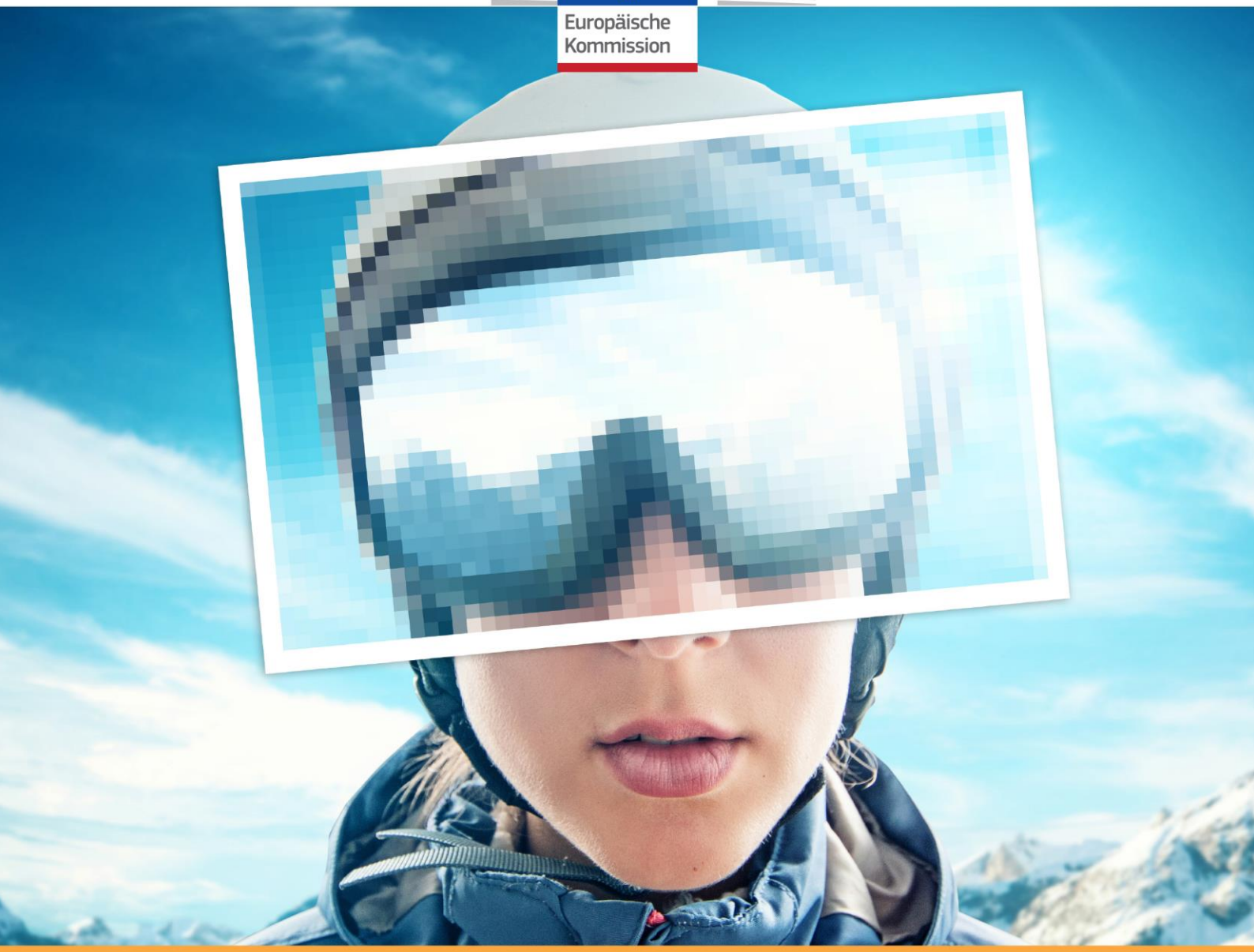
Europäische Kommission



15. Bericht

der Artikel-29-Datenschutzgruppe

Justiz und Verbraucher

Europe Direct soll Ihnen helfen, Antworten auf Ihre Fragen zur Europäischen Union zu finden

Gebührenfreie Telefonnummer (*)**:**

00 800 6 7 8 9 10 11

(*) Sie erhalten die bereitgestellten Informationen kostenlos, und in den meisten Fällen entstehen auch keine Gesprächsgebühren (außer bei bestimmten Telefonanbietern sowie für Gespräche aus Telefonzellen oder Hotels).

Zahlreiche weitere Informationen zur Europäischen Union sind verfügbar über Internet, Server Europa (http://europa.eu).

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2015

ISBN 978-92-79-38254-3
doi: 10.2838/10635
ISSN: 2363-1015

DE

15. Bericht der Artikel-29-Datenschutzgruppe

Berichtsjahr 2011

Angenommen am 3.12.2013

DE

Inhaltsverzeichnis

VORWORT DES VORSITZENDEN DER ARTIKEL-29-DATENSCHUTZGRUPPE

Dieser Jahresbericht der Artikel-29-Arbeitsgruppe zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten stellt einen Überblick über die Arbeit der Gruppe im Jahr 2011 dar. Die Datenschutzgruppe ist ein unabhängiges Beratungsgremium, in dem alle 27 nationalen Datenschutzbehörden der Mitgliedstaaten der Europäischen Union sowie der Europäische Datenschutzbeauftragte und die Europäische Kommission vertreten sind. Die Datenschutzgruppe gibt Stellungnahmen oder Empfehlungen zu allen Angelegenheiten bezüglich des Schutzes personenbezogener Daten heraus und trägt somit zur einheitlichen Anwendung und Interpretation der Datenschutzgesetze in den Mitgliedstaaten der Europäischen Union bei.

In den letzten Jahren hat sich die Datenschutzgruppe intensiv mit der Datenschutzreform auseinandergesetzt. Zum Zeitpunkt der Abfassung hat die Europäische Kommission bereits die Vorschläge für die Reform der Datenschutzvorschriften vorgelegt, die aus einer allgemeinen Datenschutzverordnung und einer Richtlinie für den Bereich der Strafverfolgung bestehen. Die Datenschutzgruppe ruft seit jeher zu Einheitlichkeit auf und war daher etwas enttäuscht, als zwei unterschiedliche Instrumente präsentiert wurden. Dennoch kann Einheitlichkeit nach wie vor erzielt werden, wenn die Instrumente die gleichen Rechte, Prinzipien und Schutzmechanismen bereitstellen. Die Datenschutzgruppe hat sich in den Reformprozess eingebracht und wird dies auch in Zukunft tun.

