appellationshofs war für die belgische Datenschutzbehörde von besonderem Interesse:

Am 30. Juni 2010 entschied das Genter Berufungsgericht, dass die Yahoo-Portal-Website, ein Suchmaschinen- und Webmail-Anbieter, nicht gezwungen werden kann, personenbezogene Daten der Nutzer ihrer E-Mail-Dienste an die belgische Justiz weiterzuleiten. Im Zusammenhang mit einer Cyberkriminalität-Ermittlung überwachten Mitarbeiter/-innen der Federal Computer Crime Unit (eine Sonderabteilung der Föderalen Polizei Belgiens) eine Gruppe von Betrügern, die Yahoo-E-Mail-Adressen nutzten. Mithilfe vertraulicher Bankdaten von Unternehmen bestellten sie Computer und andere digitale Geräte. Yahoo weigerte sich, den belgischen Behörden mit diesen E-Mail-Adressen verbundene personenbezogene Daten zur Verfügung zu stellen und begründete dies damit, dass das belgische Recht nicht anwendbar sei, weil Yahoo keinen Standort in Belgien habe und auf belgischem Hoheitsgebiet keine personenbezogenen Daten bevorratet worden seien. Des Weiteren verwies Yahoo auf ein zwischen den Vereinigten Staaten und Belgien geschlossenes Abkommen, das für diese Art Anforderung ein Eingreifen der US-amerikanischen Behörden vorsieht. Ein belgisches Gericht erster Instanz akzeptierte die Begründung von Yahoo indes nicht und belegte das Unternehmen im März 2009 mit einer Geldbuße von 10 000 EUR für jeden Tag, an dem keine Daten übermittelt würden. Dieses Urteil wurde später durch das Genter Berufungsgericht aufgehoben.

BULGARIEN



A. Zusammenfassung der Aktivitäten und Neuerungen

A.1 Gesetzesänderungen

Ende 2010 wurde das Gesetz zum Schutz personenbezogener Daten geändert und im Hinblick auf zwei zentrale Aspekte ergänzt: Stärkung der behördlichen Kompetenzen der Kommission zum Schutz personenbezogener Daten (CPDP) und Gewährleistung des Zugriffs von Einzelpersonen auf ihre personenbezogenen Daten.

Die Gesetzesänderungen verliehen der CPDP hinsichtlich folgender Aspekte zusätzliche Kompetenzen:

Unterstützung der Umsetzung staatlicher Programme im Bereich des Schutzes personenbezogener Daten;

Beteiligung an den Aktivitäten internationaler Organisationen im Bereich des Schutzes personenbezogener Daten;

Beteiligung an den Verhandlungen zu und dem Abschluss von bilateralen und multilateralen Vereinbarungen zum Schutz personenbezogener Daten;

Organisation und Koordination der Schulung von für die Datenverarbeitung Verantwortlichen im Bereich des Schutzes personenbezogener Daten.

Die zweite Gesetzesänderung, die den freien Zugang zu personenbezogenen Daten gewährleistet, folgt einer Empfehlung im Rahmen der Beurteilung des Stands der Vorbereitungen Bulgariens auf den Beitritt zum Schengen-Raum.

A.2 Maßnahmen im Zusammenhang mit Bulgariens Schengen-Beitritt

Entsprechend den Bestimmungen des nationalen Schengen-Aktionsplans, denen zufolge der bulgarische Staat Maßnahmen durchführt, um die Bereitschaft des Landes für den Schengen-Beitritt zu gewährleisten, startete der CPDP 2010 eine Informationskampagne zur Sensibilisierung der Öffentlichkeit über die im Schengen-Raum geltenden Datenschutzrechte des Einzelnen. Die Informationskampagne beinhaltete Werbung für die CPDP-Webseite in den meistfrequentierten Online-Medien und auf den Webseiten staatlicher Institutionen sowie den Druck und die Ausgabe von 40 000 Broschüren (20 000 auf Bulgarisch und 20 000 in anderen Sprachen) an besonders prominenten Stellen. Dies ist die einzige direkt auf die Zivilbevölkerung ausgerichtete Maßnahme im nationalen Schengen-Aktionsplan, der sich nicht darauf beschränkt, die Verwaltungskapazitäten des Landes zu verbessern.

Was die von der CPDP durchgeführten Prüfmaßnahmen betrifft, hat die Kommission im Jahr 2010 neun Luftfahrtunternehmen im Zusammenhang mit der Verarbeitung personenbezogener Daten von Passagieren überprüft und damit begonnen, die Überprüfung wichtiger für die Datenverarbeitung Verantwortlicher N.SIS-Mitarbeiter zu organisieren.

Hinsichtlich der Umsetzung der Vorschriften zur Regelung der Verarbeitung personenbezogener Daten im SIS wurden – organisiert vom Innenministerium – die für Schengen-Fragen zuständigen CPDP-Experten in die Funktionsweise des Schengener Informationssystems eingewiesen.

Ende 2010 richtete die CPDP ein Verfahren für die Schaffung eines (inzwischen geschaffenen) EU-Registers für geschützte Informationen ein sowie ein Verfahren für den Zugang zu automatischen Informationssystemen und -netzwerken.

A.3 Stellungnahmen zu zentralen Themen

2010 wurde die Kommission zum Schutz personenbezogener Daten gebeten, zu verschiedenen Fragen Stellung zu nehmen. Von erheblichem öffentlichem Interesse waren die Stellungnahmen zu folgenden Punkten: welche technischen Mindestanforderungen es gibt und welche Dokumente erforderlich sind für die Weitergabe von Daten im Zusammenhang mit Kindern, die in Drittländern auf die Genehmigung ihrer Adoption warten; die Pflege einer Webseite für vermisste Kinder – bulgarische Bürger; und der Hinweis auf ein „Videoüberwachungs"-Register in Fällen, in denen Daten im Rahmen von Videoüberwachungsaktivitäten verarbeitet werden.

Organisation	
Vorsitz und/oder Gremium	Kommission, bestehend aus einer Leiterin – Frau Veneta Shopova – und vier Mitgliedern – Krassimir Dimitrov, Valentin Enev, Mariya Mateva und Veselin Tselkov.
Budget	Zugewiesenes Budget – BGN 2 650 000 (Bulgarische Leva), ausgegebene Haushaltsmittel – BGN 2 393 350.
Personal	Gesamtzahl der Mitarbeiter/-innen – 67: 49 Personen in Amtsverhältnis (Staatsbeamte) 18 Personen in sonstigen Arbeitsverhältnissen
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die Kommission erließ: 115 Verwaltungsakte im Zusammenhang mit eingereichten Beschwerden; 22 verbindliche Anweisungen (gerichtet an für die Datenverarbeitung Verantwortlichein den Bereichen Gesundheit, Telekommunikation, Handel und Dienstleistungen, Transport und öffentliche Verwaltung); 46 Stellungnahmen (auf Anfrage von für die Datenverarbeitung Verantwortlichen zur Anwendung des Gesetzes zum Schutz personenbezogener Daten sowie im Zusammenhang mit Rechtsvorschriften, die ein institutionsinternes Beratungsverfahren durchlaufen); 35 Beschlüsse zur Genehmigung der Weitergabe personenbezogener Daten in Drittländer.
Meldungen	86 664 für die Datenverarbeitung Verantwortliche wurden neu ins CPDP-Verzeichnis aufgenommen.
Vorabprüfungen	1 432
Anträge betroffener Personen	844
Beschwerden betroffener Personen	221 – meistens im Zusammenhang mit dem Bereich „Telekommunikation und Informationsgesellschaft" sowie mit „Finanz-, Kredit, Leasing- und Versicherungsdienstleistungen".
Vom Parlament bzw. der Regierung angeforderte Beratung	Die CPDP nahm Stellung zu primär- und sekundärrechtlichen Rechtsakten im Zusammenhang mit dem Handelsregister, bulgarischen Ausweisen, dem Zugang zur nationalen Bevölkerungsdatenbank, dem Binnenmarktinformationssystem und der Funktionsweise des Nationalen SIS sowie zu bilateralen Verträgen im Bereich der polizeilichen und rechtlichen Kooperation.

Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Unsere Behörde führte sechs Schulungseinheiten für Mitarbeiter, die für die Verarbeitung verantwortlich sind, mit Schwerpunkt auf der Anwendung der im Gesetz für den Schutz personenbezogener Daten enthaltenen Bestimmungen durch. Zielgruppen waren Vertreter lokaler Regierungs- und Verwaltungsbehörden, Vertreter der nationalen diplomatischen Dienste, Leiter von Bildungseinrichtungen – das Balkan Institute for Labour and Social Policy, die National Union of Jurisconsults und Studierende. Darüber hinaus hat das CPDP eine Informationskampagne zur Sensibilisierung der Öffentlichkeit für die Rechte des Einzelnen im Schengen-Raum initiiert und durchgeführt.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Durchgeführte Prüfungen insgesamt: 1 537 (hauptsächlich in den Bereichen Gesundheit, Handel und Dienstleistungen, Bildung, Soziale Dienste, Tourismus etc.)
Sanktionsmaßnahmen	
Sanktionen	Die CPDP hat 1 511 Prüfungsberichte und 36 Feststellungen tatsächlicher Verwaltungsdelikte vorgelegt.
Geldbußen	Von unserer Behörde auferlegte Geldbußen und finanzielle Sanktionen in Höhe von BGN 29 500.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. Rechtsprechung

k.A.

C. Sonstige wichtige Informationen

2010 wurde die Kommission zum Schutz personenbezogener Daten gebeten, sich mit Beschwerden zu befassen; in den meisten Fällen ging es um die Verletzung des Rechts der betroffenen Person, informiert zu werden, wenn Daten über sie via Internet verarbeitet werden. Die größte Anzahl von Beschwerden richtete sich gegen Service-Provider im Bereich „Telekommunikation und Informationsgesellschaft“ (zur Offenlegung von Daten gegenüber Dritten zu Inkassozwecken), gefolgt von den Bereichen „Finanz-, Kredit, Leasing- und Versicherungsdienstleistungen“.

Ein besonderer Fall zu Letzterem betraf die Offenlegung der Daten eines Unternehmens im Handelsregister einschließlich personenbezogener Daten, die nach Ermessen unserer Behörde über die Zwecke, zu denen das Register eingerichtet wurde, hinausgingen. Hinzu kam, dass bei der Verarbeitung der offengelegten Daten die Zulässigkeitsbestimmungen nicht eingehalten wurden.

Des Weiteren gab es einen Anstieg der Zahl der Beschwerden im Zusammenhang mit der Verarbeitung personenbezogener Daten durch für die Datenverarbeitung Verantwortliche sowie Anbieter von Direktmarketingdiensten.

Viele der bei der Kommission für den Schutz personenbezogener Daten eingereichten Beschwerden betrafen die Nichtgewährleistung des Zugangs zu personenbezogenen Daten oder die stillschweigende Verweigerung der Bereitstellung solcher Daten gegenüber Einzelpersonen. Außerdem ermittelte unsere Behörde Rechtswidrigkeiten im Zusammenhang mit der Verletzung des Verhältnismäßigkeitsgrundsatzes, des Grundsatzes der Verarbeitung von Daten zu konkreten und rechtmäßigen Zwecken sowie der Verarbeitung personenbezogener Daten unter Missachtung eines Teils der geltenden Zulässigkeitsbestimmungen.

Mit der endgültigen Umsetzung der Richtlinie 2006/24/EG in bulgarisches Recht im Mai 2010 erhielt die Kommission für den Schutz personenbezogener Daten die rechtliche Befugnis, gespeicherte Daten auf Sicherheitsaspekte zu überprüfen. Neben den der CPDP im Gesetz zum Schutz personenbezogener Daten erteilten Befugnissen ermöglicht ihr das Gesetz zur Elektronischen Kommunikation: 1) innerhalb ihres Zuständigkeitsbereichs Unternehmen, die öffentliche elektronische Kommunikationsnetze anbieten, und/oder Dienstleister zur Vorlage von Informationen aufzufordern; 2) Weisungen auszusprechen, denen unmittelbar Folge zu leisten ist.

ZYPERN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Mai 2010 wurde Frau Panayiota Polychronidou zur Kommissarin für den Schutz personenbezogener Daten ernannt. Frau Polychronidou ist die Nachfolgerin von Frau Goulla Frangou, die diese Aufgabe zwei Amtszeiten lang innehatte.

Ein Entwurf unseres Büros zur Änderung des Gesetzes 138(I)/2001 zwecks besserer Umsetzung der Bestimmungen der Richtlinie 95/46/EG und zwecks Verbesserung der effektiven Durchsetzung der von unserem Büro vorbereiteten nationalen Datenschutzgesetze ist in Vorbereitung.

Als Teil der Sensibilisierungsbemühungen unseres Büros wurden im Rahmen der Aktivitäten anlässlich des Europäischen Datenschutztages Mittel in Höhe von 15 000 Euro bereitgestellt, mithilfe deren am 28. Januar 42 000 Informationsbroschüren an die Leser von vier Tageszeitungen ausgeteilt wurden, was einer Deckung von ungefähr 93 % der Tagesauflage entspricht. Am selben Tag verteilten Mitarbeiter unseres Büros Flyer und Kaffeetassen mit dem Aufdruck „28. Januar – Europäischer Tag des Datenschutzes“ an die Besucher der als zentrale Anlaufstellen dienenden Bürgerämter (Citizen Service Centers) und beantworteten den Bürgerinnen und Bürgern Fragen zum Schutz personenbezogener Daten.

Nach Vorlage der Ergebnisse des Berichts des Generalinspektors, denen zufolge mehreren Personen, die von der Sozialversicherung (SIS) Sozialleistungen/Renten aufgrund von Arbeitsunfähigkeit – unter anderem wegen Blindheit – erhielten, von der Verkehrsbehörde (RTD) eine Fahrerlaubnis für berufliche Zwecke ausgestellt wurde, erging an unser Büro die Bitte um Rat bezüglich der Frage, wie die betroffenen Stellen unter Einhaltung der gesetzlichen Datenschutzbestimmungen Informationen austauschen können, um die Ausgabe von Fahrerlaubnissen für berufliche Zwecke an aus medizinischer Sicht ungeeignete Personen zu verhindern. Unter Berücksichtigung der geltenden Rechtsvorschriften zur Regelung der Kompetenzen der SIS und der RTD sowie einer relevanten Stellungnahme des Staatsanwalts der Republik, nach dessen Ermessen die Ausgabe einer Fahrerlaubnis für berufliche Zwecke keinen Nachweis der Nutzung dieser Erlaubnis darstellt, teilte die Kommissarin den antragstellenden Parteien mit, dass Vorfälle dieser Art durch den Austausch relevanter Daten im Zuge einer Verknüpfung der elektronischen Speichersysteme beider Stellen vermieden werden könnten; hierzu erforderlich ist eine Genehmigung der Kommissarin gemäß Abschnitt 8 des Gesetzes. Die Verknüpfung würde es der RTD gestatten, nach Erhalt eines Antrags für eine Fahrerlaubnis für berufliche Zwecke mittels HIT/NO-HIT-Methode zu prüfen, ob der/die Antragstellende von der Sozialversicherung (SIS) aus medizinischen Gründen Sozialleistungen/Renten aufgrund von Arbeitsunfähigkeit erhält. Bei positivem Bescheid (HIT) bittet der Director der RTD die SIS um zusätzliche Informationen hinsichtlich der von dem/der Antragstellenden angeführten medizinischen Gründe für den Erhalt der Sozialleistungen/Rentenzahlungen und verweist die/den Antragstellende(n) gegebenenfalls an den ärztlichen Dienst der RTD, um zu überprüfen, ob die angeführten medizinischen Gründe in seinem/ihrem Fall der Erteilung einer Fahrerlaubnis für berufliche Zwecke entgegenstehen. Darüber hinaus sprach die Kommissarin sich dafür aus, technische Einschränkungen vorzusehen, um zu gewährleisten, dass Nutzer seitens der RTD ausschließlich auf Daten zugreifen können von Personen, die eine Fahrerlaubnis für berufliche Zwecke beantragt haben, und zu verhindern, dass auf Daten von Personen zugegriffen werden kann, die Sozialleistungen/Rentenzahlungen erhalten, aber keine Fahrerlaubnis für berufliche Zwecke beantragt haben.

Organisation	Büro der Kommissarin für den Schutz personenbezogener Daten
Vorsitz und/oder Gremium	Frau Panayiota Polychronidou
Budget	Zugewiesenes Budget: 318 091 EUR Ausgegebene Haushaltsmittel: 235 487 EUR
Personal	7 Verwaltungsbedienstete 2 Informationstechnologie-Fachkräfte 5 Bürofachkräfte 2 Hilfskräfte
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Stellungnahmen: 39 zentrale Themen
Meldungen	Anzahl der Meldungen: 222
Vorabprüfungen	Anzahl der Vorabprüfungen: k. A.
Anträge betroffener Personen	Anzahl der Anträge: k. A.
Beschwerden betroffener Personen	Anzahl der Beschwerden: 804
Vom Parlament bzw. der Regierung angeforderte Beratung	Anzahl der Beratungsanträge: 16 der 29 Stellungnahmen wurden infolge zuvor eingegangener Anfragen von Regierungsstellen abgegeben.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Genehmigungen für die Verknüpfung von Speichersystemen: 32 Genehmigungen für die Weitergabe personenbezogener Daten an Drittländer: 33 Genehmigungen für die Verarbeitung sensibler Daten im Bereich Arbeitsrecht: 0
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen 19 (18 im Banksektor und 1 in der Asylabteilung) 2010 setzte unser Büro die im Jahr 2009 begonnene Überprüfung von 18 in Zypern operierenden Geschäftsbanken fort. Im Zuge der Überprüfung wurden die Banken gebeten, einen Modell-Fragebogen auszufüllen, und viele Kundenantragsformulare wurden unter die Lupe genommen. In Fällen, in denen ein Formular die Angabe personenbezogener Kundendaten erforderte und gegen den Grundsatz der Verhältnismäßigkeit verstieß, verlangte die Kommissarin die Änderung des betreffenden Formulars entsprechend den gesetzlichen Bestimmungen. Nach Vorlage der Auswertung der beantworteten Fragebögen gab die Kommissarin Richtlinien mit den Schwerpunkten schwarze Listen, Kriterien für unterschiedliche Aufbewahrungsfristen – insbesondere hinsichtlich

	aktueller und ehemaliger Bankkunden – sowie Korrektheit von Daten aus. Im Rahmen einer im Dezember 2010 von der Koordinierungsgruppe für die Aufsicht über Eurodac beschlossenen Prüfung bat unser Büro die Asylabteilung um Vervollständigung und Einreichung eines speziellen von der Gruppe vorbereiteten Fragebogens zur Überprüfung der nationalen Praktiken hinsichtlich vorzeitiger Löschungen und der Verifizierung des Alters minderjähriger Asylantragsteller sowie der Einhaltung der relevanten Bestimmungen der Verordnung (EG) 2725/2000.
Sanktionsmaßnahmen	
Sanktionen	14
Geldbußen	12 Geldbußen (insges. 17 000 EUR)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

TSCHECHISCHE REPUBLIK

A. Zusammenfassung der Aktivitäten und Neuerungen

2010 ging das Amt für den Schutz personenbezogener Daten (nachstehend „ASPD" bzw. „Amt") ins elfte Jahr seines Bestehens und seiner Tätigkeit, und es war das erste Jahr von Präsident Igor Němec nach seiner Wiederwahl (für eine Amtszeit von fünf Jahren).

Die wichtigste Veranstaltung war die vom ASPD organisierte ***Konferenz der europäischen Datenschutzbeauftragten*** am 29. und 30. April in Prag. Die Konferenz mit dem anspruchsvollen Motto „Über die Vergangenheit reflektieren, an die Zukunft denken" umfasste vier Themenblöcke: „Internet of things: ubiquitous monitoring in space and time", „Children in a cobweb of networks", „Personal data protection at the crossroads", „Public sector: respected partner or privileged processor?"; den Abschluss bildete eine Diskussionsrunde zum Thema Ethnic Profiling (Profilerstellung auf Grundlage ethnischer Merkmale). Es wurden vier Beschlüsse gefasst: zum Einsatz von Körperscannern für die Sicherheit an Flughäfen, zu dem geplanten Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über Datenschutzstandards im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen, zur künftigen Entwicklung von Datenschutz und Privatsphäre sowie zur Durchführung gemeinsamer Aktionen zur Sensibilisierung und Aufklärung von Kindern auf europäischer und internationaler Ebene (nähere Informationen hierzu unter http://www.uoou.cz/uoou.aspx?menu=125&submenu=614&loc=690&lang=en).

Die Regierung ist verpflichtet, das Amt im Rahmen des Gesetzgebungsprozesses um Stellungnahme zu ersuchen. Bei einem wesentlichen Teil der gesetzgeberischen Aktivitäten des Amts ging es daher auch 2010 um ***spezifische Rechtsvorschriften*** mit Bedeutung für den Schutz der Privatsphäre und personenbezogener Daten. Eine der wichtigsten Aufgaben, an denen sich das Amt beteiligte, war die Arbeit einer Expertengruppe, die mit der Ausarbeitung einer gesetzlichen *Regelung für die Verarbeitung menschlicher DNS-Proben* befasst war. In der Tschechischen Republik gibt es bis dato kaum spezielle Rechtsvorschriften für polizeiliche DNS-Datenbanken; der Umgang mit DNS seitens der Polizei kann gegenwärtig in erheblichem Maße auf bloße Anordnung des Polizeipräsidenten geregelt werden. Darüber hinaus fehlen in der Tschechischen Republik gleichermaßen tragfähige spezielle Rechtsvorschriften zum Einsatz von *Kameraüberwachungssystemen;* das Amt hat diesbezüglich eine Stellungnahme zu einem Gesetzesentwurf abgegeben, der 2010 noch nicht verabschiedet wurde. Das Amt hielt es für sinnvoller, ausschließlich eine gesetzliche Regelung für den immer wieder problematischen viel diskutierten Einsatz von Kameras an öffentlich zugängigen Orten und Einrichtungen auszuarbeiten.

Hinsichtlich der Kompetenzen des Amts und seiner Aktivitäten, insbesondere im Bereich elektronische Kommunikation und Dienstleistungen in der Informationsgesellschaft, war 2010 der Beginn der Umsetzung der Richtlinie 2009/136/EG von grundlegender Bedeutung. Das Amt legte für das Gesetz über elektronische Kommunikation (für das es auch die mit dem Schutz personenbezogener Daten verbundenen Aspekte kontrolliert) mehrere Stellungnahmen vor.

Neben vielen anderen Entwürfen, zu denen Stellungnahmen abgegeben wurden, ist der Änderungsentwurf für das Strafregistergesetz von besonderer Bedeutung.

Ende 2010 wurde das Amt gebeten, eine Stellungnahme zum Entwurf für eine ***Regierungsstrategie zur Bekämpfung von Korruption*** für den Zeitraum 2010–2012 gebeten; diese enthält verschiedene legislative, direkt das Thema Schutz personenbezogener Daten betreffende Maßnahmen. Grundsätzlich stellte das Amt fest, dass spezielle Maßnahmen die Prinzipien des Schutzes personenbezogener Daten respektieren und dementsprechend detailliert formuliert sein müssen, um zu gewährleisten, dass die Verarbeitung und Offenlegung personenbezogener Daten ausschließlich zu genau spezifizierten Zwecken erfolgen darf und diese Daten nur eindeutig abgegrenzten autorisierten Stellen im Rahmen genau spezifizierter Verfahren und nur in dem unbedingt zur Bekämpfung von Korruption erforderlichen Ausmaß zugänglich sein dürfen. Spezielle Einwände wurden z. B. im Zusammenhang mit Maßnahmen wie dem *Register für strafbare Handlungen* vorgebracht, in denen das Amt herausstellte, dass nicht eindeutig nachvollziehbar sei, warum es notwendig sei, die Erfassung der strafbaren Handlungen in verschiedenen Bereichen des menschlichen Lebens komplett zu zentralisieren, und feststellte, dass für die ///Handhabung des Registers mit solch sensiblen Daten angemessene Garantien ähnlich dem strengen Strafregister-Modell ///gelten

müssen. Ein Teil der Stellungnahmen betraf die *Zuverlässigkeitsprüfungen* bei Personen, die in öffentlichen Behörden arbeiten, und das *zentrale Bankkontenregister*.

2009 bekam das ASPD neue Befugnisse und Aufgaben zugewiesen, die 2010 begannen und ausgestaltet wurden: Ausarbeitung (bis Juni 2012) und anschließende Realisierung des ORG-Informationssystems als Teil des mit dem *eGovernment-Programm* verbundenen Grundregistersystems. Das von der EU kofinanzierte ORG-IS dient der Konvertierung von Identifikatoren; hierbei werden die gegenwärtig verwendeten universellen Geburtennummern (rodné číslo) durch ein System bedeutungsloser, für die individuellen Agenden oder Agenden-Gruppen unterschiedlicher Identifikatoren ersetzt.

Der Umfang der aus dem Staatshaushalt zugewiesenen Gelder für das oben genannte eGovernment-Spezialprogramm (ORG-IS-Programm) ist in der unten aufgeführten Summe (s. Tabelle) nicht enthalten.

Organisation	
Vorsitz und/oder Gremium	Igor Němec, Präsident des ASPD
Budget	Gesamtausgaben: ca. 97 Mio. CZK, d. h. ungefähr 3,9 Mio. EUR
Personal	97 Mitarbeiter/-innen 61,5 % mit Universitätsabschluss, 51 % Frauen
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2 Stellungnahmen (zur Weitergabe von Daten ins Ausland, zu Datenschutz-Aspekten bei privatdetektivischen Leistungen). 10 Stellungnahmen zu aktuellen wichtigen Themen, veröffentlicht auf Webseiten oder in Bulletins (z. B. zum Thema DNS).
Meldungen	4 037
Vorabprüfungen	64 (mit Meldungen verbundene Verfahren)
Anträge betroffener Personen	3 822 bürgerseitige Beratungsanfragen und -anträge
Beschwerden betroffener Personen	1 039 Beschwerden und Ersuche gemäß Datenschutzgesetz sowie 2 834 Beschwerden und Ersuche im Zusammenhang mit unerbetenen Werbenachrichten
Vom Parlament bzw. der Regierung angeforderte Beratung	217
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	317 Beratungen für juristische Personen 219 Beratungen für natürliche, unternehmerisch tätige Personen
Prüfmaßnahmen	
Prüfungen, Untersuchungen	106 Prüfungen im Zusammenhang mit dem Datenschutzgesetz sowie 163 Kontrollverfahren im Zusammenhang mit unerbetenen Werbenachrichten

Sanktionsmaßnahmen	
Sanktionen	209 finanzielle Sanktionen in Höhe von insges. 254 000 EUR, davon 19 600 EUR im Zusammenhang mit unerbetenen Werbenachrichten; finanzielle Sanktionen gehen meistens mit der Anordnung von Maßnahmen einher.
Geldbußen	(s. hierzu auch oben – finanzielle Sanktionen) Die höchsten Geldbußen wurden im öffentlichen Sektor erhoben (Zentralregister für Medikamente, Studierende, Einwohner – 92 000, 32 000, 16 000 EUR respektive). Im Privatsektor lagen die höchsten Geldbußen im Einzelfall nicht über 7 200 EUR (Hotels, Kameras in Geschäften und Privatunterkünften, etc.)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. Rechtsprechung

Die Tschechische Republik ist kein klassisches fallrechtbasiert Recht sprechendes Land im Sinne einer Zugrundelegung vorheriger gerichtlicher Entscheidungen.

Hinsichtlich der datenschutzrechtlichen Vorschriften ist die Gerichtszuständigkeit von relativ hoher Bedeutung, da die Gerichte bei Beschwerden gegen Entscheidungen des ASPD als zweite Instanz fungieren (erste Instanz ist der Präsident des Amtes) und jeder das Gericht auch direkt anrufen kann.

2010 wurden im Bereich Datenschutz 18 neue Klagen vorgelegt. Sieben Klagen gegen Entscheidungen des Amtes wurden vom Gericht abgewiesen und sechs Entscheidungen des Amtes wurden vom Gericht aufgehoben.

Als Beispiele nachstehend drei typische Urteile, bei denen es in allen Fällen um eine Beschwerde gegen die Entscheidung des Amtes ging und die Entscheidungen aufgehoben wurden:

- das Urteil des Amtsgerichts Prag (11 Ca 433/2008-89) zum Thema Schutz der Privatsphäre versus Schutz von Eigentum im Zusammenhang mit einem Kamerasystem in einem Hotel;
- das Urteil des Amtsgerichts Prag (9 Ca 4/2008-33) zur Verarbeitung personenbezogener Daten in einem Reisebüro;

das Urteil des obersten Verwaltungsgerichts (1 As 93/2009-121) zu grundsätzlichen Fragen im Zusammenhang mit der Art von Kontroll- und Verwaltungsverfahren.

C. Sonstige wichtige Informationen

2010 verzeichnete das ASPD eine sinkende Zahl von Anträgen zur *Genehmigung der Weitergabe personenbezogener Daten in Drittländer*. Diese Tendenz war insbesondere darauf zurückzuführen, dass die für die Datenverarbeitung Verantwortlichen verstärkt Instrumente einsetzten, die von der Europäischen Kommission eingerichtet wurden, um einen angemessenen Schutzes in Drittländern zu gewährleisten, insbesondere die Standard-Vertragsklauseln und das für die Datenübermittlung in die Vereinigten Staaten geltende Safe-Harbor-Abkommen. Ungeachtet dessen vertrauen die für die Datenverarbeitung Verantwortlichen meistens auf die Bestimmungen des Datenschutzgesetzes, das die Übermittlung auf Grundlage der Einwilligung oder Vorgaben des Datensubjekts gestattet; hierfür ist weiterhin die Genehmigung des Amtes erforderlich.

Im Rahmen seiner *internationalen Kooperationsaktivitäten* beteiligte sich das Amt weiterhin an den Tätigkeiten der Artikel-29-Datenschutzgruppe und verschiedenen ihrer Untergruppen. Der Präsident des ASPD, Igor Němec, wurde im

Oktober 2010 bei der 77. Sitzung der Artikel-29-Datenschutzgruppe zu deren stellvertretendem Vorsitzenden ernannt.

Das Amt – und insbesondere seine Experten – wurden gebeten, sich verschiedenen internationalen Teams anzuschließen, die im Rahmen EU-finanzierter Projekte in Ländern tätig sind, die an der Einführung oder Verbesserung des Datenschutzes in ihren Ländern arbeiten. Einer der für das Amt tätigen Juristen, Jiří Maštalka, wurde zum Hauptzuständigen für ein Projekt in Albanien ernannt, und das Amt benannte vier für kurze Zeit eingesetzte Experten für ein vergleichbares Projekt in der Ehemaligen Jugoslawischen Republik Mazedonien. Bei dem zweitägigen Workshop in Prag wurden bulgarischen Kollegen die im Laufe der Kontrollverfahren des Amtes gesammelten praktischen Erkenntnisse vorgestellt. Außerdem tauschten sich die Experten des Amtes mit ihren polnischen und ungarischen Kollegen über gemeinsame, im Rahmen des EU-Programms Leonardo da Vinci finanzierte Aktivitäten aus.

Der Schwerpunkt der *Sensibilisierungsaktivitäten* des ASPD und seiner Kommunikation mit den Medien lag auf alltäglichen Diensten und der Bereitstellung aktueller Informationen über seine Webseite und der Veranstaltung von Pressekonferenzen. Das Interesse der Journalisten an den Pressekonferenzen war durchaus zufriedenstellend: An den Konferenzen nahmen rund 20–25 Journalisten teil; vertreten war eine umfassende Bandbreite von Medien – Agenturen ebenso wie elektronische und Printmedien. Die Zahl der in den Medien veröffentlichten Berichte zum Thema Datenschutz im Anschluss an die Pressekonferenzen lag bei rund 30 bis 60 innerhalb von drei Tagen nach der Pressekonferenz. Als Anlage zu Pressemitteilungen stellt das Amt regelmäßig Informationen zu abgeschlossenen Untersuchungen bereit, die mit der Verhängung von Bußgeldern gekoppelt sind.

Bei der traditionell am Tag des Datenschutzes stattfindenden Winter-Pressekonferenz eröffnete das Amt den vierten Wettbewerb für Kinder und Jugendliche „Meine Privatsphäre!“ „Nicht gucken, nicht herumschnüffeln!“, dessen Ziel dieses Jahr lautet, Kinder und junge Menschen auf die Risiken im Zusammenhang mit der Kommunikation im Internet und der Nutzung sozialer Netzwerke aufmerksam zu machen.

DÄNEMARK

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
Vorsitz und/oder Gremium	Für das Tagesgeschäft der DSB ist das Sekretariat zuständig; die Leitung obliegt dem/der jeweiligen Direktor(in). Fälle von erheblichem Interesse (ungefähr 15 Fälle pro Jahr) werden dem Rat zur Entscheidung vorgelegt. Vorsitzende/-r des Rates ist ein Richter/eine Richterin des Obersten Gerichtshofs.
Budget	20,3 Mio. DKK
Personal	Ungefähr 35
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A. (siehe Angaben weiter unten)
Meldungen	2 660
Vorabprüfungen	2 660
Anträge betroffener Personen	2 018 (Anträge und Beschwerden)
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	383
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	52 Fälle im Zusammenhang mit Sicherheitsfragen
Prüfmaßnahmen	
Prüfungen, Untersuchungen	64
Sanktionsmaßnahmen	
Sanktionen	Die DSB kritisiert jedes Jahr eine Reihe von für die Verarbeitung Verantwortlichen für die Nichteinhaltung des Gesetzes über die Verarbeitung personenbezogener Daten.
Geldbußen	Verhängung von Geldbußen in 3 Fällen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A. (im dänischen Recht nicht vorgesehen).

B. Rechtsprechung

Öffentliche Behörden und Kommunikation per SMS

2009 wandte die Stadtverwaltung von Kopenhagen sich an die DSB bezüglich des Einsatzes von Textnachrichten der Behörden an ihre Bürger per Mobiltelefon. Hintergrund war die Idee der Behörde, Personen an ihre Termine mit der Stadtverwaltung zu erinnern.

Die dänische DSB erklärte, dass ihrer Ansicht nach Mitteilungen über ein Mobilfunknetz keine sichere Art der Kommunikation sind und Behörden sensible und/oder vertrauliche Informationen deshalb nicht an das Mobiltelefon einer Person senden dürfen.

Vor dem Hintergrund dieser grundsätzlichen Regelung stimmte die dänische DSB 2010 einer Ausnahmeregelung zu, sofern bestimmte Vorgaben befolgt werden.

Diese Vorgaben lauten:

Es dürfen ausschließlich Erinnerungen und vergleichbare Mitteilungen (d. h. kurze, neutral formulierte Mitteilungen) auf diesem Weg versendet werden.

Der/die Bürger/-in muss dieser Form der Kommunikation vorab zugestimmt haben.

Die Nachrichten dürfen keine personenbezogenen Identifikationsnummern beinhalten.

Die jeweilige Person darf nur Informationen erhalten, die sie selbst oder ihre Kinder betreffen.

Die technische Lösung muss gewährleisten, dass die für die Mitteilungen verwendete Telefonnummer korrekt ist.

Die dänischen Behörden haben ein technisches System namens nemsms entwickelt, das Bestandteil des Kommunikationssystems der Behörden ist.

Cloud computing

2010 erhielt die dänische DSB eine Anfrage der Stadtverwaltung Odense zur Nutzung der Online-Office-Suite Google Apps mit Kalender- und Dokumentenverarbeitungsfunktionen.

Die Stadtverwaltung Odense wollte, dass Lehrkräfte die Lösung für die Einreichung von Informationen zur Unterrichtsplanung und die Beurteilung von Unterrichtsplänen und der schulischen Entwicklung einzelner Schüler/-innen verwenden. Des Weiteren sollten die Lehrkräfte Aufzeichnungen zur Kooperation von Klassen und Schüler/-innen machen und die Kinder betreffende Briefe an die Eltern vorbereiten. Außerdem sollte die Lösung für die Planung und den Versand von Einladungen für Sitzungen und die Verbreitung von Informationen zu schulischen Aktivitäten genutzt werden.

Dies wäre mit sensiblen Daten verbunden gewesen, so z. B. Daten zur Gesundheit, zu schweren sozialen Problemen und anderen rein privaten Aspekten.

Die dänische Datenschutzbehörde erörterte das Thema in einer Sitzung des Datenschutzrates.

Die dänische Datenschutzbehörde sah in verschiedenen Bereichen Probleme hinsichtlich der Anforderungen des Gesetzes über die Verarbeitung personenbezogener Daten und der dänischen Sicherheitsverordnung (Sikkerhedsbekendtgørelsen). Die dänische Datenschutzbehörde stimmte daher der Einschätzung der Stadtverwaltung Odense, vertrauliche und sensible Daten über Schüler/-innen und Eltern könnten mit Google Apps verarbeitet werden, nicht zu.

Als problematisch angesehen wurden unter anderem:

die Übermittlung personenbezogener Daten in Drittländer;

allgemeine Informationen über die Verarbeitungssicherheit in Verbindung mit der Verwendung von Google Apps durch die Stadtverwaltung Odense;

die Bestimmungen des Gesetzes über die Verarbeitung personenbezogener Daten hinsichtlich der Datenschutzanforderungen bei Nutzung eines externen Auftragsverarbeiters;

die Löschung personenbezogener Daten;

die Übermittlung und Anmeldung;

die Überwachung zurückgewiesener Datenzugriffsversuche;

die Protokollierung.

Die dänische Datenschutzbehörde ist bereit, den Fall noch einmal zu prüfen und ihre Stellungnahme zu überdenken, wenn die Stadtverwaltung weiter an dem Fall arbeitet und Lösungen für die benannten Probleme sucht.

C. Sonstige wichtige Informationen

Im dreizehnten Jahresbericht berichtete die dänische DSB über einen geplanten, dem Parlament vorzulegenden Gesetzentwurf, der eine Videoüberwachung in Taxis zur Pflicht macht. Hieran anknüpfend kann die dänische DSB berichten, dass das Gesetz am 22. April 2010 vom dänischen Parlament verabschiedet und am 1. Juli 2010 in Kraft trat.

ESTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Schutz personenbezogener Daten in der estnischen Rechtsprechung erstreckt sich auf alle Gesellschaftsbereiche. Er gilt auch für alle Privatpersonen, die personenbezogene Daten anderer Menschen außerhalb ihrer Privatsphäre verarbeiten (z. B. im Internet). Alle Institutionen sowie alle Personen des Privatrechts, die öffentliche Aufgaben wahrnehmen oder öffentliche Gelder in Anspruch nehmen, sind Besitzer öffentlicher Informationen.

Die estnische Datenschutzinspektion (Andmekaitse Inspektsioon/AKI) ist eine kleine Behörde mit 17 Mitarbeiter/-innen. Dies wirft unweigerlich Fragen auf, z. B. wie wir ungeachtet der quantitativen Indikatoren in unserem Zuständigkeitsbereich Einfluss nehmen können. Deshalb haben wir unsere Tätigkeitsstrategie in den letzten Jahren grundlegend geändert.