Aufgrund der zunehmenden technischen Möglichkeiten für die Verarbeitung personenbezogener Daten sowohl im privaten als auch im öffentlichen Bereich muss dem Schutz personenbezogener Daten von natürlichen Personen sogar noch mehr Aufmerksamkeit zukommen. Eine europaweite Studie von Eurobarometer zu den Einstellungen europäischer Bürger zum Thema Datenschutz und elektronische Identität[1] hat gezeigt, dass Einzelpersonen in der Regel nicht den Eindruck haben, Kontrolle über ihre personenbezogenen Daten zu haben.[2]

Da personenbezogene Daten zu einer neuen Währung geworden sind – man sehe sich den Shareholder Value von Unternehmen wie Facebook, Google und Twitter an, die mit personenbezogenen Daten handeln –, ist besonders diese Branche offenbar sehr daran interessiert, möglichst viele personenbezogenen Daten von Verbrauchern zu sammeln. Oftmals legen Unternehmen Profile von Personen an, um diese gezielt anzusprechen und dadurch ihre Gewinne zu maximieren bzw. ihre Risiken zu minimieren. Die Eurobarometer-Umfrage sowie regelmäßige Kontakte zwischen Bürgern und Datenschutzbehörden haben gezeigt, dass Menschen oft gar nicht wissen, dass ihre Daten erfasst werden. Und falls man sich doch der Menge der erfassten personenbezogenen Daten bewusst ist, fühlt man sich zwar unbehaglich, weiß aber nicht, was man dagegen tun kann.

Diese Unwissenheit der Bürger bezüglich des Umgangs Dritter mit ihren personenbezogenen Daten ist umso schockierender, wenn man bedenkt, dass Datenschutz innerhalb der EU zu den Grundrechten zählt. Es ist daher unerlässlich, dass Bürger der Erfassung und Verarbeitung ihrer personenbezogenen Daten durch Dritte ausdrücklich zustimmen müssen, wenn es für diese Dritten keinen anderweitigen Rechtsgrund für ihr Handeln gibt. In ihrer Stellungnahme zum Thema Einwilligung betonte die Datenschutzgruppe, dass lediglich Erklärungen oder Handlungen eine gültige Einwilligung darstellen und nicht bloßes Schweigen

[1] Eurobarometer, Special Eurobarometer 359, *Attitudes on Data Protection and Electronic Identity in the European Union,* Juni 2011.

[2] Der Bericht zeigt, dass einerseits 74 % der Europäer die Offenlegung personenbezogener Daten zunehmend als Teil des modernen Lebens erachten – insbesondere in Verbindung mit dem Internet. Andererseits sind europäische Bürger nicht der Ansicht, die Offenlegung ihrer personenbezogenen Daten unter Kontrolle zu haben: Gerade einmal 26 % der Nutzer sozialer Netzwerke und 18 % der Online-Shopper gaben an, dass dies bei ihnen der Fall sei. 70 % der Bürger sind misstrauisch, dass Unternehmen ihre personenbezogenen Daten für Zwecke verwenden, für die sie ursprünglich nicht erfasst wurden.

oder Untätigkeit. Durch die ausdrückliche Einwilligung bekommen Bürger wieder die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten.

Eine solche ausdrückliche Einwilligung von Einzelpersonen wird von der Industrie jedoch nicht immer eingeholt. 2011 entwickelte die Industrie für verhaltensorientierte Werbung im Internet (Online Behavioural Advertising, OBA) als Selbstregulierungsmaßnahme einen neuen Verhaltenskodex für OBA. Die Datenschutzgruppe untersuchte diesen Verhaltenskodex und kam zu dem Schluss, dass er nicht zu einer Einhaltung der europäischen Datenschutzgesetze führen würde. Die Datenschutzgruppe mahnte an, dass man eine Situation vermeiden solle, in der die Befolgung eines Verhaltenskodex nicht zu einer Einhaltung der europäischen Datenschutzgesetze führt.

Des Weiteren äußerte die Datenschutzgruppe ihre Bedenken zu zwei Vorschlägen der Europäischen Kommission bezüglich des Zugriffs auf Daten von Privatunternehmen zu Strafverfolgungszwecken. Der erste Vorschlag umfasste die Einrichtung eines europäischen Systems, das es Strafverfolgungsbehörden ermöglicht, auf Fluggastdatensätze (Passenger Name Records, PNR) zuzugreifen, die Fluggesellschaften über Flüge mit EU-Mitgliedstaaten als Abreise- oder Zielort gespeichert haben. Laut den europäischen Datenschutzbehörden sei die Notwendigkeit des vorgeschlagenen Systems nicht erwiesen. Das vorgeschlagene System sei nicht datenschutzfreundlich, und die Ziele könnten auch auf anderem Wege ohne eine Verletzung der Datenschutzvorschriften erreicht werden.

Die Datenschutzgruppe hatte außerdem Bedenken bezüglich des Vorschlags, ein europäisches Pendant zum derzeit in den USA verwendeten System zum Aufspüren der Terrorismusfinanzierung (Terrorist Financial Tracking System, TFTS) einzurichten. Das Programm ermöglicht es bestimmten Strafverfolgungsbehörden, auf die Daten internationaler Banktransaktionen zuzugreifen, die innerhalb der EU vorgenommen werden. Die Daten werden in großen Datenbanken gespeichert, die nach Spuren einer Finanzierung eventueller Terroraktivitäten durchsucht werden können. Die Datenschutzbehörden waren von einer Notwendigkeit oder Verhältnismäßigkeit eines europäischen TFTS nicht überzeugt und gaben zu verstehen, dass lediglich der Mehrwert der vom System erhaltenen Informationen nicht ausreichend sei. In einem Schreiben an die Europäische Kommission ruft die Datenschutzgruppe die Kommission dazu auf, diese nachzuweisen, falls ein endgültiger Vorschlag unterbreitet werden sollte.

Das zuvor erwähnte Eurobarometer hat gezeigt, dass Einzelpersonen darüber besorgt sind, wie ihre personenbezogenen Daten erfasst, verarbeitet und gespeichert werden. Daher ist es von entscheidender Bedeutung, dass die Verarbeitung personenbezogener Daten sowohl durch private als auch durch staatliche Organisationen unter Einhaltung der europäischen Datenschutzgesetze erfolgt. Die Datenschutzbehörden werden diese Gesetze, falls erforderlich, sowohl einzeln als auch gemeinsam durchsetzen.

Jacob Kohnstamm.

Kapitel Eins

Fragen, zu denen die Artikel-29-Datenschutzgruppe Stellung genommen hat[3]

[3] 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

1.1 DATENÜBERMITTLUNG IN DRITTLÄNDER

1.1.1 Passagierdaten/PNR

Stellungnahme 10/2011 (WP181) zu dem Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität

Am 2. Februar 2011 veröffentlichte die Europäische Kommission ihren Vorschlag für eine Richtlinie über die Verwendung von Fluggastdatensätzen zu Zwecken der Verhütung, Aufdeckung, Aufklärung und strafrechtlichen Verfolgung von terroristischen Straftaten und schwerer Kriminalität. Die Datenschutzgruppe hat auch zu dem von der Kommission am 6. November 2007 unterbreiteten vorangegangenen PNR-Vorschlag (Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken) eine Stellungnahme vorgelegt. Die Datenschutzgruppe hat sich außerdem bereits in mehreren Stellungnahmen ausführlich zu den verschiedenen zwischen der EU und Drittländern bestehenden PNR-Abkommen sowie zu dem in der Mitteilung der Kommission vom 21. September 2010 dargelegten Konzept der Kommission geäußert. Darüber hinaus hat die Datenschutzgruppe in verschiedenen Schreiben an die Kommissionsmitglieder Barrot und Malmström, Generaldirektor Faull und den LIBE-Ausschuss des Europäischen Parlaments ihre Bedenken in Bezug auf PNR-Fragen mehrfach wiederholt.

Diese Stellungnahme richtet sich an die an der Erörterung und Erarbeitung des jüngsten Vorschlags Beteiligten, insbesondere die Kommission, die Arbeitsgruppe GENVAL des Rates und das Europäische Parlament.

Fazit

Die Datenschutzgruppe ist der Auffassung, dass die Notwendigkeit eines EU-PNR-Systems noch nicht erwiesen ist und die vorgeschlagenen Maßnahmen dem Grundsatz der Verhältnismäßigkeit insbesondere deshalb nicht entsprechen, weil das System die Erfassung und Speicherung sämtlicher Daten über alle Reisenden auf allen Flügen vorsieht. Sie hegt außerdem ernste Zweifel an der Verhältnismäßigkeit eines systematischen Abgleichs aller Fluggäste mit bestimmten im Voraus festgelegten Kriterien.

Die Datenschutzgruppe empfiehlt zunächst die bestehenden Systeme und Methoden der Zusammenarbeit und ihr Zusammenwirken zu bewerten um etwaige Sicherheitslücken zu ermitteln. Falls Sicherheitslücken bestehen, sollte dann untersucht werden, wie sie am besten geschlossen werden können, was nicht notwendigerweise mit der Einführung eines völlig neuen Systems verbunden sein muss. Vielmehr könnten die bestehenden Mechanismen weiter genutzt und verbessert werden.

Falls die vorgeschlagene Richtlinie in Kraft tritt, sollte sie geeignete und angemessene Datenschutzmaßnahmen und -garantien enthalten. Die Kommission sollte außerdem prüfen, ob bestehende Systeme wie die API-Richtlinie aufgehoben werden können, um Maßnahmenüberschneidungen zu vermeiden.

1.1.2. Angemessenheit

Stellungnahme 11/2011 (WP182) zum Schutz personenbezogener Daten in Neuseeland

Die Datenschutzgruppe wurde 2009 gebeten, die Angemessenheit der neuseeländischen Datenschutzgesetzgebung zu prüfen. Die dafür zuständige Untergruppe erhielt diesen Auftrag in der Plenarsitzung im Dezember 2009.

Die Europäische Kommission legte den angeforderten Bericht zur Angemessenheit des Datenschutzes in Neuseeland vor, der von Professor Roth, Fakultät für Rechtswissenschaft, Universität Otago, Dunedin, Neuseeland, verfasst wurde. Dieser Bericht wurde unter der Aufsicht des Centre de Recherches Informatique et Droit (CRID) der Universität Namur erstellt. In dem Bericht wird untersucht, inwieweit das neuseeländische Rechtssystem unter dem Aspekt der materiellen Gesetzgebung und der Verfügbarkeit von Mechanismen zur Anwendung von Rechtsvorschriften zum Schutz personenbezogener Daten den einschlägigen Anforderungen entspricht. Diese Anforderungen 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 Artikel-29-Datenschutzgruppe am 24. Juli 1998 (WP12) angenommen worden war. Des Weiteren wird auf nichtgesetzliche Vorschriften, die Anwendung in der Praxis sowie auf die allgemeine Verwaltungs- und Unternehmenskultur eingegangen, die in Bezug auf Datenschutz existieren.

Die Untergruppe berücksichtigte diesen Bericht, die von der neuseeländischen Datenschutzbehörde und dem neuseeländischen Justizministerium abgegebenen Kommentare zu diesem Bericht sowie das Schreiben vom Justizministerium bezüglich des neuseeländischen Datenschutzgesetzes (Privacy [Cross-border Information] Amendment Act 2010). Außerdem bat die Untergruppe die neuseeländische Datenschutzbeauftragte (die nationale Aufsichtsbehörde) um weitere Informationen sowie um die Klarstellung bezüglich einiger Aspekte, die im Folgenden aufgeführt werden. Die Untergruppe berücksichtigte anschließend die erhaltenen Informationen, welche Leitlinien der Datenschutzbeauftragten zur Anwendung des Privacy (Cross-border Information) Amendment Act nach dessen Inkrafttreten am 7. September 2010 umfasste.

Diese Stellungnahme beruht weitgehend auf Professor Roths Bericht, der gut formuliert und hilfreich strukturiert war, um die Gesetzgebung Neuseelands mit den Anforderungen in WP 12 abzugleichen.

Ergebnis der Beurteilung

Das neuseeländische Datenschutzgesetz geht der EU-Richtlinie größtenteils zeitlich voraus und setzt die OECD-Leitlinien um. Vor Kurzem hat es jedoch einige Änderungen gegeben, die speziell aufgrund der Bedenken hinsichtlich der „Angemessenheit“ für Übermittlungen personenbezogener Daten aus der EU vorgenommen wurden. Die Datenschutzgruppe weist darauf hin, dass Angemessenheit nicht Gleichwertigkeit mit der Richtlinie bedeutet, auch wenn nach wie vor einige Bedenken bestehen.

Daher kommt die Datenschutzgruppe zu der Schlussfolgerung, dass Neuseeland ein angemessenes Schutzniveau gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr aufweist.

Die Datenschutzgruppe ruft die neuseeländischen Behörden jedoch dazu auf, die notwendigen Schritte in die Wege zu leiten, um Schwächen des derzeitigen Rechtsrahmens anzusprechen. Insbesondere ruft die Datenschutzgruppe die Datenschutzbeauftragte dazu auf, ihre Bemühungen zur Stärkung des Gesetzes in Bezug auf Direktmarketing fortzusetzen und eine effektive Aufsicht der Datenübermittlungen von Neuseeland an Drittländer beizubehalten, die selbst nicht einer Angemessenheitsfeststellung unterzogen

wurden. Die Datenschutzgruppe fordert außerdem, dass die Datenschutzbeauftragte bei der Entscheidung, ob ein Übermittlungsverbot verhängt werden soll, neben den OECD-Leitlinien und der EU-Richtlinie auch relevante Entscheidungen der Europäischen Kommission und Leitlinien der Artikel-29-Datenschutzgruppe berücksichtigen soll.