Als erstes beschlossen wir, den Teil unserer Tätigkeiten, bei dem wir reagieren müssen (Registrierung, Bearbeitung von Informationsfragen und Prüfung von Beschwerden), zu rationalisieren, um den Umfang der von uns in Eigeninitiative eingeleiteten Kontrollen und anderer proaktiver Maßnahmen ausweiten zu können. Nachstehend einige Beispiele;

- 2008 bis 2009 starteten wir eine groß angelegte Aktion, die für die Verarbeitung sensibler personenbezogener Daten zuständige Personen aufforderte, die Meldungspflicht einzuhalten, mit dem Ergebnis, dass in diesem Bereich heute weniger Kontrollen erforderlich sind;
- eine Telefon-Hotline reduziert die Arbeitslast, da die Beantwortung einfacher Fragen per Telefon weniger zeitintensiv ist als schriftliche Korrespondenz;
- für weniger komplizierte Probleme haben wir ein vereinfachtes Kontrollverfahren eingeführt;
- was das Reagieren auf Verstöße betrifft, arbeiten wir mit risikobasiert abgestuften Maßnahmen.

Dadurch, dass wir den Umfang der „reaktiven Tätigkeiten" unter Kontrolle bekommen haben, können wir heute strategisch regulierend agieren:

- wir intervenieren auf eigene Initiative, wenn ein erhöhtes Risiko besteht und die Intervention größere Auswirkungen hat;
- wir setzen neue Formen der Überwachung ein: umfangreiche vergleichende Kontrollen und Audits, die es uns ermöglichen, das Gesamtbild zu erfassen;
- anstelle von „Einzelschulungen" konzentrieren wir uns auf die Ausarbeitung von Richtlinien und „Schulungen en gros";
- wir verbessern die Effizienz der Kooperation;
- wir verbessern die Effizienz unserer Medienarbeit.

Ein Teil der Aktivitäten der AKI der letzten Jahre ist der nachstehenden Tabelle zu entnehmen. Der Umfang der Aufklärungs- und Beratungstätigkeit (Bearbeitung von Informationsfragen, Hotline) hat sich, verglichen mit den Indikatoren der vergangenen Jahre, stabilisiert. Die Zahl der Beschwerden und Klagen hat sich allerdings verdoppelt. Unserer Erachtens wurde diese Zunahme nicht durch eine plötzliche Abwärtsentwicklung im Bereich des Informationsrechts verursacht, sondern dadurch, dass die Menschen besser über ihre Rechte informiert sind.

Die Zahl der Entscheidungen hat sich nahezu verdreifacht; bedingt ist dies durch die gestiegene Zahl der Beschwerden und Klagen, aber auch die neue Form der Überwachung – vergleichende Kontrollen. Zig bzw. Hunderte von Kontrollobjekten werden in einer Kontrollsitzung geprüft, und auf schwerwiegende Versäumnisse reagieren wir mit Empfehlungen und Entscheidungen. 2009 fanden drei Kontrollsitzungen statt, 2010 waren es sechs solcher Sitzungen.

Eine weitere neue Form der Kontrolle sind Compliance- und Angemessenheitsprüfungen, die wir 2010 viermal durchführten. Diese Audits geben uns ein umfassendes Bild bezüglich der Einhaltung der Datenschutzanforderungen bei großen und mit sensiblen Daten arbeitenden Systemen. Für die Durchführung dieser Audits verwenden wir international übliche Methoden.

Bis Ende Januar 2010 wurde die Verarbeitung sensibler personenbezogener Daten verstärkt per Internet gemeldet. Automatische Fehlerfilter und Standardformulare je nach Art der Meldung vereinfachen das Verfahren für den Sender wie auch für den Empfänger. Auch die Verfügungen an diejenigen, die die Meldungspflicht ignorieren, sind standardisiert. Deshalb haben wir die Meldungsbearbeitung an unsere Verwaltungsabteilung abgetreten; so können sich unsere Hauptabteilungen auf spezifischere Aktivitäten konzentrieren.

Im letzten Jahr haben wir im Bereich Schutz personenbezogener Daten und Aufklärung der Öffentlichkeit fünf Leitfäden vorgelegt: Publication of Default of Payment Data (Veröffentlichung von Zahlungsausfalldaten), The Use of Personal Data in Election Campaigns (Verwendung personenbezogener Daten in Wahlkampagnen), Transfer of Personal Data to a Foreign Country (Übermittlung personenbezogener Daten ins Ausland), Private Legal Persons as Holders of Information (Leitfaden für den Besitz von Informationen seitens Personen des Privatrechts) und The kind of Information which may be Published (Leitfaden zur Frage, welche Art von Daten veröffentlicht werden dürfen.

Organisation	
Vorsitz und/oder Gremium	Dr Viljar Peep
Budget	551 190 EUR
Personal	17 Amtsmitarbeiter/-innen
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	5 Richtlinien im Bereich Datenschutz und Informationsfreiheit
Meldungen	468 Meldungen zur Verarbeitung sensibler personenbezogener Daten
Vorabprüfungen	k.A.
Anträge betroffener Personen	893 schriftliche Anträge und 1 061 telefonische Anfragen
Beschwerden betroffener Personen	592 Beschwerden und Klagen
Vom Parlament bzw. der Regierung angeforderte Beratung	21 Stellungnahmen zu Gesetzentwürfen
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	139 Genehmigungen für Datenbanken im öffentlichen Sektor
Prüfmaßnahmen	
Prüfungen, Untersuchungen	5 vergleichende Kontrollen, 6 Audits und 58 vor-Ort-Prüfungen
Sanktionsmaßnahmen	
Sanktionen	203 Verfügungen 35 Verfahren wegen Verstößen
Geldbußen	15 von der AKI verhängte Geldbußen und Ordnungsstrafen – Gesamtbetrag 13 470 EUR

Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	2010 wurden 156 Datenschutzbeauftragte ernannt

B. Rechtsprechung

Thema Privatsphäre in Beschäftigungsverhältnissen

Das Hauptaugenmerk der AKI lag in den letzten Jahren auf dem Thema personenbezogene Daten von Beschäftigten. Hierunter fällt die Erfassung und Verwendung der Daten von Arbeitsuchenden, Beschäftigten und ehemaligen Mitarbeiter/-innen sowie die Überprüfung von Beschäftigten durch Background-Checks.

Gesetzliche Grundlage hierfür ist das estnische Arbeitsvertragsgesetz, das vorschreibt, dass ein Arbeitgeber im Rahmen der Vorbereitung von Arbeitsverträgen Informationen von Personen nur einholen darf, wenn der Arbeitgeber ein berechtigtes Interesse an diesen hat. Während des Beschäftigungsverhältnisses muss der Arbeitgeber die Privatsphäre seiner Beschäftigten respektieren und darf die Erfüllung ihrer Aufgaben nur so überprüfen, dass die Grundrechte des/der Beschäftigten nicht verletzt werden. Darüber hinaus beinhaltet das Estnische Gesetz über den Schutz personenbezogener Daten allgemeine Grundsätze hierzu (Eingrenzung des Verwendungszwecks, Verhältnismäßigkeit etc.)

Dies sind allerdings nur die allgemeinen Grundsätze. Als wir begannen, deren Umsetzung in die Praxis zu beraten, war die einzige mehr oder weniger eindeutige und einstimmige Meinung, dass Beschäftigte in Toiletten- und Duschräumen nicht per Kamera überwacht werden dürfen.

Im Laufe der Beratungen kamen Hunderte praktischer Fragen auf: Wie dürfen Background-Checks über Arbeitsuchende und Beschäftigte durchgeführt werden? Wer darf E-Mail-Nachrichten lesen, die den Namen des/der Beschäftigten und den Domain-Namen des Arbeitgebers beinhalten? Wie darf die Gesundheit von Beschäftigten überprüft werden? Wie verhält es sich mit dem Thema Überwachung von Beschäftigten per Videokamera etc.?

Außerdem gab es Unstimmigkeiten bezüglich grundlegender Fragen zur Gesetzestheorie, beispielsweise: Wann ein Arbeitgeber die personenbezogenen Daten eines/einer Beschäftigten auf Grundlage der (widerrufbaren) Zustimmung des/der Betreffenden verarbeitet, und wann dies geschehen darf, um die Einhaltung des Arbeitsvertrages zu gewährleisten?

Wir stellten fest, dass es keine gesetzliche Grundlage gab, auf der wir einfache Schlussfolgerungen hätten ziehen können. Es gab in Estland keine bereits durchgeführten grundlegenden rechtlichen Analysen, da die Rechtsliteratur nur einige wenige Aspekte abdeckte und die nationale Rechtsprechung noch weniger hergab. Letztendlich beschlossen wir, das Thema Schutz der Privatsphäre in Beschäftigungsverhältnissen auf unserer jährlichen Konferenz am 27. Januar 2010 und anschließend an einem runden Tisch mit Arbeitgebern und den wichtigsten Arbeitnehmervertreterorganisationen, an dem noch andere Stellen und Experten teilnahmen, zu erörtern. Die endgültige Fassung Isikuandmete töötlemine töösuhetes (Verarbeitung personenbezogener Daten in Beschäftigungsverhältnissen) lag schließlich am 24. Januar 2011 vor.

C. Sonstige wichtige Informationen

Zusammenarbeit mit Betreibern von Datenbanken

Seit 2010 hat die AKI ihre Zusammenarbeit mit den größten für die Verarbeitung von Daten und den Betrieb von Datenbanken zuständigen Anbietern in Estland verstärkt. Je sensibler die in einer Datenbank enthaltenen Daten, desto strenger die internen Kontrollmaßnahmen, die der Betreiber einer Datenbank bei der Verwendung der betreffenden Daten vorzusehen hat. So ist zum Beispiel die interne Kontrolle der Verwendung des Bevölkerungsregisters relativ effizient – die AKI wird über jeden verdächtigen Fall oder Missbrauch informiert.

Die Verwaltung von Datenbeständen, unter anderem die Zuteilung von Zugangsrechten, wurde nach der Zusammenlegung der beiden Behörden zentral dem Polizei- und Grenzschutzamt unterstellt, und das interne Kontrollsystem wurde effizienter gestaltet. Die AKI rät anderen Behörden, die große und sensible Daten beinhaltende Datenbanken betreiben, sich mit der Einrichtung eines vergleichbaren Systems zu befassen.

Für Personen, die die Polizeidatenbank missbräuchlich nutzen, wurde eine Nulltoleranz-Regelung eingeführt; im Falle einer missbräuchlichen Verwendung drohen disziplinarische Maßnahmen und ein Ordnungswidrigkeitsverfahren. Zwischen der Polizei und der AKI findet diesbezüglich ein regelmäßiger Datenaustausch statt. Dies hat spürbare positive Veränderungen innerhalb der Organisation mit sich gebracht.

Darüber hinaus haben wir ein mit der internen Kontrolle der oben genannten Datenbanken vergleichbares Kooperationsprogramm im Bereich E-Gesundheit gestartet.

FINNLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Büro des Datenschutzbeauftragten befasste sich proaktiv mit einer drastischen Veränderung unseres operativen Umfeldes. Die Aufgaben des Büros nehmen ständig zu, während das nationale Programm zur Steigerung der Produktivität unsere Ressourcen gekürzt hat. Wir haben unser umfassendes System der Beratung, Planung und Überwachung verbessert, um seine Effizienz zu erhöhen. Um das Engagement aller Mitarbeiter/-innen zu gewährleisten, haben wir gemeinsam unsere Vision, unseren operativen Plan sowie unsere Werte und unsere Strategie erneuert. Unsere Vision legt unsere Ziele dar, unser operativer Plan definiert die Art unserer Tätigkeit, unsere Werte dienen als Leitfaden für unsere Entscheidungsfindung, und unsere Strategien bestimmen die Mittel, die wir verwenden.

Entsprechend unseren Zielen lag der Schwerpunkt der Tätigkeit des Büros auf Präventivmaßnahmen. Um Einfluss auf die Öffentlichkeit zu nehmen, lag der Schwerpunkt unserer Arbeit auf der Bereitstellung angemessener Beratung und Anleitung sowie der Mitarbeit in Arbeitsgruppen und Ausschüssen, die im Bereich Datenschutz von Bedeutung sind. Wir sind an etwa 80 verschiedenen Arbeitsgruppen beteiligt.

Datenverwaltung war das zentrale Thema unserer Tätigkeiten im Bereich Beratung. Finnland hat ein spezielles Finanzdateninformationsverfahren eingeführt, das die Geschäftsführung von Unternehmen bei ihren Verwaltungs- und Bilanzierungstätigkeiten unterstützt und es dem Datenschutzbeauftragten gleichzeitig ermöglicht, Maßnahmen zur Durchsetzung von Rechtsvorschriften effizienter durchzuführen.

In Finnland gibt es zusätzlich zum Europäischen Datenschutztag einen gesonderten Datensicherheitstag, der Teil der nationalen Strategie zur Informationssicherheit ist. Er soll dazu dienen, die Bürgerinnen und Bürger stärker für Sicherheitsbedrohungen zu sensibilisieren und ihr Wissen über die Mittel zur Bekämpfung von Bedrohungen sowie die Möglichkeiten von Datensubjekten, ihre Rechte zu schützen, zu verbessern.

Unser Büro hat eng mit zahlreichen Interessengruppen zusammengearbeitet. Verschiedene Lenkungsausschüsse zum Thema Datenschutz waren unter anderem in den Bereichen öffentliche Gesundheitsfürsorge, Sozialfürsorge, Telekommunikation und Bildung tätig. Außerdem wurde im Laufe des Jahres ein gemeinsamer Lenkungsausschuss des Datenschutzbeauftragten für das Büro- und Geschäftswesen eingerichtet, dessen Schwerpunkt auf aktuellen Datenschutzfragen im Bereich Marketing- und Kundenbeziehungsmanagement lag. Zudem haben die ersten vom privaten Sektor organisierten Netzwerke von Datenschutzexperten ihre Tätigkeit aufgenommen.

Ein vom Parlament verabschiedetes Gesetz zur elektronischen Identifizierung ist in Kraft getreten. Gleichzeitig schlug die Sondergruppe Identitätsverwaltung in Zusammenarbeit mit dem Innenministerium vor, den Tatbestand des Identitätsdiebstahls unter Strafe zu stellen.

Schließlich wurde nach dem Urteil zu Steuerdaten und Massenmedien das Gesetz zum Schutz personenbezogener Daten zur Umsetzung der Datenschutzrichtlinie 95/46/EG auf Initiative des Justizministeriums geändert.

Die nachstehende Tabelle fasst die wesentlichen Daten des Büros des Datenschutzbeauftragten zusammen.

Organisation	
Vorsitz und/oder Gremium	Reijo Aarnio ist seit dem 1. November 1997 Datenschutzbeauftragter
Budget	Das Jahresbudget beläuft sich auf insgesamt 1 541 403 EUR
Personal	Die Personalstärke beträgt 20 Mitarbeiter/-innen
Allgemeine Aktivitäten	

Beschlüsse, Stellungnahmen, Empfehlungen	2 601
Meldungen	284
Vorabprüfungen	Siehe Meldungen
Anträge betroffener Personen	881
Beschwerden betroffener Personen	(Zugang und Korrekturen) 174
Vom Parlament bzw. der Regierung angeforderte Beratung	110
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Zusammenarbeit mit für die Datenverarbeitung Verantwortlichen in den folgenden Bereichen: Bildung, Gesundheitswesen, Sozialwesen, Telekommunikation, Beschäftigung und Wirtschaft.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	1 972
Sanktionsmaßnahmen	82
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	> 1 000
Zahlenangaben zu DPO	

B. Rechtsprechung

Privatsphäre

Der Oberste Gerichtshof verurteilte die Autoren des Buches *Die Braut des Premierministers* wegen der Verbreitung diffamierender Informationen über das Privatleben des Premierministers. Der Oberste Gerichtshof zog Autor und Verlag zur Verantwortung, da in dem Buch intime Details aus dem Privatleben des Premierministers sowie Informationen über private Veranstaltungen veröffentlicht wurden. Der Oberste Gerichtshof betonte, dass die Position einer Person als Premierminister sowie die Fähigkeit, erhebliche politische Macht auszuüben, üblicherweise einen enger gefassten Schutz des Privatlebens dieser Person mit sich bringt, jedoch auch das Privatleben eines führenden Politikers sowie insbesondere der intime Bereich seines Privatlebens nicht ungeschützt bleiben dürfe (Oberster Gerichtshof 2010.39).

Das Oberste Verwaltungsgericht hat ein Urteil hinsichtlich der Ergebnisse eines Eignungstests gefällt. Sowohl X als auch Y hatten sich um eine Stelle als Direktor beworben. Nachdem Y für die Stelle ausgewählt wurde, forderte X die

Ergebnisse des Eignungstests von Y an. X forderte die Informationen im Rahmen von Artikel 11 des Gesetzes über die Transparenz staatlichen Handelns an, da der Eignungstest von Y Auswirkungen auf die Klärung einer X betreffenden Angelegenheit gehabt haben könnte. X Informationen im Zusammenhang mit Ys Eignungstest zu geben, hätte dem obersten Verwaltungsgericht zufolge jedoch gegen ein wichtiges privates Interesse verstoßen. Das Oberste Verwaltungsgericht bezog sich auf den Vorschlag der Regierung, demzufolge die Veröffentlichung der Ergebnisse von Eignungstests im Widerspruch zum Menschenrecht auf Schutz der Privatsphäre steht (Oberstes Verwaltungsgericht 2010:60).

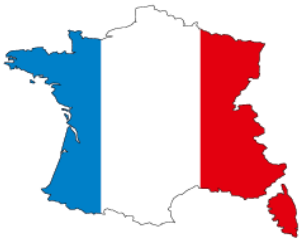
Datenschutz

Das Oberste Verwaltungsgericht fällte ein Urteil hinsichtlich des Rechts der Polizei auf Zugang zu Sozialversicherungsdaten, bei dem es um die von einer Person erworbenen Medikamente ging, die für die polizeiliche Untersuchung eines vermuteten Mordes verwendet werden sollten. Das Oberste Verwaltungsgericht genehmigte der Polizei den Zugang zu den Informationen gemäß Artikel 35 des Polizeigesetzes (Oberstes Verwaltungsgericht 2010:42).

Ein Antragsteller fragte bei der Datenschutzbehörde an, ob Informationen zur Reparaturhistorie von Kraftfahrzeugen als personenbezogene Daten gemäß Artikel 3 des Gesetzes über den Schutz personenbezogener Daten einzustufen sind. Der Antragsteller bat um die Genehmigung zur Verarbeitung dieser Informationen zur Erstellung einer neuen Datenbank, um die erfassten Informationen zu verarbeiten, zu pflegen und weiterzugeben. Die Datenschutzbehörde wies den Antrag ab, da die Verarbeitung nicht den Genauigkeitsanforderungen entsprach, da falsche, unvollständige oder veraltete Daten verarbeitet werden könnten. Zudem war auch die Anforderung der Exklusivität des Zwecks nicht erfüllt, da diese zusätzliche Verarbeitung vor der Erfassung der Daten nicht definiert wurde. Laut Datenschutzbehörde sind Kraftfahrzeug-Kennzeichen als personenbezogene Daten einzustufen (Datenschutzbehörde 2/932/2009).

Das Verwaltungsgericht Turku bestätigte im Rahmen des Falls zu Steuerdaten und Massenmedien (Veropörssi) die Entscheidung der Datenschutzbehörde hinsichtlich des Verbots der Verarbeitung und Weitergabe von Daten zu Erwerbs- und Kapitaleinkünften natürlicher Personen durch einen SMS-Dienst (Verwaltungsgericht Turku 10/0846/2).

FRANKREICH



A. Zusammenfassung der Aktivitäten und Neuerungen

Die Jugendlichen – prioritäre Zielgruppe der CNIL

Jugendliche sind die Hauptakteure der digitalen Welt von heute und morgen. 2010 erklärte die CNIL die Sensibilisierung von Jugendlichen und Fachleuten des Bildungssektors zu einer ihrer Prioritäten.

Deshalb unternahm sie die bislang größten Anstrengungen in Bezug auf diese Zielgruppen und wendete über 500.000 EUR für eine Aktion auf, die vor allem der Veröffentlichung von zwei Sonderausgaben von Zeitungen für die Altersgruppen von 10–14 und von 14–18 Jahren diente und der Frage des Datenschutzes im Internet gewidmet war.

Die CNIL – eine Behörde mit pragmatischem Ansatz

In der Überzeugung, dass die Verbreitung der Datenschutzkultur mit einem verbesserten Nutzerservice einhergeht, bietet die CNIL ab jetzt die Möglichkeit, die vorab zu erledigenden Formalitäten online abzuwickeln oder auch direkt online Beschwerden einzureichen. Heute werden bereits knapp 20 % der Beschwerden elektronisch an die CNIL übermittelt.

Zudem hat die CNIL eine sehr aktive Kontrollpolitik umgesetzt.

So stieg 2010, während der Rechtsrahmen für die Kontrollen präzisiert wurde[6], die Anzahl der durchgeführten Kontrollen auf 308, gegenüber 270 im Vorjahr. Besondere Aufmerksamkeit galt den Kontrollen von Videoüberwachungsvorrichtungen, die unter das französische Datenschutzgesetz fallen. An diesen Vorrichtungen wurden 55 Kontrollen durchgeführt. Dabei wurden zahlreiche Versäumnisse festgestellt, die insbesondere fehlende Hinweise, unverhältnismäßige Datenverarbeitung, eine übermäßig lange Aufbewahrung der Aufzeichnungen und mangelnde Informationen oder Sicherheit betrafen.

Darüber hinaus ist die CNIL eine Behörde, die es verstanden hat, die Empfehlungen und Beratungen den neuen Problemstellungen anzupassen, die durch Online-Spiele, Online-Wahlen oder IT-Tools zur administrativen und pädagogischen Verwaltung von Schülern aufgetreten sind.

Dieser Pragmatismus und die Bestrebung, so nahe wie möglich an der tatsächlichen Internetnutzung zu sein, wird gestützt durch die Arbeit des Expertendienstes der CNIL, dessen Mitarbeiterzahl erhöht wurde und der die jüngsten Entwicklungen im Bereich Neue Technologien verfolgt; auf diese Weise ist die CNIL in der Lage, neue Problemlagen im Vorfeld zu erkennen und Unternehmen entsprechend zu beraten.

Die CNIL – eine zukunftsorientierte Behörde

Um die Entwicklungen besser feststellen und vorhersehen zu können und sich der enormen Entwicklung im Bereich Neue Technologien zu stellen, die Auswirkungen auf den Schutz personenbezogener Daten haben könnte, wurde innerhalb der CNIL eine neue Direktion eingerichtet: die Direction des Etudes, de l'Innovation et de la Prospective (DEIP).

In diesem Bestreben, Einfluss auf die künftige Entwicklung des Datenschutzes zu nehmen, war die CNIL im Rahmen der Überprüfung der Richtlinie 95/46 besonders aktiv.

[6] Vergleiche hierzu die beiden Entscheidungen des Conseil d'Etat Nr. 304300 und N. 304301 vom 6. November 2009 – der Staatsrat beschloss, die beiden von der CNIL ausgesprochenen Sanktionen mit der Begründung aufzuheben, dass die Kontrollen vor Ort, auf deren Grundlage diese Sanktionen erlassen wurden, unrechtmäßig waren, weil die für die Datenverarbeitung Zuständigen nicht informiert worden waren. Infolgedessen musste die CNIL ihre Praktiken ändern und informiert seitdem regelmäßig die Personen, die Gegenstand einer Kontrolle vor Ort sind, über ihr Einspruchsrecht in Bezug auf diese Kontrolle.

Organisation	Commission Nationale de l'Informatique et des Libertés – CNIL (Frankreich)
Vorsitz und/oder Gremium	Vorsitzender: Alex Türk.
Budget	Stellvertretende Vorsitzende: Isabelle Falque-Pierrotin, Emmanuel de Givry.
Personal	Zusammensetzung des Gremiums: 4 Mitglieder des Parlaments/ 2 Mitglieder des Wirtschafts- und Sozialrates/ 6 Richter des Obersten Verwaltungsgerichtes/ vom Kabinett (3), dem Vorsitzendender Nationalversammlung (1) und dem Vorsitzenden des Senats (1) benannte qualifizierte Personen.
Allgemeine Aktivitäten	Gesamtbudget für 2010: 14,7 Millionen EUR
Beschlüsse, Stellungnahmen, Empfehlungen	Personalstärke: 148
Meldungen	
Vorabprüfungen	1 659 Beschlüsse/ Stellungnahmen/ Empfehlungen
Anträge betroffener Personen	Bei der CNIL gingen 68 863 Meldungen ein
Beschwerden betroffener Personen	Genehmigungsanträge: 1 682 Genehmigungsanträge und 4 273 Genehmigungsanträge mit der Verpflichtung von für die Datenverarbeitung Verantwortlichen zur Einhaltung einer Einzelgenehmigung der CNIL.
Vom Parlament bzw. der Regierung angeforderte Beratung	
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Genehmigungen: 1 346 Genehmigungen und 4 273 Genehmigungen nach Bestätigung seitens der für die Datenverarbeitung Verantwortlichen, einer Einzelgenehmigung der CNIL einzuhalten.
Prüfmaßnahmen	Anträge der Öffentlichkeit: 28 490 schriftliche Anträge und 10 000 Anrufe pro Monat.
Prüfungen, Untersuchungen	Anträge von Datensubjekten: 1 877 Anträge auf indirekten Zugang in Fällen, in denen die Verarbeitung die Sicherheit oder Verteidigung des Staates oder die öffentliche Sicherheit betraf.
Sanktionsmaßnahmen	4 821 Beschwerden von Datensubjekten (Arbeit: 20 %, Bankwesen: 20 %, Wirtschaft: 20 %, Internet/Telekommunikation: 20 %, Gesundheits-/Sozialwesen: 5 %, Sonstige: 15%).
Sanktionen	8 Stellungnahmen zu Verordnungen.
Geldbußen	78 Stellungnahmen zur Verarbeitung von Daten im Namen des Staates.
Datenschutzbeauftragte (DPO)	500 000 EUR für eine Kampagne zur Sensibilisierung der Öffentlichkeit
Zahlenangaben zu DPO	

DEUTSCHLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Auch nach der Novellierung des Bundesdatenschutzgesetzes (BDSG) 2009 wurde die Diskussion um die nötige Modernisierung des Datenschutzrechts in Deutschland fortgesetzt. Im März 2010 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Eckpunktepapier „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ verabschiedet. Das Eckpunktepapier dient als Beitrag zur Diskussion über eine Reform des nationalen Datenschutzrechts und enthält wichtige Grundprinzipien für eine Modernisierung des Datenschutzrechts.

Einzelne Änderungen des BDSG traten 2010 in Kraft:

- Mit Bezug auf Auskunfteien und das Ermitteln von Scoring-Werten gelten seit 1. April 2010 verbesserte Datenschutzregeln (§ 28b BDSG), die nun genauer festlegen, welche personenbezogenen Daten über eine Forderung an eine Auskunftei übermittelt werden dürfen. Zudem werden erstmals die Bedingungen für die Anwendung und Durchführung eines Scoring-Verfahrens gesetzlich definiert. Die Auskunftsansprüche der Betroffenen wurden gestärkt: insbesondere besteht nun ein Anspruch auf kostenlose Auskunft, welche Scorewerte an Dritte übermittelt worden sind und wie der individuelle Score-Wert zustande gekommen ist.
- Durch die am 11. Juni 2010 in Kraft getretene Umsetzung der Verbraucherkreditrichtlinie sichert das BDSG nunmehr die Gleichbehandlung von europäischen Darlehensgebern beim Zugang zu inländischen Auskunfteisystemen (§ 29 Abs. 6 BDSG).
- Für mehr Transparenz sorgt die neue Regelung, wonach der Verbraucher unverzüglich unterrichtet werden muss, wenn im Zusammenhang mit Verbraucherdarlehensverträgen oder Verträgen über eine entgeltliche Finanzierungshilfe sein Vertragsangebot wegen einer (negativen) Auskunfteiabfrage abgelehnt wird (§ 29 Abs. 7 BDSG).

Im Berichtsjahr haben fast alle Bundesländer entsprechende Aktivitäten eingeleitet, um die vom EuGH (Urteil vom 9. März 2010 – C-518/07) geforderte völlige Unabhängigkeit der Datenschutzaufsicht im nicht-öffentlichen Bereich umzusetzen In der weit überwiegenden Anzahl der Länder ist vorgesehen, die Aufsicht über den nicht-öffentlichen Bereich auf den Landesdatenschutzbeauftragten zu übertragen, sofern dies nicht bereits geschehen ist. Die Exekutive soll keinerlei Einfluss auf die Datenschutzbehörden ausüben. Daher müssen die Datenschutzbehörden auch die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation besitzen. Offen ist hingegen, inwieweit aus dem EuGH-Urteil Konsequenzen für die Stellung des BfDI gezogen werden. Auch wenn sich das Urteil explizit nur auf die Datenschutzaufsicht in den Ländern bezieht, sind die darin betonten Grundsätze auch in Bezug auf die Datenschutzkontrolle auf Bundesebene anwendbar.

Wie in den Jahren zuvor konnte auch in 2010 ein starker Anstieg der Aufgaben und des Arbeitsanfalls verzeichnet werden: So stieg etwa die Zahl der Eingaben, die meine Dienststelle erreichten, von 5066 im Jahr 2009 auf 6087 im Jahr 2010. Daher ist es umso erfreulicher, dass meine Dienststelle mit dem Haushaltsjahr 2010 12,5 neue Personalstellen erhalten hat. Dadurch stieg die Anzahl der Mitarbeiterinnen und Mitarbeiter von 69 auf 81. Das zusätzliche Personal ermöglicht es meiner Dienststelle, die bestehenden gesetzlichen Aufgaben der datenschutzrechtlichen Kontrolle und Beratung besser zu bewältigen und neue Aufgaben proaktiv aufzugreifen. So konnte insbesondere die Kompetenz im technologischen Datenschutz ausgebaut sowie meine Kontroll-und Aufsichtsarbeit gestärkt werden. Nicht zuletzt habe ich mein Informationsangebot für die Öffentlichkeit ausgebaut, z.B. durch neue themenbezogene Flyer oder durch einen kurzen Film auf meiner Internet-Seite über die Bedeutung des Datenschutzes und über die Aufgaben meiner Dienststelle.

Nähere Einzelheiten zu meinen Aktivitäten im Berichtsjahr 2010 können meinem 23. Tätigkeitsbericht, der die Jahre 2009 und 2010 abdeckt, entnommen werden. Diesen Tätigkeitsbericht finden Sie auf meiner Internet-Seite unter

http://www.bfdi.bund.de/DE/Oeffentlichkeitsarbeit/Taetigkeitsberichte/TB_node.html und meine Presseerklärung hierzu in englischer Sprache unter

http://www.bfdi.bund.de/EN/PublicRelations/PressReleases/2011/23rdActivityReport.html?nn=410156

Hinweis: In Deutschland gibt es nicht nur den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der als oberster Datenschutzexperte fungiert. Auf der Ebene der Bundesländer gibt es zusätzlich die Büros der Datenschutzbeauftragten der Länder sowie in einigen Ländern separate Aufsichtsbehörden für den privaten Sektor.

Die nachstehende Tabelle bezieht sich ausschließlich auf das Büro des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Organisation	
Vorsitz und/oder Gremium	Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)
Budget	6,5 Millionen EUR
Personal	81
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A.
Meldungen	k. A.
Vorabprüfungen	k. A.
Anträge betroffener Personen	13 257
Beschwerden betroffener Personen	6 087
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Im Dezember 2010 wurden die verbindlichen unternehmensinternen Vorschriften der Deutsche Post AG verabschiedet
Prüfmaßnahmen	
Prüfungen, Untersuchungen	52
Sanktionsmaßnahmen	
Sanktionen	30 Beschwerden (2009 und 2010) gemäß Artikel 25 des Bundesdatenschutzgesetzes
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Decision of the Federal Constitutional Court on the retention of telecommunications traffic data:

Already in 2008, through two decisions in the provisional legal protection proceedings, the Federal Entscheidung des Bundesverfassungsgerichts zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten:

Bereits im Jahr 2008 schränkte das Bundesverfassungsgericht mit zwei Beschlüssen im einstweiligen Rechtsschutzverfahren die Nutzung der auf Vorrat gespeicherten Daten stark ein. Mit Urteil vom 02.03.2010 erklärte das Bundesverfassungsgericht die gesetzlichen Vorschriften zur Vorratsdatenspeicherung für verfassungswidrig und dementsprechend nichtig. Damit war die mit über 35.000 Beschwerdeführern größte Massenverfassungsbeschwerde in der Geschichte der Bundesrepublik Deutschland erfolgreich.

Während das Gericht einerseits das deutsche Umsetzungsgesetz als verfassungswidrig aufhob, führte es in diesem Zusammenhang andererseits aus, dass eine anlasslose Speicherung von personenbezogenen Daten über einen Zeitraum von sechs Monaten auf Vorrat lediglich dann strikt verboten sei, wenn sie zu unbestimmten und noch nicht bestimmbaren Zwecken erfolgte. Eine verfassungsgemäße Umsetzung der europäischen Richtlinie zur Vorratsdatenspeicherung wäre somit grundsätzlich möglich. Sie unterliege allerdings sehr strengen Anforderungen, da der mit der Vorratsdatenspeicherung verbundene Eingriff in das Fernmeldegeheimnis als äußerst schwerwiegend bewertet wurde.

Im Hinblick auf eine mögliche Neuregelung des Gesetzes benannte das Gericht vier Bereiche, die zur verfassungsgemäßen Ausgestaltung einer Vorratsdatenspeicherung beachtet werden müssten. Neben einem hohen Standard der Datensicherheit, hinreichender Transparenz und einem effektiven Rechtsschutzsystem müsse der Gesetzgeber vor allem auch klare Regelungen zum Umfang der Datenverwendung gesetzlich vorschreiben.

Darüber hinaus stellte das Gericht noch generell fest, dass vorsorglich anlasslose Datenspeicherungen grundsätzlich eine Ausnahme bleiben müssten und – insbesondere auch zusammen mit anderen bereits bestehenden Datensammlungen – nicht zu einer Rekonstruierbarkeit praktisch aller Aktivitäten der Bürger führen dürften. Hierfür müsse sich die Bundesrepublik Deutschland auch im europäischen und internationalen Zusammenhang einsetzen.

Fundstellen:

http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html (Urteil in Deutsch)
http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011.html (Pressemitteilung in Deutsch)
http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10-011en.html (Pressemitteilung in Englisch)"

Der Ankauf von Steuerdaten-CD, die aus "zwielichtigen Quellen" im Ausland stammen und Informationen zu mutmaßlichen deutschen Steuerhinterziehern enthalten, durch die deutschen Finanzbehörden hat im Berichtszeitraum zu einer kontroversen Diskussion geführt. Inzwischen hat das Bundesverfassungsgericht entschieden, dass der Anfangsverdacht für weitere steuerrechtliche Ermittlungen auf Daten aus einer durch deutsche Behörden angekauften Steuerdaten-CD gestützt werden kann. In dem durch das Gericht zu entscheidenden Fall hatte ein Informant aus Lichtenstein eine CD-Rom mit Informationen zu mutmaßlichen Steuersündern an den Bundesnachrichtendienst verkauft, die dieser den Finanzbehörden zur Verfügung stellte (vgl. BVerfG, Beschluss vom 9. November 2010, 2 BvR 2101/09).

C. Sonstige wichtige Informationen

Datenschutzkonformer Umgang mit Internet-Geodaten

Als Reaktion auf die anhaltenden Diskussionen über den Internet-Geodatendienst Google Street View hat die Internetwirtschaft unter Federführung des Branchenverbands BITKOM im Dezember 2010 einen Datenschutzkodex vorgelegt, der den Interessen der Eigentümer und Bewohner bei der Veröffentlichung von Gebäudeansichten im Internet Rechnung tragen soll. Der Kodex ist nicht mit den deutschen Datenschutzbehörden abgestimmt und aus datenschutzrechtlicher Sicht unzureichend, weil die Selbstverpflichtung der Internetwirtschaft lediglich ein Widerspruchsrecht nach der Veröffentlichung der Gebäudeansichten im Internet vorsieht und nur für die Unternehmen bindend ist, die den Kodex unterzeichnet haben. Die Datenschutzbehörden halten hingegen ein Widerspruchsrecht vor der Veröffentlichung für notwendig und haben zudem gefordert, dass der Kodex nicht nur Ansichten aus der Straßenperspektive, sondern auch Schrägaufnahmen aus der Luft umfasst. Die Datenschutzbehörden haben daher den Gesetzgeber zur Tätigkeit aufgefordert.

Das neue Personalausweisgesetz

Mit Inkrafttreten des geänderten Personalausweisgesetzes am 01. November 2010 wurde der neue Personalausweis in Deutschland eingeführt. Dieser verfügt über die Besonderheit, dass er neben der Erfüllung hoheitlicher Funktionen als elektronischer Identitätsnachweis genutzt werden kann. Er ist mit einem Chip ausgestattet, der abgeschottete Bereiche für die zu hoheitlichen Zwecken gespeicherten Biometrie- und Identifizierungsdaten, für eine elektronische Signatur und für die elektronische Identitätsfunktion (eID-Funktion) enthält. Die Nutzung der eID-Funktion sowie der elektronischen Signatur ist freiwillig, auch die zusätzliche Speicherung von Fingerabdrücken neben einem obligatorischen Lichtbild entscheidet der Ausweisinhaber selbst.

Aus datenschutzrechtlicher Sicht positiv an dem neuen Personalausweis ist insbesondere die Möglichkeit, mittels eines dienste- und kartenspezifischen Kennzeichens sicher und pseudonym Angebote im Internet nutzen zu können.

RFID (Radio Frequency Identification)

Um beim Einsatz von RFID Datenschutzbedrohungen zu untersuchen, wurde auf europäischer Ebene ein Konzept zur Datenschutzfolgenabschätzung – Privacy Impact Assessment (PIA) – entwickelt, bei dessen Entwicklung sich auch die Deutsche Industrie beteiligt hat. Zukünftig sollen PIA Reports von der RFID einsetzenden Industrie, dem Handel und der Wirtschaft erstellt und den nationalen Aufsichtsbehörden vor Inbetriebnahme zur Prüfung vorgelegt werden. Das hierbei erstellte PIA wurde im April 2011 offiziell durch die europäische Kommission angenommen.

Ferner hat das Bundesamt für Sicherheit in der Informationstechnik ein neues Grundlagendokument zu Datensicherheit und Datenschutz bei RFID-Anwendungen veröffentlicht. Das Werk erläutert die komplementäre Bedeutung der Technischen Richtlinien für den sicheren RFID-Einsatz des BSI und des PIA Framework der Europäischen Kommission.

GRIECHENLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Jahr 2010 wurde nach zweijährigen Bemühungen mittels Beschluss des stellvertretenden Finanzministers eine progressive Erhöhung der Personalstärke um 25 Mitarbeiter/-innen (19 Rechtsanwälte und IT-Experten sowie 6 Verwaltungsbeamte) über einen Zeitraum von drei Jahren genehmigt. Allerdings besteht aufgrund der aktuellen finanziellen Situation des Staates das Risiko, dass diese Erhöhung lediglich auf dem Papier stehen bleibt. Aus diesem Grund kann die griechische Datenschutzbehörde (HDPA) die zahlreichen von Bürgerinnen und Bürgern sowie von für die Datenverarbeitung Verantwortlichen eingereichten Anträge weiterhin nicht zeitnah bearbeiten.

Die einzige realistische Lösung für die HDPA, angesichts der aktuellen Umstände effektiv zu arbeiten, ist die Verfolgung zweier Hauptziele: Präventivmaßnahmen sowie die selektive Bearbeitung von Beschwerden und Anträgen. Im Hinblick auf das zweite Ziel wurde eine Änderung des Datenschutzgesetzes (Artikel 19 Absatz 1) verabschiedet, die es der HDPA ermöglicht, die zu bearbeitenden Fälle nach Wichtigkeit und allgemeinem Interesse des Falles zu priorisieren.

In Bezug auf das erste Ziel erklärte die HDPA das Jahr 2010 zum Jahr der Präventivmaßnahmen. Die HDPA veröffentlichte einen Leitfaden und entwarf zwei weitere (die Anfang 2011 veröffentlicht wurden), gab vier Stellungnahmen zu neuen Gesetzesvorschlägen heraus, veröffentlichte Pilotentscheidungen zu Angelegenheiten, mit denen sich für die Datenverarbeitung Verantwortliche aus verschiedenen Bereichen befassen, und führte *ex-officio*-Inspektionen der IT-Systeme zahlreicher wichtiger Krankenhäuser mit dem Zweck durch, um in naher Zukunft Leitlinien zu bewährten Verfahrensweisen zu veröffentlichen.

Die HDPA beriet die Regierung im Einzelnen mittels folgender Stellungnahmen und Entscheidungen: Stellungnahme 1/2010 (zur Veröffentlichung von Verwaltungsgesetzen im Internet aus Transparenzgründen, die personenbezogene Daten enthalten), Stellungnahme 2/2010 (zur Nutzung von Überwachungskameras zum Zweck der nationalen Sicherheit sowie zur Vorbeugung und Untersuchung von Straftaten), Stellungnahme 4/2010 (zur „e-card" zur elektronischen Speicherung von Kaufbelegen zu steuerlichen Zwecken), Entscheidung 43/2010 (zur Erfassung der Daten von Staatsbediensteten und zur Speicherung der relevanten Informationen auf einer Website der Regierung), Entscheidung 56/2010 (zur Aufnahme der Sozialversicherungsnummer – aus der das Geburtsdatum hervorgeht – von Ärzten und Apothekern auf Rezepten) usw.

Außerdem veröffentlichte die HDPA die folgende Stellungnahme und Pilotentscheidung: Stellungnahme 3/2010 (zur Eingabe der Daten von Ausländern in das Schengener Informationssystem und die Nationale Datenbank unerwünschter Ausländer) sowie Entscheidung 73/2010 (zum Recht des Beklagten auf Zugang zu den Identifikationsdaten des Klägers bei Einreichung einer Klage bei einer öffentlichen Behörde). Die ebenfalls verfasste Leitlinie 1/2010 befasst sich mit der Verarbeitung personenbezogener Daten zum Zweck der politischen Kommunikation.

Am Europäischen Datenschutztag veranstaltete die HDPA verschiedene Aktivitäten. Ein Informationskiosk vor den Geschäftsräumen der HDPA diente der Behörde dazu, auf das Thema Datenschutz und ihre Arbeit aufmerksam zu machen, die Bürgerinnen und Bürger mit der Nutzung ihrer Website vertraut zu machen, Informationsmaterial zu verteilen und verschiedene Video-Clips zu zeigen, unter anderem den norwegischen Beitrag zur Kampagne „Deine Entscheidung". Zwei Informationsbroschüren wurden erstellt und verteilt, eine zu allgemeinen Grundsätzen des Datenschutzes und eine zu unerbetenen Nachrichten. Außerdem wurde ein Poster für die Veranstaltung gestaltet, das die Aufmerksamkeit der Bürgerinnen und Bürger auf Situationen lenken sollte, in denen sie nach ihren personenbezogenen Daten gefragt werden. Schließlich organisierte die HDPA eine Pressekonferenz, um wichtige aktuelle Fragen zum Thema Datenschutz wie z. B. rechtliche Entwicklungen, soziale Netzwerke und Straßenansichtsdienste zu erläutern.

Der Justizminister richtete auf Antrag des griechischen Parlaments einen Gesetzgebungsausschuss ein, der die potenzielle Zusammenlegung unabhängiger Behörden mit ähnlichen Verantwortungsbereichen sowie die Verbesserung ihres rechtlichen Status' gemäß den Bestimmungen von Gesetz Nr. 3051/2002 untersuchen soll.

Organisation	
Vorsitz und/oder Gremium	Christos Yeraris (Vorsitz)
Budget	2 923 500 EUR
Personal	Abteilung Audit: 16 Juristen und 11 IT-Experten (davon befinden sich 7 in Mutterschutz, und 2 wurden für einen Teil des Jahres als nationale Experten an europäische Gremien abgeordnet); Abteilung Kommunikation und Öffentlichkeitsarbeit: 6 (davon 1 zurückgetreten, 1 abgeordnet, 1 für ein halbes Jahr abgeordnet und 1 ein halbes Jahr lang in Mutterschutz); Abteilung Personal und Finanzen: 17 (davon 1 in Mutterschutz) und 1 von einem anderen öffentlichen Dienst abgeordnet.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die HDPA veröffentlichte 11 Entscheidungen, 4 Stellungnahmen und 1 Leitlinie, alle mit Auswirkungen auf den Bereich Datenschutz im Allgemeinen.
Meldungen	Die HDPA untersuchte 759 Meldungen (430 davon betrafen die Installation und den Betrieb von Überwachungskameras, 73 betrafen die Übermittlung von Daten in Länder außerhalb der EU).
Vorabprüfungen	Die HDPA bewilligte bzw. erneuerte 63 Genehmigungen zur Verarbeitung sensibler Daten, zur Verknüpfung von Akten sowie zur Datenübermittlung in Länder außerhalb der EU.
Anträge betroffener Personen	1 507 (Datensubjekte und für die Datenverarbeitung Verantwortliche)
Beschwerden betroffener Personen	674 (Strafverfolgungsbehörden und Ordnungsamt: 8, Verteidigungsministerium: 1, öffentliche Verwaltung und lokale Behörden: 32, Steuerwesen/Finanzministerium: 6, Gesundheitswesen: 17, Sozialversicherung: 31, Bildung und Forschung: 12, Bankwesen: 45, Privatwirtschaft: 208, elektronische Kommunikation: 97, Arbeitsbeziehungen: 45, Massenmedien: 9)
Vom Parlament bzw. der Regierung angeforderte Beratung	7 (Stellungnahme 1/2010, Stellungnahme 2/2010, Stellungnahme 3/2010, Stellungnahme 4/2010, Entscheidung 43/2010, Entscheidung 56/2010, Entscheidung 19/2010)
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	11 Prüfungen im Gesundheitswesen, 1 bei einem Sozialversicherungsfonds/einer Sozialversicherungsorganisation
Sanktionsmaßnahmen	

Sanktionen	8 Sanktionen (1 Verwarnung, 7 Geldbußen), verhängt vom Datenschutzbeauftragten in den folgenden Bereichen: Gesundheitswesen (1), Versicherungen (2), Bankwesen (1), Privatwirtschaft (2), Massenmedien (2)
Geldbußen	Beträge: 1 000 EUR – 10 000 EUR (insgesamt 29 500 EUR) verhängt von der HDPA
Datenschutzbeauftragte (DPO)	k. A.
Figures on DPOs	k. A.

B. Rechtsprechung

Leitlinie 1/2010

Die HDPA legte die Vorschriften für eine rechtmäßige Verarbeitung personenbezogener Daten zum Zweck der politischen Kommunikation fest. Die Leitlinie beinhaltet Regelungen bezüglich rechtmäßiger Quellen zur Erfassung von Daten sowie zu den zur politischen Kommunikation verwendeten Kanälen (Post/elektronische Form).

Stellungnahme 1/2010

Die HDPA veröffentlichte eine Stellungnahme zu einem Gesetzentwurf hinsichtlich der obligatorischen Veröffentlichung von Verwaltungsakten, die personenbezogene Daten enthalten, im Internet. Die Behörde forderte eine zeitliche Begrenzung der Veröffentlichung solcher Akte im Internet sowie technische Maßnahmen zur Verhinderung der Nutzung dieser Daten zu anderen Zwecken. Sie gelangte zu dem Schluss, dass Gesetze, die sensible Daten enthalten, nicht online veröffentlicht werden dürfen.

Stellungnahme 2/2010

Nach ihrer Stellungnahme 1/2010 formulierte die HDPA bestimmte Vorschläge für den Betrieb von Überwachungskameras an öffentlichen Plätzen zu Zwecken der nationalen Sicherheit, der Prävention und Untersuchung von Straftaten sowie der Verkehrsüberwachung. Die Vorschläge der HDPA flossen im Wesentlichen in Artikel 14 von Gesetz Nr. 3917/2011 ein. Ein Präsidialdekret soll die Kriterien und Schutzmechanismen für den Betrieb von Überwachungskameras zu den vorgenannten Zwecken weiter spezifizieren. Die HDPA ist an der Erarbeitung dieses Dekrets beteiligt. Anfang 2011 veröffentlichte die HDPA Leitlinie 1/2011 zum Betrieb von Überwachungskameras zu Zweck des Schutzes von Personen und Gütern.

Stellungnahme 3/2010

Bei der HDPA gehen jedes Jahr zahlreiche Beschwerden von Ausländern ein, die auf der Grundlage von Artikel 96 zum Übereinkommen zur Umsetzung des Schengener Abkommens eine Löschung aus dem Schengener Informationssystem (SIS) sowie der Nationalen Datenbank unerwünschter Ausländer (NRUA) beantragen. Aus diesem Grund und nach Rücksprache mit dem Ministerium für Bürgerschutz veröffentlichte die HDPA Stellungnahme 3/2010.

Stellungnahme 4/2010

Es wurde eine Stellungnahme zur Einrichtung eines optionalen Systems zur Registrierung der Kaufbelege von Steuerzahlern veröffentlicht, das dazu dienen sollte, die Steuerzahler hinsichtlich der Aufbewahrung dieser Belege für steuerliche Zwecke zu entlasten und gleichzeitig die Einhaltung der Steuergesetze auf Unternehmensseite zu prüfen. Grundlage ist eine neue Magnetkarte, die mit den vorhandenen Kartenterminals für Transaktionen via Bank- und

Kreditkarten kompatibel ist. Die HDPA forderte eine klare rechtliche Basis für diese Art der Verarbeitung, die eine optionale Nutzung des Systems seitens der Steuerzahler sicherstellt und die Einzelheiten der Verarbeitung definiert, um die Einschätzbarkeit der Bestimmungen zu gewährleisten. Darüber hinaus wurde die Notwendigkeit geeigneter Sicherheitsmaßnahmen betont, damit die als Auftragsverarbeiter agierenden Banken die Daten nicht für eigene Zwecke nutzen können.

Entscheidung 7/2010

Die HDPA wies einen Antrag des Verbandes der griechischen Autoverleiher hinsichtlich der Erstellung einer schwarzen Liste zahlungsunfähiger Kunden zurück, da a) das finanzielle Risiko nicht so groß ist, dass es diesen bestimmten Wirtschaftszweig bedrohen würde, b) der finanzielle Schaden, den kleine Unternehmen aufgrund des Diebstahls nicht versicherter Fahrzeuge erleiden, allein in ihrem Verantwortungsbereich liegt und c) der Verband nicht berücksichtigt hatte, ob der gleiche Zweck auch mit Mitteln zu erreichen wäre, die nicht so weit in die Privatsphäre eindringen.

Entscheidung 8/2010

Die HDPA entschied, dass die Veröffentlichung sensibler Daten zu einem Strafverfolgungsverfahren in der elektronischen Ausgabe einer Zeitung unrechtmäßig sei, da der Beschuldigte keine Person des öffentlichen Lebens war. Die HDPA verhängte eine Geldbuße gegen den für die Datenverarbeitung Verantwortlichen und untersagte die weitere Veröffentlichung des strittigen Artikels in der gedruckten Ausgabe der Zeitung. Zudem forderte es die Anonymisierung des bereits online veröffentlichten Artikels und empfahl Maßnahmen zur Vermeidung zukünftiger Verstöße.

Entscheidung 31/2010

Die HDPA untersuchte ein biometrisches System zur Zugangskontrolle zu bestimmten wichtigen Infrastrukturen des internationalen Flughafens „Macedonia“ in Thessaloniki, das im Rahmen eines Forschungsprojekts eingerichtet werden sollte. Ziel dieses Projekts war die Entwicklung einer datenschutzgerechten biometrischen Methode zur Zugangskontrolle auf der Grundlage von Fingerabdrücken. Die HDPA entschied, dass das System vorbehaltlich der Einhaltung der folgenden Bedingungen im Einklang mit Gesetz Nr. 2472/1997 steht: der für die Datenverarbeitung Verantwortliche muss Sicherheitsvorgaben für die Verarbeitung der Daten ausarbeiten und die HDPA über die Löschung der Daten nach dem für die Datenverarbeitung erforderlichen Zeitraum von einem Jahr informieren. Die Speicherung der biometrischen Rohdaten in einer zentralen Datenbank wurde nicht gestattet.

Entscheidung 43/2010

Die HDPA untersuchte sowohl von Amts wegen als auch als Reaktion auf Beschwerden den Prozess der Erfassung der Daten von Staatsbediensteten, der im Juli 2010 nach einem Ministerialerlass eingeführt wurde. Die HDPA entschied, dass die gegebene Rechtsgrundlage lediglich eine Verarbeitung zu Gehaltsabrechnungszwecken gestattete und jegliche sonstige Daten, die nicht zu diesem Zweck benötigt werden, nicht verarbeitet werden dürfen. Hinsichtlich der Sicherheitsmaßnahmen forderte die HDPA konkrete Maßnahmen im Hinblick auf das Authentifizierungsverfahren und den Schutz der Daten vor unbefugtem Zugriff.

Entscheidung 56/2010

Die HDPA befand, dass die Rechtsvorschrift zur Kontrolle der öffentlichen Ausgaben im Gesundheitswesen sowie diesbezüglich die Vorschrift der Aufnahme der Sozialversicherungsnummern (SVN) von Ärzten und Apothekern auf allen Rezepten zum Zweck der eindeutigen Identifizierung den verfassungsmäßigen Grundsatz der Verhältnismäßigkeit erfüllt. Die SVN beinhalte zwar das Geburtsdatum, doch dies beeinträchtige nicht ernsthaft die Privatsphäre der Ärzte und Apotheker, da das Alter, wie gesetzlich eindeutig festgelegt, nur einer begrenzten Anzahl von Nutzern unter besonderen Bedingungen zugänglich gemacht wird. Die HDPA sprach jedoch die Empfehlung aus, dass der Staat die SVN so gestalten solle, dass personenbezogene Daten nicht direkt offensichtlich sind.

Entscheidung 73/2010

Die HDPA war der Ansicht, dass ein Angeklagter das Recht auf Zugang nicht nur zum Inhalt der bei einer öffentlichen Behörde eingereichten Klage selbst, sondern auch zu allen Einzelheiten hinsichtlich der Quelle dieser Daten hat, einschließlich der Identifikationsdaten des Klägers. Dieses Recht kann eingeschränkt werden, wenn der Zugang die behördlichen Untersuchungen gefährden würde, wenn das Dokument Informationen enthält, die speziellen Geheimhaltungsverpflichtungen unterliegen, Angaben zum Privat- oder Familienleben einer dritten Person enthalten, oder wenn eine Offenlegung das Leben des Klägers gefährden würde. Der Kläger muss zum Zeitpunkt der Einreichung der Klage angemessen informiert werden und aufgefordert werden, etwaige Einwänden gegen die Offenlegung schriftlich darzulegen.

UNGARN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Laufe der Überprüfung der Verfassung wurden die Vorschläge des Datenschutzbeauftragten an den für die Erarbeitung des neuen Grundgesetzes zuständigen Ad-hoc-Ausschuss übersandt. Der Standpunkt des Datenschutzbeauftragten lautet wie folgt: (1) statt eines Datenschutzbeauftragten wäre die Ernennung eines Informationsbeauftragten wünschenswert; im Hinblick auf nachhaltige Vorschriften als wirksame Lösungen sollte die Datenschutzbehörde mit der Aufsicht über Vorschriften im Bereich der Informationsfreiheit betraut werden; (2) durch Änderung der Vorschriften sollte die Unabhängigkeit der Einrichtung gestärkt werden und (3) ein für zwei Arten von Informationsrechten zuständiger Informationsbeauftragter sollte über wirksame Instrumente für deren Durchsetzung verfügen.

Vom Datenschutzbeauftragten durchgeführte Sensibilisierungsmaßnahmen orientierten sich am erfolgreichen Muster der Vorjahre. Es wurden zahlreiche Informationsveranstaltungen organisiert. Die am Datenschutztag organisierte Datenschutzkonferenz war der Analyse problematischer Fragen zu Überwachungssystemen gewidmet sowie der Entwicklung von Überwachungstechnologien, der Reaktion des Gesetzgebers auf diese Entwicklungen, der Beantwortung der Frage, ob diese Systeme wirksame Instrumente für die Durchsetzung der Gesetze sind, was der tatsächliche Nutzen für die Gesellschaft sein könnte, und ob diese Systeme angesichts des vorgesehenen Zwecks als verhältnismäßige Mittel eingestuft werden können.

Ziel der am 28. September organisierten internationalen Konferenz war es, ein Gleichgewicht zwischen Datenschutz und Informationsfreiheit zu finden.

Im Jahr 2009 wurde gemeinsam mit dem polnischen und dem tschechischen Datenschutzbeauftragten die Erarbeitung einer Veröffentlichung gestartet. Der Schwerpunkt dieser Veröffentlichung lag auf Datenschutzfragen im Bereich Beschäftigung bzw. im Zusammenhang mit Unternehmern, die in diesen drei Ländern tätig sind. Die Publikation, die Informationen zu relevanten EU- und nationalen Gesetzen, landesspezifische bewährte Verfahrensweisen und Empfehlungen enthält, sollte 2011 herausgegeben werden.

Organisation	
Vorsitz und/oder Gremium	Herr Dr. András Jóri Parlamentarischer Kommissar für Datenschutz und Informationsfreiheit.
Budget	374 109 000 HUF
Personal	48
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Keine Statistiken verfügbar.
Meldungen	15 161
Vorabprüfungen	k. A.
Anträge betroffener Personen	Beide Kategorien zusammen: 2 013
Beschwerden betroffener Personen	
Vom Parlament bzw. der Regierung	639

angeforderte Beratung	
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Konsultationen: 1 035
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Keine Statistiken verfügbar.
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Der Datenschutzbeauftragte initiierte proaktiv zahlreiche, den Vorgaben der Richtlinie 95/46/EG entsprechende Projekte zu den wichtigsten Themen.

Ein umfassendes Forschungsprojekt wurde abgeschlossen; Ergebnis war eine Empfehlung, in der es insbesondere um die Verarbeitung von Daten in der Presse und den Medien ging. Das Projekt untersuchte Verordnungen und die Praxis und benannte für den Schutz der Privatsphäre und personenbezogener Daten in der Presse/den Medien relevante Bereiche, insbesondere im Hinblick auf: die Analyse der Wechselbeziehung zwischen persönlichen Rechten zum Schutz personenbezogener Daten und der Privatsphäre, den Inhalt von in den Medien erscheinenden personenbezogenen Daten, die Quellen von Daten, gesetzliche Befugnisse, die Verpflichtung der Information von Datensubjekten und die Auflage der Zweckbindung, Verfahren im Zusammenhang mit Einverständniserklärungen im Rahmen von Medienauftritten, Beschwerden, die Rechtsreform, die Auswirkungen von Verordnungen zum investigativen Journalismus auf Datenschutzverordnungen sowie Verordnungen zur Justizberichterstattung.

Das Projekt zur Kameraüberwachung analysierte die gesellschaftlichen Auswirkungen sowie die Vor- und Nachteile des Betriebs solcher Systeme. Ziel war die Festlegung eindeutiger und praktischer, in Diskussionen effektiv verwendbarer Lösungen und Argumente. Die Kameraüberwachung passt nicht in das rechtliche Umfeld und erfüllt oftmals nicht die gesetzlichen Vorschriften, was sich wiederum nachteilig auf den Datenschutz auswirkt. Zweck des Projekts war eine Aktualisierung der vorherigen Empfehlung zu diesem Thema.

Aufgrund der verstärkten Bemühungen des Gesetzgebers zur Einführung eines umfassenden Kreditinformationssystems, bezüglich dessen der Datenschutzbeauftragte zahlreiche Stellungnahmen veröffentlicht hatte, da er die Schutzmaßnahmen bezüglich der freiwilligen Natur der Einwilligung der Kreditnehmer als nicht angemessen erachtete, wurde ein Projekt gestartet, um zu untersuchen, wie die Schutzgarantien eingehalten werden können.

Vertreter von Google initiierten Diskussionen mit dem Büro des Datenschutzbeauftragten hinsichtlich der für den Start des Dienstes Google Street View in Ungarn geltenden Datenschutzanforderungen. Im Laufe der Prüfung forderte der Datenschutzbeauftragte Google auf, bis zur Klärung der Rechtsgrundlage keine weiteren Fotos anzufertigen. Bereits im Voraus wurde festgehalten, dass die Aufnahme von Fotos von öffentlichen Plätzen gemäß dem Datenschutzgesetz und dem Bürgerlichen Gesetzbuch nicht illegal sei. Vor Aufnahme der Tätigkeiten seitens Google mussten jedoch eindeutige Vorgaben festgelegt werden. Bei den Diskussionen sowie der vorläufigen Stellungnahme berücksichtigte der Datenschutzbeauftragte die diesbezüglichen europäischen Perspektiven. Die

endgültige Entscheidung erfolgt abhängig von den Antworten von Google auf die Fragen des Datenschutzbeauftragten und den Ergebnissen der durchgeführten Prüfung im Jahr 2011.

Aufgrund der Nutzung der praktisch überall verfügbaren modernen Technologien untersuchte der Datenschutzbeauftragte viele Bereiche. Im Bereich Beschäftigung ist die Tendenz unverändert typisch: Arbeitgeber nutzen oftmals Systeme zur Kameraüberwachung und Geolokalisierung, Lügendetektoren und andere Mittel, Postfächer werden geprüft und sogar medizinische Untersuchungen von Arbeitgebern angefordert. Angesichts dieser Konstanz zeigte die hohe Zahl an Beschwerden, dass der Bereich Beschäftigung sich zu einem Bereich entwickelt hat, für den umfassendere, konzeptionelle und detaillierte Regelungen erforderlich sind.

Auch im Bereich Bildung waren Verletzungen der Privatsphäre zu verzeichnen. Bildungseinrichtungen führten Anmeldungssysteme ein und setzten hierfür Technologien ein, die den Zugang erleichtern sollen, aber nicht angemessen angewendet wurden. Überwachungskameras und biometrischen Identifizierungssysteme gehörten zu den häufigsten Beispielen, in denen der Datenschutzbeauftragte die Nichteinhaltung der Grundsätze der Verhältnismäßigkeit und Zweckbindung seitens der betreffenden Einrichtungen feststellte. In einem Fall, in dem es um internationale Prüfungen ging, mussten die Prüflinge zusätzlich zur Vorlage ihrer persönlichen Identifikationsdokumente ihre Fingerabdrücke abgeben und ihre Unterschrift digital erfassen lassen, bevor sie an der Prüfung teilnehmen konnten. Hätten sie diese Informationen nicht bereitgestellt, wären sie von der Prüfung ausgeschlossen worden. In diesem Fall war der strittige Punkt die „Freiwilligkeit" der Einverständniserklärung.

Schließlich gab es einen Fall im Bereich Telekommunikation, in dem Fotos und Identifikationsdaten (oftmals Name, Telefonnummer usw.) zusammen mit obszönen Bemerkungen und Kommentaren zum Beschwerdeführer auf die Seite eines sozialen Netzwerks hochgeladen wurden. Da eindeutig personenbezogene Daten betroffen waren, wäre die Verarbeitung dieser Informationen nur dann rechtmäßig gewesen, wenn eine Einverständniserklärung des Datensubjekts vorgelegen hätte. In dem gegebenen Fall wurde die Einverständniserklärung als nicht vorliegend erachtet, so dass der Datenschutzbeauftragte Anzeige bei der Polizei erstattete (Tatbestand des Missbrauchs personenbezogener Daten). Die Polizei leitete eine Untersuchung ein, die betreffenden Inhalte wurden jedoch in vollem Umfang von dem ungarischen Portal gelöscht und auf anderen Filesharing-Seiten in Ländern außerhalb der Gerichtsbarkeit der ungarischen Polizei hochgeladen.

IRLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Büro des Datenschutzbeauftragten befasste sich 2010 mit der Untersuchung von 783 formellen Beschwerden (viele Beschwerden werden informell abgehandelt, indem den Beschwerdeführern die entsprechenden Informationen zu ihren Rechten zur Verfügung gestellt werden). Wie in den vorangegangenen Jahren wurde die Mehrheit der Beschwerden einvernehmlich gelöst. Lediglich bei 14 Beschwerden waren formelle Entscheidungen erforderlich. Informationen zu Strafverfolgungsverfahren im Jahr 2010 sind in Abschnitt B dieses Berichts zu finden. Die Anzahl der beim Büro eingegangenen Meldungen von Verletzungen des Schutzes personenbezogener Daten stieg deutlich an, hauptsächlich infolge der Einführung eines neuen Praxiskodex gegen die Verletzung des Schutzes personenbezogener Daten im Jahr 2010. Der Datenschutzbeauftragte setzte seine Zusammenarbeit mit großen Organisationen des öffentlichen Sektors hinsichtlich des Umfangs des Datenaustausches im öffentlichen Sektor fort. Auf der Grundlage dieser Zusammenarbeit sowie einer Reihe von Prüfungen bei Organisationen in diesem Sektor erarbeitete der Datenschutzbeauftragte eine Reihe von Leitlinien für alle Einrichtungen des öffentlichen Sektors, in denen es vor allem um das Prinzip der Transparenz und der Verhältnismäßigkeit geht. Als weitere Leitlinien wurden unter anderem die revidierten Leitlinien zur Meldung von Datenschutzverletzungen, die revidierten Leitlinien zur Datensicherheit sowie die neuen Leitlinien zum Datenschutz bei Sicherheitsüberprüfungen von Beschäftigten herausgegeben.

Organisation	Büro des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Billy Hawkes
Budget	1 272 000 EUR (ausgegeben: 1 449 329 EUR)
Personal	22
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	3 (Leitlinien)
Meldungen	2010 wurden etwa 5 000 Meldungen registriert.
Vorabprüfungen	k. A.
Anträge betroffener Personen	7 200
Beschwerden betroffener Personen	783 (Zugangsrechte – 39 %, elektronisches Direktmarketing – 30 %, Offenlegung – 10 %, unlautere Verarbeitung – 10 %, Sonstige – 11 %)
Vom Parlament bzw. der Regierung angeforderte Beratung	54
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	410 Meldungen über Verletzungen des Schutzes personenbezogener Daten von 123 verschiedenen Einrichtungen
Prüfmaßnahmen	

Prüfungen, Untersuchungen	32 Audits (Prüfungen)
Sanktionsmaßnahmen	
Sanktionen	2010 wurden 8 Unternehmen und Einzelpersonen strafrechtlich verfolgt.
Geldbußen	11 050 EUR + Kosten (Geldbußen/von Gerichten verhängte Vergleichszahlungen)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

In den meisten Fällen, in denen Beschwerden gemäß Abschnitt 10 der irischen Datenschutzgesetze von 1988 und 2003 beim Datenschutzbeauftragten eingereicht wurden, wurden diese gütlich beigelegt, ohne dass ein formeller Beschluss oder eine Vollstreckungsmaßnahme erforderlich wurde. Eine solche gütliche Einigung kann beispielsweise eine finanzielle Leistung seitens des betreffenden für die Datenverarbeitung Verantwortlichen an den Geschädigten oder an eine geeignete wohltätige Einrichtung sein. Gegebenenfalls können auch Vollstreckungsmaßnahmen angewendet werden – so zum Beispiel, wenn der für die Datenverarbeitung Verantwortliche die Zugangsrechte der Geschädigten nicht respektiert. In einigen Fällen werden für die Datenverarbeitung Verantwortliche auch in Fallstudien im Jahresbericht des Kommissars namentlich erwähnt. Im Laufe des Jahres 2010 war der Datenschutzbeauftragte mehrfach an der erfolgreichen strafrechtlichen Verfolgung von Fällen im Zusammenhang mit den Rechten von Datensubjekten gemäß den Datenschutzgesetzen von 1988 und 2003 sowie der Rechtsverordnung 535 des Jahres 2003 (zur Umsetzung der Richtlinie 2002/58/EG in Irland) beteiligt. Im Jahr 2010 wurden sieben Unternehmen wegen verschiedener Verstöße strafrechtlich verfolgt, und das Büro leitete erstmals die strafrechtliche Verfolgung zweier Einzelpersonen ein (die für eine der Personen zu einer Eintragung im Strafregister führte). Diese strafrechtliche Verfolgung betraf unerbetene schriftliche Werbemitteilungen.

C. Sonstige wichtige Informationen

Ebenfalls im Jahr 2010 führte der Datenschutzbeauftragte eine umfassende Untersuchung einer gemeinsamen Schadensfall-Datenbank der Versicherungsbranche mit der Bezeichnung „Insurance Link“ durch. Zum Zeitpunkt der Untersuchung enthielt die Datenbank Einzelheiten zu fast 2,5 Millionen Schadensfällen. Der anschließende Bericht stellte mangelnde Transparenz, unzureichende Zugangskontrollen und Muster unbefugten Zugangs fest.

ITALIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Laufe des Jahres 2010 war die Garante hauptsächlich in den folgenden Bereichen tätig:

- Gesundheitswesen (elektronische Patientendaten und Krankenakten, Online-Untersuchungsberichte, Erfassung und Speicherung von Untersuchungsberichten in Apotheken, wissenschaftliche und pharmakologische Forschung, ein Projekt zur epidemiologischen Überwachung von Soldaten in Bosnien, Erfassung von HIV-Daten in Einrichtungen des Gesundheitswesens, das Recht auf Privatsphäre in Krankenhäusern/Einrichtungen des Gesundheitswesens, Speicherung medizinischer Dokumente);

- Öffentliche Verwaltung (Verbreitung von Daten zu Immobilien im Besitz öffentlicher Körperschaften, Transparenz von durch öffentliche Behörden gebilligten Zuschüssen und Gehältern, Online-Veröffentlichung und Verbreitung personenbezogener Daten durch öffentliche Einrichtungen, Pädophiliedatenbank, Obdachlosenverzeichnis, Sicherheitsmaßnahmen für die *Anagrafe tributaria* [d. h. das Informationssystem des Finanzamts], Verknüpfung und Sicherheit öffentlicher Datenbanken;

- Marketing (unerbetene Anrufe und „Opt-Out"-Register [*Registro delle opposizioni*], Spam, Faxe und unerbetene E-Mails);

- elektronische Kommunikation (Smartphones und Tablets, Speicherung von Telefon- und Internetdaten zu justiziellen Zwecken, „Inverssuche", Sicherheitsmaßnahmen, Kundenprofilerstellung);

- Journalismus und Information (Gerichtsberichte der Presse, Schutz des Rechts auf Privatsphäre von Kindern und Opfern von Gewalt, Daten zu Gesundheit und sexueller Aktivität, Adoption, Bilder von inhaftierten Personen, Online-Zeitungsarchive);

- Beschäftigung (Erkennungssysteme auf der Grundlage biometrischer Daten, Systeme zur Bestimmung des Standorts von Beschäftigten, Überwachung der Internetnutzung von Beschäftigten, Videoüberwachung am Arbeitsplatz);

- Polizei und Justiz (justizielle Daten im Zusammenhang mit Vermittlungstätigkeiten zur Beilegung zivil- und handelsrechtlicher Streitsachen; digitale Zivilprozesse [e-justice], Sicherheitsmaßnahmen für Justizbehörden, neues Informationssystem für Verwaltungsgerichte, CED-IT-Datenbank der Polizei-Abteilung für öffentliche Sicherheit, Daten von Flugpassagieren, Sicherheitsmaßnahmen für die Schengen-Datenbank);

- Internet (Suchmaschinen, Google Street View, Google Buzz, Facebook und soziale Netzwerke, unrechtmäßige Speicherung von Internet-Nutzungsdaten, Foren und Blogs, vereinfachte Sicherheitsmaßnahmen für kleine Internet-Dienstanbieter, Erstellung von Online-Profilen);

- neue Technologien (Geolokalisierung, RFID-Technologien);

- Schulen und Hochschulen (*anagrafe nazionale degli studenti* [nationales Studentenregister], Nutzung von Videoüberwachung in Schulen, Veröffentlichung von Noten und Prüfungsergebnissen, Schüler-Ranglisten, zur Anmeldung an Hochschulen verwendete personenbezogene Daten);

- private Einrichtungen (*tessera del tifoso* [Fußball-Fankarte], Hochzeitsagenturen, Skipass, Eigentumswohnungen);

- Unternehmen (Übermittlung von Daten in Drittländer, Daten zur Sozialversicherung, Rating-Agenturen und Überwachung von Interessenkonflikten, vereinfachte Datenschutzmaßnahmen, Informationen kommerzieller Natur);

- Banken, Finanzinstitute und Versicherungsunternehmen (Zugang zu Kundendaten von Banken, Sicherheitsmaßnahmen, Informationssysteme zu Kredithistorien, Zugang zu Verbraucherkreditdaten durch EU-Kreditgeber).

Die Datenschutzbehörde wurde mehrmals im Rahmen **parlamentarischer Anhörungen** zu wichtigen Fragen zu Rate gezogen, unter anderem und insbesondere zur Einwanderungspolitik, zur Steuerdatenbank *anagrafe tributaria* und zur Vereinfachung der Beziehung zwischen der öffentlichen Verwaltung und den Bürgerinnen und Bürgern.

Außerdem verabschiedete die Garante wichtige **Leitlinien**, insbesondere zur Offenlegung von Informationen über juristische Personen, zu den für öffentliche Behörden geltenden Vorschriften für die Veröffentlichung von Verwaltungsakten und -dokumenten, die personenbezogene Daten enthalten („öffentliche Verwaltung im Internet") sowie zur Ermittlung der Kundenzufriedenheit im Gesundheitswesen.

Die Garante fasste **allgemeine Beschlüsse** zu bestimmten Bereichen: Videoüberwachung, Wahlkampf, *tessera del tifoso* (Fußball-Fankarte), Telemarketing, Nummernübertragbarkeit, Kreditinformationssysteme, Telefonverzeichnisse und „Inverssuche" (d. h. die Möglichkeit, über die Telefonnummer des Nutzers nutzerbezogene Daten abzurufen); Nutzung von Daten im *pubblico registro automobilistico* (Register für Fahrzeugdaten) sowie Sicherheitsmaßnahmen für Kundendaten im Besitz von Banken.

Im Hinblick auf internationale Beziehungen und die Zusammenarbeit der Garante mit anderen Datenschutzbehörden beteiligt sich die Garante neben ihrer Tätigkeit im Rahmen der Artikel-29-Datenschutzgruppe sowie deren thematischen Untergruppen (in denen die Garante als Berichterstatterin für gemeinsame Maßnahmen zur Umsetzung der Richtlinie über die Vorratsdatenspeicherung 2006/24/EG fungiert) aktiv an Arbeitsgruppen zum Datenschutz bei der OECD (Arbeitsgruppe Informationssicherheit und Privatsphäre – WPISP) und beim Europarat (Beratender Ausschuss zur Konvention 108/1981 (T-PD) und T-PD-Büro, dem die Garante als Mitglied angehört).

Die italienische Datenschutzbehörde ist zudem Mitglied der Gemeinsamen Kontrollstelle sowie anderer Mehrparteien-Aufsichtsgremien, die auf Rechtsinstrumenten der Europäischen Union basieren und gemeinsame Informationssysteme eingerichtet haben (JSB Europol, Schengen, Zoll, Eurodac).

Die Datenschutzbehörde nimmt an Treffen der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation (IWGDPT) sowie an Treffen des im Rahmen der Frühlingskonferenz der europäischen Datenschutzbehörden eingeführten Workshops zur Fallbearbeitung teil.

Im Bereich der justiziellen und polizeilichen Zusammenarbeit nahm die italienische Datenschutzbehörde ihre Aufgaben zur Förderung und Umsetzung des Datenschutzes im Kontext der WPPJ (Arbeitsgruppe Polizei und Justiz) wahr, deren Vorsitz der Präsident der Garante, Prof. Pizzetti, inne hat.

Wie üblich war die Datenschutzbehörde direkt an der in diesem Jahr veranstalteten europäischen sowie der internationalen Konferenz beteiligt.

Die Garante konzentrierte sich entsprechend ihrer früheren Tätigkeiten auch auf Initiativen zur Sensibilisierung, insbesondere von Jugendlichen und insbesondere durch die Veröffentlichung von Broschüren zu sozialen Netzwerken, Schulen und dem Gesundheitswesen. Im Einklang mit diesem Ziel startete die italienische Datenschutzbehörde einen Wettbewerb für Sekundarschüler mit dem Titel „Privatsphäre 2.0. Jugend und neue Technologien".

Die Garante ist rechtlich dazu verpflichtet, dem Parlament einen Jahresbericht zu ihrer Tätigkeit vorzulegen. Dem Jahresbericht für 2010 waren zwei Informationsdokumente – zu Cloud-Computing sowie Smartphones und Tablets – beigefügt, die den Entwicklungen im Bereich der neuen Technologien angepasste allgemeine Grundsätze und Leitlinien zum Thema Datenschutz enthalten und teilweise auf der Erfahrung und dem Fachwissen der Datenschutzbehörde basieren (siehe Abschnitt C).