Die Datenschutzgruppe weist ferner mit Nachdruck darauf hin, dass sie im Rahmen aller Entscheidungen der Kommission die Entwicklungen zum Thema Datenschutz in Neuseeland sowie die Art und Weise, wie die Behörde der Datenschutzbeauftragten die im Dokument WP12 und in diesem Dokument enthaltenen Grundsätze des Datenschutzes anwendet, genau verfolgen wird.

1.2. ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

Stellungnahme 12/2011 (WP183) zur intelligenten Verbrauchsmessung („Smart Metering“)

Die Artikel-29-Datenschutzgruppe verfolgt mit dieser Stellungnahme das Ziel, den rechtlichen Rahmen darzulegen, der für den Betrieb intelligenter Verbrauchsmessgeräte („Smart Meters“) im Energiesektor gilt. Diese Stellungnahme soll keinen erschöpfenden Überblick über sämtliche spezifischen Aspekte von Programmen zur intelligenten Verbrauchsmessung geben, da dies aufgrund der Uneinheitlichkeit der gegenwärtigen Situation nicht möglich wäre. Intelligente Verbrauchsmessgeräte bieten neue Funktionalitäten, wie z. B. die Bereitstellung detaillierter Informationen über den Energieverbrauch, die Möglichkeit einer Fernablesung der Verbrauchszähler, die Entwicklung neuer Tarife und Dienstleistungen auf Grundlage von Energieprofilen sowie die Möglichkeit der Fernabschaltung der Energieversorgung.

Intelligente Stromversorgungsnetze („Smart Grids“) bieten noch mehr Entwicklungsspielraum und Möglichkeiten für die Verarbeitung zusätzlicher personenbezogener Daten. Die Datenschutzgruppe möchte zum gegenwärtigen Zeitpunkt ihre Stellungnahme nicht auf die „Smart-Grid“-Funktion ausdehnen, schließt aber nicht aus, dass sie sich eingehender mit intelligenten Stromnetzen befassen wird, sobald sich das Bild weiter konkretisiert hat.

In der EG-Richtlinie über Endenergieeffizienz und Energiedienstleistungen (2006/32/EG) werden Energieeinsparziele festgelegt, die von den einzelnen Mitgliedstaaten übernommen werden müssen. Um diese Ziele – vorbehaltlich bestimmter Ausnahmefälle – zu erreichen, werden die Mitgliedstaaten nach Artikel 13 der Richtlinie verpflichtet, den Verbrauchern Verbrauchsmessgeräte zur Verfügung zu stellen, die ihren Energieverbrauch exakt wiedergeben und Informationen zur tatsächlichen Nutzungszeit liefern. Diese intelligenten Verbrauchsmessgeräte sind Teil der Bestrebungen, die Ziele der Europäischen Union im Hinblick auf den Aufbau einer nachhaltigen Energieversorgung bis zum Jahr 2020 umzusetzen.

Fazit

Mit der Einführung intelligenter Verbrauchsmessungen, die den Weg für intelligente Stromversorgungsnetze ebnen, entsteht ein völlig neues, komplexes Modell gegenseitiger Wechselbeziehungen, das besondere Herausforderungen für die Anwendung des Datenschutzrechts darstellt. Aus den Antworten auf den Fragebogen der Generaldirektion Energie geht hervor, dass die Situation in den EU-Mitgliedstaaten sehr unterschiedlich ist, sowohl hinsichtlich der Fortschritte bei der Einführung als auch hinsichtlich der Energieversorgungssysteme, wodurch sich die Sachlage weiter verkompliziert. Die immense Tragweite intelligenter Verbrauchsmessungen steht jedoch außer Frage: Bis 2020 dürften entsprechende Systeme in den Haushalten der überwiegenden Mehrheit der Bürger Europas installiert sein.

In dieser Stellungnahme wird die Anwendbarkeit des Datenschutzrechts erläutert; dabei wird dargelegt, dass von den Messgeräten personenbezogene Daten verarbeitet werden und somit die Datenschutzvorschriften Anwendung finden. Mit dieser Stellungnahme wird aufgezeigt, dass intelligente Verbrauchsmessungen das Potenzial für vielfältige neue Formen der Datenverarbeitung und der Kundendienstleistungen bieten. Unabhängig davon, wie die Datenverarbeitung erfolgt – ob auf ähnliche Weise wie vor der Einführung intelligenter Systeme oder in völlig neuartiger Form –, der für die Datenverarbeitung Verantwortliche muss eindeutig ermittelt werden und sich der aus dem Datenschutzrecht erwachsenden Pflichten, auch in Bereichen wie „eingebautem Datenschutz" („Privacy by Design"), Datensicherheit und Rechten der betroffenen Person, bewusst sein. Die betroffenen Personen müssen angemessen darüber unterrichtet werden, wie ihre Daten verarbeitet werden, und sich über die grundlegenden Unterschiede bei der Verarbeitung ihrer Daten im Klaren sein, so dass sie ihre Einwilligung in rechtsgültiger Form geben können.

Stellungnahme 13/2011 (WP185) zur Ortsbestimmung auf intelligenten mobilen Geräten

Geografische Informationen spielen in unserer Gesellschaft eine wichtige Rolle. Fast alle menschlichen Aktivitäten und Entscheidungen haben eine geografische Komponente. Im Allgemeinen steigt der Wert der Informationen, wenn diese mit einem Ort in Verbindung gebracht werden. Alle Arten von Informationen können mit einem geografischen Ort in Verbindung gebracht werden, wie z. B. Finanzdaten, Gesundheitsdaten und weitere Daten zum Konsumverhalten. Durch die rasante technologische Entwicklung und die breite Akzeptanz intelligenter mobiler Geräte entsteht eine völlig neue Kategorie standortbezogener Dienstleistungen.

Mit dieser Stellungnahme soll der rechtliche Rahmen für Ortsbestimmungsdienste geklärt werden, die auf intelligenten, internetfähigen und mit Ortungsdiensten wie z. B. GPS ausgestatteten mobilen Geräten verfügbar sind bzw. von diesen generiert werden. Beispiele für derartige Dienste sind Karten und Navigation, geo-personalisierte Dienste (einschließlich nahegelegener Points of Interest), erweiterte Realität, Geotagging von Online-Inhalten, Verfolgung der Aufenthaltsorte von Freunden, Kinderbeaufsichtigung und standortbasierte Werbung.

Diese Stellungnahme befasst sich außerdem mit den drei Hauptinfrastrukturtypen für Ortsbestimmungsdienste, d. h. GPS, GSM-Basisstationen und WLAN. Besonderes Augenmerk gilt der neuen, auf Standorten von WLAN-Zugangspunkten basierenden Infrastruktur.