Organisation	Garante per la protezione dei dati personali
Vorsitz und/oder Gremium	Vorsitz: Prof. Francesco Pizzetti Gremium: Giuseppe Chiaravalloti Mauro Paissan Giuseppe Fortunato
Budget	Ungefähr 16,5 Millionen EUR
Personal	118
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Beschlüsse des Gremiums: etwa 600
Meldungen	1 197
Vorabprüfungen	Etwa 10
Anträge betroffener Personen	Anträge insgesamt: etwa 4 000 Auskunftsersuchen (quesiti): 353 Im Jahr 2010 von Datensubjekten erhaltene Berichte und Forderungen (segnalazioni und reclami): 3 359
Beschwerden betroffener Personen	(Durch das Datenschutzgesetz speziell geregelte formelle Beschwerden betreffend den Zugang zu personenbezogenen Daten einer Person) Etwa 350
Vom Parlament bzw. der Regierung angeforderte Beratung	Stellungnahmen zu parlamentarischen Untersuchungen: 4 Stellungnahmen für Ministerien und das Büro des Premierministers: 16 Themen: Polizei, öffentliche Sicherheit: 4 Rechtsprechungstätigkeit: 1 E-Government und Datenbanken: 5 Aus- und Weiterbildung: 2 Beschäftigung in öffentlichen Behörden: 1 Gesundheitswesen: 1 Unternehmen: 1 Sozialhilfe: 1 Marketing (über Telefonate): 1
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	In der Zentrale der Datenschutzbehörde gingen im Jahr 2010 über 26 000 Anrufe und E-Mails ein, die überwiegend die Bereiche Telemarketing, Spam per E-Mail und Fax, Videoüberwachung, das Internet und soziale Netzwerke sowie den Schutz der Privatsphäre am Arbeitsplatz (sowohl im öffentlichen

	als auch im privaten Sektor) betrafen. Nationale Genehmigungen für verbindliche unternehmensinterne Vorschriften: 2
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen und/oder Untersuchungen (vor Ort): etwa 500 (in 55 Fällen wurden Verstöße krimineller Natur bei den Justizbehörden zur Anzeige gebracht). Wichtige Themen: fehlende Informationsschreiben, fehlende Sicherheitsmaßnahmen, unterbliebene Bereitstellung von Informationen und/oder Dokumenten für die Garante, Verstoß gegen eine Entscheidung der Garante, Verstoß gegen die Vorschriften zur Vorratsspeicherung von Daten, Mehrfachverstöße seitens des Verantwortlichen für die Verarbeitung von Daten in großen Datenbanken bzw. Datenbanken mit sensiblen Daten.
Sanktionsmaßnahmen	
Sanktionen	Etwa 500
Geldbußen	Betrag: etwa 4,8 Millionen EUR, im Namen der Datenschutzbehörde verhängt von der für Kontrollen zuständigen Finanzpolizei.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A. (im italienischen Rechtssystem sind keine Datenschutzbeauftragten vorgesehen)

B. Rechtsprechung

Das **Gericht von Mailand** entschied, dass die Verantwortlichen von Google gegen Paragraph 167 (unrechtmäßige Verarbeitung von Daten einschließlich der Verbreitung sensibler Daten) des Gesetzes zum Schutz der Privatsphäre [Gesetzesverordnung Nr. 196 vom 30. Juni 2003] verstoßen haben. Der Verstoß bestand in der Verbreitung eines Videos auf einer Website, auf dem ein minderjähriger Behinderter von seinen Klassenkameraden schikaniert wurde (Entscheidung von 24. Februar 2010).

Das **Gericht von Palermo** urteilte, dass eine Bank gegenüber zwei Kunden wegen der Tätigung einer nicht autorisierten Überweisung in ein Drittland über den Onlinedienst der Bank, der nicht angemessen durch Sicherheitsmaßnahmen geschützt war, haftbar sei. Die Entscheidung basiert insbesondere auf Paragraph 15 des Gesetzes zum Schutz der Privatsphäre, der besagt, dass derjenige, der als Folge einer Verarbeitung personenbezogener Daten einen Schaden für einen anderen verursacht, gemäß Paragraph 2050 des Bürgerlichen Gesetzbuches schadenersatzpflichtig ist [die Haftbarkeit ergibt sich aus der Durchführung unsicherer Aktivitäten] (Entscheidung vom 20. Dezember 2009).

Der **Staatsrat (die höchste verwaltungsrechtliche Instanz)** urteilte, dass das Recht von Datensubjekten auf Korrektur ihrer Daten gemäß Paragraph 7 des Gesetzes zum Schutz der Privatsphäre stets gewährleistet sein muss, um die Korrektheit der im *casellario giudiziale* (Strafregister) erfassten Daten sicherzustellen (Entscheidung Nr. 473/2010).

Der **Staatsrat** entsprach der Forderung – betreffend die Aufhebung einer Ehe – auf Zugang zu Verwaltungsregistern zur Offenlegung sensibler Daten zum Gesundheitszustand des Ehepartners. Das in diesem Fall eingelegte

Rechtsmittel (d. h. die Aufhebung) stellte tatsächlich einen Rechtsanspruch dar, der nicht vom Recht des Datensubjekts auf den Schutz der Privatsphäre außer Kraft gesetzt wurde. Aus diesem Grund gab das Oberste Verwaltungsgericht gemäß Paragraph 60 des Gesetzes zum Schutz der Privatsphäre dem Antrag auf Offenlegung sensibler gesundheitsbezogener Daten statt (Entscheidung Nr. 7166/2010).

Der **Kassationshof** urteilte, dass die Entlassung eines Mitarbeiters auf der Grundlage der Tatsache, dass dieser mehrfach das Internet zu privaten Zwecken genutzt hatte, als unrechtmäßig einzustufen ist. Tatsächlich wurde besagter Tatbestand durch – vom Arbeitgeber eingesetzte – Software festgestellt, die einen Zugang zu den auf den von dem Mitarbeiter verwendeten Computern gespeicherten Daten ermöglichte. Gemäß Gesetz Nr. 300/1970 („Arbeitnehmerstatut" – *statuto dei lavoratori*) bestätigte das Gericht ausdrücklich, dass: „die Kontrolle der Tätigkeiten von Mitarbeitern" zwar erforderlich sei, jedoch „unter Berücksichtigung der ‚menschlichen Dimension' zu erfolgen hat und nicht durch den Einsatz von Technologien verschärft werden darf, die eine Verletzung aller Formen der Privatsphäre und Eigenständigkeit hinsichtlich der beruflichen Tätigkeit mit sich bringen". IT-Systeme, „die eine Überwachung der Internethistorie ermöglichen", sind als „Ressourcen zur Fernüberwachung von Angestellten" einzustufen. Aus diesem Grund unterliegt der Einsatz solcher Systeme am Arbeitsplatz „einer Vereinbarung mit den Vertretern der Gewerkschaft oder, in Ermangelung einer solchen Vereinbarung, der Genehmigung durch die Arbeitsaufsichtsbehörde (Abschnitt 4.2 des Arbeitnehmerstatuts)". Daten, die unter Verletzung dieser Bestimmung erfasst werden, können nicht vor Justizbehörden verwendet werden (Entscheidung Nr. 4375/2010).

Der **Kassationshof** urteilte – in einem Fall, der sich ebenfalls mit der gleichen Frage der Berechtigung der Entlassung eines Mitarbeiters befasste –, dass die Wahrung des Rechts auf Schutz der Privatsphäre die Ausübung anderer Grundrechte wie z. B. des Rechts auf Verteidigung oder des Rechts auf Arbeit nicht *per se* unterbindet. In diesen Fällen ist es von größter Bedeutung, das richtige Gleichgewicht zwischen den betreffenden unterschiedlichen Rechten zu finden (Entscheidung Nr. 18279/2010).

C. Sonstige wichtige Informationen

Die Datenschutzbehörde startete eine Erhebung zu den wichtigsten Herstellern von Softwaresystemen für **Smartphones**, um zu untersuchen, ob die Sicherheitsmaßnahmen hinsichtlich der für solche Systeme entwickelten mobilen Apps angemessen sind. Die bisher eingegangenen Rückmeldungen haben gezeigt, dass sich die ergriffenen Sicherheitsmaßnahmen in vielerlei Hinsicht unterscheiden. Die wesentlichen Kritikpunkte, die sich im Rahmen dieser Erhebung ergeben haben, wurden in einem Dokument mit dem Titel „Smartphones und Tablets: Aktuelles Szenario und operative Perspektiven" beschrieben, das dem jährlichen Tätigkeitsbericht der Garante für 2010 beigefügt war.

In Form einer Broschüre mit dem Titel *Cloud-Computing: Leitlinien für eine fachkundige Nutzung dieser Dienste* bot die Garante eine erste Orientierungshilfe für Nutzer von Cloud-Computing-Diensten (z. B.: Notwendigkeit einer Vorab-Risikobewertung einschließlich des Themas Zuverlässigkeit des jeweiligen Anbieters, sowie Prüfung der spezifischen Vertragsklauseln einschließlich des Standortes des Cloud-Servers, Typologie der angebotenen Dienstleistungen sowie Schulung des für die Verarbeitung von Daten verantwortlichen Personals), um eine verantwortungsbewusste Nutzung von Dienstleistungen dieser Art und die Festlegung spezieller Vorgaben für entsprechende Sicherheitsmaßnahmen in der nahen Zukunft zu fördern.

Videoüberwachung: mit diesem Thema befasste sich ein **allgemeiner Beschluss** vom 27. April 2010, der die Installation von Überwachungskameras und Videoüberwachungssystemen betrifft und sowohl für öffentliche als auch für private Körperschaften verbindlich ist. Die in diesem allgemeinen Beschluss festgelegten Vorschriften beinhalten spezifische Maßnahmen zum Schutz der Privatsphäre von Personen, deren Daten über solche Systeme erfasst und verarbeitet werden. Der Beschluss tritt an die Stelle eines im Jahr 2004 von der Datenschutzbehörde veröffentlichten Beschlusses und berücksichtigt nicht nur die neue Gesetzgebung, sondern auch die neuen Technologien und den deutlichen Anstieg der Nutzung von Videoüberwachung zu unterschiedlichsten Zwecken. Ein besonderes Augenmerk kam den Maßnahmen zur Information von Datensubjekten über den Betrieb von Überwachungskameras in den Bereichen/Geschäftsräumen zu, die sie betreten (Verpflichtung zur Anbringung gezielter Hinweise außer im Fall von Überwachungskameras, die der öffentlichen Sicherheit dienen), sowie den Einschränkungen der Speicherung von Daten, die mit Überwachungskameras und Videoüberwachungssystemen erfasst werden (aufgezeichnete Bilder dürfen nur für einen begrenzten Zeitraum gespeichert werden, der 24 Stunden

nicht überschreiten darf. Für bestimmte Fälle wie z. B. Untersuchungen durch Polizei und Justiz, die Sicherheit von Banken usw. ist eine längere Speicherdauer vorgesehen).

LETTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Die 2010 vorgenommenen Änderungen am Gesetz zum Schutz personenbezogener Daten wurden am 6. Mai 2011 vom Parlament der Republik Lettland angenommen (in Kraft seit 2. Juni 2010). Insbesondere Artikel 10, Kapitel 4 des Gesetzes zum Schutz personenbezogener Daten wurde geändert, um die Ausnahmen festzulegen, in denen eine Verarbeitung personenbezogener Daten zu Zwecken erlaubt ist, die nicht ursprünglich im Rahmen von Strafverfahren vorgesehen waren. Eine weitere wichtige Änderung betrifft die Beschlüsse der Datenschutzbehörde (Artikel 31, Kapitel 2) – die Anfechtung von bzw. Berufung gegen von der Datenschutzbehörde veröffentlichte Verwaltungsakte betreffend die Sperrung der Verarbeitung personenbezogener Daten sowie betreffend das permanente oder vorübergehende Verbot der Verarbeitung personenbezogener Daten setzt nicht die Umsetzung des Beschlusses der Datenschutzbehörde außer Kraft (es sei denn, er wird durch die Entscheidung der Berufungsinstanz außer Kraft gesetzt).

Auf nationaler Ebene gab die lettische Datenschutzbehörde Stellungnahmen zu verschiedenen Rechtsakten und politischen Maßnahmen heraus, darunter vor allem:

- Gesetzesentwurf zum Kreditregister – Stellungnahme für die lettische Nationalbank betreffend das Recht von Datensubjekten auf Zugang zu diesem Register, da dieses Recht anfänglich eingeschränkt war, was nicht den Bestimmungen des Gesetzes zum Schutz personenbezogener Daten entspricht; die Stellungnahme der Datenschutzbehörde wurde berücksichtigt.
- Gesetzesentwurf zur Schuldeneintreibung – nach entsprechender Stellungnahme der Datenschutzbehörde wurde festgelegt, dass personenbezogene Informationen nicht in eine Kreditreferenz-Datenbank aufgenommen werden dürfen, wenn die betreffende Person der Existenz der Schuld widersprochen hat.
- Gesetzesentwurf zu den Änderungen des Rechts zum Schutz der Verbraucherrechte – die Stellungnahme der Datenschutzbehörde floss an den Stellen ein, an denen darauf hingewiesen wurde, dass die Änderungsentwürfe nicht die Anwendungsbeschränkungen der Richtlinie 2008/48/EG hinsichtlich der Höhe des Kredits und der Bedingungen berücksichtigen, unter denen eine Prüfung der Kreditwürdigkeit eines Kunden nicht erforderlich ist.
- Die lettische Datenschutzbehörde war nicht an Projekten auf nationaler Ebene zur Einführung des eHealth-Projekts beteiligt. Im Jahr 2010 führte die Datenschutzbehörde jedoch eine Prüfung im Zusammenhang mit der Verarbeitung sensibler personenbezogener Daten im Gesundheitswesen durch. Die Untersuchungen sollten im Jahr 2011 fortgesetzt werden.

Wichtige Themen, zu denen öffentliche Behörden Beratung anforderten

Die Datenschutzbehörde verfügt nicht über Statistiken zu den von öffentlichen Behörden angeforderten Beratungen. Bei der Datenschutzbehörde gehen jedoch täglich Anrufe von verschiedenen öffentlichen Behörden zu einer Vielzahl von Aspekten im Zusammenhang mit der Verarbeitung personenbezogener Daten ein – so beispielsweise zur Notwendigkeit, die Verarbeitung personenbezogener Daten mitzuteilen, sowie auch komplexere Fragen, deren Beantwortung eine gründliche Analyse zur Bestimmung der besten Lösung im Hinblick auf den Schutz personenbezogener Daten erfordert.

Informationen zu Sensibilisierungsaktivitäten

Die Datenschutzbehörde organisierte für unterschiedliche Zielgruppen mehrere Seminare zu Fragen im Bereich des Schutzes personenbezogener Daten – beispielsweise für Leiter von Bildungseinrichtungen, Lehrer usw. Die Datenschutzbehörde bietet Seminare an, die für alle Interessierten zugänglich sind (2010 wurden drei solcher Seminare organisiert).

Organisation	Lettische Datenschutzbehörde (Datu valsts inspekcija)

Vorsitz und/oder Gremium	Leiterin – Signe Plūmiņa
Budget	266 907 LVL (ungefähr 370 457 EUR)
Personal	19 (einschließlich Verwaltungs- und Wartungspersonal)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Statistiken zu Beschlüssen, Stellungnahmen – k. A. Empfehlung – die Empfehlung wurde in sozialen Netzwerken veröffentlicht (und richtete sich an die Nutzer von sozialen Netzwerken).
Meldungen	352 (einschließlich der Meldungen über Änderungen der Verarbeitung personenbezogener Daten)
Vorabprüfungen	267
Anträge betroffener Personen	k. A.
Beschwerden betroffener Personen	234 Beschwerden von Datensubjekten im Zusammenhang mit einer möglichen Verletzung des Schutzes personenbezogener Daten. 2 Beschwerden von Datensubjekten aus Drittländern im Zusammenhang mit der Verarbeitung ihrer Daten im SIS. 22 Beschwerden im Zusammenhang mit Spam (es wurden 15 Untersuchungen durchgeführt). 15 Untersuchungen durchgeführt).
Vom Parlament bzw. der Regierung angeforderte Beratung	9 (betreffend Änderungen des Gesetzes zum Schutz personenbezogener Daten sowie den Entwurf für das Gesetz zur Sicherheit der Informationstechnologie)
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Bei Anfragen per Telefon lauteten die wichtigsten Fragen der Anrufer wie folgt: • Werden bestimmte Informationen als personenbezogene Daten eingestuft? • Wer darf wann und wo Videoüberwachung nutzen? • Wie kann ich gegen eine unrechtmäßige Verarbeitung personenbezogener Daten im Internet vorgehen? • Wie sind die Vorschriften zur Verarbeitung personenbezogener Daten im Bereich der Schuldeneintreibung? • Wann ist die Verarbeitung persönlicher Codes erlaubt, und wer darf diese Codes verarbeiten?
Prüfmaßnahmen	
Prüfungen, Untersuchungen	234 Beschwerden: Die meisten Menschen, die die lettische Datenschutzbehörde kontaktierten, meldeten eine mögliche Verletzung des Gesetzes zum Schutz personenbezogener Daten in den folgenden Bereichen: • Verarbeitung personenbezogener Daten im Internet (auch in

	Fällen, in denen der für die Datenverarbeitung Verantwortliche keine angemessenen technischen Mittel zum Datenschutz vorgesehen hat); • Verarbeitung personenbezogener Daten im Bereich Schuldeneintreibung sowie Einrichtung einer Kredithistorie; • Identitätsdiebstahl – Angabe personenbezogener Daten einer anderen Person und somit unrechtmäßige Verarbeitung personenbezogener Daten (in vielen Fällen ging es um die Angabe falscher personenbezogener Daten gegenüber der Staats- oder der lokalen Polizei im Zusammenhang mit verschiedenen Verwaltungsverstößen); • Verarbeitung von Daten durch Hausmeisterdienste; • Videoüberwachung.
Sanktionsmaßnahmen	
Sanktionen	Die Befugnis zur Verhängung von Sanktionen durch die Datenschutzbehörde ist im lettischen Gesetz über Verwaltungsverstöße festgeschrieben. In 42 Fällen wurde eine Verletzung des Gesetzes zum Schutz personenbezogener Daten festgestellt, und es wurden Geldbußen verhängt. Nicht alle eingeleiteten Untersuchungen wurden 2010 abgeschlossen
Geldbußen	Beträge (Angabe, ob diese von Gerichten oder der Datenschutzbehörde verhängt wurden). Von der Datenschutzbehörde verhängte Geldbußen – 28 Verwarnungen, 14 Geldbußen – der Betrag belief sich insgesamt auf 14 250 LVL (ungefähr 19 249 EUR).
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	9 registrierte Datenschutzbeauftragte. Durchführung von 4 Prüfungen für Datenschutzbeauftragte.

B. Rechtsprechung

Im Jahr 2010 stieg die Zahl der Verletzungen des Gesetzes zum Schutz personenbezogener Daten an. Die Sanktionen für solche Verletzungen sind im Strafrecht festgeschrieben. Daher wurden diese Fälle an die Generalstaatsanwaltschaft weitergeleitet.

Die Datenschutzbehörde kam zu dem Schluss, dass eine bessere Zusammenarbeit auf EU-Ebene erforderlich ist, um Verletzungen des Datenschutzes im Internet effektiver zu bekämpfen und somit die Wahrung des Rechts der Bürgerinnen und Bürger der EU auf den Schutz ihrer Daten zu gewährleisten.

LITAUEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Gesetz zur Änderung und Ergänzung des Gesetzes zum Schutz personenbezogener Daten (Amtsblatt, 1996, Nr. 63-1479; 2008, Nr. 22-804) wurde am 12. Mai 2011 verabschiedet und tritt am 1. September 2011 in Kraft. Der neue Wortlaut des Gesetzes zum Schutz personenbezogener Daten (nachstehend „LLPPD") besagt, dass Finanzinstitute, die Finanzdienstleistungen anbieten, hinsichtlich der Übernahme des Risikos und der Bewertung der Kreditwürdigkeit untereinander personenbezogene Daten zum Familienstand, der beruflichen Situation und Bildung zum Zweck der finanziellen Risikobewertung und Schuldenverwaltung von Datensubjekten, für die diese Institute Finanzdienstleistungen erbringen oder dies beabsichtigen, austauschen dürfen, sofern die betreffenden Datensubjekte ihr Einverständnis dazu gegeben haben. Der neue Wortlaut besagt außerdem, dass bei der Durchführung von Sozialerhebungen und öffentlichen Umfragen personenbezogene Daten verarbeitet werden dürfen, wenn das Datensubjekt sein Einverständnis dazu gegeben hat.

Das der Umsetzung des Rahmenbeschlusses 2008/977/JI des Rates dienende Gesetz zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, wurde am 21. April 2011 verabschiedet und sollte am 1. Juli 2011 in Kraft treten.

Am 27. November 2010 trat eine neue Fassung des Rechtes der Regierung der Republik Litauen in Kraft. Ein neuer Wortlaut spezifiziert Veränderungen des Rechtsstatus des Leiters der Datenschutzbehörde der Republik Litauen (nachstehend „SDPI"). Die neue Fassung besagt, dass der Leiter der SDPI ein Staatsbediensteter wird. Der neuen Fassung dieses Rechts gemäß agiert die SDPI im Einklang mit dem vom Justizminister genehmigten strategischen Plan. Zudem besagt das neue Recht, dass der Justizminister der Regierung die Möglichkeit einräumen muss, den Leiter der SDPI zu ernennen oder zu entlassen, ihn zu befördern oder Geldbußen gegen ihn zu verhängen. Darüber hinaus entscheidet der Justizminister über die Urlaubszeiten des Leiters und kann ihn zu Missionen entsenden. Gemäß diesem Recht ist der Direktor der SDPI gegenüber der Regierung und dem Justizminister auskunfts- und rechenschaftspflichtig.

Am 23. Dezember 2009 verabschiedete die Regierung der Republik Litauen eine Entschließung zum Beschluss 2009/371/JI des Rates zur Errichtung des Europäischen Polizeiamts (Europol). Gemäß Artikel 3 dieser Entschließung wurde die SDPI als Aufsichtsbehörde benannt und mit der Umsetzung von Artikel 33 des Beschlusses 2009/371/JI des Rates (der am 1. Januar 2010 in Kraft trat) betraut.

Am 28. Januar 2010 wurde der Europäische Datenschutztag gefeiert. Es wurde eine Versammlung im Europäischen Informationsbüro der Seimas organisiert. Diese Veranstaltung war den verschiedenen staatlichen Institutionen, Agenturen und Organisationen gewidmet, die im Bereich des Schutzes personenbezogener Daten tätig sind. Vertreter des öffentlichen Sektors wurden über aktuelle Themen im Bereich des Schutzes personenbezogener Daten in Litauen und anderen Ländern informiert. Ein besonderes Augenmerk lag auf dem Bereich Videoüberwachung. Zu diesem Thema wurden drei Berichte vorgestellt: „Rechtsvorschriften zur Videoüberwachung", „Technische Fragen zur Videoüberwachung" und „Fragen zur Videoüberwachung in der Hauptstadt Wilna – heute und früher".

Zusammen mit dem Unternehmen Expozona veranstaltete die SDPI am 26. Mai 2010 eine Konferenz mit dem Titel „Datenschutz in den neuesten Technologien und dem elektronischen Raum (E-Space)". Der Schwerpunkt der Veranstaltung lag auf den Themen Identitätsmanagement, Privatsphäre und Datenschutz in den Informations- und Kommunikationstechnologien sowie Mobilität. Diese Themen deckten die wichtigsten im Rahmen der vier PrivacyOS-Projektkonferenzen analysierten (Privacy Open Space) Themen ab. PrivacyOS bringt die Industrie, KMU, die Regierung, Akademiker und die Zivilgesellschaft an einen Tisch, um die Entwicklung und Anwendung von europäischen Infrastrukturen für die Wahrung der Privatsphäre zu fördern. An der Konferenz nahmen mehr als 60 Vertreter des öffentlichen und des privaten Sektors teil.

Zusammen mit dem Unternehmen Expozona veranstaltete die SDPI auch eine Konferenz mit dem Titel „Werden personenbezogene Daten in Litauen rechtmäßig verarbeitet? Probleme, Ursachen und Lösungsmöglichkeiten" am 24. November 2010. Diese Veranstaltung war auf Leiter von Unternehmen, Institutionen und Organisationen, Rechtsanwälte und Fachleute ausgerichtet, die für die Verarbeitung der personenbezogenen Daten von

Arbeitnehmern und Kunden verantwortlich sind. Die Redner der SDPI und der Rechtsanwaltskanzlei LAWIN Lideika, Petrauskas, Valiūnas und Partner hielten sechs Vorträge zu verschiedenen Themen: "Was muss man wissen, um personenbezogene Daten rechtmäßig verarbeiten zu können?", „Die Verarbeitung der personenbezogenen Daten von Arbeitnehmern. Probleme und Lösungsmöglichkeiten", „Die Prüfung von Beschwerden in der Praxis. Wichtige Gerichtsurteile zum Thema Datenschutz", „Rechtmäßige Übermittlung von personenbezogenen Daten an Empfänger im Ausland", „Die Verarbeitung bestimmter Kategorien von personenbezogenen Daten. Die Praxis in Litauen und der Europäischen Union" sowie „Aktuelle Fragen zum Thema Datenschutz in Litauen und Europa".

Organisation	
Vorsitz und/oder Gremium	Dr. Algirdas Kunčinas
Budget	Zugewiesen und ausgegeben: 1 886 Millionen LTL
Personal	30
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Empfehlung zur „Umsetzung des Rechts des Einzelnen auf Achtung des Privatlebens sowie Grundsätze des Datenschutzes bezüglich der Anwendung von Radiofrequenz-Identifikationssystemen".
Meldungen	760 (zur Verarbeitung von Daten)
Vorabprüfungen	204
Anträge betroffener Personen	8
Beschwerden betroffener Personen	270
Vom Parlament bzw. der Regierung angeforderte Beratung	1
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	3 294 Konsultationen; 102 öffentliche Mitteilungen; 7 Zusammenfassungen der Ergebnisse der Untersuchungen von Beschwerden und der Rechtsprechung; 6 Anträge betreffend die Verarbeitung von Daten im C.SIS; 86 Schlussfolgerungen zu Dokumenten der EU und des Europarates; 92 Antworten auf Anfragen von Parteien im Zusammenhang mit dem Übereinkommen (ETS Nr. 108); 238 koordinierte Rechtsakte und Dokumente von für die Datenverarbeitung Verantwortlichen; 5 vorbereitete Rechtsakte
Prüfmaßnahmen	
Prüfungen, Untersuchungen	80 (Zulässigkeit und Umfang der Verarbeitung der Daten von bei sozialen Netzwerken angemeldeten Benutzern; Zulässigkeit der Verarbeitung von Daten bei der Bereitstellung von Schnellkreditdiensten; Zulässigkeit der Speicherung von Internetverbindungsdaten bei der Bereitstellung von Internetdiensten; Umfang und Zulässigkeit der Veröffentlichung personenbezogener Daten auf den Internetseiten von Gemeinden; Zulässigkeit der Verarbeitung personenbezogener Daten von Kunden in privaten Sportvereinen)

Sanktionsmaßnahmen	
Sanktionen	Die SDPI erstellte 41 Protokolle über Verwaltungsverstöße (im Jahr 2010 wurden lediglich 29 Protokollbeschlüsse vom Gericht herausgegeben).
Geldbußen	23
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Videoüberwachung in einem Schönheitssalon

Bei der SDPI ging eine Beschwerde darüber ein, dass in einem Schönheitssalon Videoüberwachungskameras installiert worden waren und dass eine dieser Kameras versteckt und so ausgerichtet war, dass sie den gesamten Körper des Kunden/der Kundin filmen konnte. Eine weitere Kamera war im Umkleideraum des Personals installiert. Die SDPI stellte fest, dass die betreffende Videoüberwachung ohne ein schriftliches Dokument des für die Verarbeitung der Daten Verantwortlichen zur Regelung der Überwachung erfolgt war und dass die Kameras in Räumen angebracht waren, in denen die Datensubjekte von einem absoluten Schutz ihrer Privatsphäre ausgingen. Die SDPI stellte außerdem fest, dass der für die Datenverarbeitung Verantwortliche keine Kontaktangaben für die Datensubjekte bereitgestellt, das Personal nicht schriftlich über die Videoüberwachung informiert und die SDPI nicht über die automatische Verarbeitung von Daten in Kenntnis gesetzt hatte. Hinsichtlich der Verletzungen des LLPPD erstellte die SDPI ein Register für die vom Eigentümer des Schönheitssalons begangenen Verwaltungsvergehen. Das erste Bezirksgericht der Stadt Wilna ließ das Register der Verwaltungsvergehen zu und verhängte eine Geldbuße gegen den Eigentümer des Schönheitssalons.

Das Recht von Anwälten auf die Erfassung sensibler personenbezogener Daten

Bei der SDPI ging eine Beschwerde darüber ein, dass der Leiter eines Krankenhauses auf die Anfrage eines Rechtsanwalts im Rahmen der Rechtsvertretung seines Mandanten die Offenlegung der gesamten Krankenakte des Beschwerdeführers und somit die möglicherweise illegale Veröffentlichung dieser Akte genehmigte.

Nach einer Untersuchung wurde festgestellt, dass der Anwalt auf der Grundlage seines Rechtsvertretungsvertrages und Artikel 44 des Gesetzes über die Rechtsanwaltschaft der Republik Litauen vom Krankenhaus eine Abschrift der Krankenakte des Beschwerdeführers angefordert hatte. Die Abschrift sollte als Beweisstück vor Gericht dienen, um zu belegen, ob die durch einen Hundeangriff (im Rahmen dessen kein physischer Kontakt zwischen dem Beschwerdeführer und dem Hund stattgefunden hatte) ausgelösten Angstzustände Auswirkungen auf die Gesundheit des Beschwerdeführers hatten und, wenn ja, in welchem Umfang. Der Anfrage wurde entsprochen, und der Rechtsanwalt legte die Krankenakte bei Gericht vor.

Artikel 180 der Zivilprozessordnung der Republik Litauen besagt, dass ein Gericht vorgelegte Informationen nur dann annehmen darf, wenn sie Umstände be- oder widerlegen, die für den Fall relevant sind.

Im Einklang mit dem LLPPD und der Zivilprozessordnung kam die SDPI zu dem Schluss, dass die Bereitstellung einer kompletten Abschrift der Krankenakte des Beschwerdeführers für den Anwalt statt der Bereitstellung eines auf den Hundeangriff beschränkten Auszugs aus der Krankenakte in diesem Fall nicht unverhältnismäßig war und somit keine Verletzung der Bestimmungen des LLPPD vorlag.

Der Beschwerdeführer legte Berufung gegen die Entscheidung der SDPI beim regionalen Bezirksverwaltungsgericht in Wilna ein. Das Gericht wies die Berufung jedoch aus den gleichen Gründen ab, die auch der Entscheidung der SDPI zugrunde lagen. Der Beschwerdeführer legte auch gegen diese Entscheidung Berufung ein, jedoch wurde diese vom Obersten Verwaltungsgericht der Republik Litauen (nachstehend „Oberstes Verwaltungsgericht“) abgewiesen.

Von der Polizei zum Zwecke interner Untersuchungen erfasste personenbezogene Daten

Bei der SDPI ging eine Beschwerde ein, die Polizei habe illegal personenbezogene Daten des Beschwerdeführers erfasst. Die SDPI ermittelte, dass bei der Polizei ein anonymer Hinweis dahingehend eingegangen war, dass ein Polizeibeamter (der Bruder des Beschwerdeführers) bei seinem Antrag auf Erstattung von Reisekosten falsche Angaben zu seinem Wohnort und seinem Fahrzeug gemacht habe. Auf der Grundlage dieses anonymen Hinweises leitete die Polizei eine interne Untersuchung ein und überprüfte die personenbezogenen Daten des Beamten. Es wurde festgestellt, dass das Fahrzeug, für das der Polizeibeamte eine Erstattung beantragt hatte, auf den Beschwerdeführer zugelassen war. Aus diesem Grund überprüfte die Polizei die Daten des Beschwerdeführers im Kraftfahrzeugregister der Republik Litauen, um festzustellen, welche Kraftfahrzeuge sich im Besitz des Beschwerdeführers befanden.

Die SDPI entschied, dass diese Art der Erfassung der personenbezogenen Daten des Beschwerdeführers eine Verletzung von Artikel 3 Absatz 1 des LLPPD darstellte und erließ eine Anweisung. Das regionale Bezirksverwaltungsgericht in Wilna wies die Argumente der SDPI jedoch zurück und stellte fest, dass die personenbezogenen Daten des Beschwerdeführers aufgrund legitimer Interessen zur Durchführung einer gründlichen internen Untersuchung verarbeitet wurden. Die SDPI legte Berufung gegen diese Entscheidung ein, und das Oberste Verwaltungsgericht gab der Berufung statt, da der Umfang der erfassten personenbezogenen Daten über die Erfüllung des Zwecks der internen Untersuchung hinausging.

C. Sonstige wichtige Informationen

Die SDPI arbeitet an der Umsetzung des Projekts „Elektronisches Dienstleistungssystem der SDPI“. Ziel des Projekts ist die Umstellung von vier öffentlichen Diensten der SDPI (zwei Dienste für Einwohner und zwei für Unternehmen) auf das elektronische Umfeld zur Verbesserung der Qualität der Dienstleistungen, zur Förderung des Datenschutzes im elektronischen Umfeld sowie als Beitrag zur Entwicklung der Informationsgesellschaft.

LUXEMBURG

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetzesänderungen

Das Gesetz vom 30. Mai 2005 über Sonderregelungen zum Schutz der Privatsphäre im Bereich elektronische Kommunikation wurde durch ein Gesetz vom 24. Juli 2010 abgeändert. Dieses Gesetz setzt die Bestimmungen von Richtlinie 2006/24/EG über die Vorratsdatenspeicherung in luxemburgisches Recht um. Es besagt, dass Daten sechs Monate lang von den verschiedenen nationalen Anbietern von Telekommunikationsdiensten bzw. Netzbetreibern gespeichert werden dürfen. Auf richterliche Ermächtigung hin darf nur von den Strafverfolgungsbehörden zum Zweck der Untersuchung, Aufdeckung sowie strafrechtlichen Verfolgung „schwerer Straftaten" darauf zugegriffen werden. Als schwere Straftaten sind Straftaten definiert, die mit einer Freiheitsstrafe von mindestens einem Jahr bewehrt sind. Die großherzogliche Verordnung vom 24. Juli 2010 umfasst eine detaillierte Liste der unterschiedlichen Datenkategorien, die für Mobilfunk- und Festnetz- sowie Internetverbindungen zu speichern sind.

Wichtige Themen

Die Datenschutzkommission (*Commission nationale, CNPD*) beriet die luxemburgische Regierung im Laufe des Jahres 2010 zu einer Vielzahl gesetzgeberischer Fragen. Die wichtigsten Themen hierbei waren folgende:

- das vorgenannte Gesetz zur Umsetzung der Bestimmungen von Richtlinie 2006/24/EG;
- der Entwurf für eine großherzogliche Verordnung zur Einrichtung einer nationalen Schülerdatenbank beim Bildungsministerium;
- der Gesetzesentwurf über elektronische Krankenakten;
- der Gesetzesentwurf zur Umsetzung der Bestimmungen von Richtlinie 2009/136/EG.

Neuerungen

Die Verarbeitung sensibler Daten zu medizinischen und wissenschaftlichen Zwecken machte einen Großteil der Arbeit der Kommission im Bereich der Vorabgenehmigungen und Beratung von für die Datenverarbeitung Verantwortlichen aus.

Die CNPD veröffentlichte allgemeine Leitlinien zur Verarbeitung der Daten von Bürgerinnen und Bürgern durch lokale Behörden. Die Datenschutzbehörde wurde auch im Zusammenhang mit der Vorbereitung der allgemeinen Volkszählung Anfang 2011 konsultiert.

Hinsichtlich der „unbeabsichtigten" Erfassung von Wi-Fi-Daten durch Google im Rahmen der Erfassungsfahrten für „Street View" beschloss die Datenschutzbehörde die Durchführung einer Untersuchung, in deren Rahmen ein Auto von Google mit Hilfe eines externen Spezialisten inspiziert wurde. Dieser kam zu dem Schluss, dass alle strittigen Vorrichtungen aus dem Auto entfernt worden waren. Darüber hinaus erhielt die Datenschutzbehörde zufrieden stellende Antworten auf alle von ihr gestellten Fragen.

Im Laufe des Jahres 2010 musste die Datenschutzbehörde in verschiedenen Fällen von Verletzungen des Datenschutzes bzw. von mangelnden Sicherheitsmaßnahmen eingreifen, unter anderen im Zusammenhang mit der unbeabsichtigten Übermittlung personenbezogener Daten an nicht vorgesehene Empfänger, Datenverluste, Verletzungen des Datenschutzes im Zusammenhang mit Kundenakten sowie vielen Fällen von gehackten Websites (d. h. mangelhafter Sicherheitsmaßnahmen).

Wichtige Veranstaltungen und Sensibilisierung

Die CNPD setzte ihre Informations- und Sensibilisierungskampagne auch im Jahr 2010 fort. Zusätzlich zu einer umfassenden Informationskampagne anlässlich des Europäischen Datenschutztages beteiligte sich die *Commission*

nationale zusammen mit dem Ministerium für Wirtschaft und Handel aktiv an einer Sensibilisierungskampagne zum Thema Sicherheit von Passwörtern. Die CNPD beteiligte sich außerdem an der Entwicklung einer Broschüre mit dem Titel „Wie schütze ich meine Daten im Internet", die sich insbesondere an Kinder und Jugendliche richtet. Im Jahr 2010 wurden insgesamt 21 Konferenzen und Schulungen sowie zahlreiche Treffen mit Vertretern des öffentlichen oder privaten Sektors organisiert.

Um die Transparenz gegenüber der Öffentlichkeit zu verbessern, hat die Kommission alle für die Datenverarbeitung Verantwortlichen, die eine Vorabgenehmigung zur Durchführung einer Videoüberwachung erhalten haben, aufgefordert, spezielle von der CNPD gestaltete Hinweisschilder zu verwenden. Diese Hinweisschilder sind neben den Überwachungskameras zu platzieren, um die Öffentlichkeit über das Vorhandensein eines Überwachungssystems zu informieren. Auf den Hinweisschildern ist unter anderem die Genehmigungsnummer ausgewiesen, anhand derer die Öffentlichkeit den Umfang und Beschränkungen der genehmigten Datenverarbeitung im öffentlichen Register verifizieren kann.

Organisation	*Commission nationale pour la protection des données* (CNPD)
Vorsitz und/oder Gremium	Herr Gérard Lommel – Präsident Herr Thierry Lallemang – Kommissar Herr Pierre Weimerskirch – Kommissar
Budget	1 440 000 EUR
Personal	Rechtsabteilung: 4 Meldungen und Vorabprüfungen: 2 Allgemeine Verwaltung: 3 Kommunikation und Dokumentation: 1 Gesamt: 13
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	436
Meldungen	310
Vorabprüfungen	483
Anträge betroffener Personen	242
Beschwerden betroffener Personen	145
Vom Parlament bzw. der Regierung angeforderte Beratung	6
Treffen und Konsultationen (öffentlicher/privater Sektor)	110
Informationssitzungen und Konferenzen	21

Verbindliche unternehmensinterne Vorschriften als leitende Datenschutzbehörde	2
Prüfmaßnahmen	
Prüfungen, Untersuchungen	16
Sanktionen	
Sanktionen	3
Geldbußen	k.A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Im Laufe des Jahres 2010 ernannte Datenschutzbeauftragte: 10 (Zum Zeitpunkt der Erstellung des Berichts) insgesamt ernannte Datenschutzbeauftragte: 55

.

B. Rechtsprechung

Das in Zivilsachen zuständige Friedensgericht (Tribunal de Paix) zum Schadenersatz aufgrund eines in einer nationalen Zeitung veröffentlichten Artikels

Ein Zeitungsartikel enthielt die Initialen, den Beruf sowie eine Beschreibung der Tätigkeit eines Gemeindeangestellten; darüber hinaus stellte der Artikel einen direkten Zusammenhang zwischen dem Kläger und einem Vergehen wegen Trunkenheit am Steuer her. Das Gericht sah die Erwähnung dieser Informationen als Verletzung der Privatsphäre des Klägers an. Wenngleich sich dieser Fall nicht direkt auf die Bestimmungen des Datenschutzgesetzes bezieht, kann er dennoch als Präzedenzfall im Bereich des Schutzes der Privatsphäre eingestuft werden, da die Richter einen Test festlegten, mithilfe dessen das Recht auf den Schutz der Privatsphäre und das Recht auf Pressefreiheit miteinander in Einklang gebracht werden können.