Die Datenschutzgruppe ist sich bewusst, dass es viele andere Dienste gibt, die Standortdaten verarbeiten und ebenfalls Bedenken im Hinblick auf Datenschutz aufwerfen. Zu nennen wären dabei E-Ticketing-Systeme, Mautsysteme für Autos, Satellitennavigationsdienste, Ortsbestimmung z. B. durch Kameras sowie die Ortsbestimmung von IP-Adressen. Angesichts der rasanten technologischen Entwicklung, vor allem bezüglich der Ortung von WLAN-Zugangspunkten, zusammen mit der Tatsache, dass neue Marktteilnehmer sich auf die Entwicklung neuer standortbasierter Dienste auf Grundlage von Basisstations-, GPS- und WLAN-Daten vorbereiten, hat sich die Datenschutzgruppe jedoch dazu entschlossen, insbesondere die rechtlichen Anforderungen dieser Dienste gemäß der Datenschutzrichtlinie zu erläutern.

In der Stellungnahme werden zunächst die Technologien beschrieben, daraufhin die Datenschutzrisiken identifiziert und beurteilt und anschließend Schlussfolgerungen zur Anwendung der entsprechenden rechtlichen Artikel durch die verschiedenen für die Datenverarbeitung Verantwortlichen gezogen, die standortbasierte Daten über mobile Geräte erfassen und verarbeiten. Hierzu gehören zum Beispiel Anbieter von Ortsbestimmungsinfrastruktur, Smartphone-Hersteller und Entwickler von standortbasierten Anwendungen.

Diese Stellungnahme stellt keine Beurteilung spezifischer Geotagging-Technologien dar, die mit dem sogenannten Web 2.0 in Verbindung stehen und mit deren Hilfe Nutzer georeferenzierte Daten in soziale Netzwerke wie Facebook oder Twitter integrieren. Des Weiteren wird mit dieser Stellungnahme nicht auf einige andere Ortsbestimmungstechnologien eingegangen, mit denen Geräte innerhalb eines relativ kleinen Bereichs (Einkaufszentren, Flughäfen, Bürogebäude usw.) miteinander verbunden werden, wie z. B. Bluetooth, ZigBee, Geofencing und WLAN-basierte RFID-Tags, obwohl viele der Schlussfolgerungen dieser Stellungnahme im Hinblick auf rechtmäßige Gründe, Daten und die Rechte betroffener Personen auch für diese Technologien gelten, falls diese zur Standortbestimmung von Personen über deren Geräte verwendet werden.

Mithilfe von Ortsbestimmungstechnologien, wie z. B. Basisstationsdaten, GPS und ermittelte WLAN-Zugangspunkte, können intelligente mobile Geräte von allen möglichen Verantwortlichen zu Zwecken wie z. B. verhaltensorientierte Werbung oder Kinderbeaufsichtigung geortet werden.

Da Smartphones und Tablet-Computer aufs Engste mit ihren Besitzern verbunden sind, stellen die Bewegungsmuster der Geräte einen äußerst intimen Einblick in das Privatleben der Benutzer dar. Ein großes Risiko besteht darin, dass Benutzer sich nicht darüber im Klaren sind, dass und an wen sie ihren Standort übermitteln. Ein weiteres damit zusammenhängendes Risiko liegt darin, dass die Zustimmung einer Nutzung standortbasierter Daten bei bestimmten Anwendungen ungültig ist, da die Informationen über die Kernelemente der Verarbeitung unverständlich, veraltet oder anderweitig unzulänglich sind.

Die unterschiedlichen Beteiligten, darunter die Entwickler der Betriebssysteme, Anbieter von Anwendungen und Dritte, wie z. B. Social-Media-Websites, die Ortsbestimmungsfunktionen für mobile Geräte in ihre Plattformen integrieren, haben unterschiedliche Verpflichtungen.

Fazit

Rechtsrahmen

- Der Rechtsrahmen der EU für die Nutzung von Standortdaten von intelligenten mobilen Geräten ist in erster Linie die Datenschutzrichtlinie. Standortdaten von intelligenten mobilen Geräten sind personenbezogene Daten. Die eindeutige MAC-Adresse zusammen mit dem berechneten Standort eines WLAN-Zugangspunktes sollten als personenbezogene Daten gehandhabt werden;

- Darüber hinaus gilt die überarbeitete Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG nur für die Verarbeitung von Basisstationsdaten durch Telekommunikationsbetreiber.

Verantwortliche

- Es ist zwischen drei Verantwortlichen zu unterscheiden: Verantwortliche für Ortsbestimmungsinfrastruktur (insbesondere Verantwortliche für ermittelte WLAN-Zugangspunkte), Anbieter von Ortsbestimmungsanwendungen und -diensten sowie Entwickler von Betriebssystemen für intelligente mobile Geräte.

Rechtmäßige Gründe

- Da Standortdaten von intelligenten mobilen Geräten intime Details über das Privatleben der Besitzer preisgeben, ist die wichtigste anwendbare Rechtsgrundlage eine vorherige Einwilligung nach Inkenntnissetzung;

- Eine Einwilligung kann nicht durch allgemeine Geschäftsbedingungen eingeholt werden;

- Eine Einwilligung muss vom Verantwortlichen spezifisch für die verschiedenen Zwecke eingeholt werden, für die die Daten verarbeitet werden, wie z. B. Profilerstellung oder verhaltensorientierte Werbung. Wenn die Verarbeitungszwecke sich wesentlich ändern, muss der Verantwortliche erneut eine Einwilligung einholen;

- Standortdienste müssen standardmäßig deaktiviert sein. Eine mögliche Rücktrittsoption stellt keine angemessene Methode für die Einholung einer Einwilligung dar;

- Einwilligungen sind im Hinblick auf Arbeitnehmer und Kinder problematisch. Hinsichtlich Arbeitnehmern dürfen Arbeitgeber diese Technologie nur dann einführen, wenn sie nachweisbar einem legitimen Zweck dient und die gleichen Ziele nicht mit weniger in die Privatsphäre eindringenden Mitteln erreicht werden können. Im Falle von Kindern müssen die Eltern beurteilen, ob die Nutzung einer derartigen Anwendung in bestimmten Umständen gerechtfertigt ist. Sie müssen ihre Kinder zumindest darüber informieren und ihnen sobald wie möglich erlauben, sich an der Entscheidung zur Nutzung einer derartigen Anwendung zu beteiligen;

- Die Datenschutzgruppe empfiehlt, den Umfang einer Einwilligung zeitlich einzuschränken und Benutzer mindestens einmal pro Jahr zu erinnern. Die Datenschutzgruppe empfiehlt außerdem eine ausreichende Granularität der Einwilligung bezüglich der Präzision der Standortdaten;

- Betroffene Personen müssen dazu in der Lage sein, ihre Einwilligung ohne Weiteres und ohne negative Konsequenzen für die Nutzung ihrer Geräte zu widerrufen;

- Bezüglich der Ortung von WLAN-Zugangspunkten können Unternehmen für den spezifischen Zweck der Bereitstellung von Ortsbestimmungsdiensten ein legitimes Interesse an der nötigen Erfassung und Verarbeitung der MAC-Adressen und berechneten Standorte der WLAN-Zugangspunkte haben. Der Interessenausgleich zwischen den Rechten der Verantwortlichen und den Rechten der betroffenen Personen erfordert, dass Verantwortliche das Recht gewähren, sich ohne das Verlangen zusätzlicher personenbezogener Daten problemlos und permanent gegen die Aufnahme in die Datenbank zu entscheiden.

Informationen

- Informationen müssen klar, vollständig, für ein breites, technisch nicht versiertes Publikum verständlich sowie ständig und problemlos zugänglich sein. Die Gültigkeit der Einwilligung ist aufs Engste mit der Qualität der Informationen über den Dienst verknüpft;

- Dritte, wie z. B. Browser und Social-Media-Websites, nehmen bezüglich Sichtbarkeit und Qualität der Informationen über die Verarbeitung von Standortdaten eine wichtige Rolle ein.

Rechte von betroffenen Personen

- Die verschiedenen für die Verarbeitung Verantwortlichen von Ortsbestimmungsdaten mobiler Geräte sollten ihren Kunden die Möglichkeit einräumen, auf ihre Standortdaten in einem für Menschen unmittelbar lesbaren Format zuzugreifen und diese ohne eine übermäßige Erfassung personenbezogener Daten zu ändern und zu löschen;

- Betroffene haben außerdem das Recht, auf eventuelle, mithilfe der Standortdaten erstellte Profile zuzugreifen sowie diese zu ändern oder zu löschen;

- Die Datenschutzgruppe empfiehlt die Einrichtung eines (sicheren) Online-Zugriffs.

Aufbewahrungsfristen

- Anbieter von Ortungsanwendungen oder -diensten sollten Aufbewahrungsrichtlinien einführen, um dafür zu sorgen, dass Standortdaten oder mithilfe solcher Daten erstellte Profile nach einem angemessenen Zeitraum gelöscht werden;

- Falls der Entwickler des Betriebssystems bzw. der Verantwortliche der Ortungsinfrastruktur bezüglich der Standortdaten eine eindeutige Nummer, wie z. B. eine MAC-Adresse oder eine UDID, verarbeitet, darf die eindeutige Identifikationsnummer nur zu betrieblichen Zwecken und für maximal 24 Stunden gespeichert werden.

Stellungnahme 16/2011 (WP188) zur EASA/IAB-Best-Practice-Empfehlung für verhaltensorientierte Werbung im Internet

Im November 2009 nahmen das Europäische Parlament und der Rat die Richtlinie 2009/136/EG an. Diese Richtlinie ist eine Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG). Eine der wichtigsten Änderungen betrifft die Mechanismen für die Einspeisung von Daten in das Endgerät des Nutzers. Die existierende Rücktrittsoption, die es Nutzern ermöglicht, einer Verarbeitung der durch Endgeräte erfassten Daten (wie „Cookies“) zu widersprechen, wurde abgelehnt. Stattdessen wurde das Verfahren der Einwilligung nach Inkenntnissetzung zum Standard. Diese Änderungen spielen für verhaltensorientierte Werbung im Internet (Online Behavioural Advertising, OBA) eine wichtige Rolle, da die Branche stark von Cookies und ähnlichen Technologien Gebrauch macht, die in den Endgeräten der Benutzer Daten speichern und auf diese zugreifen.

Diese Einwilligungsanforderung spiegelte die wachsenden Bedenken von Bürgern, Politikern, Datenschutzbehörden, Verbraucherorganisationen und politischen Entscheidungsträgern wider, dass die technischen Möglichkeiten zur Verfolgung individuellen Online-Verhaltens über längere Zeit und Website-übergreifend im Internet stark zunehmen würden. Des Weiteren konnten die Möglichkeiten, die Bürgern zum Schutz ihres Privatlebens und ihrer personenbezogenen Daten vor dieser Art der Rückverfolgung zur Verfügung standen, mit diesem Wachstum nicht Schritt halten. 2009 hatten politische Entscheidungsträger starke Zweifel an der Option, sich bezüglich einer verstärkten Aufklärung der Öffentlichkeit zum Thema verhaltensorientierte Werbung im Internet sowie der diesbezüglichen vermehrten Bereitstellung von Auswahlmöglichkeiten auf die verantwortliche Werbeindustrie zu verlassen. Viele öffentliche Befragungen haben bislang gezeigt, dass durchschnittliche Internetnutzer sich nicht darüber im Klaren sind, dass ihr Verhalten mit der Hilfe von Cookies und anderen eindeutigen Kennungen rückverfolgt wird und wer dies zu welchem Zweck tut. Dieses mangelnde Bewusstsein steht im krassen Gegensatz zu der Tatsache, dass immer mehr europäische Bürgerinnen und Bürger für ganz alltägliche Dinge wie Einkaufen, Lesen, Kommunikation mit Freunden und Recherchieren auf einen Internetzugang angewiesen sind. Außerdem ersetzt das Internet auf rasante Weise zahlreiche Offline-Aktivitäten, wie z. B. den Zugang zu öffentlichen Dienstleistungen. Der schnelle Austausch „stationärer“ Internetzugänge mit mobilen Zugängen hat die Fähigkeit der Internetnutzer, sich selbst mit technischen Hilfsmitteln zu schützen, sogar noch weiter verkompliziert.

Bald nachdem die Einwilligung nach Inkenntnissetzung in Europa zur rechtlichen Norm geworden war, nahm die Artikel-29-Datenschutzgruppe die Stellungnahme 2/2010 zu verhaltensorientierter Werbung im Internet[4] (im Folgenden Stellungnahme 2/2010 genannt) an. Die Stellungnahme beschreibt die Rollen und

[4] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Verantwortlichkeiten der verschiedenen Akteure im Bereich verhaltensorientierter Werbung im Internet und klärt den anzuwendenden Rechtsrahmen. Die Stellungnahme konzentriert sich auf die Verfolgung des Online-Verhaltens über längere Zeit und auf verschiedenen Websites als Quelle der gravierendsten Datenschutzbedenken in Bezug auf OBA.

Im April 2011 verabschiedeten die verantwortlichen Akteure im Bereich OBA, vertreten durch die European Advertising Standards Alliance (EASA) und das Internet Advertising Bureau Europe (IAB), zu Selbstregulierungszwecken eine Best-Practice-Empfehlung zu OBA (im Folgenden der EASA/IAB-Kodex genannt)[5]. Im August 2011 schrieb die Artikel-29-Datenschutzgruppe einen offenen Brief[6] an die EASA und das IAB und legte darin die Datenschutzbedenken um die im EASA/IAB-Kodex vorgeschlagene Rücktrittsoption dar. Bei einem darauffolgenden Treffen mit der Artikel-29-Datenschutzgruppe äußerten Vertreter der EASA und des IAB, dass „der Kodex in erster Linie für die Schaffung gleicher Ausgangsbedingungen gedacht" sei und dass sein Zweck nicht in der Einhaltung der überarbeiteten Datenschutzrichtlinie für elektronische Kommunikation liege[7].