MALTA

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Berichtszeitraum wurden keine legislativen Änderungen am Datenschutzgesetz sowie den entsprechenden Verordnungen vorgenommen. Unbeschadet dessen arbeitete die Datenschutzbehörde eng mit der Kommunikationsbehörde von Malta zusammen, um mit der Umsetzung von Richtlinie 2009/136/EG zu beginnen, die unter anderem Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ändert. Ein Entwurf für einen rechtlichen Hinweis zur Einführung der neuen und revidierten Bestimmungen wurde erarbeitet und vom Büro des Generalstaatsanwalts überprüft. Die Veröffentlichung war für das zweite Quartal 2011 vorgesehen. Die Zusammenarbeit mit der Kommunikationsbehörde von Malta bei der Umsetzung war erforderlich, da die Richtlinie 2002/58/EG im Jahr 2003 teilweise im Rahmen des Datenschutzgesetzes umgesetzt wurde, während der technische Teil im Rahmen des Gesetzes über die elektronische Kommunikation umgesetzt wurde.

Es gab zwei Fälle, in denen sich eine beteiligte Partei von der Entscheidung des Kommissars benachteiligt fühlte und daher gemäß Artikel 49 des Gesetzes Berufung vor dem Berufungsausschuss für Datenschutzfragen einlegte. In einem Fall entschied der Ausschuss zugunsten des Kommissars. Angesichts der Tatsache, dass der Berufungskläger nicht innerhalb des festgelegten Zeitrahmens Berufung gegen die Entscheidung des Ausschusses einlegte, wurde der Fall geschlossen. Im anderen Fall zog der Berufungskläger nach der zweiten Sitzung des Ausschusses seine Berufung zurück und hielt sich an die vom Kommissar ausgesprochenen Anweisungen. Der Berufungskläger akzeptierte die Entscheidung des Kommissars, und der Fall wurde geschlossen.

Des Weiteren wurden Anträge von für die Datenverarbeitung Verantwortlichen auf Vorabprüfung betreffend die Einführung biometrischer Systeme und die Installation von Überwachungskameras am Arbeitsplatz sowie in anderen Bereichen, in denen die Verarbeitung von Daten ein besonderes Risiko der Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen mit sich brachte, eingereicht.

Die Behörde ist verpflichtet, zum Nutzen der Bürgerinnen und Bürger sowie zum Nutzen der verschiedenen Sektoren und für die Datenverarbeitung Verantwortlichen für das Thema Datenschutz zu sensibilisieren. Um dieses Ziel zu erreichen, werden regelmäßig Präsentationen organisiert, Interviews für lokale Zeitungen gegeben und Zeitungsbeiträge verfasst. Im Laufe dieses Jahres organisierte die Behörde Präsentationen in verschiedenen Einrichtungen zur Anwendbarkeit der Datenschutzbestimmungen in spezifischen Sektoren. Unter anderem wurden Präsentationen für den Arbeitgeberverband von Malta, die maltesische Polizei, die Beschäftigungs- und Ausbildungskorporation, Young Enterprise sowie die Universität von Malta organisiert. Im Berichtsjahr hatte die Behörde die Gelegenheit, in Form eines monatlichen Artikels im IT-Teil der Times of Malta einen Beitrag zu liefern. Diese Artikel befassten sich mit Fragen zum Thema Datenschutz in verschiedenen Bereichen der digitalen Welt wie z. B. biometrische Geräte, Cloud-Computing, verhaltensorientierte Internetwerbung und Überwachungskameras. Diese Initiative zur Sensibilisierung stieß auf positives Feedback.

Am 28. Januar feierte die maltesische Datenschutzbehörde zusammen mit den anderen europäischen Datenschutzbehörden den Europäischen Datenschutztag. Um vor Ort auf diesen Tag aufmerksam zu machen, verteilte die Datenschutzbehörde Informationsmaterial an Schüler in allen staatlichen, privaten und kirchlichen Schulen. Dieses Material diente hauptsächlich dem Zweck, den Bürgerinnen und Bürgern, insbesondere den jungen, zu vermitteln und sie dafür zu sensibilisieren, welche Risiken 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. Solche Veränderungen brauchen 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, und die Datenschutzbehörde hat es 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.

Im Laufe des Jahres 2010 traten bestimmte Bestimmungen des Gesetzes über die Informationsfreiheit in Kraft. Mit dem gleichen Gesetz wurden auch Verordnungen zu den für den Zugang zu Dokumenten erhobenen Gebühren, zum Zeitrahmen, innerhalb dessen eine Beschwerde bzw. ein Antrag auf Untersuchung vorgebracht werden muss, sowie

Muster für Antragsformulare zur Einreichung von Auskunftsersuchen durch die Öffentlichkeit veröffentlicht. Die übrigen wichtigen Bestimmungen sollen in naher Zukunft eingeführt werden.

Organisation	
Vorsitz und/oder Gremium	Informations- und Datenschutzbeauftragter
Budget	290 000 EUR
Personal	Fachpersonal – 4 Technische Unterstützung – 2 Administrative Unterstützung – 2
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Entscheidungen – 16 Entscheidungen/ hinsichtlich der bei der Behörde eingegangenen formellen Beschwerden wurden Anweisungen ausgesprochen. Es wurden 22 Stellungnahmen/Empfehlungen herausgegeben. Hierbei handelte es sich um Stellungnahmen in Form von Zeitungsartikeln, die sich sowohl an die allgemeine Öffentlichkeit als auch an für die Datenverarbeitung Verantwortliche richteten, sowie um sonstige Stellungnahmen und Empfehlungen, die für die Datenverarbeitung Verantwortlichen zu spezifischen Themen bereitgestellt wurden.
Meldungen	184 neue Meldungen
Vorabprüfungen	4 Anträge auf Vorabprüfung
Anträge betroffener Personen	Anfragen per Telefon – durchschnittlich 35 Anrufe pro Woche Anfragen per E-Mail – 191.
Beschwerden betroffener Personen	44 Beschwerden
Vom Parlament bzw. der Regierung angeforderte Beratung	k.A.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	k.A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Im Jahr 2010 wurden insgesamt 8 Prüfungen durchgeführt: 3 Prüfungen betrafen die Verarbeitung von Daten durch die Strafverfolgungsbehörden und wurden zentral von den Gemeinsamen Aufsichtsbehörden koordiniert; 4 Prüfungen wurden zur Untersuchung bestimmter Beschwerden durchgeführt; 1 Prüfung wurde nach vorherigem Antrag auf Vorabprüfung durchgeführt.

Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Im Jahr 2010 wurden 22 Datenschutzbeauftragte ernannt.

B. Rechtsprechung

Im Berichtszeitraum gab es keine neue Rechtsprechung.

NIEDERLANDE

A. Zusammenfassung der Aktivitäten und Neuerungen

Um einen so effektiven und sinnvollen Schutz personenbezogener Daten wie möglich zu gewährleisten, setzt die niederländische Datenschutzbehörde Prioritäten. Grundlage dieser Priorisierung ist eine Risikobewertung, die unser Büro jährlich durchführt und die anhand der bei uns eingehenden Hinweise zahlreicher Quellen wie z. B. Zeitungen oder die für Bürgerinnen und Bürger eingerichtete Hinweisfunktion unserer Website immer wieder aktualisiert wird. Bei dieser Risikobewertung werden die Schwere des zur Last gelegten Vergehens, die Anzahl der betroffenen Personen, die Eindeutigkeit der Anhaltspunkte für den Verstoß sowie die rechtliche Durchführbarkeit und die Auswirkungen der umfassenden Nutzung neuer Technologien berücksichtigt. Im Allgemeinen konzentriert sich die niederländische Datenschutzbehörde auf die Umsetzung von Strategien, um insgesamt ein höheres Maß der Einhaltung von Vorschriften zu erreichen.

Im Jahr 2010 wurde die von der niederländischen Datenschutzbehörde durchgeführte Untersuchung der Sicherheitsmaßnahmen von Krankenhäusern bezüglich der Patientendaten abgeschlossen. Nach Durchsetzungsmaßnahmen zu abgestuften Bußgeldzahlungen führte das zuletzt untersuchte Krankenhaus eine zufrieden stellende erneute Risikoanalyse durch und erfüllte somit die Sicherheitsstandards für das Gesundheitswesen. Nachdem das Krankenhaus die Datenschutzbehörde über die ergriffenen Korrekturmaßnahmen in Kenntnis gesetzt hatte, konnte die Untersuchung abgeschlossen werden. Die niederländische Datenschutzbehörde untersuchte auch die Erfassung und den anschließenden Verkauf sensibler Daten und Profile von Personen, die eine Website aus dem Bereich Gesundheit besucht hatten.

Zudem untersuchte die niederländische Datenschutzbehörde unter anderem die folgenden Arten von Datenverarbeitung:

- die Erfassung von Wi-Fi-Daten durch Street-View-Fahrzeuge von Google;
- die Verarbeitung personenbezogener Daten von Studenten über eine Chipkarte für den öffentlichen Verkehr;
- die Verknüpfung von Dateien durch den Untersuchungsdienst der Sozialversicherung;
- die Einspeisung polizeilicher Informationen in das Informationssystem von Europol;
- die Nutzung der automatischen Kennzeichenerkennung durch zwei Polizeikräfte;
- den Austausch von Patientendaten unter Verwendung regionaler elektronischer Patientenakten.

In einigen Situationen musste die Datenschutzbehörde unmittelbar reagieren, so beispielsweise in dem Fall, in dem sie Diskussionen mit den Bürgermeistern der Städte Ede und Enschede hinsichtlich der ethnischen Registrierung von Roma in diesen Städten initiierte.

Neben der Durchführung von Untersuchungen berät die niederländische Datenschutzbehörde die Regierung zu Gesetzesentwürfen, bevor diese dem Parlament vorgelegt werden. Nach der Beratung durch die niederländische Datenschutzbehörde werden die Vorschläge (oftmals) abgeändert, um Verletzungen der Privatsphäre vorzubeugen. So wurde unter anderem der Gesetzesvorschlag zur Einführung intelligenter Zähler auf der Grundlage von Vorschlägen der niederländischen Datenschutzbehörde zugunsten der Verbraucher abgeändert. Auch der Gesetzesvorschlag zur Einführung einer Alkoholsperre bei Kraftfahrzeugen wurde geändert, um sicherzustellen, dass die Daten nicht länger als erforderlich gespeichert werden.

Schließlich beabsichtigt das niederländische Kabinett, das im vergangenen Jahr seine Tätigkeit aufgenommen hat, die Vorlage eines aktualisierten Gesetzes zum Schutz personenbezogener Daten im Einklang mit den Intentionen des vorherigen Kabinetts. Die niederländische Datenschutzbehörde hat sich aktiv in den Konsultationsprozess vor der eigentlichen Erarbeitung des Gesetzesentwurfes eingebracht, um sicherzustellen, dass ein gutes Gesetz entworfen wird, von dem die Datensubjekte, die für die Datenverarbeitung Verantwortlichen und auch die Datenschutzbehörde selbst profitieren.

Organisation	Niederländische Datenschutzbehörde
Vorsitz und/oder Gremium	Jacob Kohnstamm, Vorsitzender. Jannette Beuving, Mitglied des Gremiums und stellvertretende Vorsitzende. Madeleine McLaggan, Mitglied des Gremiums.
Budget	Zugewiesen: 7 679 000 EUR Ausgegeben: 7 699 000 EUR
Personal	77 Vollzeitangestellte (88 Angestellte)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	775 (Untersuchungen, Leitlinien, Verhaltensregeln, Vorabprüfungen, Sanktionen und Beratung zu Gesetzgebungsverfahren)
Meldungen	3 720
Vorabprüfungen	642
Anträge betroffener Personen	Der Datenschutzbehörde über die Website gemeldete Fälle: 974. Eingegangene E-Mails: 2 814. Eingegangene Anrufe: 2 417. Von all diesen eingegangenen Anfragen wurden 172 Beschwerden, 226 Auskunftsersuche und 154 Schlichtungsfälle umfassend bearbeitet.
Beschwerden betroffener Personen	Anzahl der bearbeiteten berechtigten Beschwerden: 172
Vom Parlament bzw. der Regierung angeforderte Beratung	35
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	60
Sanktionsmaßnahmen	
Sanktionen	35
Geldbußen	k.A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Der Datenschutzbehörde wurden 310 Datenschutzbeauftragte gemeldet.

B. Rechtsprechung

1. Verwendung von Überwachungskameras und deren Rolle bei Gerichtsverfahren

Eine Person wurde schwer verletzt, als ihr in einem Lokal ein Bierglas ins Gesicht geschlagen wurde. Der Vorfall wurde von einer Überwachungskamera in dem Lokal aufgezeichnet. Als die Polizei in der gleichen Nacht am Tatort eintraf, nahmen sie das Videomaterial in Augenschein. Der Inhaber des Lokals beschloss, das Videomaterial aufzubewahren und es auf einer CD zu speichern – angeblich, um sicherzugehen, dass die Polizei das Material gegebenenfalls erneut in Augenschein nehmen könne.

In diesem Fall war das Gericht der Ansicht, dass der Inhaber der Polizei das Videomaterial auf der Grundlage von Artikel 8 Absatz f sowie von Artikel 9 und 43 des niederländischen Gesetzes zum Schutz personenbezogener Daten auf freiwilliger Basis und im Interesse der Vorbeugung, Erkennung und strafrechtlichen Verfolgung von Straftaten zur Verfügung stellen durfte. Das Gericht war zudem der Ansicht, dass ein möglicher Verstoß gegen das niederländische Gesetz zum Schutz personenbezogener Daten durch Bereitstellung der Videoaufnahmen für die Polizei gemäß den Bestimmungen des Gesetzes die Aufnahmen nicht zwangsläufig für ein Gerichtsverfahren unverwertbar macht, da es der Polizei möglich gewesen wäre, die Aufnahmen gemäß Artikel 126nd des Strafgesetzbuches anzufordern.

Darüber hinaus erachtete das Gericht die Daten in diesem Fall nicht als sensible Daten im Sinne von Artikel 126nf des Strafgesetzbuches, da die Videoaufnahmen nicht mehr umfassten als das, was im Lokal anwesende Personen auch hätten beobachten können. Außerdem enthielten sie keine zusätzlichen Informationen zu den gefilmten Personen.

Dieses Urteil des Gerichts steht im Einklang mit dem Urteil des Europäischen Gerichtshofs für Menschenrechte im Fall Perry ./. Vereinigtes Königreich, in dem der Gerichtshof entschied, dass der normale Einsatz von Überwachungskameras an öffentlichen Orten nicht zu einer Verletzung der Privatsphäre führt.

2. Das Recht auf Berichtigung

Eine Person beantragte die Herausgabe von Dokumenten, die zur Erstellung eines individuellen Berichts verwendet wurden, der als Grundlage zur Bewertung ihres Antrags auf Aufenthaltsgenehmigung diente, und beantragte anschließend eine Richtigstellung der Dokumente und des individuellen Berichts. Der Antrag wurde abgelehnt. Der Staatsrat (der höchste Verwaltungsgerichtshof) befand, dass der Zweck des Rechts auf Richtigstellung nicht die Korrektur oder Löschung von Eindrücken, Meinungen, Untersuchungsergebnissen und Schlussfolgerungen im Rahmen von Beratungen ist, mit denen die betreffende Person nicht einverstanden ist. Darüber hinaus entschied der Staatsrat, dass der Justizminister sich rechtmäßig auf Artikel 43 Absatz e des niederländischen Datenschutzgesetzes berufen konnte, da bestimmte Abschnitte des individuellen Berichts unkenntlich gemacht worden waren.

3. Das Recht auf Zugang zu sowie Berichtigung von personenbezogenen Daten

Beim Justizminister ging ein Antrag einer natürlichen Person auf Zugang zu und Berichtigung von Daten sowohl der Person selbst als auch einer Stiftung ein, die vom „Bureau BIBOB“ geleitet wird (BIBOB steht für das Gesetz zur Förderung der Integrität von Entscheidungen der öffentlichen Verwaltung). Der die Daten der Stiftung betreffende Antrag wurde abgelehnt, da eine Stiftung keine natürliche Person ist und somit Artikel 35 und 36 nicht herangezogen werden konnten. Der Antrag auf Zugang zu und Berichtigung der personenbezogenen Daten der betreffenden Person wurde abgelehnt, da der Justizminister befand, dass das BIBOB-Gesetz enge Vorschriften für die Übermittlung von Daten enthält und dadurch das niederländische Datenschutzgesetz nicht anwendbar sei.

Das Gericht entschied jedoch, dass das BIBOB-Gesetz Anträge auf der Grundlage der Artikel 35 und 36 des niederländischen Datenschutzgesetzes nicht ausschließt. Das Gericht leitete diese Entscheidung aus der Rechtsgeschichte ab. Aus diesem Grund sei das niederländische Datenschutzgesetz anwendbar. Zusätzlich gelten die engen Vorschriften für die Übermittlung von Daten des BIBOB-Gesetzes nur für Daten von Dritten und nicht für die vom Bureau gespeicherten Daten zu der den Antrag auf Zugang zu und Berichtigung von Daten stellenden Person. Aus diesem Grund forderte das Gericht das Bureau BIBOB auf, die Anträge des Antragstellers erneut zu prüfen.

POLEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Jahr 2010 jährte sich das Gesetz zum Schutz personenbezogener Daten vom 29. August 1997 zum 12. Mal.

2010 wurde ein neuer Generalinspektor für den Schutz personenbezogener Daten (GIODO) ernannt. Am 25. Juni 2010 betraute der Sejm (eine der beiden Parlamentskammern der Republik Polen) Dr. Wojciech Rafał Wiewiórowski mit diesem Posten. Nach der Zustimmung durch den Senat der Republik Polen und nach seiner Vereidigung am 4. August 2010 nahm Dr. Wojciech Rafał Wiewiórowski seine Arbeit als GIODO auf und begann somit seine vierjährige Amtszeit.

In diesem Jahr wurden auch legislative Arbeiten zur Revision des polnischen Gesetzes zum Schutz personenbezogener Daten durchgeführt, die zur Inkraftsetzung des Gesetzes vom 29. Oktober 2010 zur Änderung des Gesetzes zum Schutz personenbezogener Daten durch das Parlament führten.

Zu den bedeutendsten durch die Änderung des Gesetzes eingeführten Änderungen gehören neue Kompetenzen des GIODO wie beispielsweise die Befugnis zur Verhängung von Geldbußen als Durchsetzungsmaßnahme für Körperschaften, die sich nicht an die Entscheidungen des GIODO halten.

Zudem wurde ein explizites Recht für den GIODO eingeführt, die zuständigen Behörden aufzufordern, bei Fällen betreffend den Schutz personenbezogener Daten legislative Maßnahmen zu ergreifen und Rechtsakte zu erlassen oder zu ändern. Körperschaften, denen eine formelle Stellungnahme bzw. Aufforderung des GIODO zugestellt wurde, sind nunmehr verpflichtet, binnen 30 Tagen nach Eingang zu reagieren.

Mit den geänderten Bestimmungen des Gesetzes zum Schutz personenbezogener Daten wurde eine neue Art der Straftat eingeführt, nämlich die Ver- oder Behinderung der Durchführung von Inspektionen durch den GIODO. Die Strafe für dieses Vergehen kann in Form einer Geldbuße, einer Freiheitsbeschränkung oder einer Gefängnisstrafe von bis zu zwei Jahren ausgesprochen werden und nicht nur gegen den für die Datenverarbeitung Verantwortlichen verhängt werden, sondern auch gegen alle Personen, die an der Inspektion beteiligt sind oder die Durchführung dieser Inspektion be oder verhindern. Das Gesetz zur Änderung des Gesetzes zum Schutz personenbezogener Daten wurde 2010 verabschiedet und tritt am 7. März 2011 in Kraft.

Organisation	Büro des Generalinspektors für den Schutz personenbezogener Daten (Generalny Inspektor Ochrony Danych Osobowych)
Vorsitz und/oder Gremium	Dr. Wojciech Rafał Wiewiórowski, Generalinspektor für den Schutz personenbezogener Daten
Budget	13 842 000 PLN
Personal	127
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden 1 412 Verwaltungsentscheidungen herausgegeben, wovon 879 die Anmeldung von Dateien mit personenbezogenen Daten, 137 Inspektionen, 359 Beschwerden und 37 die Übermittlung personenbezogener Daten in Drittländer betrafen.
Meldungen	Es wurden 9 921 Dateien mit personenbezogenen Daten gemeldet.
Vorabprüfungen	Als Folge der Anmeldeverfahren (Vorabprüfungen) wurden 1 650 Dateien mit personenbezogenen Daten in das Register der Dateien mit personenbezogenen Daten aufgenommen; die Verarbeitung personenbezogener Daten durch solche Systeme kann nach Abschluss des

	Anmeldeverfahrens aufgenommen werden.
Anträge betroffener Personen	3 448 Rechtsfragen
Beschwerden betroffener Personen	1 114 Beschwerden über Verletzungen des Schutzes personenbezogener Daten, unter anderem in folgenden Bereichen: • Öffentliche Verwaltung (149 Beschwerden); • Gerichte, Staatsanwaltschaft, Polizei, Gerichtsvollzieher (55 Beschwerden); • Banken und andere Finanzinstitute (119 Beschwerden); • Internet (157 Beschwerden); • Marketing (59 Beschwerden); • wohnungsbezogen (52 Beschwerden); • Sozial-, Sach- und Personenversicherungen (28 Beschwerden); • Schengener Informationssystem (38 Beschwerden); • Telekommunikation (57 Beschwerden); • Beschäftigung (77 Beschwerden); • sonstiges (323 Beschwerden).
Vom Parlament bzw. der Regierung angeforderte Beratung	Dem GIODO wurden 617 Gesetzesentwürfe zur Prüfung vorgelegt.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	55 – Anzahl der durch den GIODO durchgeführten Schulungen zu den Bestimmungen zum Schutz personenbezogener Daten, insbesondere für öffentliche Einrichtungen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	196 Inspektionen, unter anderem bei: • Universitäten, Einrichtungen der Hochschulbildung (26 Inspektionen); • Investmentfirmen mit Vermittlungstätigkeiten (16 Inspektionen); • Steuerprüfungsbüros (10 Inspektionen); • Anbieter von Telekommunikationsdienstleistungen (14 Inspektionen); • Kommunale Körperschaften (16 Inspektionen); • Versicherungsunternehmen (12 Inspektionen)
Sanktionsmaßnahmen	
Sanktionen	Im Jahr 2010 gab der GIODO 23 Meldungen zu vermuteten Rechtsverletzungen heraus. Die Gerichte verhängten gegen keine der betreffenden Körperschaften strafrechtliche Sanktionen
Geldbußen	
Datenschutzbeauftragte (DPO)	

Zahlenangaben zu DPO	k.A.

.

B. Rechtsprechung

Eine wichtige Entscheidung stellte die Anordnung des regionalen Verwaltungsgerichts in Warschau vom 12. Mai 2012 (II SA/Wa 652/10) dar, die die Entscheidung des GIODO bestätigt, keine Informationen zur Inspektion eines staatlichen Versorgungsunternehmens in Form eines Inspektionsprotokolls zu veröffentlichen – der entsprechende Antrag wurde als nicht zulässig abgewiesen. Der GIODO hatte sich unter Berufung auf das die angefragten Informationen betreffende Betriebsgeheimnis geweigert, die Informationen zu veröffentlichen.

Das Oberste Verwaltungsgericht war, ebenso wie der GIODO, der Ansicht, dass Körperschaften, die anderen Personen Produkte oder Dienstleistungen verkaufen, im Falle von Ansprüchen betreffend diese Produkte oder Dienstleistungen gemäß Artikel 23 Absatz 1 Ziffer 5 sowie Artikel 23 Absatz 4 Ziffer 1 des Gesetzes zum Schutz personenbezogener Daten keine personenbezogenen Daten zu Marketingzwecken verarbeiten (NSA Urteil vom 5. Januar 2010, Fallnummer I OSK 399/09). Das Gericht stellte fest, dass ein Autohändler verpflichtet ist, das Einverständnis potenzieller Kunden (d. h. Personen, die am Kauf eines Autos interessiert sind, jedoch keine Probefahrt durchführen) hinsichtlich der Verarbeitung personenbezogener Daten zu Marketingzwecken einzuholen. Die Verarbeitung von Daten auf der Grundlage einer Händlervereinbarung fällt nicht in die Kategorie der Vermarktung eigener Produkte und Dienstleistungen. Somit kann Artikel 23 Absatz 1 Ziffer 5 des Gesetzes (zum Schutz personenbezogener Daten), also das vom für die Datenverarbeitung Verantwortlichenverfolgte berechtigte Interesse, nicht herangezogen werden.

In einem anderen Fall bestätigte das regionale Verwaltungsgericht in Warschau den Standpunkt des GIODO, dass ab dem Moment, ab dem eine natürliche Person in einem Benutzerkonto auf einer Website angemeldet ist, der für die Datenverarbeitung Verantwortliche aufgrund der Identifizierung die vom Datensubjekt geäußerten Einwände gegen die Verarbeitung personenbezogener Daten zu Marketingzwecken berücksichtigen muss, dass also die Anzeige von Werbung einzustellen ist (Urteil des Verwaltungsgerichts in Warschau vom 15. Juni 2010, Fallnummer II SA/WA 556/10).

C. Sonstige wichtige Informationen

Im Jahr 2010 gingen beim Generalinspektor **617 Gesetzesentwürfe mit Bitte um Stellungnahme** ein. Bei der Datenschutzbehörde kamen Bedenken aufgrund der Tendenzen verschiedener Körperschaften auf, sogenannte Mega-Datenbanken mit personenbezogenen Daten zu Millionen von Menschen zu erstellen. Im Jahr 2010 gab der GIODO Stellungnahmen zu verschiedenen Gesetzesentwürfen ab, die Folgendes beinhalteten: Einführung eines Informationssystems im Gesundheitswesen („System Informacji Medycznej“, SIM,) Einführung eines Bildungs-Informationssystem („System Informacji Oświatowej“, SIO), das die statistische Erfassung von Daten beinhaltet und Dateien mit personenbezogenen Daten, darunter auch sensible Daten zu Vorschul- und Schulkindern, Studierenden und Lehrern, umfassen soll, sowie Einführung eines zentralen Körperschaftsregisters, d. h. eines nationalen Steuerzahler-Registers, das teilweise auf Daten der somit in größerem Umfang verfügbaren Sozialversicherungsdatenbank als Referenz zurückgreift, auch für die Zusammenarbeit mit den Steuerbehörden.

Der GIODO war im Jahr 2010 aktiv an der legislativen Arbeit zu Gesetzen zur Umsetzung des geänderten Gesetzes zur Computerisierung von Körperschaften, die öffentliche Aufgaben erfüllen, sowie an Maßnahmen hinsichtlich der Ziele des Gesetzes über die Bereitstellung von Dienstleistungen mithilfe elektronischer Mittel beteiligt. Ein besonderes Augenmerk bei dieser Arbeit lag auf der Vereinbarkeit der Gesetzesentwürfe mit den allgemeinen Grundsätzen des Datenschutzes sowie der Notwendigkeit der Umsetzung der Bestimmungen von Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der

elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

2010 prüfte der GIODO den aktuellen Stand des Schutzes personenbezogener Daten, die in Videoüberwachungssystemen verarbeitet werden. Ziel dieser Prüfung war der Start einer Gesetzgebungsmaßnahme zur umfassenden Regulierung dieses Themas. Diesbezüglich wird der GIODO mit dem Ombudsmann (RPO) zusammenarbeiten.

Im Jahr 2010 wurden im Vergleich zu den Vorjahren mehr Dateien mit personenbezogenen Daten registriert (2008: 3 760, 2009: 6 465, 2010: 9 921). Dies lag möglicherweise daran, dass die Fehlerquote der Erklärungen im Vergleich zu den vergangenen Jahren geringer war. Zweifellos war dieses Ergebnis unter anderem auf die Maßnahmen des GIODO zurückzuführen, die zur Änderung eines Computerprogramms zur Hilfe bei der Ausfüllung eines Antragsformulars führten, das auf der Grundlage der Verordnung des Ministers für Inneres und Verwaltung vom 11. Dezember 2008 hinsichtlich einer Vorlage für die Meldung von Dateien mit personenbezogenen Daten zur Registrierung durch den Generalinspektor für Datenschutz eingeführt worden war.

Im Jahr 2010 führte der GIODO Bildungsmaßnahmen durch, unter anderem:

- Unterzeichnung einer Absichtserklärung mit dem Arbeitgeberverband der Internetbranche IAB Polen. Ziel der Erklärung ist zu gewährleisten, dass Anbieter von Internetdiensten bei ihren Aktivitäten die Grundsätze des Datenschutzes einhalten, insbesondere in Form einer gemeinsamen Entwicklung von Leitlinien für bewährte Verfahrensweisen. Die wichtigsten Medien-Websites sowie andere Unternehmen dieser Branche wollen durch diese Absichtserklärung betonen, dass ihnen der ordnungsgemäße Schutz personenbezogener Daten wichtig ist, um zu erreichen, dass sich die Nutzer der unterschiedlichen Inhalte und Dienste im Internet sicher fühlen können;
- Entwicklung eines Leitfadens für Nutzer öffentlich verfügbarer Telekommunikationsdienste („Guide for users of publicly available telecommunications services“) zusammen mit dem Büro für elektronische Kommunikation (UKE), der sowohl auf die Bedürfnisse der Menschen ausgerichtet ist, die eine Entscheidung hinsichtlich der Nutzung bestimmter Telekommunikationsdienste treffen möchten, als auch auf die, die bereits verschiedene Formen der elektronischen Kommunikation nutzen;

Organisation verschiedener Konferenzen, unter anderem der Konferenz zum Thema Schutz der Privatsphäre („Reform of privacy protection“), die offiziell die öffentliche Debatte zum Thema Datenschutz im Zeitalter der modernen Technologie einleitete. Die öffentliche Debatte soll in eine Stellungnahme zu den Änderungen münden, die an der polnischen und der EU-Gesetzgebung in den Bereichen Datenschutz und Recht auf Privatsphäre vorgenommen werden müssen.

PORTUGAL

A. Zusammenfassung der Aktivitäten und Neuerungen

Dieses Jahr war geprägt von der Vorbereitung von Online-Meldeverfahren, die im Januar 2011 eingeführt werden sollen. Diese Arbeit umfasste die Entwicklung umfassender elektronischer Akten zur deutlichen Reduzierung der Belastung von für die Datenverarbeitung Verantwortlichen hinsichtlich der Erfüllung ihrer Verpflichtungen sowie zur Verkürzung der Reaktionszeit unbeschadet einer korrekten Bewertung. Außerdem wurde das interne Informationssystem der Datenschutzbehörde verbessert, was einen weiteren Schritt im Entmaterialisierungsprozess darstellte, der vor einigen Jahren gestartet wurde. Es wurde ein Verwaltungssystem zur besseren Bearbeitung von Auskunftsersuchen von Datensubjekten und für die Datenverarbeitung Verantwortlichen sowie zur Einreichung von Beschwerden eingerichtet. All diese technischen Entwicklungen mussten nicht ausgelagert werden, sondern wurden durch interne Experten durchgeführt.

Die Datenschutzbehörde beschloss eine Erhöhung der Meldegebühren ab 2011 auf 75 EUR für eine Registrierung und 150 EUR für eine Vorabprüfung der Verarbeitung von Daten.

Das steigende Arbeitspensum (fast 10 000 neue Verfahren) für die gleiche Anzahl von Mitarbeitern (28) sowie die extreme Schwierigkeit des Ausbaus des Personalbestandes aufgrund restriktiver Verwaltungsvorschriften sollten erwähnt werden.

Andererseits wurde eine wesentliche Änderung am Organisationsgesetz der Datenschutzbehörde eingeführt. Das bisher in vollem Umfang aus dem Budget des Parlements stammende Budget kommt nunmehr aus verschiedenen Töpfen und zum Teil aus dem Budget eines Ministeriums – in Höhe des den eigenen Einnahmen der Datenschutzbehörde entsprechenden Betrags. Die Datenschutzbehörde war der Ansicht, dass diese rechtliche Änderung sehr negative Auswirkungen auf ihre Unabhängigkeit hat, da die Verwendung dieser Mittel der Genehmigung einer Dienststelle unterliegen, die direkt der Regierung unterstellt ist. Zudem deckt der weiterhin vom Parlament eingehende Betrag nicht die Kosten der Datenschutzbehörde, was bedeutet, dass die Funktionsweise der Datenschutzbehörde in inakzeptabler Weise von Regierungsentscheidungen abhängt. Die Datenschutzbehörde ist mit umfassenden Kompetenzen im öffentlichen Sektor ausgestattet und sollte daher in der Ausführung ihrer Aufgaben in keiner Weise eingeschränkt werden.

Ebenfalls zu erwähnen ist die Fortführung des Projekts Dadus – ein im Jahr 2008 für Schulen gestartetes Projekt zur Förderung der Sensibilisierung von Kindern im Alter von 10 bis 15 Jahren. Grundlage ist eine Internetplattform, auf der eine Vielzahl von Informationen zum Thema Datenschutz für junge Menschen, Lehrer und Eltern abrufbar ist. Die Datenschutzbehörde entwickelte ein Programm zur Verwendung im Unterricht, im Rahmen dessen von der Datenschutzbehörde erarbeitete multimediafähige Materialien zu verschiedenen Themen eingesetzt werden.

Außerdem startete die Datenschutzbehörde im Jahr 2010 einen zweiten Wettbewerb für Schüler mit dem Titel „Um Slogan pela Privacidade“ (Ein Slogan für den Datenschutz) und beteiligte sich an Dutzenden Schulsitzungen. Für dieses Projekt haben sich bereits mehr als 2 000 Lehrer angemeldet.

Organisation	CNPD – *Comissão Nacional de Protecção de Dados*
Vorsitz und/oder Gremium	Luís Lingnau da Silveira (Vorsitz), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Durão Barroso, Luís Paiva de Andrade, Vasco Almeida
Budget	Zugewiesenes Budget: Etwa 3,480 Millionen EUR (etwa 2,140 Millionen EUR aus den eigenen Einnahmen der Datenschutzbehörde (Geldbußen und Meldegebühren). Ausgegebene Haushaltsmittel: etwa 2 Millionen EUR.
Personal	28

Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	7 120 Beschlüsse. 75 Stellungnahmen zu Gesetzesentwürfen des Parlaments oder der Regierung.
Meldungen	8 269
Vorabprüfungen	7 320
Anträge betroffener Personen	Etwa 5 600 per E-Mail (diese Zahl umfasst auch Anfragen von für die Datenverarbeitung Verantwortlichen an die Zentrale). Anrufe: etwa 11 000 (über die spezielle Datenschutz-Hotline).
Beschwerden betroffener Personen	Etwa 200 (es liegen keine genauen Zahlen vor, da die Beschwerden in der Zahl der von der Datenschutzbehörde eingeleiteten Prüfungen enthalten sind). Die Beschwerden betrafen zumeist unerbetene elektronische Nachrichten (E-Mail und Anrufe) sowie verschiedene Arten der Überwachung von Angestellten am Arbeitsplatz (Videoüberwachung, unangemessene Gesundheitsprüfungen, Überwachung von E-Mail und Internet, Installation von Geolokalisierungsmechanismen in Autos, wie z. B. GPS, sowie in GSM Mobiltelefonen für Angestellte, die diese auch zu privaten Zwecken nutzen dürfen).
Vom Parlament bzw. der Regierung angeforderte Beratung	83 angeforderte Stellungnahmen. Die wesentlichen Themen lauteten: verschiedene bilaterale Abkommen zwischen Portugal und anderen Staaten in folgenden Bereichen: Sozialversicherung, Zusammenarbeit in den Bereichen Steuern und Strafverfolgung, Videoüberwachung öffentlicher Plätze, elektronische Überwachung im Rahmen von Strafverfahren, Datenbanken der Polizei für öffentliche Sicherheit, Einrichtung einer zentralen Bankkonten-Datenbank zur Bekämpfung der Korruption, Umsetzung der Richtlinien 2006/123/EG, 2006/22/EG, 2008/48/EG und 2007/59/EG, relevante Datenschutzfragen betreffend den Staatshaushalt, Aufzeichnung von Telefonaten durch Call Center sowie die allgemeine Regelung von Gefängnisdiensten.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Anträge auf Zugang zu und Löschung von Daten im Schengener Informationssystem (SIS), ein Recht, das indirekt über die Datenschutzbehörde in Anspruch genommen werden kann: 149 Beratungen für Personen, die für die Verarbeitung von Daten verantwortlich sind, zu spezifischen Datenschutzbestimmungen zu folgenden Themen: • Aufzeichnung von Telefonaten in drei Kontexten (Vertragsbeziehung mit Kunden, Notrufe und Bewertung der Qualität der Angestellten in Call Centern); • Aktualisierung von Leitlinien für Gesundheits- und Sicherheitsdienste am Arbeitsplatz als Folge von Änderungen des Arbeitsgesetzes; • Alkohol- und Drogentests am Arbeitsplatz.

Prüfmaßnahmen	
Prüfungen, Untersuchungen	Prüfungen – 863 Prüfungen vor Ort – 189 (privater und öffentlicher Sektor)
Sanktionsmaßnahmen	
Sanktionen	248 Geldbußen
Geldbußen	Die Datenschutzbehörde verhängte 69 Geldbußen in Höhe von insgesamt 507 291,69 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. Rechtsprechung

Für die Zwecke des vorliegenden Berichts gab es keine bedeutende Rechtsprechung.

C. Sonstige wichtige Informationen

Die Datenschutzbehörde war im Rahmen der Umsetzung ihrer Mission an zahlreichen Kooperationsverfahren beteiligt.

Daher ist die Beteiligung an nationalen Arbeitsgruppen wie beispielsweise der Arbeitsgruppe zum Nationalen Plan für eine sichere Identität, der Plattform für Gesundheit und Sicherheit am Arbeitsplatz oder auch an den mit verschiedenen Ministerien veranstalteten Sitzungen zu nennen, im Rahmen deren aktuell in der Entwicklung befindliche Rechtsinstrumente der EU diskutiert werden. Ebenfalls erwähnenswert sind die regelmäßigen Kontakte zu anderen unabhängigen Gremien in ähnlichen Bereichen.

Auf internationaler Ebene ist die Datenschutzbehörde Mitglied des ibero-amerikanischen Datenschutznetzwerks und organisiert gemeinsam mit der spanischen Datenschutzbehörde eine jährliche Sitzung zur Erörterung gemeinsamer Interessen.

Darüber hinaus spielt die Datenschutzbehörde eine aktive Rolle bei der Zusammenarbeit mit anderen Mitgliedstaaten in Schengen-Angelegenheiten.

RUMÄNIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Jahr 2010 sah sich die Aufsichtsbehörde nicht nur Budgetbeschränkungen gegenüber, sondern konnte auch nicht alle gesetzlich vorgegebenen 50 Positionen mit Mitarbeitern besetzen. Ein weiteres großes Problem ist die Tatsache, dass die Aufsichtsbehörde (zum Zeitpunkt der Erstellung dieses Berichts) noch immer nicht über geeignete Geschäftsräume verfügt, um einen Betrieb der nationalen Aufsichtsbehörde für die Verarbeitung personenbezogener Daten unter rechtmäßigen Bedingungen sicherzustellen.

Im Laufe des Jahres 2010 beantragten zahlreiche juristische Personen des öffentlichen und privaten Sektors eine Stellungnahme der Aufsichtsbehörde zur Definition des Begriffs „Für die Datenverarbeitung Verantwortlicher" oder „Auftragsverarbeiter" im Hinblick auf die von ihnen durchgeführte Verarbeitung personenbezogener Daten sowie hinsichtlich der Notwendigkeit der Meldung einer Verarbeitung personenbezogener Daten durch auf rumänischen Gebiet ansässige Auftragsverarbeiter für in anderen Ländern der Europäischen Union ansässige für die Datenverarbeitung Verantwortliche.

Informationen und Stellungnahmen wurden auch hinsichtlich der Verarbeitung biometrischer Daten (Fingerabdrücke) angefordert, die wahrscheinlich im Rahmen eines Systems zur Zugangskontrolle verarbeitet werden würden. Im Zusammenhang mit den rechtlichen Bestimmungen sowie der Notwendigkeit, einen wirksamen Schutz des Rechts auf ein Intim-, Familien- und Privatleben hinsichtlich der Verarbeitung personenbezogener Daten zu gewährleisten, wurde die Erfassung und Verarbeitung biometrischer Daten gemessen am angegebenen Zweck der Verarbeitung als unverhältnismäßig angesehen. Es wurde empfohlen, alternative Lösungen zur Zugangskontrolle sowie zur Erfassung der Arbeitsstunden von Angestellten zu verwenden (beispielsweise die Verwendung eines PIN-Codes zusammen mit anderen Identifikationsdaten des Angestellten).

In Bezug auf die Übermittlung von Daten in andere Länder betraf die Mehrheit der im Jahr 2010 geklärten Fälle die Übermittlung von Daten in andere EU-Mitgliedstaaten oder in Länder, die ein angemessenes, auch von der Europäischen Kommission anerkanntes Maß an Schutz für personenbezogene Daten bieten.

Die im Jahr 2010 von der Aufsichtsbehörde durchgeführten Untersuchungen betrafen Verletzungen der Rechte von Datensubjekten, konkreter gesagt Verletzungen des Rechts auf Zugang zu Daten und des Rechts auf Widerspruch gegen die Verarbeitung von Daten, sowie die Verarbeitung personenbezogener Daten in Dateien von Kreditbüros – die Übermittlung negativer Daten an Kreditbüros ohne vorherige Benachrichtigung und andere Fälle.

Auf der Grundlage der Bestimmungen von Artikel 21 Absatz 3 Buchstabe h des Gesetzes Nr. 677/2001 über die Verarbeitung personenbezogener Daten und den freien Datenverkehr hat die Aufsichtsbehörde eine Reihe von Mitteilungen zu Entwürfen von Rechtsakten durch verschiedene öffentliche Institutionen und Behörden herausgegeben, da diese unter anderem auch Fragen zur Erfassung und Verarbeitung personenbezogener Daten betrafen. Im Laufe des Jahres 2010 gab die Aufsichtsbehörde Mitteilungen zu insgesamt 48 Gesetzesentwürfen, Vereinbarungen, Regierungsbeschlüssen, Ministerialerlassen usw. heraus.

Organisation	Nationale Aufsichtsbehörde für den Schutz personenbezogener Daten (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal)
Vorsitz und/oder Gremium	Frau Georgeta Basarabescu – Präsidentin
Budget	Zugewiesenes Budget: 3 679 000 RON – etwa 876 000 EUR
Personal	46 besetzte Stellen sowie Präsidentin und Vize-Präsident
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Wie in den Vorjahren forderten auch im Jahr 2010 sowohl Datensubjekte als auch für die Datenverarbeitung Verantwortliche Stellungnahmen der Aufsichtsbehörde zu den rechtlichen Bedingungen der Verarbeitung

	personenbezogener Daten an. Insgesamt wurden 250 Stellungnahmen angefordert, was auf ein erhöhtes Interesse an der Einhaltung der rechtlichen Bestimmungen betreffend die Verarbeitung personenbezogener Daten hindeutet.
Meldungen	Es gingen 8 956 Meldungen von für die Datenverarbeitung Verantwortlichen ein.
Vorabprüfungen	1 Vorabkontrolle
Anträge betroffener Personen	Im Jahr 2010 gingen bei der Aufsichtsbehörde ein: 50 (spezifische) Auskunftsersuche; 47 Petitionen. Eingegangene Anrufe sind in diesen Zahlen nicht enthalten.
Beschwerden betroffener Personen	569 Beschwerden
Vom Parlament bzw. der Regierung angeforderte Beratung	Die Aufsichtsbehörde gab Mitteilungen zu 48 Gesetzesentwürfen, Vereinbarungen, Regierungsbeschlüssen, Ministerialerlassen usw. heraus.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	240 Untersuchungen
Sanktionsmaßnahmen	
Sanktionen	70 Sanktionen. 7 Beschlüsse zur Beendigung der Verarbeitung personenbezogener Daten bzw. zur Löschung der verarbeiteten personenbezogenen Daten.
Geldbußen	59 600 RON – etwa 14 200 EUR. 43 Verwarnungen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Hierfür gibt es im rumänischen Recht keine entsprechenden Vorschriften.

SLOWAKEI

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Jahr 2010 setzte die Behörde zum Schutz personenbezogener Daten (im Weiteren „Datenschutzbehörde“ genannt) ihre Arbeit an der Formulierung eines neuen Wortlautes für das aktuell geltende Datenschutzgesetz fort. Durch den Gesetzesentwurf wird das Datenschutzgesetz unter Berücksichtigung der Empfehlungen aus dem strukturierten Dialog mit den Vertretern der Europäischen Kommission, aus Erfahrungen mit der praktischen Anwendung des Datenschutzgesetzes sowie aus den aktuellen Entwicklungen nach dem Start eines umfassenden Konzepts für den Datenschutzrahmen der EU geändert werden. Im Dezember 2010 wurde der Änderungsentwurf der Öffentlichkeit präsentiert und einem ressortübergreifenden Konsultationsverfahren unterzogen. Das Gesetzgebungsverfahren war zum Ende des Jahres noch nicht abgeschlossen.

Die Behörde sah sich außerdem einer radikalen Kürzung ihres Budgets gegenüber. Im Vergleich zum Vorjahr standen ihr gut 23 % weniger Mittel zur Verfügung. Da es nicht möglich war, im letzten Quartal des Jahres alle Gehälter der Angestellten voll auszuzahlen, stellte die Behörde sogar einen Antrag an das Finanzministerium, die Mittel aus den in den Vorjahren eingesparten Kapitalaufwendungen für die Zahlung der Gehälter freizugeben, was schließlich auch unter bestimmten Vorbehalten umgesetzt wurde.

Das für die Jahre 2011–13 sogar noch niedrigere Budget wurde vor dem Hintergrund einer insgesamten Reduzierung der Ausgaben öffentlicher Verwaltungsbehörden festgelegt. Die aktuelle Situation wirkt sich negativ auf die Kontrolle des Schutzes personenbezogener Daten sowie die Ausführung der Arbeiten der Datenschutzbehörde aus. Darüber hinaus schadet die ständige Abwesenheit der Vertreter der Datenschutzbehörde in den relevanten Arbeitsgruppen und Konferenzen der internationalen Reputation der Behörde.

Organisation	Behörde für den Schutz personenbezogener Daten der Slowakischen Republik (Úrad na ochranu osobných údajov Slovenskej republiky)
Vorsitz und/oder Gremium	Herr Gyula Veszelei
Budget	728 696 EUR
Personal	34
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	467+16 auf der Grundlage des Gesetzes über den Zugang der Öffentlichkeit zu Informationen
Meldungen	40; sowie Meldungen der PDPO (Beauftragten für den Schutz personenbezogener Daten) – 1020
Vorabprüfungen	0
Anträge betroffener Personen	483
Beschwerden betroffener Personen	121 35
Vom Parlament bzw. der Regierung angeforderte Beratung	85

Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Inspektionsverfahren – 277 Prüfung von Meldungen – 324 An einzelne für die Datenverarbeitung Verantwortliche gerichtete verbindliche Anordnungen der Behörde – 144 Entscheidungen zur Erhebung von Einsprüchen gegen Entscheidungen der Behörde – 12 Grenzübergreifende Übermittlung von Daten – 11 Entscheidungen zu Genehmigungen von Datenübermittlungen in Drittländer Strafanzeigen – 3
Prüfmaßnahmen	
Prüfungen, Untersuchungen	125; 73 Anträge auf Erläuterungen; Zusätzlich: Prüfungen von Amts wegen – 121 Wichtige Themen und Fragen: • Veröffentlichung personenbezogener Daten von Dienstleistungsanbietern im Gesundheitswesen, insbesondere von Geburtskliniken zum Zweck der Versicherung von Neugeborenen; • Verstöße durch Anbieter von Satelliten- und Kabelfernsehen sowie durch Anbieter von Karten- und Geodatendiensten; • unzureichende Bereitstellung von Informationen für Datensubjekte beim Online-Handel; • Bereitstellung falscher Informationen seitens der Herausgeber von Treuekarten; • illegales Kopieren und Scannen persönlicher Dokumente; • unangemessene Kennzeichnung von videoüberwachten Bereichen; unverhältnismäßige Erfassung personenbezogener Daten, die über den eigentlichen Zweck der Verarbeitung hinaus geht bzw. nicht mit dem eigentlichen Zweck vereinbar ist.
Sanktionsmaßnahmen	
Sanktionen	21
Geldbußen	60 578 EUR
Datenschutzbeauftragte (DPO)	k.A.

B. Rechtsprechung

Im Jahr 2010 wurden drei Anträge auf die juristische Prüfung von Entscheidungen der Datenschutzbehörde bei Gericht eingereicht. Ein für die Datenverarbeitung Verantwortlicher eines Informationssystems, das Daten zum Zweck des Online-Handels verarbeitete, verklagte die Behörde, da diese gegen ihn eine Sanktion verhängt hatte, weil er der Behörde die erforderliche Zusammenarbeit verweigerte. Die gegen ihn verhängte Geldbuße war disziplinarischer Natur. Die Entscheidung der Behörde wird derzeit vom erstinstanzlichen Gericht geprüft.

Gegenstand der beiden anderen Fälle waren gegen einen für die Datenverarbeitung Verantwortlichen verhängte „Korrekturmaßnahmen" bzw. deren Rechtmäßigkeit. In einem Fall forderte die Behörde einen für die Datenverarbeitung Verantwortlichen (Bezirk Bratislava – Altstadt) auf, die ohne rechtliche Grundlage auf seiner Website veröffentlichten personenbezogenen Daten von Datensubjekten zu löschen. Das erstinstanzliche Gericht hat in der Sache noch kein Urteil gefällt. In einem anderen Fall forderte die Behörde einen für die Datenverarbeitung Verantwortlichen (Multimediaverlag) auf, in einem wöchentlich erscheinenden Society-Magazin veröffentlichte sensible personenbezogene Daten (Gesundheitsdaten) zu löschen. Auch in diesem speziellen Fall hat das Gericht noch kein Urteil gefällt.

SLOWENIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Gemäß den Bestimmungen des slowenischen Gesetzes zum Schutz personenbezogener Daten (GSPD) fungiert die Informationsbeauftragte als Inspektions- und Strafverfolgungsbehörde im Bereich Datenschutz. Im Jahr 2010 initiierte die Informationsbeauftragte 599 Fälle zu einer vermuteten Verletzung der Bestimmungen des GSPD (davon 202 im öffentlichen und 397 im privaten Sektor). Im öffentlichen Sektor betrafen die häufigsten mutmaßlichen Verletzungen die unbefugte Übermittlung von Daten an Dritte, die unrechtmäßige Veröffentlichung von Daten, die unrechtmäßige Erfassung von Daten, die Verweigerung des Zugangs zu Daten des Datensubjekts sowie die mangelnde Datensicherheit. Im privaten Sektor betrafen die häufigsten vermuteten Verletzungen den Missbrauch von Daten zu Direktmarketingzwecken, die unrechtmäßige Erfassung von Daten, die unrechtmäßige Veröffentlichung von Daten, die unrechtmäßige Videoüberwachung und die Übermittlung von Daten an unbefugte Dritte. Die Informationsbeauftragte verhängte Sanktionen für 179 Vergehen. Die Anzahl der Inspektionen und eingeleiteten Verfahren war mit dem Vorjahr vergleichbar.

Zusätzlich zu ihren Kompetenzen im Bereich Inspektionen und Strafverfolgung erledigt die Informationsbeauftragte auch andere Aufgaben gemäß den Vorgaben des GSPD. Die Informationsbeauftragte gibt nicht-verbindliche Stellungnahmen und Klarstellungen zu spezifischen Fragen im Bereich Datenschutz heraus, die von Einzelpersonen, für die Datenverarbeitung Verantwortlichen, öffentlichen und internationalen Stellen vorgebracht werden. Im Jahr 2010 gab die Informationsbeauftragte 1 859 Stellungnahmen und Klarstellungen heraus, ein deutlicher Anstieg im Vergleich zum Vorjahr (1 334). Dies könnte der transparenten Arbeit sowie den intensiven öffentlichen Kampagnen der Informationsbeauftragten geschuldet sein. Die Informationsbeauftragte ist gemäß GSPD außerdem befugt, Vorabprüfungen hinsichtlich biometrischer Maßnahmen, der Übermittlung von Daten in Drittländer sowie der Verknüpfung von Dateien mit personenbezogenen Daten durchzuführen. In diesen Fällen müssen die für die Datenverarbeitung Verantwortlichen zunächst die Genehmigung der Informationsbeauftragten einholen. Die Anzahl der Vorabprüfungen ist im Vergleich zum Vorjahr nicht angestiegen.

Im Laufe ihrer Sensibilisierungsmaßnahmen setzte die Informationsbeauftragte ihre Präventivarbeit (Vorträge, Konferenzen, Workshops für verschiedene öffentliche Gruppen) fort. Gemeinsam mit dem slowenischen Zentrum für sichereres Internet führte die Informationsbeauftragte Sensibilisierungsaktivitäten für Kinder und Jugendliche durch (Vorträge an Schulen, Veröffentlichungen). Die Informationsbeauftragte veröffentlichte vier Leitlinien zu verschiedenen Datenschutz-Themen (Onlineforen, Bewertungen der Auswirkungen auf die Privatsphäre, Leitlinien für Anbieter von Dienstleistungen im Gesundheitswesen sowie Leitlinien für Entwickler von Informationslösungen) und veröffentlichte zwei Broschüren zu Patientendaten sowie zum Datenschutz für Verbraucher. Im Zusammenhang des Europäischen Datenschutztages organisierte die Informationsbeauftragte ein Rundtischgespräch, dessen Schwerpunkt auf direkter und gezielter Werbung durch Einzelhändler lag, die oftmals gegen die Rechte von Verbrauchern verstoßen. Zu diesem Anlass verlieh die Informationsbeauftragte drei für die Datenverarbeitung Verantwortlichen Auszeichnungen für bewährte Verfahrensweisen zum Schutz personenbezogener Daten – eine dieser Auszeichnungen wurde für Bemühungen zur Einhaltung des „Privacy by Design"-Grundsatzes verliehen. Ergebnis dieser Aktivitäten ist eine sehr gute Reputation der Informationsbeauftragten und das Vertrauen der Öffentlichkeit, was sich in den Ergebnissen der repräsentativen Meinungsumfrage „Politbarometer" widerspiegelt. Hinsichtlich des Vertrauens der Bürgerinnen und Bürger Sloweniens in verschiedene Institutionen rangiert die Informationsbeauftragte auf dem zweiten Platz.

Die Informationsbeauftragte nahm an einer Reihe ressortübergreifender Arbeitsgruppen zu Projekten im Bereich E-Government wie z. B. E-Gesundheit, E-Sozialdienste, E-VEM (Portal für Unternehmer) und E-Archivierung sowie an der ressortübergreifenden Arbeitsgruppe für die Strategie zur Entwicklung der Informationsgesellschaft 2011–15 teil. Die Informationsbeauftragte wurde vom Gesetzgeber und den zuständigen Behörden zu 51 Gesetzen und anderen Rechtstexten konsultiert. Außerdem war sie an einer Reihe internationaler Gremien beteiligt: Artikel-29-Datenschutzgruppe, Gemeinsame Kontrollinstanz von Europol, Gemeinsame Kontrollinstanz von Schengen, Gemeinsame Kontrollinstanz für den Zoll, EURODAC, Arbeitsgruppe Polizei und Justiz (WPPJ), International Working Group on Data Protection in Telecommunications und Beratungsausschuss des Europarates für das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (T-PD). Die Informationsbeauftragte führte ihre Arbeit als Vize-Präsidentin der Gemeinsamen Kontrollinstanz von Europol fort.

Organisation	Informationsbeauftragte der Republik Slowenien
Vorsitz und/oder Gremium	Frau Nataša Pirc Musar
Budget	1 500 000 EUR
Personal	33 Angestellte: Kabinett (4), Verwaltung (3), Rechtsberater für den Zugang zu öffentlichen Informationen (11), Datenschutzforscher und -berater (5), Datenschutzbeauftragte (10)
Allgemeine Aktivitäten	Datenschutz und Zugang zu öffentlichen Informationen
Beschlüsse, Stellungnahmen, Empfehlungen	575 Stellungnahmen und Empfehlungen auf der Grundlage von Anfragen von Datensubjekten und für die Datenverarbeitung Verantwortlichen
Meldungen	250 Meldungen zu Dateien mit personenbezogenen Daten
Vorabprüfungen	25 Vorabprüfungen: 8 betreffend Biometrik, 10 betreffend die Übermittlung von Daten in Drittländer, 7 betreffend die Verknüpfung von Dateien mit personenbezogenen Daten
Anträge betroffener Personen	1 859 Anträge auf Stellungnahmen/Klarstellungen von Datensubjekten
Beschwerden betroffener Personen	Insgesamt 628 Beschwerden von Datensubjekten. 477 zulässige Beschwerden: 102 betreffend die unrechtmäßige Erfassung von Daten, 101 betreffend die unrechtmäßige Übermittlung von Daten, 90 betreffend die unrechtmäßige Veröffentlichung von Daten, 86 betreffend Direktmarketing, 85 betreffend die Verweigerung des Zugangs zu Daten für das Datensubjekt, 59 betreffend Videoüberwachung, 47 betreffend Datensicherheit, 58 sonstige.
Vom Parlament bzw. der Regierung angeforderte Beratung	Der Gesetzgeber und die für die Erarbeitung von Gesetzesentwürfen zuständigen Behörden konsultierten die Informationsbeauftragte zu 51 Gesetzen und sonstigen Rechtstexten, unter anderem betreffend das Gesetz zum Schutz der Privatsphäre, die Strafprozessordnung, das Ausländergesetz, das Gesetz für Staatsanwaltschaften, das Gesetz für Fahrzeugführer, das Versicherungsgesetz, das Bankengesetz, das Glücksspielgesetz, das Gesetz über den Schutz im Straßenverkehr usw.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Weitere Tätigkeiten der Informationsbeauftragten im Jahr 2010: • Fortsetzung der Präventivarbeit (Vorträge, Konferenzen) gemeinsam mit dem slowenischen Zentrum für sichereres Internet; • Beteiligung an einer Reihe von ressortübergreifenden Arbeitsgruppen im Bereich E-Government, E-Sozialdienste E-Gesundheit, E-Archivierung usw.; Veröffentlichung von 4 Leitlinien zu verschiedenen Themen im Bereich Datenschutz: Onlineforen, Bewertungen der Auswirkungen auf die Privatsphäre, Leitlinien für Anbieter von Dienstleistungen im Gesundheitswesen sowie Leitlinien für Entwickler von Informationslösungen; sowie Veröffentlichung von 2 Broschüren: Patientendaten und Datenschutz für Verbraucher.

Prüfmaßnahmen	
Prüfungen, Untersuchungen	599 Inspektionen: 202 im öffentlichen, 397 im privaten Sektor.
Sanktionsmaßnahmen	
Sanktionen	Es wurden 179 Verfahren eingeleitet (45 im öffentlichen, 82 im privaten Sektor), davon wurden 36 Verwarnungen und 81 Ermahnungen ausgesprochen sowie 35 Geldbußen und 10 Zahlungsanordnungen verhängt.
Geldbußen	Die Datenschutzbehörde verhängte Geldbußen in Höhe von 157 417 EUR.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. Rechtsprechung

Das öffentliche Verkehrsunternehmen von Ljubljana (LPP) hat ein ***elektronisches Fahrkartensystem auf der Grundlage einer anonymen bzw. personalisierten elektronischen Fahrkarte eingeführt***. Das Unternehmen verarbeitet außerdem die Standortdaten von Fahrgästen (Daten zu Zeit und Ort des Einstiegs in den Bus sowie zur vom Fahrgast genutzten Buslinie). Die Informationsbeauftragte war der Ansicht, dass eine Verarbeitung von Standortdaten bei personalisierten Fahrkarten durch das Unternehmen nicht erforderlich ist, da der Fahrgast einen festen monatlichen Betrag zahlt. Das Unternehmen hatte das Einverständnis der Fahrgäste nicht eingeholt. Somit kam die Informationsbeauftragte zu dem Schluss, dass das Unternehmen die oben genannten Standortdaten ohne angemessene Rechtsgrundlage verarbeitet hatte. Das Unternehmen wurde aufgefordert, die erfassten Standortdaten zu löschen und das System anzupassen, damit diese Daten künftig nicht mehr verarbeitet werden.

Bei der Informationsbeauftragten ging eine Beschwerde einer Person ein, die einen SMS-Dienst abonniert, sich bald darauf wieder abgemeldet hatte, aber weiterhin Werbenachrichten erhielt. Das für den Betrieb des SMS-Dienstes verantwortliche Unternehmen argumentierte, dass ***Mobilfunknummern*** allein ***nicht als personenbezogene Daten einzustufen*** sind, da sie auf ein Gerät und nicht zwangsläufig auf eine Person verweisen. Die Informationsbeauftragte war der Ansicht, dass Mobilfunknummern als personenbezogene Daten einzustufen sind, da die Person – berücksichtigt man alle dem für die Datenverarbeitung Verantwortlichen zur Verfügung stehenden Mittel – über die Nummer identifiziert werden kann. Direktmarketing per SMS ist nur dann erlaubt, wenn die betreffende Person ihr Einverständnis hierzu gegeben hat. Der für die Datenverarbeitung Verantwortliche muss die Daten von Personen, die ihr Abonnement gekündigt haben, löschen oder anonymisieren. Das Verwaltungsgericht bestätigte diese Entscheidung später.

Bei einem Zeitungsvertrieb wurde eine **GPS-Überwachung von Zeitungsausträgern** eingeführt. Das Unternehmen holte zwar das Einverständnis der Angestellten ein. Wenn diese das Gerät jedoch nicht mitführten, würde dies zu einer Beendigung ihres Beschäftigungsverhältnisses führen. Die Informationsbeauftragte entschied, dass eine GPS-Überwachung in diesem Fall eine Verarbeitung von Daten darstellt und dass es für das Unternehmen keine angemessene Rechtsgrundlage für diese Verarbeitung nachwies. Die Verarbeitung personenbezogener Daten auf der Grundlage des persönlichen Einverständnisses ist nicht ausreichend bei Beschäftigungsverhältnissen, bei denen der Arbeitgeber die stärkere Partei ist. Außerdem kann der Angestellte keine gültige Einverständniserklärung abgeben, wenn ihm mit der Beendigung des Beschäftigungsverhältnisses gedroht wird. Die Informationsbeauftragte forderte das Unternehmen auf, die Verwendung der GPS-Geräte zu diesem Zweck einzustellen.

In einer Gemeinde wurde die ***Prüfung von Videoüberwachungsaufnahmen zur Feststellung von Verstößen beim ruhenden Verkehr (Falschparken)*** gestartet. Die Verkehrspolizisten der Stadt stellten die Verstöße nicht „vor Ort“ fest, sondern nahmen Aufzeichnungen von Überwachungskameras in Augenschein und prüften diese hinsichtlich möglicherweise falsch parkender oder anhaltender Fahrzeuge. Hiernach stellten die Verkehrspolizisten

die Identität der Fahrer fest und stellten ihnen einen Strafzettel zu. Die Informationsbeauftragte entschied, dass ein solches Vorgehen unverhältnismäßig sei und vor allem einer Rechtsgrundlage entbehre. Die Informationsbeauftragte verbot der Gemeinde die weitere Inaugenscheinnahme der Aufzeichnungen aus dem Videoüberwachungssystem zum Zweck der Einleitung von Ordnungswidrigkeitsverfahren.

Bei der Informationsbeauftragten ging eine erhebliche Anzahl von Beschwerden hinsichtlich der *Veröffentlichung personenbezogener Daten in den Medien, im Internet sowie besonders auf Websites von sozialen Netzwerken* ein. Die Informationsbeauftragte kann nur in Fällen tätig werden, die Daten betreffen, die in einer Datei mit personenbezogenen Daten enthaltensind. Aus diesem Grund kann die Informationsbeauftragte in den meisten Fällen (z. B. bei beleidigenden Inhalten in Onlineforen, gefälschten Profilen bei sozialen Netzwerken) den betroffenen Personen lediglich die Empfehlung aussprechen, ihre Beschwerde bei der Polizei oder der zuständigen Staatsanwaltschaft vorzubringen, damit diese entsprechend tätig werden können. Der Missbrauch personenbezogener Daten ist gemäß dem slowenischen Strafgesetzbuch eine Straftat. Die geschädigte Partei kann überdies eine Zivilklage bei einem Gericht einreichen. In Fällen, in denen es um eine Veröffentlichung von Daten aus Dateien mit personenbezogenen Daten geht (z. B. die Veröffentlichung von Anklagen, Krankenakten usw.), leitet die Informationsbeauftragte eine Inspektion ein.

C. Sonstige wichtige Informationen

Auch im Bereich der bilateralen internationalen Zusammenarbeit war die Informationsbeauftragte tätig. Im Jahr 2010 organisierte die Informationsbeauftragte einen Studienbesuch von Vertretern aus Polen, Ungarn und dem Kosovo sowie eines Beamten des Europäischen Fonds für die Balkanländer (European Fund for the Balkans).

Zusammen mit dem österreichischen Ludwig Boltzmann Institut für Menschenrechte nahm die Informationsbeauftragte an einem Twinning-Projekt mit dem Titel „Montenegro: Implementierung der Strategie zum Schutz personenbezogener Daten“ teil. Der Schwerpunkt des Projekts lag auf der Einrichtung einer nationalen Datenschutzbehörde sowie auf der Festlegung und Umsetzung eines rechtlichen Rahmens für den Datenschutz in Montenegro.

Im Hinblick auf politische Fragen, mit denen sich die Informationsbeauftragte umfassend befasst hat, ist die zunehmende Nutzung der Videoüberwachung zu nennen. Als Reaktion hierauf schlug sie Änderungen der vorhandenen Gesetze vor, die die Rechte in dieser Hinsicht besser schützen sollten. Zudem stellt die Informationsbeauftragte fest, dass die Nutzung von Videoüberwachungssystemen mit intelligenter Gesichtserkennung schnell voranschreitet. Im Hinblick auf die IT-Lösungen in privaten Unternehmen sowie dem öffentlichen Sektor stellt die Informationsbeauftragte fest, dass die Sicherheit solcher Systeme oftmals nicht ausreicht, um die vom GSPD vorgeschriebenen Anforderungen zu erfüllen. Ein wichtiges Thema, das viele Bedenken aufwirft, ist das Recht von Angestellten auf Privatsphäre und Datenschutz am Arbeitsplatz. Als Reaktion hierauf schlug die Informationsbeauftragte den Entwurf eines Gesetzes über die Privatsphäre der Kommunikation am Arbeitsplatz vor. Ein besonderes Augenmerk legte die Informationsbeauftragte auf die Unterstützung und Ausbildung von für die Datenverarbeitung Verantwortlichen zum „Privacy by Design“-Konzept, und zwar bei Projekten betreffend den Wechsel zum elektronischen Handel, die Security-Information-and-Event-Management-Tools sowie die Einführung von Messgeräten zur Bestimmung der Durchschnittsgeschwindigkeit auf Straßen. Die Informationsbeauftragte beobachtet aufmerksam die Entwicklungen im Bereich Cloud Computing, die Bedenken im Hinblick auf die Datensicherheit und die Verantwortlichkeiten der für die Datenverarbeitung Verantwortlichen mit sich bringen, sowie das sogenannte Internet der Dinge.

SPANIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Um für die Datenverarbeitung Verantwortlichen und Auftragsverarbeitern die Einhaltung der Bestimmungen des Verfassungsgesetzes zum Schutz personenbezogener Daten sowie der Durchführungsverordnung zu vereinfachen, wurde ein Instrument zur Selbstbewertung (EVALÚA) auf der Website der Behörde bereitgestellt. Es ermöglicht Nutzern die Prüfung der Einhaltung der gesetzlichen Bestimmungen, die Bewertung der in der Verordnung festgelegten Sicherheitsmaßnahmen sowie die Erstellung eines Berichts über etwaig festgestellte Mängel, damit bei Bedarf entsprechende Korrekturmaßnahmen durchgeführt werden können. Bis Ende 2010 wurde 20 294 Mal auf EVALÚA zugegriffen.

Die Behörde setzte ihre Strategie der Information von Experten und Einzelpersonen, die an das Datenschutzgesetz (LOPD) gebunden sind, fort und veranstaltete die 3. offene Jahresversammlung der Datenschutzbehörde (AEPD), an der mehr als 800 Personen teilnahmen. Zudem wurde der Katalog mit informativen Leitfäden zum Datenschutzgesetz durch die Veröffentlichung der gemeinsam mit dem Nationalen Institut für Kommunikationstechnologie (INTECO) erarbeiteten Leitlinien für Sicherheit und Privatsphäre im Bereich der RFID-Technologien („Guía sobre seguridad y privacidad de la tecnología RFID“) sowie durch die Neuauflage der Sicherheitsleitlinien („Guía de Seguridad de Datos“) erweitert. Diese beinhalten unter anderem eine Vorlage für ein Sicherheitsdokument, das als Leitfaden dienen und die Umsetzung der Vorschriften im Bereich Datenschutz sowie deren Einhaltung erleichtern soll.

Darüber hinaus unterzeichneten der Generaljustizrat und die AEPD eine Kooperationsvereinbarung, mit der ein Protokoll für die Durchführung von Inspektionen betreffend den Datenschutz in Justizbehörden sowie Maßnahmen zur Umsetzung eingeführt werden, die eine effektive Anwendung der Datenschutzvorschriften in den Justizbehörden insgesamt fördern sollen.

Im Einklang hiermit nahm die AEPD angesichts der Bedeutung von Gesundheitsdaten und der Feststellung einer Zunahme der Fälle von Verstößen gegen das Datenschutzgesetz (hauptsächlich Verstöße gegen die im Datenschutzgesetz genannten Pflichten zur Gewährleistung der Sicherheit und Geheimhaltung) eine Initiative zur Erstellung eines Berichts über die Einhaltung des Datenschutzgesetzes in Krankenhäusern an. Zur Durchführung der Bewertung wurde ein Fragebogen an mehr als 600 im nationalen Krankenhausregister erfasste Zentren verschickt, der von 92 % ausgefüllt wurde. Die von den Adressaten eingetragenen Antworten wurden entsprechend geprüft und nachbereitet.

Darüber hinaus steht die AEPD weiterhin in Kontakt mit wichtigen sozialen Netzwerken wie Tuenti und Facebook, um deren Datenschutzrichtlinien zu verbessern und zu verhindern, dass Minderjährige unter 14 Jahren diese Netzwerke nutzen.

Im Juni 2009 übernahm die AEPD die Leitung eines in Kroatien zu entwickelnden Partnerschaftsprojekts. Ziel dieses Projekts ist eine Zusammenarbeit mit der kroatischen Datenschutzbehörde zur Vorbereitung auf den Beitritt zur EU. Die EU stellte finanzielle Mittel in Höhe von 1 350 000 EUR zur Verfügung. Die Laufzeit des Projekts soll 22 Monate betragen. Im Jahr 2010 wurde das Partnerschaftsprojekt mit Israel erfolgreich abgeschlossen. Auch dieses Projekt mit einer Laufzeit von 20 Monaten wurde von der AEPD geleitet.

Wie in der nachstehenden Tabelle zu sehen ist, ist eine Zunahme der Registrierungen und Inspektionen zu verzeichnen.

Organisation	Spanische Datenschutzbehörde (Agencia Española de Protección de Datos)
Vorsitz und/oder Gremium	Herr Artemi Rallo / Herr José Luis Rodriguez (seit Juni 2011)
Budget	15 425 160 EUR
Personal	147 Beamte + 7 Nicht-Beamte sowie 1 Kommissar
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Entscheidungen zu Anfragen: 6 189; Berichte: 120
Meldungen	623 148 Registrierungen (öffentliche und private Dateien). Insgesamt gemeldete Dateien: 2 144 872 (+ 31 %).
Vorabprüfungen	k.A.
Anträge betroffener Personen	104 826 Anfragen über die Hotline (schriftlich, telefonisch, online sowie über die Zentrale) (+8,2 %). 597 Anforderungen von Berichten an die Rechtsabteilung (298 aus der öffentlichen Verwaltung und 229 von Bürgerinnen und Bürgern bzw. Unternehmen).
Beschwerden betroffener Personen	4 300 Beschwerden von Datensubjekten. Sektoren: z. B. Telekommunikation und Videoüberwachung (29 % bzw. 14 %), Internet und Werbung usw.
Vom Parlament bzw. der Regierung angeforderte Beratung	Die AEPD gab rechtliche Stellungnahmen zu insgesamt 97 allgemeinen Vorschriften heraus, unter anderem zum Gesetzesentwurf für nachhaltige Wirtschaft, zum Gesetz über das Personenstandsregister, zum Gesetz über Verbraucherkredite und die Glücksspielverordnung sowie zu Entwürfen für königliche Dekrete.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	2 499 179 Zugriffe auf die Website (durchschnittlich 7 619 pro Tag). 2 508 850 Konsultationen des öffentlichen Registers. 560 Genehmigungen des Direktors für internationale Datenübermittlungen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	4 302 Voruntersuchungen und 1 643 Anträge von Datensubjekten. 6 189 Beschlüsse aus Inspektionen (+ 5,76 %), davon 1 830 Anträge auf den Schutz von Rechten (Zugang, Berichtigung, Löschung und Widerspruch) und 4 359 Verfahren betreffend die Sanktionsbefugnis. Die Abteilung für Inspektionen reagierte nicht nur auf spezifische Probleme, sondern war in verschiedenen Bereichen auch von Amts wegen tätig: • Datenschutz in Krankenhäusern; • Übermittlung von Unternehmensdaten;

	• Inspektionen betreffend den Verkauf von Schulden durch Telekommunikationsanbieter und Finanzinstitute; • Inspektion des Schengener Systems in Spanien; • Analyse der Vertragsbestimmungen von Telekommunikationsanbietern; Untersuchung der Zugangskriterien zum Immobilienregister, zum Fahrzeugregister und zum Katasterregister auf der Grundlage legitimer Interessen.
Sanktionsmaßnahmen	
Sanktionen	591 Sanktionsbeschlüsse; 92,49 % zum Datenschutzgesetz; 7,23 % zum Gesetz über Dienste der Internetgesellschaft (Spam); 0,28 % zum Telekommunikationsgesetz (Werbung, Fax)
Geldbußen	17 497 410.02 EUR (-29.65% im Vergleich zu 2009)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. Rechtsprechung

Zu einem der am heftigsten diskutierten Themen im Bereich neuer Internetdienste hat sich das „Recht auf Vergessen" im Internet entwickelt. Die spanische Datenschutzbehörde hat auf die Beschwerden der Öffentlichkeit hinsichtlich der von multinationalen Unternehmen angebotenen Dienste reagiert und entschieden, dass das spanische Datenschutzgesetz in Fällen anwendbar ist, in denen verschiedene Kriterien wie die Verwendung von Mitteln in Spanien, die Existenz einer Niederlassung und Nutzer-Targeting erfüllt sind. Gegen einige der Urteile wurde Berufung vor dem spanischen Zentralgericht (*Audiencia Nacional*) eingelegt, jedoch wurden noch keine Entscheidungen verkündet.

Die spanische Datenschutzbehörde war einer der Unterzeichner eines gemeinsamen Briefes mehrerer Behörden verschiedener Regionen an Google Inc. betreffend Google Buzz. Hierdurch sowie durch andere Aktivitäten hat die Datenschutzbehörde in Zusammenarbeit mit anderen Behörden ihr Engagement hinsichtlich der Weiterentwicklung des Schutzes von Internetnutzern unter Beweis gestellt. Diese Weiterentwicklung hat auch zur Untersuchung vermuteter Gesetzesverstöße geführt. Im Oktober 2010 leitete die AEPD ein Sanktionsverfahren gegen Google Inc. und Google Spanien wegen der Erfassung und Speicherung von Informationen zu WLAN-Netzen über die für den „Street View"-Dienst verwendeten Fahrzeuge ein. Ebenfalls im Oktober wurden Inspektionen von Facebook gestartet. Diese umfassten die Anforderung von Informationen darüber, ob Nutzer in Spanien von der Weitergabe von Daten an Werbetreibende oder sonstige Unternehmen durch die beliebtesten Anwendungen auf Facebook betroffen waren. Im November wurden ähnliche Maßnahmen betreffend MySpace ergriffen.

Beschlüsse der AEPD:

Das Recht auf Löschung personenbezogener Daten in einem Blog auf der Plattform Google Blogger wurde bestätigt. Die AEPD ist der Ansicht, dass die personenbezogenen Daten in diesem Fall gelöscht werden müssen, da das Recht auf freie Meinungsäußerung andere Rechte einschränkt. Diesbezüglich entschied der nationale Gerichtshof, dass die Datenschutzrechte auch dann gelten, wenn die veröffentlichten Informationen für die Öffentlichkeit nicht von Bedeutung sind. Die Suchmaschine ist zwar nicht für die Inhalte des Blogs auf ihren Plattformen verantwortlich, muss jedoch, wenn die AEPD als zuständige Behörde dies beschließt und sie tatsächlich Kenntnis davon hat, die Löschung anordnen oder den Zugriff verhindern (TD/00242/2010 und TD/00021/2010).

Versand kommerzieller Massenmails ohne Verwendung der BCC-Funktion und somit Veröffentlichung der Adressen. Dies umfasst zwei Verstöße. Einerseits gelten die Mails als unerbetene Nachrichten (Spam) und somit als Verstoß gegen Artikel 21 des Gesetzes über Dienste der Informationsgesellschaft und über den elektronischen Geschäftsverkehr (Ley de servicios de la sociedad de la información y de comercio electrónico, LSSI). Andererseits gelten E-Mail-Adressen als personenbezogene Daten, wodurch ein Versand einer E-Mail unter Veröffentlichung mehrerer Adressen für unterschiedliche Empfänger ohne deren Einverständnis als Verstoß gegen Artikel 10 des Datenschutzgesetzes hinsichtlich der Geheimhaltung und Vertraulichkeit von Daten gewertet wird (PS/00228/2010).