Wie bereits in der Stellungnahme 2/2010 zu lesen war, begrüßt die Artikel-29-Datenschutzgruppe die selbstregulierenden Initiativen der OBA-Branche. Der EASA/IAB-Kodex enthält in der Tat einige interessante Ansätze (wie z. B. Grundsatz V – Unterweisung), die die Einwilligungsmechanismen effektiver gestalten können, falls sie weiterentwickelt und umgesetzt werden. Der EASA/IAB-Kodex an sich ist jedoch nicht angemessen, um eine Einhaltung des aktuellen europäischen Rechtsrahmens zum Datenschutz zu gewährleisten. Zur Vermeidung von Missverständnissen hat die Artikel-29-Datenschutzgruppe beschlossen, gezielt zu analysieren, inwieweit der Kodex die relevanten rechtlichen Vorschriften einhält (siehe ergänzend dazu www.youronlinechoices.eu).

Genauer gesagt, konzentriert sich die aktuelle Stellungnahme auf die ersten beiden Grundsätze des EASA/IAB-Kodex und dessen praktische Anwendung auf www.youronlinechoices.eu, d. h. Grundsatz I (Benachrichtigung) und Grundsatz II (Wahlmöglichkeit der Nutzer). Darüber hinaus werden einige andere Grundsätze des Kodex sowie weitere Problembereiche (wie z. B. Datenspeicherung) besprochen. Ferner nutzt die Artikel-29-Datenschutzgruppe die Gelegenheit, um den Unterschied zwischen Tracking-Cookies und anderen Arten von Cookies zu erläutern, die von einer Einwilligung ausgeschlossen sein könnten, wobei sie praktische Beispiele von ausgenommenen Cookies nennt und mögliche Ansätze zu einer rechtlichen Einholung einer Einwilligung, wann immer diese erforderlich ist, darlegt.

Fazit

Wie bereits in Stellungnahme 2/2010 zu lesen war, stellt die Artikel-29-Datenschutzgruppe nicht die wirtschaftlichen Vorteile in Frage, die verhaltensorientierte Werbung mit sich bringen mag, doch sie ist fest davon überzeugt, dass solche Praktiken nicht auf Kosten der Rechte des Einzelnen auf Privatsphäre und Datenschutz gehen können. Der EU-Rechtsrahmen für Datenschutz sieht Schutzmechanismen vor, die eingehalten werden müssen.

Die Einhaltung des EASA/IAB-Kodex zu verhaltensorientierter Werbung im Internet bzw. die Teilnahme an der Website www.youronlinechoices.eu führt nicht zu einer Einhaltung der aktuellen Datenschutzrichtlinie für elektronische Kommunikation. Der Kodex und die Website führen vielmehr zu dem Trugschluss, man

[5] http://www.easa-alliance.org/binarydata.aspx?type=doc/EASA_BPR_OBA_12_APRIL_2011_CLEAN.pdf/download

[6] Schreiben der Artikel-29-Datenschutzgruppe an die Branche für verhaltensorientierte Werbung im Internet (Online Behavioural Advertising, OBA) bezüglich des Selbstregulierungsrahmens, 3. August 2011 http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2011/20110803_letter_to_oba_annexes.pdf

[7] Pressemitteilung der Artikel-29-Datenschutzgruppe vom 14. September 2011 http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20110914_press_release_oba_industry_final_en.pdf

könne sich beim Surfen im Internet gegen eine unfreiwillige Datenerfassung entscheiden. Dieser Trugschluss kann sowohl für Nutzer als auch für die Branche schädlich sein, falls Letztere der Ansicht ist, dass sie durch eine Einhaltung des Kodex die Anforderungen der Richtlinie erfüllt.

Die Werbebranche muss die exakten Anforderungen der Richtlinie für elektronische Kommunikation einhalten. Diese Stellungnahme zeigt, dass viele praktische Lösungen verfügbar sind, um dies zufriedenstellend zu gewährleisten und gleichzeitig ein zufriedenstellendes Nutzererlebnis sicherzustellen.

1.3. RFID

Stellungnahme 9/2011 (WP180) zu dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutz-Folgenabschätzungen für RFID-Anwendungen

Diese Stellungnahme knüpft an die Stellungnahme 5/2010 (WP 175) zum Vorschlag der Branche für einen Rahmen für Datenschutz-Folgenabschätzungen für RFID-Anwendungen an. Wenngleich in der Einleitung einige Hintergrundinformationen wiederholt werden, die zum Verständnis des Zwecks und des Umfangs dieser neuen Stellungnahme erforderlich sind, wird der Leser dennoch dazu aufgefordert, die Stellungnahme 5/2010 für weitere Einzelheiten zu lesen.

Am 12. Mai 2009 gab die Europäische Kommission eine Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen aus. In dieser Empfehlung werden die Mitgliedstaaten dazu aufgefordert, dafür zu sorgen, dass die Branche in Zusammenarbeit mit den jeweiligen Beteiligten einen Rahmen für Datenschutz-Folgenabschätzungen aufstellt, der der Artikel-29-Datenschutzgruppe zur Prüfung vorgelegt werden sollte. Sobald dieser Rahmen für die Datenschutz-Folgenabschätzungen vorliegt, sollen die Mitgliedstaaten dafür sorgen, dass RFID-Anwendungsbetreiber vor der Einführung von RFID-Anwendungen eine Datenschutz-Folgenabschätzung durchführen und die dabei erstellten Berichte der zuständigen Behörde zur Verfügung stellen.

Am 31. März 2010 legten Branchenvertreter der Artikel-29-Datenschutzgruppe einen Vorschlag für einen Rahmen für Datenschutz-Folgenabschätzungen zur Prüfung vor. Wenngleich dieser Vorschlag einen guten Ausgangspunkt darstellte, erhielt er nicht die volle Zustimmung der Datenschutzgruppe, insbesondere da in dem vorgeschlagenen Rahmen die folgenden drei wesentlichen Bestandteile fehlten:

1. Ein klar definiertes Risikobewertungskonzept.

2. Die Berücksichtigung der RFID-Tags, die von Personen außerhalb der Reichweite der Anwendung mitgeführt werden.

3. Eine Methode zur ausdrücklichen Berücksichtigung der Grundsätze zur Deaktivierung der Tags im Einzelhandel, die von der Europäischen Kommission in der Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen festgelegt sind.