Rechtsprechung: Nationaler Gerichtshof

In einem Urteil vom 10. Februar 2010 stellte der Nationale Gerichtshof fest, dass eine Zeitung durch die Veröffentlichung einer gegen einen Beamten ausgesprochenen Disziplinarentscheidung, einschließlich der Einzelheiten der Beschuldigungen und präziser Informationen, auf deren Grundlage die Strafe im Rahmen eines Strafverfahrens gegen den Beamten verhängt wurde, sowie durch die wörtliche Veröffentlichung des Urteils des Strafverfahrens des Klägers und somit der Veröffentlichung von Straftatbestand und Urteil gegen die Geheimhaltungspflicht verstoßen hatte. Der Nationale Gerichtshof entschied, dass die Veröffentlichung dieser Daten für den beabsichtigten Zweck der Veröffentlichung unverhältnismäßig war.

In einem Urteil vom 23. Februar 2010 entschied der Nationale Gerichtshof, dass das Recht auf Informationsfreiheit in Fällen der Veröffentlichung von Daten zu Gehältern und Verträgen des Managers eines öffentlichen Unternehmens sowie seiner Frau in digitalen Zeitungen Vorrang habe.

Rechtsprechung: Oberster Gerichtshof

In einem Urteil vom 2. Juni 2010 bestätigte der Oberste Gerichtshof den aktuell geltenden Grundsatz zu Verstößen gegen die Geheimhaltung im Fall der Veröffentlichung von Dokumenten insofern, als der Verstoß dem beschwerdeführenden Unternehmen zuzuordnen ist, wenn die Dokumente von einem Dritten zugänglich gemacht wurden, von dem in der Folge festgestellt wurde, dass er für besagtes Unternehmen gearbeitet hatte.

In Urteilen vom 22. Juli und 5. Oktober 2010 betonte der Oberste Gerichtshof die Notwendigkeit eines Vertrags für Dienstleistungen eines Auftragsverarbeiters, in dem die Inhalte gemäß Artikel 12 Absatz 2 des Datenschutzgesetzes schriftlich oder in anderer Form als Beleg festzuhalten sind. Dies war im zu prüfenden Fall nicht geschehen.

Im Hinblick auf die Klärung von Berufungen, die gegen die Verordnungen zur Umsetzung des Datenschutzgesetzes eingelegt wurden, sind drei Urteile vom 15. Juli 2010 sowie zwei vorläufige Gerichtsentscheidungen betreffend Artikel 10 Absatz 2 Buchstabe b der vorgenannten Verordnung (der sich mit den berechtigten Interessen befasst) besonders relevant. Der Oberste Gerichtshof unterstützte die Verordnung vollumfänglich und annullierte lediglich fünf ihrer 158 Punkte. Artikel 10 Absatz 2 Buchstabe b blieb hierbei unverändert, was die Rechtssicherheit im spanischen Datenschutzsystem erhöht hat.[7].

[7] Weitere Informationen sind über den folgenden Link abrufbar (auf Spanisch)
https://www.agpd.es/portalwebAGPD/jornadas/3_sesion_abierta_2010/common/SESION_ABIERTA_2010_SEGUNDA_PARTE.pdf

SCHWEDEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Entwicklungen in der Gesetzgebung

Änderungen der schwedischen Verfassung

Im Laufe des Jahres 2010 wurden einige Gesetze erlassen und Gesetzesvorschläge eingebracht, die Auswirkungen auf die Privatsphäre hatten. Unter anderem stimmte das schwedische Parlament (Riksdag) am 24. November für eine Reihe von Änderungen der Verfassung, einschließlich einer Stärkung des Schutzes der Privatsphäre. Diese Änderung soll gewährleisten, dass der Staat und die Kommunen keine neuen umfassenden Datenbanken ohne explizite Rechtsgrundlage einführen, und eine Beurteilung dazu liefern, ob die gesetzgeberische Maßnahme im Hinblick auf eine Verletzung der Privatsphäre verhältnismäßig ist. Die Änderung ist das Ergebnis der Kritik eines Regierungsausschusses – des Ausschusses für den Schutz der Privatsphäre –, die dieser auf der Grundlage einer in zwei Berichten von 2007 und 2008 präsentierten umfassenden Erhebung und Analyse geäußert hatte. Der Datenschutzbehörde wurden im Laufe der Jahre zahlreiche Gesetzesentwürfe vorgelegt, bei denen die Analyse der Auswirkungen auf die Privatsphäre entweder komplett fehlte oder nur sehr mangelhaft war.

Das Kreditinformationsgesetz

In früheren Berichten haben wir bereits über das *Kreditinformationsgesetz* sowie darüber informiert, dass eine Änderung des *Grundgesetzes über die Meinungsäußerung* (ein Verfassungsgesetz) im Jahr 2003 es ermöglichte, Kreditinformationen auf Websites zu veröffentlichen, ohne dabei die strengen Regeln des *Kreditinformationsgesetzes* einhalten zu müssen. Dies führte zu Verletzungen der Privatsphäre sowie zu zahlreichen Beschwerden. Im Juni 2010 verabschiedete der Riksdag den Vorschlag der Regierung betreffend Änderungen am *Kreditinformationsgesetz* mit dem Ziel eines besseren Schutzes von Einzelpersonen im Internet.

Die Richtlinie über die Vorratsspeicherung von Daten

Die *EG-Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden*, wurde noch immer nicht in schwedisches Recht umgesetzt. Die schwedische Regierung hat einen Gesetzesentwurf zur Vorratsspeicherung von Verbindungsdaten zu Strafverfolgungszwecken vorgelegt, um die Richtlinie in Schweden umzusetzen. Eine Minderheit aus drei Parlamentsparteien setzte jedoch ein Minderheitenveto gemäß Kapitel 2 Abschnitt 22 des Regierungsinstrumentes (eines der Grundgesetze) durch. Somit konnte der Gesetzesentwurf bis März 2012 nicht vom Riksdag verabschiedet werden.

Aufsichtstätigkeiten und andere interessante Themen

Das Gesetz über Signalüberwachung

Am 12. Februar 2009 beauftragte die Regierung die Datenschutzbehörde mit der Untersuchung der Handhabung personenbezogener Daten durch den Nachrichtendienst „Radioanstalt der Verteidigung“ (Försvarets Radioanstalt, FRA) bei der Signalüberwachung zu Verteidigungszwecken. Hintergrund ist das Inkrafttreten eines neuen *Gesetzes über Signalüberwachung* am 1. Januar sowie die Tatsache, dass der Riksdag trotz einer Reihe von in diesem Gesetz enthaltenen Vorschriften zum Schutz der Privatsphäre weitere Kontrollmechanismen fordert. Die Datenschutzbehörde stellte der Regierung im Dezember 2010 ihre Ergebnisse vor. Unsere Behörde analysierte unter anderem, welche Probleme sich bei der Signalüberwachung durch den FRA für die Privatsphäre ergeben. Die Datenschutzbehörde prüfte außerdem die bei diesen Aktivitäten angewendeten Verfahren und Leitlinien, um festzustellen, ob sie im Hinblick auf die möglichen Probleme angemessen sind. Nach Anmerkungen der Datenschutzbehörde verbesserte der FRA seine Verfahren zur Handhabung personenbezogener Daten. Unter anderem wurden systematische und regelmäßige Prüfungen von Protokollen eingeführt, die eine Verfolgung unkorrekter bzw. unbefugter Zugriffe auf personenbezogene Daten ermöglichen.

Überwachung des aktuellen Systems zur nationalen elektronischen Identifizierung (e-id)

Der schwedische Rechnungshof hat festgestellt, dass die Überwachung des aktuellen Systems zur nationalen elektronischen Identifizierung (e-id) unzureichend ist. Es wurden keine Prüfungen der Informationssicherheit entlang der gesamten Ereigniskette bzw. bei allen an der Ausgabe oder Verifizierung einer e-id beteiligten Parteien durchgeführt. Die Datenschutzbehörde hat ein Projekt gestartet, das darauf abzielt, die unterschiedlichen Schritte der Ausgabe einer e-id besser zu verstehen und die beteiligten Interessengruppen zu erfassen, so zum Beispiel die beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeiter. Das Projekt umfasst eine Reihe von Inspektionen bei Herausgebern (z. B. Banken) und Nutzern (z. B. öffentliche Behörden), um festzustellen, ob das e-id-System die Datenschutzbestimmungen erfüllt.

Website gegen Verstöße im Internet

Anfang 2010 startete die Datenschutzbehörde eine Website – kränkt.se bzw. krankt.se –, die sich an junge Menschen richtet und ihnen Beratung für den Fall eines Verstoßes im Internet bietet.

Jahresbericht zur Privatsphäre

Auch im Jahr 2010 erstellte die Datenschutzbehörde einen Bericht über die Privatsphäre (*Privatsphäre 2010*), der, ebenso wie die Berichte der beiden Vorjahre, eine umfassende Untersuchung der neuen Gesetzgebung, Vorschläge, Entscheidungen und Techniken umfasst, die den Bereich der Privatsphäre im laufenden Jahr betrafen.

Organisation	Datenschutzbehörde (Datainspektionen)
Vorsitz und/oder Gremium	Die Datenschutzbehörde wird vom Generaldirektor geleitet. Zusätzlich gibt es einen Beratungsausschuss, dem fünf Mitglieder angehören.
Budget	3.3 million EUR
Personal	44 (27 mit juristischen Abschlüssen, 4 IT-Spezialisten und 1 Personalsachbearbeiter, 2 im Bereich Kommunikation sowie 10 Verwaltungsmitarbeiter)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Leitlinien zum Whistleblowing; Checkliste zur Nutzung von Lokalisierungstechnologien; Bericht über Handhabung und Schutz sensibler Daten bei privaten Versicherungsunternehmen; Empfehlungen für die Regierung betreffend das Binnenmarktinformationssystem IMI.
Meldungen	289 – es sollte darauf hingewiesen werden, dass der schwedische Gesetzgeber fast alle Möglichkeiten für Ausnahmeregelungen zur Meldepflicht genutzt hat.
Vorabprüfungen	344
Anträge betroffener Personen	2 100 Mails und 5 300 Anrufe mit Fragen zum Datenschutzgesetz, 527 telefonische Anfragen zum Kreditinformationsgesetz, 884 telefonische Anfragen zum Gesetz über die Schuldeneinziehung.
Beschwerden betroffener Personen	332 zum Gesetz zum Schutz personenbezogener Daten; 18 zum Kreditinformationsgesetz; 154 zum Gesetz über die Schuldeneinziehung.
Vom Parlament bzw. der Regierung	74 Konsultationen sowie 50 informelle Konsultationen betreffend

angeforderte Beratung	Gesetzesentwürfe mit möglichen Auswirkungen auf die Privatsphäre.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Die Datenschutzbehörde hat eine neue Verwaltungsvorschrift zum Whistleblowing herausgegeben und sich im Rahmen ihrer Kooperationstätigkeiten (nicht in leitender Funktion) mit mehr als 70 Konsultationen mit Datenschutzbeauftragten und etwa 10 verbindlichen Unternehmensregeln befasst.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	210 Inspektionen – Beispiele für wichtige Themen: Geldwäsche, soziale Medien, Lokalisierungstechnologie im Arbeitsleben, Videoüberwachung, eCall, Polizeidatenbanken und der Apothekenmarkt.
Sanktionsmaßnahmen	
Sanktionen	Keine im Jahr 2010
Geldbußen	k.A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Meldungen von Datenschutzbeauftragten insgesamt: 6 442, davon 206 neue im Jahr 2010. Die Gesamtzahl der Datenschutzbeauftragten beläuft sich auf 3 828 (ein Datenschutzbeauftragter kann mehrere Mandate haben).

B. Rechtsprechung

Die Entscheidung des Obersten schwedischen Verwaltungsgerichts zur Veröffentlichung von Insolvenzgläubigern im Internet

In diesem Fall ging es um die Anwendung von Paragraph 10 Absatz f des Gesetzes zum Schutz personenbezogener Daten im Hinblick auf die Abwägung der Interessen des für die Datenverarbeitung Verantwortlichen mit denen des Datensubjekts. Ein Beratungsunternehmen hatte die Namen, Adressen und Einlagen einer großen Zahl von Gläubigern sowie Informationen zu den Schuldnern eines bankrotten Finanzunternehmens auf seiner Website veröffentlicht. Die Datensubjekte hatten der Veröffentlichung nicht zugestimmt, und das Oberste Verwaltungsgericht stellte fest, dass durch die Veröffentlichung im Internet sehr einfach auf die Informationen zugegriffen und diese umfassend verbreitet werden konnten. Das Gericht entschied, dass das Interesse des für die Verarbeitung der personenbezogenen Daten Verantwortlichen nicht schwerer wog als das Interesse der Datensubjekte hinsichtlich des Schutzes ihrer Privatsphäre.

Entscheidung des Verwaltungsberufungsgerichts zu elektronischen Schlüsseln

Ein Wohnungsunternehmen hatte ein System mit elektronischen Schlüsseln eingeführt, mit denen die Bewohner Außen- und Innentüren von Gebäuden öffnen sollten. Die elektronischen Schlüssel sind jeweils mit einer bestimmten Wohnung verknüpft und generieren einen Eintrag in einem Zugangsprotokoll, aus dem hervorgeht, wann und wo der betreffende Bewohner seinen Schlüssel verwendet hat. Ein Zweck der Protokolle war unter anderem die Kontrolle des Zugangs zum Waschraum als Reaktion auf Probleme, die dort aufgetreten waren. Für die Verarbeitung der Daten der Zugangsprotokolle gab es keine Einverständniserklärung. Das Gericht entschied, ebenso wie die Datenschutzbehörde, dass die Interessen der Datensubjekte hinsichtlich des Schutzes ihrer

Privatsphäre schwerer wogen als das Interesse des für die Datenverarbeitung Verantwortlichen, also der Wohnungsgesellschaft, auf die Probleme im Waschraum zu reagieren.

Entscheidung des Verwaltungsberufungsgerichts zur Nutzung von SMS des Sozialversicherungsamts

Die Datenschutzbehörde hatte das Sozialversicherungsamt („das Amt“) aufgefordert, unter anderem eine Analyse des Risikos und der Schwachstellen der Nutzung der vom Amt zur Meldung von befristeten Elternzuschüssen angebotenen SMS durchzuführen. Das Amt argumentierte, dass es nicht verpflichtet sei, die Analyse durchzuführen, da es, solange die per SMS gesendeten Informationen die Empfangsstelle auf der Website des Amts noch nicht erreicht hätten, nicht für die Verarbeitung der Daten verantwortlich sei. Sowohl die Datenschutzbehörde als auch die Gerichte entschieden, dass das Sozialversicherungsamt bereits ab dem Zeitpunkt, an dem die betreffenden Personen die Informationen abschickten, als für die Datenverarbeitung Verantwortlicher anzusehen sei. Das Verwaltungsberufungsgericht entschied, dass die Datenschutzbehörde in ihrer Funktion als Aufsichtsbehörde in Einzelfällen entscheiden müsse, welche Sicherheitsmaßnahmen der für die Datenverarbeitung Verantwortliche zu ergreifen habe. Das Gericht war der Ansicht, dass die genannte Analyse eine solche Maßnahme darstelle und dass die Analyse nicht teuer oder anderweitig unangemessen sei.

Entscheidung des Verwaltungsgerichts zum Whistleblowing

Ein Unternehmen beantragte die Genehmigung der Datenschutzbehörde zur Verarbeitung personenbezogener Daten im Rahmen eines Whistleblowing-Systems. Die Genehmigung wurde erteilt, jedoch nur in einem gewissen Umfang und unter bestimmten Bedingungen. Eine der Bedingungen war, dass personenbezogene Daten zu Rechtsverletzungen nur für Personen in wichtigen Positionen bzw. in einer leitenden Position des Unternehmens verarbeitet werden dürfen. Das Unternehmen legte Berufung gegen diese Beschränkung ein und forderte die Aufnahme aller Angestellten in das Meldesystem. Das Gericht entschied zunächst, dass hier überaus sensible personenbezogene Daten verarbeitet werden, und zwar Berichte über mutmaßliche Rechtsverletzungen. Nach Abwägung der Interessen entschied das Gericht, dass die Interessen des Unternehmens nicht schwerer wogen als die der Datensubjekte hinsichtlich des Schutzes vor Verletzungen ihrer Privatsphäre.

Entscheidung des Verwaltungsgerichts zur Videoüberwachung von Angestellten

Ein öffentliches Verkehrsunternehmen hatte als Reaktion auf ernste Probleme wie z. B. die Sabotage von Bussen und Fahrkartenautomaten einen Monat lang eine Videoüberwachung in einem ihrer Busdepots durchgeführt. Am betreffenden Arbeitsplatz waren etwa 600 Angestellte beschäftigt, von denen höchstens 1 % an kriminellen Aktivitäten beteiligt war. Das Gericht entschied, dass die Videoüberwachung insbesondere die Privatsphäre verletzt habe, da nicht auf die Überwachung hingewiesen worden sei. Weiterhin entschied es, dass die Überwachung zu einem Eingriff in die Privatsphäre der Datensubjekte geführt habe, die im Hinblick auf den Zweck der Überwachung unverhältnismäßig gewesen sei.

C. Sonstige wichtige Informationen

Im Laufe des Jahres 2010 stieg die Zahl der Inspektionen erheblich an.

Im Jahr 2010 beschloss der Riksdag eine Erhöhung des Budgets der Datenschutzbehörde von fast 10 %.

VEREINIGTES KÖNIGREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Januar: Der Gesetzesentwurf zu Gerichtsmedizinern und Justiz („Coroners' and Justice Bill") erhielt die königliche Zustimmung. Dementsprechend hat die Datenschutzbehörde die Befugnis, Regierungsbehörden auch ohne deren Zustimmung zu prüfen.

Zum Anlass des Europäischen Datenschutztages wurde die Kampagne „Think Privacy" („Denk an den Datenschutz") gestartet und für das Projekt „i in online" („Das Ich im Internet") geworben.

Februar: Als Vorbereitung für unseren Bericht für das Parlament zum aktuellen Stand im Bereich Überwachung haben wir das Netzwerk für Überwachungsstudien („Surveillance Studies Network") mit der Berichterstattung zu den Entwicklungen im Bereich Überwachung im Vereinigten Königreich seit 2006 beauftragt.

Der Labour-Partei wurde ein Vollstreckungsbescheid zugestellt, da diese unerbetene automatische Werbeanrufe getätigt und somit gegen die Verordnungen zur Privatsphäre und der elektronischen Kommunikation verstoßen hatte.

März: Die Konferenz der Datenschutzbeauftragten in Manchester wurde von uns organisiert.

Wir veröffentlichten den Bericht „The Privacy Dividend" („Der Nutzen der Privatsphäre"), der Unternehmen finanzielle Gründe zur Einführung bewährter Verfahren im Bereich Datenschutz liefert.

April: Unsere neuen Befugnisse traten in Kraft. Diese ermöglichen der Datenschutzbehörde die Verhängung von Geldbußen für schwere Verstöße gegen das Datenschutzgesetz.

Im Vorfeld der Parlamentswahlen veröffentlichten wir Leitlinien zum Datenschutz für politische Parteien und Kandidaten.

Juli: Wir veröffentlichten unseren neuen Verhaltenskodex für personenbezogene Daten im Internet. Dieser bietet Online-Unternehmen bewährte Verfahrensweisen und dient ihnen als Leitfaden in diesem Bereich.

Wir starteten eine Kampagne, um privaten Ärzten ins Gedächtnis zu rufen, dass sie der Datenschutzbehörde melden müssen, in welchen Bereichen sie personenbezogene Daten verarbeiten. Als direktes Ergebnis dieser Kampagne gingen mehr als 3 300 neue Meldungen ein.

August: Vermieter und Immobilienmakler wurden daran erinnert, dass rechtliche Schritte gegen sie eingeleitet werden können, wenn sie der Datenschutzbehörde keine Meldung über die Verarbeitung personenbezogener Daten zukommen lassen. Als direktes Ergebnis dieser Kampagne gingen mehr als 1 000 neue Meldungen ein.

Wir gaben eine Prüfung der Verfügbarkeit von Sicherheitsberatungen für kleine und mittlere Unternehmen in Auftrag, um besser verstehen zu können, wie sie sich im Hinblick auf den Schutz personenbezogener Informationen beraten lassen können.

September: : Wir empfingen eine Delegation aus Mazedonien, deren Mitglieder Beratung zur Umsetzung und Regelung von Datenschutzverordnungen gewünscht hatten.

Wir veranstalteten den europäischen Workshop zur Fallbearbeitung in Manchester, an dem 50 Vertreter aus 29 Ländern und Gebieten Europas teilnahmen.

Oktober: Der ortsansässige MP und Finanzminister George Osborne eröffnete offiziell den Anbau unseres Hauptbüros, mit dem somit alle Mitarbeiter der Datenschutzbehörde Wilmslow unter einem Dach untergebracht sind.

Wir verhängten die beiden ersten Geldbußen gegen das private Unternehmen A4e und den Grafschaftsrat von Hertfordshire wegen schwerer Verstöße gegen das Datenschutzgesetz.

Google Inc. unterzeichnete eine Erklärung zur Verbesserung der Verarbeitung von Daten, um sicherzustellen, dass sich Verstöße wie z. B. die Erfassung von WLAN-Nutzungsdaten durch Fahrzeuge von Google Street View nicht wiederholen.

November: Wir lieferten dem Parlament ein Update zum Stand der Dinge im Bereich Überwachung und wiesen darauf hin, dass die neuen Gesetze, die Auswirkungen auf die Privatsphäre haben, im Rahmen eines post-legislativen Verfahrens geprüft werden sollten.

Zwei ehemalige Angestellte von T-Mobile wurden erfolgreich strafrechtlich für Verstöße gegen Paragraph 55 des Datenschutzgesetzes verfolgt. Dieser Paragraph verbietet die Erfassung, Veröffentlichung oder den Verkauf personenbezogener Daten ohne Zustimmung des für die Datenverarbeitung Verantwortlichen.

Dezember: Wir erinnerten Schulen daran, sich nicht hinter Datenschutzmythen zu verstecken und Eltern zu verbieten, Fotos bei Krippenspielen zu machen, was zu über 100 Berichterstattungen in den Medien führte.

Wir veröffentlichten eine Reaktion auf die Ankündigung der Regierung zum Gesetzesentwurf betreffend den Schutz der Grundfreiheiten.

Weitere Informationen zu unseren Tätigkeiten im Laufe des Jahres 2010 sind den auf unserer Website www.ico.gov.uk veröffentlichten Jahresberichten für 2009/10 sowie 2010/11 zu entnehmen.

Sofern nicht anders angegeben, gelten die Zahlen für das Geschäftsjahr des Vereinigten Königreiches April 2010–April 2011.

Organisation	Büro des Informationsbeauftragten (Information Commissioner's Office, ICO)
Vorsitz und/oder Gremium	Christopher Graham, Informationsbeauftragter
Budget	Etwa 20 172 000 GBP
Personal	351 (327 Vollzeit-Mitarbeiter, inkl. Informationsfreiheit andere und nicht im Bereich Datenschutz tätige Mitarbeiter, z. B. Facility, Finanzen, Personal)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	36 öffentliche Stellungnahmen zu Themen, die nicht in den Bereich Beratung und Durchsetzungsmaßnahmen fallen. Hierzu gehörten Stellungnahmen in puncto Google, Recht auf Privatsphäre/auf den Schutz personenbezogener Daten, Sensibilisierung für Pflichten, Änderungen hinsichtlich der Datenschutzbehörde und des Datenschutzgesetzes (z. B. Cookies). 3 Verhaltenskodizes (personenbezogene Informationen im Internet, Datenaustausch, Prüfbescheide). 55 Sanktionsverfahren (siehe unten) sowie damit verbundene Stellungnahmen in den Medien.
Meldungen	339 298
Vorabprüfungen	k.A.
Anträge betroffener Personen	206 585 Anrufe bei der Hotline (diese Zahl umfasst alle Anrufe, d. h. Datenschutz, Verordnungen zur Privatsphäre und der elektronischen Kommunikation (PECR), Informationsfreiheit und Erlasse über umweltrelevante Informationen; Informationen zu schriftlichen Anfragen und Beschwerden siehe unten).
Beschwerden betroffener Personen	Es gingen 26 227 Fälle im Bereich Datenschutz ein (einschließlich schriftlicher Anfragen und PECR-Fälle). 29 685 Fälle im Bereich Datenschutz wurden abgeschlossen.

Vom Parlament bzw. der Regierung angeforderte Beratung	Das Jahr 2010 war aufgrund der Parlamentswahlen sowie der Einarbeitungsphase der neuen Regierungskoalition relativ ruhig. Wir berieten die Regierung/das Parlament zu den folgenden Themen: • Gesetzesentwurf zu Ausweisdokumenten; • Telefon-Hacking (Sonderausschuss des Innenministeriums); • IT-Governance (Ausschuss für öffentliche Verwaltung); • Update zu unserem Bericht über die Überwachungsgesellschaft (Sonderausschuss des Innenministeriums); • Überwachung einer Datenbank der für schwere und organisierte Kriminalität zuständigen Behörde (Serious Organised Crime Agency, SOCA) (Ausschuss des Oberhauses); Beratung zu Risiken für die Privatsphäre bei der Verbrechenskartierung („Crime Mapping") (Innenministerium und Polizei).
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	3 verbindliche Unternehmensregeln wurden genehmigt
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Als Folge von Inspektionen bei öffentlichen und privaten Einrichtungen wurden 26 Prüfberichte herausgegeben. Acht resultierten aus der Zustimmung von Organisationen zu einer Prüfung als Teil von Untersuchungen zu Gesetzesverstößen. 97 % der in diesem Jahr in Berichten enthaltenen Empfehlungen wurden von den Organisationen angenommen. Im Rahmen von Nachprüfungen wurde festgestellt, dass 92 % unserer Empfehlungen vollständig oder teilweise umgesetzt wurden. In folgenden Bereichen besteht Verbesserungsbedarf: Interne Sensibilisierung des Personals für den Datenschutz, relevante Personalschulungen zum Thema Datenschutz, allgemeine Sicherheit, beispielsweise mangelhafte Verschlüsselung bei tragbaren Geräten, gemeinsame Passwörter sowie mangelhafte grundlegende physische Sicherheitskontrollen, z. B. abschließbare Aufbewahrungsvorrichtungen.
Sanktionsmaßnahmen	
Sanktionen	Unternehmen: 46 Strafrechtliche Verfolgungen: 5 Zivilrechtliche Geldbußen: 4
Geldbußen	Zivilrechtliche Geldbußen – 4 Geldbußen zwischen 60 000 und 100 000 GBP (insgesamt 310 000 GBP), 3 im öffentlichen Sektor/1 im privaten Sektor. Diese werden von der Datenschutzbehörde verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

B. 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 (Police National Computer, PNC) 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, jedoch nicht, diese 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. Mit anderen Worten wollten die Kommissare sicherstellen, dass sie die Informationen zu den betreffenden Verurteilungen im PNC bevorraten 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. Daraufhin beantragten wir Berufung beim Obersten Gerichtshof. Der Antrag wurde jedoch im Jahr 2010 abgewiesen.

Die Datenschutzbehörde ist der Ansicht, dass dieses Urteil wichtige Fragen aufwirft, und zwar nicht nur für die Betroffenen, sondern auch für viele andere Personen, über die Angaben zu nicht schwerwiegenden und alten 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.

Kapitel 3

Aktivitäten der Europäischen Union und der Gemeinschaft

3. Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. EUROPÄISCHE KOMMISSION

Europäischer Datenschutztag 2010[8], 28.1.2010

Der Schutz personenbezogener Daten ist ein Grundrecht der EU. Die Charta der Grundrechte der Europäischen Union besagt: **„Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten"**.

Am 28. Januar 2010 zelebrierten die Kommission und die Mitgliedstaten des Europarates den vierten Europäischen Datenschutztag.

Dieser Tag markiert zudem den Jahrestag der Konvention Nr. 108 des Europarates, des ersten rechtlich verbindlichen internationalen Instruments für den Datenschutz.

Er bietet den Bürgerinnen und Bürgern Europas die Möglichkeit, sich stärker für den Schutz ihrer personenbezogenen Daten und ihre diesbezüglichen Rechte und Pflichten zu sensibilisieren.

Zu diesem Anlass organisierte die Europäische Kommission einen geschlossenen Workshop zum Thema „Wie werden Datensubjekte über die Verarbeitung ihrer Daten und die Wahrnehmung ihrer Rechte informiert?" (How are data subjects informed about the processing of their data and the exercise of their rights). Die Vorträge im Rahmen dieses Workshops befassten sich insbesondere mit den folgenden Themen: Information und Rechte von Datensubjekten im Gesundheitswesen; wie können Datensubjekte zu Hauptakteuren betreffend den Schutz ihrer Privatsphäre werden; Privatsphäre und Datenschutz am Arbeitsplatz; die Praxis der Europäischen Kommission hinsichtlich der Information und Rechte von Datensubjekten; Datenschutz und das Recht auf Privatsphäre im Bereich der elektronischen Kommunikation.

Konsultation der Interessengruppen: Versammlung zur Prüfung des rechtlichen Rahmens der EU im Bereich Datenschutz – 1. Juli 2010[9]

Als Nachbereitung der im Jahr 2009 gestarteten öffentlichen Konsultation zur Prüfung des rechtlichen Rahmens der EU im Bereich Datenschutz veranstaltete die Kommission eine Reihe speziell ausgerichteter Konsultationsversammlungen mit einer Reihe wichtiger Interessengruppen.

Zweck dieser Versammlungen war die **Konsultierung von Interessengruppen aus dem nicht-öffentlichen Sektor zu einer Reihe von Fragen betreffend die bestehenden Datenschutzbestimmungen, um Probleme zu identifizieren und mögliche Lösungen zu erörtern**.

Ein Hintergrundpapier mit einer Reihe von nach Themen aufgegliederten Fragen, die als Leitfaden für die Diskussionen im Rahmen der Versammlungen dienen und sie strukturieren sollen, ist erhältlich.

Öffentliche Konsultation zum zukünftigen internationalen Abkommen zwischen der EU und den USA[10]

Bei der Entwicklung von Strategien und Gesetzen konsultiert die Europäische Kommission Bürgerinnen und Bürger sowie Interessengruppen umfassend durch öffentliche Konsultationen. Aus diesem Grund fand zwischen dem 28. Januar 2010 und dem 12. März 2010 eine öffentliche Konsultation zum zukünftigen internationalen Abkommen zwischen der Europäischen Union (EU) und den Vereinigten Staaten von Amerika (USA) betreffend den Schutz

8 http://ec.europa.eu/justice/newsroom/data-protection/events/100128_en.htm

9 http://ec.europa.eu/justice/newsroom/data-protection/events/100701_en.htm

10 http://ec.europa.eu/justice/newsroom/data-protection/opinion/100128_en.htm

personenbezogener Daten und den Informationsaustausch zu Strafverfolgungszwecken statt. Ziel der Konsultation war die Einholung von Meinungen im Hinblick auf das zukünftige internationale Abkommen betreffend den Schutz personenbezogener Daten und den Informationsaustausch zu Strafverfolgungszwecken zwischen der EU und den Vereinigten Staaten.

Auf diese öffentliche Konsultation gingen 64 Antworten von Bürgern, Unternehmen (eingetragenen sowie nicht eingetragenen) und öffentlichen Behörden ein.

3.2. EUROPÄISCHER GERICHTSHOF

Urteil des Gerichtshofs (Große Kammer) vom 9. März 2010 – Europäische Kommission /Bundesrepublik Deutschland (Rechtssache C-518/07)[11]

Die Kommission leitete ein Verletzungsverfahren gegen Deutschland ein, das in ein Urteil des Europäischen Gerichtshofs vom 9. März 2010 (C-518/07) mündete. Der EuGH entschied, dass die Bundesrepublik Deutschland gegen ihre Verpflichtungen aus Artikel 28 der Richtlinie 95/46/EG verstoßen hat, indem sie die für die Überwachung der Verarbeitung personenbezogener Daten durch nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen zuständigen Kontrollstellen in den Bundesländern staatlicher Aufsicht unterstellt und damit das Erfordernis, dass diese Stellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen, falsch umgesetzt hat.

Der EuGH stellte fest, dass die Kontrollstellen objektiv und unparteiisch vorgehen und somit vor jeglicher, sei es unmittelbaren oder mittelbarer, Einflussnahme durch alle öffentlichen Behörden sicher sein müssten, nicht nur vor der Einflussnahme seitens Einrichtungen, die kontrolliert würden. Im Urteil wurde darauf hingewiesen, dass bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreiche, um deren unabhängige Wahrnehmung ihrer Aufgaben zu beeinträchtigen.

3.3. EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

A) Zusammenfassung der Aktivitäten und Neuerungen

Auf Ebene der Europäischen Union (EU) waren im Jahr 2010 einige wichtige Trends und politische Möglichkeiten zur Förderung eines effektiveren Schutzes personenbezogener Daten zu beobachten. Hierzu gehören die zunehmend sichtbaren Auswirkungen des Vertrags von Lissabon, der das Thema Datenschutz durch die Schaffung einer soliden Rechtsgrundlage für einen umfassenden Datenschutz in allen Bereichen der EU-Politik fest im Zentrum der politischen Agenda der EU etabliert hat. Des Weiteren weckt die fortlaufende Prüfung des rechtlichen Rahmens der EU im Bereich Datenschutz hohe Erwartungen, insbesondere im Hinblick auf die zunehmende Bedeutung des Datenschutzes auf internationaler Ebene. Schließlich sind sowohl das Stockholmer Programm als auch die digitale Agenda der EU für die Bereiche Privatsphäre und Datenschutz überaus wichtig.

Die Notwendigkeit einer Intensivierung der Bemühungen zur Gewährleistung eines effektiven Datenschutzes spiegelt sich in den Aktivitäten des Europäischen Datenschutzbeauftragten (EDSB) im Laufe des Jahres 2010 wider. Im Hinblick auf die **Aufsichtsfunktion** des EDSB sind folgende Punkte besonders zu erwähnen:

[11] Abl. C 113 vom 1.5.2010, S.3.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:113:0003:0004:DE:PDF

- Eine grundlegende Änderung der Gangart hinsichtlich der Durchsetzung der Datenschutzverordnung in der EU-Verwaltung zur Gewährleistung eines robusteren Durchsetzungsansatzes. Die neue Strategie legt eine Reihe von Kriterien fest, die eine aktive, kohärente und transparente Anwendung der Durchsetzungsbefugnisse des EDSB sicherstellen sollen.

- Eine Ausweitung der Aufsichtsbefugnisse des EDSB, die seit Inkrafttreten des Vertrags von Lissabon für alle Institutionen und Organe der EU gelten, einschließlich Bereichen außerhalb des Anwendungsbereichs des ehemaligen Gemeinschaftsrechts.

- Die Annahme von 55 Stellungnahmen im Rahmen einer Vorabkontrolle betreffend die Verarbeitung personenbezogener Daten in der EU-Verwaltung. Dies umfasst Kernaufgabenbereiche wie das Frühwarn- und Reaktionssystem für den Austausch von Informationen zu übertragbaren Krankheiten sowie Standardverwaltungsverfahren wie zum Beispiel Beurteilungen, Einstellung und Beförderungen von Personal.

- Eine höhere Komplexität der eingegangenen Beschwerden. Im Jahr 2010 gingen 94 Beschwerden ein, von denen etwa zwei Drittel nicht zulässig waren, da sie Themen auf nationaler Ebene betrafen. Die zulässigen Beschwerden betrafen hauptsächlich Fragen betreffend Zugang und Berichtigung, missbräuchliche Verwendung sowie übermäßige Erhebung und Löschung von Daten. In elf Fällen stellte der Europäische Datenschutzbeauftragte fest, dass gegen die Datenschutzbestimmungen verstoßen worden war.

Im Rahmen seiner **Beratungsfunktion** konzentrierte sich der EDSB besonders auf folgende Bereiche:

- Die Modernisierung des Rechtsrahmens der EU im Bereich Datenschutz: der EDSB hat durchweg einen ehrgeizigen Ansatz zur Entwicklung eines modernen, umfassenden Rahmens im Bereich Datenschutz empfohlen, der alle Bereiche der EU-Politik umfasst und einen effektiven Schutz in der Praxis sicherstellt.

- Das Stockholmer Programm und die digitale Agenda der EU: Diese beiden wichtigen politischen Programme sind für den Bereich Datenschutz von großer Bedeutung und werden daher im Rahmen seiner Beratungsfunktion genau vom EDSB überwacht. Sie zeigen außerdem, dass der Datenschutz ein wichtiges Element der Legitimität und Effektivität in diesen beiden Bereichen ist.

- Eine Rekordzahl von 19 legislativen Stellungnahmen: im Jahr 2010 wurden Stellungnahmen zu einer Reihe von Themen abgegeben, unter anderem zu wesentlichen Fragen im Zusammenhang mit der EU-Strategie der internen Sicherheit, der EU-Politik zur Terrorismusbekämpfung, einem globalen Ansatz zur Übermittlung von PNR-Daten in Drittländer, dem Informationsmanagement im Raum der Freiheit, der Sicherheit und des Rechts, dem Konzept des eingebauten Datenschutzes („Privacy by Design“) im Rahmen der digitalen Agenda sowie dem ACTA-Abkommen.

Im **Bereich Zusammenarbeit** setzte der EDSB seine enge Zusammenarbeit mit den zur gemeinsamen Überwachung großer IT-Systeme in der EU eingerichteten Behörden fort. Insbesondere im Bereich der „koordinierten Aufsicht“ des Eurodac- sowie des Zollinformationssystems, bei denen die Zuständigkeiten mit Kolleginnen und Kollegen auf nationaler Ebene geteilt werden, wurde wichtige Arbeit geleistet. In Zusammenarbeit mit dem Europäischen Hochschulinstitut Florenz organisierte der EDSB außerdem einen Workshop zum Thema „Datenschutz bei internationalen Organisationen“, der sich mit den verschiedenen Herausforderungen befasste, denen sich internationale Organisationen beim Versuch, ein gutes Datenschutzniveau ohne klare Rechtsgrundlage zu gewährleisten, gegenüber sehen.

Organisation	Europäischer Datenschutzbeauftragter
Vorsitz und/oder Gremium	Peter Hustinx, Europäischer Datenschutzbeauftragter Giovanni Buttarelli, Stellvertretender Europäischer Datenschutzbeauftragter
Budget	7 104 351 EUR
Personal	38 Beamte
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden 19 legislative Stellungnahmen zu einer Reihe von Themen abgegeben, unter anderem zu wesentlichen Fragen im Zusammenhang mit der EU-Strategie der inneren Sicherheit, der EU-Politik zur Terrorismusbekämpfung, einem globalen Ansatz zur Übermittlung von PNR-Daten in Drittländer, dem Informationsmanagement im Raum der Freiheit, der Sicherheit und des Rechts, dem Konzept „Privacy by Design" im Rahmen der digitalen Agenda sowie dem ACTA-Abkommen. Es wurden 7 förmliche Kommentare abgegeben, unter anderem zur Überarbeitung der Frontex-Verordnung, zum offenen Internet und der Neutralität des Internets, zum Binnenmarktinformationssystem, zu Sicherheitsscannern sowie zu internationalen Abkommen zum Datenaustausch.
Meldungen	Es gingen 89 Meldungen von Datenverarbeitungsvorgängen der Institutionen und Organe der EU ein, die spezielle Risiken beinhalteten.
Vorabprüfungen	Es wurden 55 Stellungnahmen im Rahmen einer Vorabkontrolle durchgeführt, insbesondere zu Gesundheitsdaten, zu Beurteilungen und zur Einstellung von Personal, zum Zeitmanagement, zu Sicherheitsermittlungen, Telefonaufzeichnungen und Instrumenten zur Leistungsbewertung.
Anträge betroffener Personen	Es gingen 141 schriftliche Auskunftsersuche bzw. Anforderungen von Beratungen aus der allgemeinen Öffentlichkeit ein.
Beschwerden betroffener Personen	94 eingegangene Beschwerden, 25 davon zulässig. Vorrangige Arten vermuteter Verstöße: Verletzung der Vertraulichkeit von Daten, unverhältnismäßige Erfassung von Daten bzw. vorschriftswidrige Verwendung von Daten durch den für die Datenverarbeitung Verantwortlichen. 10 Fälle wurden geschlossen, da der EDSB keine Verletzung von Datenschutzbestimmungen feststellen konnte. In 11 Fällen wurde eine Nichteinhaltung der Datenschutzbestimmungen festgestellt.

Vom Parlament bzw. der Regierung angeforderte Beratung	Von den 19 oben genannten legislativen Stellungnahmen wurden 11 auf Anfrage der Europäischen Kommission abgegeben.
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	35 Konsultationen zu verwaltungsrechtlichen Maßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten in der EU-Verwaltung. Die Beratungen betrafen ein breites Spektrum an rechtlichen Aspekten hinsichtlich der Verarbeitung personenbezogener Daten durch die Institutionen und Organe der EU.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Vor-Ort-Inspektion bei einer EU-Institution. Systematische Nachbereitung früherer Inspektionen sowie zielgerichtete Überwachung und Berichterstattung, einschließlich Vor-Ort-Inspektionen.
Sanktionsmaßnahmen	
Sanktionen	k.A.
Geldbußen	Annahme einer neuen Strategie für die Einhaltung und Durchsetzung der Vorschriften zur Gewährleistung eines robusteren Durchsetzungsansatzes. Die neue Strategie legt eine Reihe von Kriterien fest, die eine proaktive, kohärente und transparente Anwendung der Durchsetzungsbefugnisse des EDSB sicherstellen sollen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	47 Datenschutzbeauftragte in den EU-Institutionen und -Organen.

B. Rechtsprechung

Zugang der Öffentlichkeit zu Dokumenten mit personenbezogenen Daten

Seit Aufnahme seiner Tätigkeit hat sich der EDSB kontinuierlich mit dem zuweilen komplizierten Verhältnis zwischen den EU-Vorschriften über den Zugang der Öffentlichkeit zu Dokumenten und den EU-Vorschriften über den Datenschutz befasst. Zunächst gab der EDSB gegenüber den EU-Organen diesbezügliche Empfehlungen ab, insbesondere durch die Veröffentlichung eines Hintergrundpapiers im Jahr 2005.

Außerdem machte er seine Position als Streithelfer in dem wegweisenden Gerichtsverfahren *Bavarian Lager/Kommission* deutlich, in dem es um einen Antrag auf Zugang der Öffentlichkeit zum Protokoll einer Sitzung der Kommission einschließlich der Namen der Teilnehmer ging. Der Zugang zu diesen Namen wurde unter Berufung auf die Datenschutzvorschriften verweigert. Der Gerichtshof stimmte der Ansicht des EDSB zwar zu, jedoch hob der Berufungsgerichtshof die Entscheidung des erstinstanzlichen Gerichts in seinem Urteil vom 29. Juni 2010 auf und legte die anwendbaren EU-Vorschriften anders aus.

Angesichts des Urteils war ein Teil der im Hintergrundpapier vom 2005 präsentierten Analyse nicht länger gültig. Aus diesem Grund erstellte der EDSB ein weiteres Papier, in dem er die Notwendigkeit eines **proaktiven Ansatzes** an das

Thema betonte, d. h. dass die Institutionen die Datensubjekte – vor oder zumindest im Moment der Erfassung ihrer personenbezogenen Daten – informieren müssen, in welchem Umfang die Verarbeitung dieser Daten deren Offenlegung einschließt oder einschließen könnte. Der EDSB war der Ansicht, dass die Institutionen hierzu verpflichtet seien, da dies einer angemessenen Vorgehensweise entspreche.

Zahlreiche anhängige Verfahren wurden in Erwartung des *Bavarian Lager*-Urteils ausgesetzt. All diese Verfahren wurden nach dem entsprechenden Urteil im Juni 2010 wieder aufgenommen. Der EDSB schaltete sich in mehreren dieser Verfahren als Streithelfer ein. Wann immer möglich nutzte der EDSB die Möglichkeit, seine Meinung zur Anwendung des Urteils des Gerichts in der Rechtssache *Bavarian Lager* auf andere Situationen zu äußern. Einen solchen Beitrag leistete der EDSB auch zu einer Rechtssache, die zu dieser Angelegenheit neu eingeleitet wurde.

Das *Bavarian Lager*-Urteil führte außerdem zur Einstellung des ersten Verfahrens gegen den EDSB beim erstinstanzlichen Gericht.

Sonstige Rechtssachen

Am 15. Juni 2010 fällte der Gerichtshof für den öffentlichen Dienst in der Rechtssache *Pachtitis gegen Kommission* ein weiteres Urteil mit Beteiligung des EDSB. Einer der Streitpunkte war die Weigerung der Kommission, dem Kläger Zugang zu den Fragen eines Zulassungstests zu gewähren, an dem er teilgenommen hatte. Da diesbezüglich auf die Datenschutzbestimmungen Bezug genommen wurde und die Sache eine interessante Frage zum Umfang des Rechts auf den Zugang zu den eigenen personenbezogenen Daten aufwarf, trat der EDSB auf Seiten des Klägers dem Verfahren als Streithelfer bei. Der Kläger gewann das Verfahren, allerdings wurde nicht auf die datenschutzrechtliche Frage eingegangen. Aus diesem Grund zog sich der EDSB aus der nachfolgend von der Kommission eingelegten Berufung vor dem erstinstanzlichen Gericht zurück.

Im Juli 2010 bat der Gerichtshof für den öffentlichen Dienst den EDSB, einem Verfahren als Streithelfer beizutreten, das die Übermittlung medizinischer Daten zwischen zwei EU-Institutionen zum Gegenstand hatte. Dies war der erste Fall, bei dem der EDSB von einem Gericht um Intervention gebeten wurde. Der EDSB entsprach der Bitte und arbeitete einen Streithilfesatz aus, in dem er die anwendbaren Bestimmungen der Datenschutzverordnung klarstellte.

Kapitel 4

Die Wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

4. Die Wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

ISLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Eines der wichtigsten Themen im Jahr 2010 war der Entwurf eines Vorschlags für ein neues Gesetz zur wissenschaftlichen Forschung. Dieser Vorschlag wurde noch nicht als parlamentarischer Gesetzesentwurf vorgelegt, jedoch hat die isländische Datenschutzbehörde eine Stellungnahme zu den wesentlichen Punkten des Vorschlags abgegeben. Laut der aktuellen Gesetzgebung muss der Zugang zu Krankenakten zu wissenschaftlichen Zwecken von der Datenschutzbehörde genehmigt werden. Dem Vorschlagsentwurf zufolge ist jedoch keine Zustimmung seitens der Datenschutzbehörde mehr erforderlich. Stattdessen sollen Bioethikausschüsse (in den meisten Fällen der nationale Ausschuss für Bioethik, in einigen Fällen jedoch Ausschüsse der größten Einrichtungen des Gesundheitswesens) datenschutzrelevante Fragen bei der Erteilung von Genehmigungen für wissenschaftliche Forschungsprojekte bewerten. Die Datenschutzbehörde hat sich hiergegen ausgesprochen und unter anderem betont, dass eine unabhängige Bewertung der rechtlichen Voraussetzungen für einen Zugang zu Krankenakten unbedingt erforderlich ist.

Ein weiteres wichtiges Thema war die Umsetzung eines neuen Gesetzes zu Patienteninformationen, d. h. Gesetz Nr. 55/2009 über Krankenakten. Gemäß diesem Gesetz kann mehr als eine Einrichtung des Gesundheitswesens das gleiche Informationssystem für elektronische Krankenakten nutzen, sofern der Sozialminister eine entsprechende Genehmigung erteilt und die Datenschutzbehörde bestätigt, dass die Sicherheit der personenbezogenen Daten angemessen geschützt ist. Die Datenschutzbehörde sprach im Jahr 2010 eine entsprechende Bestätigung für ein gemeinsames System für elektronische Krankenakten für Einrichtungen des Gesundheitswesens in Nordisland aus. Laut der Entscheidung der Datenschutzbehörde in dieser Sache war eine der Voraussetzungen für die Einrichtung des Systems die Protokollierung sämtlicher Zugriffe sowie eine angemessene interne Prüfung. Darüber hinaus betonte die Datenschutzbehörde, dass die Bestimmungen des Gesetzes über Krankenakten zum Recht von Patienten auf Vermeidung des Zugangs zu den Daten angemessen umgesetzt werden müssen.

In Island wird jedem Einwohner eine eindeutige persönliche Identitätsnummer zugewiesen. Laut Datenschutzgesetz darf diese Nummer nur verwendet werden, wenn die korrekte Identifizierung einer Person erforderlich ist. Die Datenschutzbehörde bearbeitete im Jahr 2010 eine Reihe von Fällen betreffend diese Nummer, u. a. deren Verwendung durch Finanzinstitute. Gemäß dem Gesetz zur Verhinderung von Geldwäsche und Terrorismusfinanzierung stellt die korrekte Identifizierung von Kunden eine Möglichkeit dar, solche Aktivitäten zu verhindern. Gemäß Richtlinie 2005/60/EG ist die Anwendung bestimmter strenger Maßnahmen diesbezüglich nur dann verpflichtend, wenn die Transaktionssumme einen bestimmten Betrag überschreitet. Dennoch gingen bei der Datenschutzbehörde zwei Beschwerden ein, laut denen Kunden bei unbedeutenden Transaktionen (Zahlung von Rechnungen und Wechslung ausländischer Währung in isländische Währung) um Angabe ihrer persönlichen Identitätsnummer gebeten wurden. Die Datenschutzbehörde kam zu dem Schluss, dass die Anforderung der persönlichen Identitätsnummer in diesen Fällen gegen die vorgenannte Bestimmung des Datenschutzgesetzes verstieß. Die betreffenden Finanzinstitute wurden aufgefordert, ihre Verfahren zu ändern. Später wurde bekannt, dass eines der Institute dieser Aufforderung nicht nachgekommen war. Dementsprechend beschloss die Datenschutzbehörde, eine Geldbuße in Form von Tagessätzen zu verhängen, wenn das Verfahren nicht geändert würde. Angesichts dieses Beschlusses erhielt die Datenschutzbehörde eine Klarstellung zu entsprechenden Verbesserungen der Verfahren, wodurch die Geldbuße hinfällig wurde.

Ein weiteres interessantes Thema ist die Verbreitung von Bildern aus Überwachungskameras, die vermutete Diebstähle in Supermärkten und Geschäften zeigen, unter den Angestellten dieser Supermärkte und Geschäfte. Bei der Datenschutzbehörde gingen zwei Beschwerden betreffend eine solche Verbreitung in großen Warenhausketten ein. In beiden Fällen vermuteten die Beschwerdeführer, dass ihre Bilder als eine Art Warnhinweis für die Angestellten in den Geschäften verwendet werden. Die Datenschutzbehörde konnte keine Belege dafür finden, dass die Bilder der betreffenden Personen entsprechend genutzt wurden, jedoch wurde festgestellt, dass die untersuchten Warenhausketten über eine umfangreiche Sammlung an Bildern von Einzelpersonen verfügten, die als Warnung für die Angestellten dienen sollten. Darüber hinaus wurden die betreffenden Personen nicht über diese Verwendung ihrer Bilder informiert. Die Datenschutzbehörde wies darauf hin, dass eine solche Vorgehensweise

dazu führen könne, dass Menschen ungerechtfertigt als Straftäter abgestempelt werden und dass es keine Rechtsgrundlage für diese Verarbeitung von Daten gebe. Dementsprechend kam die Datenschutzbehörde zu dem Schluss, dass die Verarbeitung der Daten unrechtmäßig war, und forderte die Einstellung selbiger.

Im Jahr 2010 wurde eine Reihe von Rechtsakten verabschiedet, die Bestimmungen zur Verarbeitung personenbezogener Daten enthielten, unter anderem folgende: Gesetz Nr. 12/2010 zum Nordischen Haftbefehl, das unter anderem seine Beziehung zum Europäischen Haftbefehl und der Schengen-Kooperation betrifft; Gesetz Nr. 42/2010 zu Identifikationskarten und Überwachung am Arbeitsplatz, das es Gewerkschaften und Arbeitgeberverbänden ermöglicht, Vereinbarungen zu Karten zur Identifizierung von Arbeitnehmern in ausgewählten Branchen zu schließen und somit die Überwachung der Arbeitsmarktbestimmungen zu erleichtern; Gesetz Nr. 78/2010 zur Änderung der Rechtsakte über Devisengeschäfte, einschließlich der Einbindung der Bestimmungen in Gesetz Nr. 87/1992 zum Devisengeschäft, das der Nationalbank die Erfassung umfassender Informationen zu Transaktionen in ausländischen Währungen ermöglicht; sowie Gesetze Nr. 100 und 101/2010 zum Ombudsmann für Schuldner und zur Schuldenreduzierung für Einzelpersonen, die unter anderem Bestimmungen zu (a) den Befugnissen des Ombudsmanns hinsichtlich der Erfassung von Daten zu Einzelpersonen, die um Unterstützung hinsichtlich einer Einigung mit Gläubigern betreffend eine Schuldenreduzierung bitten, (b) zur Einverständniserklärung der Einzelpersonen hinsichtlich der Erfassung ihrer Daten sowie (c) zur Übermittlung der Daten an die Gläubiger enthalten.

Organisation	
Vorsitz und/oder Gremium	Sigrún Jóhannesdóttir, Kommissarin; Páll Hreinsson, Vorsitzender des Vorstands
Budget	66,4 Millionen ISK, das entspricht etwa 415 000 EUR
Personal	Vier Rechtsberater, eine Sekretärin
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	Etwa 70
Vorabprüfungen	407
Anträge betroffener Personen	149 Genehmigungen zur Verarbeitung von Daten
Beschwerden betroffener Personen	Etwa 300
Vom Parlament bzw. der Regierung angeforderte Beratung	135
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Etwa 50
Prüfmaßnahmen	Im Jahr 2010 wurden insgesamt 1 221 neue Fälle registriert
Prüfungen, Untersuchungen	
Sanktionsmaßnahmen	25
Sanktionen	

Geldbußen	Mit Ausnahme der verhängten Geldbußen in Form von Tagessätzen für jeden Tag, an dem die Forderungen der Datenschutzbehörde nicht erfüllt werden, hat die Datenschutzbehörde keine Sanktionsbefugnisse.
Datenschutzbeauftragte (DPO)	In einem Fall beschloss die Datenschutzbehörde, eine Geldbuße in Form von Tagessätzen zu verhängen, wenn bestimmte Verfahren nicht geändert würden, jedoch ging hierzu eine entsprechende Klarstellung ein, wodurch die Geldbuße hinfällig wurde.
Zahlenangaben zu DPO	
Vorsitz und/oder Gremium	k.A.

B. Rechtsprechung

Am 21. Oktober 2010 fällte der Oberste Gerichtshof Islands ein Urteil (Rechtssache Nr. 13/2010) betreffend den vermuteten Zugriff eines Arbeitgebers auf private, von der E-Mail-Adresse eines ehemaligen Mitarbeiters versendete Korrespondenz. In diesem Fall ging es um eine Vereinbarung zu Zahlungen an den ehemaligen Mitarbeiter nach Beendigung seines Beschäftigungsverhältnisses. Der Arbeitgeber erklärte, der ehemalige Mitarbeiter habe die Vereinbarung gebrochen, da er eine Bewerbung bei einem Mitbewerber in Erwägung gezogen habe. Dementsprechend setzte der Arbeitgeber die Zahlungen aus. Daraufhin reichte der ehemalige Angestellte Klage gegen den Arbeitgeber ein, der seinerseits die vorgenannte E-Mail-Korrespondenz als Beleg für das Fehlverhalten des ehemaligen Angestellten vorlegte.

Der Oberste Gerichtshof kam jedoch zu dem Schluss, dass nicht verifiziert werden könne, ob die E-Mail-Korrespondenz tatsächlich zwischen dem ehemaligen Angestellten und dem Mitbewerber stattgefunden habe. Angesichts dessen sowie anderer Umstände wurde dem Antrag des ehemaligen Mitarbeiters auf vertragsgemäße Bezahlung stattgegeben.

Hinsichtlich des potenziell unrechtmäßigen Zugriffs auf die Korrespondenz wurden keine Anträge gestellt. Daher wird im Urteil diesbezüglich auch nicht Stellung genommen. Der Fall wirft jedoch Fragen zur Sicherheit privater E-Mail-Korrespondenz auf.

LIECHTENSTEIN

A. Zusammenfassung der Aktivitäten und Neuerungen

Vorratsdatenspeicherung

Wie bereits vergangenes Jahr berichtet, hatte Liechtenstein bereits im Jahr 2006 die Vorratsdatenspeicherung von Verkehrsdaten im Kommunikationsgesetz (KomG)[12] eingeführt, ohne dass eine Verpflichtung zur Umsetzung der Richtlinie 2006/24/EG bestanden hätte.[13] Die Datenschutzstelle (DSS) war gegen die Einführung der Vorratsdatenspeicherung in Liechtenstein. Immerhin entschieden sich Regierung und Landtag für eine "bürger- und grundrechtsfreundliche Ausgestaltung des Datenschutzes" und im KomG wurde eine ausdrückliche Kontrollbefugnis der DSS normiert.[14] Mit der Vorbereitung einer entsprechenden Kontrolle wurde begonnen. Die Lehre in Liechtenstein bezeichnet die voraussetzungslose Vorratserfassung von Verkehrsdaten trotz der strengen Kriterien für den Zugriff auf solche Daten *„grundrechtlich jedenfalls als problematisch. Ob sie der Staatsgerichtshof als verfassungswidrig qualifizieren wird, dürfte auch wesentlich von der zukünftigen einschlägigen ausländischen Grundrechtsprechung abhängen."*[15] Es bleibt abzuwarten, ob der Staatsgerichtshof eine Gelegenheit haben wird, hierzu Stellung zu nehmen.

Google Street View

Die DSS stand vergangenes Jahr in intensivem Kontakt mit Google zwecks der Einführung des Dienstes „Street View", wobei konkrete Rahmenbedingungen für die Durchführung der Fahrten in Liechtenstein diskutiert wurden. Dabei orientierte sie sich an europäischen Entwicklungen, vor allem an der Art. 29 Datenschutzgruppe und insbesondere an Luxemburg, Österreich, Deutschland und Griechenland, aber auch der Schweiz. Dabei war auch eine Meldung der Regierung bei den Abklärungen entsprechend zu berücksichtigen. Die DSS forderte verschiedene Maßnahmen, insbesondere in Bezug auf die Information der Bevölkerung über den Zeitpunkt und die Fahrtroute sowie über die Veröffentlichung der Bilder im Internet. Auch die automatisierte Unkenntlichmachung (engl. blurring) von Gesichtern und Autonummern war ein Thema, da gerade in der Anfangsphase der Veröffentlichung zahlreiche Gesichter und Autokennzeichen ohne Einschränkung klar erkenn- und somit identifizierbar sind. Nach Kenntnis der DSS wurden bis Ende des Berichtsjahres keine Straßenansichten für den Dienst Google Street View in Liechtenstein aufgenommen.

Öffentlichkeitsarbeit

Anlässlich des Europäischen Datenschutztages am 28. Januar lud die DSS in Zusammenarbeit mit dem Institut für Wirtschaftsinformatik der Hochschule Liechtenstein zu einer öffentlichen Veranstaltung zum Thema Suchmaschinen im Internet mit dem Titel „Einblicke in die Welt von Google & Co: Von Informationsjägern und Datensammlern" ein.

Um möglichst weite Kreise der Bevölkerung zu erreichen, nutzt die DSS unterschiedliche Kanäle. Neben Veranstaltungen, Schulungen, Publikationen und der Internetseite gehört auch der jährlich erscheinende Tätigkeitsbericht[16] zu den zentralen Informationsmaßnahmen. Ein wesentliches und kostengünstiges Instrument zur Information stellt die Internetseite[17] dar. Die Zahl der Zugriffe belegt, dass dieses Angebot gut angenommen wird. Deshalb wird es fortlaufend verbessert und vergrößert. Es finden sich dort beispielsweise auch Werkzeuge für Selbsttests und andere Hilfestellungen zum Thema Datenschutz.

---

12 Im Rahmen der letzten Revision des Kommunikationsgesetzes, LGBl. 2006 Nr. 91.

13 Da die RL 2006/24/EG (noch) nicht Bestandteil des EWR-Abkommens ist, besteht auch keine Umsetzungspflicht.

14 Art. 52 KomG. Vgl. dazu auch den Tätigkeitsbericht 2010 der DSS, unter 1.3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

15 Vgl. Hilmar Hoch: Die Regelung des staatlichen Zugriffs auf Fernmeldedaten im Kommunikationsgesetz aus grundrechtlicher Sicht, in LJZ 4 / 2009, S. 103: http://www.juristenzeitung.li/papers/showpdf/LJZ_2009_04.pdf.

16 http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

17 www.dss.llv.li.

Organisation	
Vorsitz und/oder Gremium	Dr Philipp Mittelberger
Budget	470 000 EUR
Personal	2,2 Recht, 1,0 Technik, 0,8 Administration
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	26 Stellungnahmen zu Gesetzesentwürfen[18] 23 Bewilligungen von Videoüberwachungsanlagen
Meldungen	k.A.; insgesamt 542 registrierte Datensammlungen
Vorabprüfungen	k.A.
Anträge betroffener Personen	85
Beschwerden betroffener Personen	k.A.
Vom Parlament bzw. der Regierung angeforderte Beratung	Eine Meldung[19] der Regierung zu Google Street View
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	Anzahl eingegangener Fragen um 20 % gestiegen: 523 Anfragen gegenüber 431 in 2009[20]
Prüfmaßnahmen	
Prüfungen, Untersuchungen	k.A.; Kontrollen in Vorbereitung
Sanktionsmaßnahmen	
Sanktionen	k.A.
Geldbußen	k.A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k.A.

18 Vgl. Tätigkeitsbericht 2010 der DSS, unter 3., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

19 Gemäss Art. 30 Abs. 1 Datenschutzgesetz (DSG).

20 S. Statistik der DSS, Tätigkeitsbericht 2010 der DSS, unter IV., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2010.pdf.

B. Rechtsprechung

Bewilligung von Videoüberwachungsanlagen

Seit 1. Juli 2009 unterliegt der Betrieb einer Videoüberwachung im öffentlichen Bereich einer Genehmigungspflicht durch die DSS.[21]

Flächendeckende Videoüberwachung: Die Gemeinde Vaduz hatte Ende 2009 bei der DSS die Bewilligung einer bereits bestehenden Videoüberwachungsanlage im **Städtle Vaduz** beantragt. Bewilligt werden sollten 15 Farbkameras zur Überwachung einer Fläche von rund 3000 qm mit festem Blickfeld und ständiger Betriebszeit, ausgenommen montags bis freitags von 10:00h bis 18:00h, die eine Bildübermittlung in Echtzeit mit Aufzeichnungs- und weiteren Bearbeitungsmöglichkeiten sowie eine Speicherdauer von 4 Tagen zulassen. Die DSS hatte das Gesuch mit Verfügung abgewiesen. Dies im Wesentlichen mit der Begründung, die beantragte Videoüberwachungsanlage sei mangels entsprechendem Nachweis nicht erforderlich und damit unverhältnismäßig. Anlässlich einer nachfolgend durchgeführten Ortsbegehung durch die DSS wurden von manchen Kameras die Blickwinkel geändert, von anderen die Aufzeichnungszeiten reduziert, wieder andere wurden abgeschaltet und plombiert.

Die Beschwerdeführerin erhob gegen die Verfügung der DSS Beschwerde bei der Datenschutzkommission (DSK). Diese hat in ihrer Entscheidung[22] vergangenen Dezember die Ansicht der DSS grundsätzlich bestätigt, einzelne Kameras jedoch – entgegen der Ansicht der DSS – bewilligt. Die DSK hatte beispielsweise die Bewilligung zweier Kameras im Eingangsbereich des Rathauses damit begründet, dass dieses öffentliche Gebäude auch häufig als Veranstaltungsort diene, vor welchem auch in- und ausländische, mehr oder weniger prominente Besucher zirkulieren. Nach der allgemeinen Lebenserfahrung berge dieser Platz ein erhöhtes Gefahrenpotential, weshalb sich ein Nachweis konkreter Vorfälle, etwa eines Anschlags auf eine öffentlich exponierte Person, erübrige. Zwecks Kontrolle der Zutrittsberechtigung und Gewährleistung bzw. Erhöhung der Sicherheit der Rathausbesucher sei eine Videoüberwachung als erforderlich und damit als zulässig zu qualifizieren. Ebenfalls erübrige sich hinsichtlich der für das Busterminal beantragten Kameras der Nachweis eines konkreten Vorfalls, da derartige Plätze nach der allgemeinen Lebenserfahrung „häufig größere, naturgemäß oft unübersichtliche Ansammlungen von Personen unterschiedlicher Nationalität beherbergen und dadurch erfahrungsgemäß mit einem erhöhten Sicherheitsrisiko verbunden sind."

Hinsichtlich der abgeschalteten und plombierten Kameras folgte die DSK der Rechtsansicht der DSS, wonach diese als unverhältnismäßigen Eingriff in die Persönlichkeit zu qualifizieren und daher abzumontieren seien. Bei den Passanten würde fälschlicherweise der Eindruck einer Überwachung entstehen, was auch dem Grundsatz von Treu und Glauben widerspräche. Ähnliches gelte für Attrappen.

Speicherdauer von Videoaufzeichnungen: Des Weiteren hatte die DSS im Berichtsjahr in drei Fällen den Bewilligungsgesuchen für Videoüberwachungsanlagen nur teilweise stattgegeben. In allen drei Fällen handelte es sich um Anträge von Bankinstituten, die eine Speicherdauer von über 30 Tagen beantragt hatten. Das Datenschutzgesetz (DSG) sieht eine unverzügliche Löschung, spätestens jedoch nach 30 Tagen vor, wenn die Daten zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der betroffenen Personen einer weiteren Aufbewahrung entgegenstehen.[23] Die Beschwerdeführer erhoben dagegen Beschwerde bei der DSK mit dem Antrag, eine Speicherdauer bis zur Erreichung des Aufzeichnungszwecks zu bewilligen. Die DSK folgte in ihrer Entscheidung[24] in allen drei Fällen der Auffassung der DSS, wonach die 30-Tagefrist eindeutig als bedingungsunabhängige, in jedem Fall geltende absolute Höchstfrist zu verstehen sei und wies die Beschwerden als unbegründet ab.

---

21 S. auch den Beitrag Liechtensteins im 13. Jahresbericht der Art. 29 Datenschutzgruppe sowie ausführlich im Tätigkeitsbericht 2009 der DSS, unter 1.5, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2009.pdf.

22 DSK 2010/2; die vollständige Entscheidung sowie weitere Entscheidungen der DSK sind abrufbar unter: http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm.

23 Art. 6a Abs. 7 DSG, LGBl. 2002 Nr. 55.

24 DSK 2010/4; s. unter: http://www.llv.li/amtsstellen/llv-dss-datenschutzkommission/llv-dss-entscheiddatenbank-dsk.htm.

C. Sonstige wichtige Informationen

Die DSS versteht sich nicht nur als reaktive Anlaufstelle, sondern nimmt ihren Leistungsauftrag auch aktiv wahr. In diesem Sinne hatte sie bei der Regierung eine Untersuchung[25] der Datenströme im Bereich der Sozialleistungen angeregt, was auch bei der Landtagsdiskussion zum Tätigkeitsbericht 2010 der DSS aufgegriffen und bekräftigt wurde. Anlass hierfür war eine Beschwerde zum Austausch von Gesundheitsdaten zwischen verschiedenen Behörden. Der Fall zeigte klar, wie schwierig es im Dickicht von Sozialleistungen und dem zugrundeliegenden Informationsaustausch ist, den Überblick zu behalten. Informationen sind eine wesentliche Voraussetzung für die Ausschüttung bzw. Inanspruchnahme von Sozialleistungen. Nach Ansicht der DSS fehlt eine landesweite Untersuchung darüber, wie die unterschiedlichen Stellen, die wirtschaftliche Hilfe verteilen, miteinander vernetzt sind und welche Informationen zwischen den einzelnen Stellen ausgetauscht werden. Eine Untersuchung sollte datenschutzrechtliche Aspekte näher beleuchten und zu einer höheren Transparenz beitragen. So könnten auch allfällige Missbräuche vermieden und Doppelgleisigkeiten reduziert werden.

Im Rahmen der International Working Group on Data Protection in Telecommunications (IWGDPT) brachte die DSS eine Diskussionsgrundlage[26] zum Thema Datenschutz auf mobilen Endgeräten (Mobiltelefone, Notebooks, usw.) ein. Durch die kleine Bauform und das geringe Gewicht der mobilen Geräte ergeben sich spezifische Risiken für die Datensicherheit, wie z. B. der Manipulation, dem Verlust oder dem Diebstahl der Daten.

[25] Die Regierung hatte bereits 2005 eine „Analyse Sozialstaat Liechtenstein" in Auftrag gegeben, in der 25 sozialstaatliche Leistungen untersucht worden waren. Die vorgeschlagene Untersuchung könnte daran anknüpfen.

[26] http://www.datenschutz-berlin.de/attachments/724/WP_Mobile_Verarbeitung_und_Datensicherheit_final_clean_675_41_19.pdf?1292412668.

NORWEGEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das wichtigste Thema dieses Jahres war die Debatte zur Richtlinie über die Vorratsspeicherung von Daten. Es überrascht nicht, dass sich die Datenschutzbehörde gegen die Umsetzung der Richtlinie ausgesprochen hat. Das Thema hatte die seit Jahren längste parlamentarische Debatte zum Schutz personenbezogener Daten zur Folge.

Über unsere Hotline und unseren E-Mail-Dienst wurden 7 300 Anrufe und E-Mails bearbeitet, wobei 17 % der Anfragen das Thema Datenschutz am Arbeitsplatz betrafen.

Im Hinblick auf Sensibilisierungsmaßnahmen haben wir unsere Kampagne „Deine Entscheidung" fortgesetzt, die in verschiedene Sprachen übersetzt ist. Wenn Sie das Material sichten möchten, wenden Sie sich einfach an uns.

Außerdem haben wir uns an der Erarbeitung eines Tests zur Prüfung der Anfälligkeit für Identitätsdiebstahl beteiligt, der auf unserer Website abrufbar ist. Der Test wird auch von anderen Ländern verwendet.

Eine Vielzahl der Regierungsaktivitäten betraf das Gesundheitswesen. Es gab zahlreiche Vorschläge zu neuen Gesundheitsregistern, die die Datenschutzbehörde als negativ im Hinblick auf den Schutz personenbezogener Daten einstuft. Einzelpersonen haben nur wenig oder keine Kontrolle über die Nutzung ihrer in diesen Registern erfassten personenbezogenen Daten.

Die Datenschutzbehörde erarbeitete zusammen mit der Organisation „Finance Norway" eine revidierte Genehmigung für alle in Norwegen ansässigen Banken. Dies machte 251 der 357 durchgeführten Vorabprüfungen aus.

Im Laufe des Jahres starteten wir ein Projekt zu sozialen Netzwerken. Der Bericht ist auf unserer Website abrufbar. Im Rahmen dieses Projekts untersuchten wir vier verschiedene soziale Netzwerke.

Organisation	Datatilsynet – Norwegische Datenschutzbehörde
Vorsitz und/oder Gremium	
Budget	32 million NOK (etwa 4 Millionen EUR)
Personal	37 Angestellte und 3 Projektstellen
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k.A.
Meldungen	3 693
Vorabprüfungen	357
Anträge betroffener Personen	449 (Anzahl der schriftlichen Anfragen von privaten Einzelpersonen)
Beschwerden betroffener Personen	In der oben genannten Zahl enthalten
Vom Parlament bzw. der Regierung angeforderte Beratung	125
Sonstige Informationen zu relevanten allgemeinen Aktivitäten	

Prüfmaßnahmen	
Prüfungen, Untersuchungen	135 Beschäftigung – Systeme zur Zugangskontrolle und Zugriff auf E Mails: 11 Kinder und Jugendliche: 6 Elektronische Fahrscheine im öffentlichen Transportwesen: 1 Finanzwesen – Zahlungen: 2 Versicherungswesen – Kinder und Lebensversicherungen: 5 Gesundheitsforschung: 10 Gesundheit: 14 Sport – Doping: 7 Justiz – Übermittlung personenbezogener Daten: 7 Videoüberwachung – Einkaufszentren: 44 Kommunen: 7 Schengen (SIS): 2 Soziale Netzwerke: 4 Telekommunikation: 5 Bildung: 8 Sozialhilfe: 2
Sanktionsmaßnahmen	
Sanktionen	1 Zwangsmaßnahme aufgrund ausbleibender Reaktion auf eine Anfrage der Datenschutzbehörde
Geldbußen	Die Datenschutzbehörde verhängte 3 Geldbußen in Höhe von insgesamt 120 000 NOK
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	173 von der Datenschutzbehörde genehmigte Datenschutzbeauftragte
Pr. 30.04.2010	161
Pr. 31.08.2010	168
Pr. 31.12.2010	173

B. Rechtsprechung

Diese Beispiele für Fälle aus dem Jahr 2010 bieten nur einen kleinen Überblick über die Themen, von denen wir vermuten, dass sie für unsere Kolleginnen und Kollegen im restlichen Europa interessant sind.

Überwachung bei der US-Botschaft

Ein nationaler Fernsehsender deckte auf, dass norwegische Bürgerinnen und Bürger im Namen der amerikanischen Botschaft überwacht wurden. Die Datenschutzbehörde trat hierzu in Dialog mit der Polizei, die den Fall daraufhin untersuchte und unsere Ansicht hierzu zu Protokoll nahm. Die Behörde war der Ansicht, dass die Botschaft diese Form der Informationssammlung auf einen engen Bereich um die Botschaft beschränken sollte.

Datenaustausch

Die Beschwerdekammer entschied, dass es einer Rechtsanwaltskanzlei gestattet sein sollte, Personen aufzuspüren, die Daten austauschen. Die Datenschutzbehörde hatte zuvor einen entsprechenden Genehmigungsantrag abgewiesen. Man geht davon aus, dass diesbezüglich bald entsprechende Gesetze verabschiedet werden.

Kontrolle der Bereitstellung von Telefondaten für die Polizei durch Telekommunikationsunternehmen

Die Datenschutzbehörde wollte prüfen, welche Verfahren zum Austausch von Informationen zwischen Telekommunikationsunternehmen und der Polizei angewendet werden. Zudem wollten wir die Kriterien untersuchen, die im Hinblick auf einen solchen Austausch erfüllt sein müssen. Dies soll zum einen sicherstellen, dass die Polizei einfach auf diese Daten zugreifen kann, und zum anderen als Vorbereitung im Hinblick auf die unserer Ansicht zu erwartende Umsetzung der Richtlinie über die Vorratsspeicherung von Daten dienen.

Zugriff auf E-Mails von Angestellten

Im Jahr 2009 wurden neue Vorschriften für den Zugriff auf E-Mails von Angestellten eingeführt. Im Jahr 2010 verhängte die Datenschutzbehörde Geldbußen gegen zwei Unternehmen wegen des Verstoßes gegen diese Vorschriften. Im ersten Fall leitete ein Arbeitgeber alle E-Mails eines Angestellten an seine eigene E-Mail-Adresse weiter, ohne den Angestellten vorher darüber in Kenntnis zu setzen, und speicherte alle Inhalte. Im anderen Fall wurde einer Vertretung Zugang zum E-Mail-Konto eines krank gemeldeten Arbeitnehmers gewährt, ohne dass dieser zuvor darüber informiert wurde. Die Vorgehensweise im letzten Fall ist auch dann verboten, wenn der Angestellte zuvor informiert wird. Die Vorschriften besagen, dass persönliche E-Mail-Konten als personenbezogene Informationen einzustufen und entsprechend zu behandeln sind.

Kapitel Fünf
Mitglieder und Beobachter der Artikel-29-Datenschutygruppe

5. Mitglieder und Beobachter der Artikel-29-Datenschutygruppe

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE IM JAHR 2010

Österreich	Belgien
Frau Eva Souhrada-Kirchmayer (von Juli 2010) Frau Waltraut Kotschy (bis Juni 2010) Österreichische Datenschutzkommission (Datenschutzkommission) Hohenstaufengasse 31 - 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) 15, Acad.Ivan Evstratiev Geshov blvd. BG- 1431 Sofia Tel+359 2 915 3501 Fax: +359 2 915 3525 E-mail: kzld@government.bg, kzld@cpdp.bg Website: http://www.cdpd.bg	Frau Panayiota Polychronidou 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	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.uoou.cz/	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@aki.ee Website: http://www.aki.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) 228 99-7799-0 Fax: +49 (0) 228 99-7799-550 E-mail: poststelle@bfdi.bund.de Website: http://www.datenschutz.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, PC 115 23 Athen - Griechenland 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: www.adatvedelmibiztos.hu
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 Daten (Office of the Information and 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.idpc.gov.mt
Niederlande	**Polen**
Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ The Hague Tel: +31 70 8888500 Fax: +31 70 8888501 E-mail: info@cbpweb.nl Website: http://www.cbpweb.nl http://www.mijnprivacy.nl	Herr Wojciech Rafał Wiewiórowski Nationale Aufsichtsbehörde für persönliche Datenverarbeitung (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warsaw Tel: +48 22 860 7312; +48 22 860 70 81 Fax: +48 22 860 73 13 E-mail: desiwm@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 Slowakischen 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) Vošnjakova 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 José Luis Rodriguez Álvarez 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: Füllen 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 ART. 29 DATENSCHUTZGRUPPE IM JAHR 2010

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 Kim Ellertsen 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 Frau Sanja Vuk Abteilungsleiterin für EU-und Rechtsausschuss 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	
Herr Dimitar Gjeorgjievski Datenschutzdirektion (ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ) Samoilova 10, 1000 Skopje, RM Tel: +389 2 3230 635 Fax: +389 2 3230 635 E-mail: info@dzlp.mk Website: www.dzlp.mk	

Sekretariat der Art. 29 Datenschutzgruppe
Frau Marie-Hélène Boulanger Geschäftsführende Referatsleiterin Referat Datenschutz Generaldirektion Justiz, Freiheit und Sicherheit Europäische Kommission Büro: MO59 02/13 - 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/data-protection/index_en.htm

Europäische Kommission - Generaldirektion Justiz
14. Bericht der Artikel-29-Datenschutzgruppe

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2013
2013 — 134 S. — 21 × 29.7 cm

ISBN 978-92-79-29768-7
doi: 10.2838/28425

DS-AA-13-001-DE-C
doi: 10.2838/28425

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.

Amt für Veröffentlichungen

ISBN 978-92-79-29768-7