Am 13. Juli 2010 fasste die Datenschutzgruppe diese Elemente sowie weitere Bedenken in der Stellungnahme 5/2010 zusammen und forderte die Branche auf, einen überarbeiteten Rahmen für Datenschutz-Folgenabschätzungen für RFID-Anwendungen vorzuschlagen. In Bezug auf die Risikobewertung hat die Datenschutzgruppe die Branche nachdrücklich dazu aufgefordert, an die bestehenden Erfahrungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) anzuknüpfen.

In demselben Monat hat die ENISA eine unabhängige Stellungnahme mit praktischen Empfehlungen zur Verbesserung des vorgeschlagenen Rahmens veröffentlicht. Der Vorschlag der ENISA umfasste insbesondere einige erste Richtlinien für die Einführung eines umfassenden und anerkannten methodischen Risikobewertungskonzepts sowie verschiedene strukturelle Verbesserungsvorschläge.

In den folgenden Monaten hat die Branche einen überarbeiteten Rahmen für Datenschutz-Folgenabschätzungen erarbeitet, wobei sie die Beiträge sowohl der Datenschutzgruppe als auch der ENISA berücksichtigte. Am 12. Januar 2011 wurde dieser überarbeitete Rahmen für Datenschutz-Folgenabschätzungen der Artikel-29-Datenschutzgruppe zur Prüfung vorgelegt.

In dieser Stellungnahme sind die Ansichten der Datenschutzgruppe zu diesem neuen Vorschlag formell zusammengefasst.

Nachfolgend bezieht sich die „RFID-Empfehlung" auf die am 12. Mai 2009 veröffentliche Empfehlung der Europäischen Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. Der „überarbeitete Rahmen" oder nur „Rahmen" bezieht sich auf den der Artikel-29-Datenschutzgruppe am 12. Januar 2011 übermittelten und im Anhang zu dieser Stellungnahme wiedergegebenen Rahmen für Datenschutz-Folgenabschätzungen für RFID-Anwendungen.

Fazit

Die Datenschutzgruppe befürwortet den überarbeiteten Rahmen, der am 12. Januar 2011 vorgelegt wurde. Dieser Rahmen tritt spätestens sechs Monate nach der Veröffentlichung dieser Stellungnahme in Kraft.

Eine Datenschutz-Folgenabschätzung ist ein Instrument, mit dem der „eingebaute Datenschutz" (Privacy by Design), eine bessere Unterrichtung des Einzelnen sowie Transparenz und der Dialog mit den zuständigen Behörden gefördert werden sollen. Da einige RFID-Anwendungen in mehreren Mitgliedstaaten umgesetzt werden, ist es wichtig, die Berichte zu Datenschutz-Folgenabschätzungen zu übersetzen und den zuständigen Behörden in der Sprache ihres Landes zur Verfügung zu stellen.

Die Datenschutzgruppe wird auch weiterhin den Dialog mit der Branche unterstützen, damit auf Grundlage der Erfahrungen und Rückmeldungen aller Beteiligten Verbesserungen und Klarstellungen in Bezug auf den Aufbau und die Umsetzung des Rahmens für Datenschutz-Folgenabschätzungen für RFID-Anwendungen durchgeführt werden können.

1.4. PERSONENBEZOGENE DATEN

Stellungnahme 14/2011 (WP186) zu Fragen des Datenschutzes im Zusammenhang mit der Verhinderung von Geldwäsche und Terrorismusfinanzierung

Die Artikel-29-Datenschutzgruppe hat 44 Empfehlungen zum Schutz von Privatsphäre und Daten im Zusammenhang mit der Verhinderung von Geldwäsche und Terrorismusfinanzierung (AML/CFT) abgegeben, die dieser Stellungnahme als Anhang beigefügt sind.

Die Artikel-29-Datenschutzgruppe wird die beigefügten Empfehlungen und die einschlägigen Entwicklungen im Gesetzesbereich und in der Praxis im Gesamtbereich der Verhinderung von Geldwäsche und Terrorismusfinanzierung sowie des Datenschutzes und des Schutzes der Privatsphäre weiter verfolgen.

Stellungnahme 15/2011 (WP187) zur Definition von Einwilligung

Die vorliegende Stellungnahme bietet eine gründliche Analyse des Konzepts der Einwilligung, wie es derzeit in der Datenschutzrichtlinie und in der Datenschutzrichtlinie für elektronische Kommunikation verwendet wird. Ausgehend von den Erfahrungen der Mitglieder der Artikel-29-Datenschutzgruppe werden in der Stellungnahme zahlreiche Beispiele für gültige und ungültige Einwilligungen gegeben, wobei der Schwerpunkt auf die Schlüsselelemente der Einwilligung wie die Bedeutung von „Willensbekundung", „ohne jeden Zwang", „für den konkreten Fall", „ohne jeden Zweifel", „ausdrücklich", „in Kenntnis der Sachlage" usw. gelegt wird. Die Stellungnahme stellt auch einige Aspekte in Bezug auf den Begriff „Einwilligung" klar, beispielsweise den Zeitpunkt, zu dem die Einwilligung vorliegen muss, die Unterschiede zwischen Widerspruchsrecht und Einwilligung usw.

Die Einwilligung ist eine von mehreren Rechtsgrundlagen für die Verarbeitung personenbezogener Daten. Sie spielt zwar eine wichtige Rolle, schließt aber je nach Kontext nicht aus, dass möglicherweise andere Rechtsgrundlagen sowohl aus der Sicht des für die Datenverarbeitung Verantwortlichen als auch aus der Sicht der betroffenen Person relevanter sind. Wenn die Einwilligung richtig genutzt wird, ermöglicht sie der betroffenen Person die Kontrolle über die Verarbeitung ihrer personenbezogenen Daten. Wird sie nicht richtig angewendet, wird eine Kontrolle durch die betroffene Person illusorisch, und die Einwilligung stellt dann keine angemessene Grundlage für die Verarbeitung mehr dar.

Die vorliegende Stellungnahme wird teilweise aufgrund einer Anfrage der Kommission im Zusammenhang mit der gerade stattfindenden Überprüfung der Datenschutzrichtlinie verfasst. Deshalb enthält sie Empfehlungen, die bei der Überprüfung erwogen werden sollten. Dazu zählen unter anderem:

i. Die Bedeutung von Einwilligung „ohne jeden Zweifel" sollte klargestellt werden und es sollte erklärt werden, dass nur eine Einwilligung, die auf Erklärungen oder Handlungen beruht, mit denen die Zustimmung zum Ausdruck gebracht wird, eine gültige Einwilligung darstellt.

ii. Die für die Datenverarbeitung Verantwortlichen sollten zur Einführung von Mechanismen verpflichtet werden, mit denen die Einwilligung dargelegt wird (im Rahmen einer allgemeinen Rechenschaftspflicht).

iii. Es sollte eine ausdrückliche Vorschrift bezüglich der Qualität und Zugänglichkeit der Informationen eingefügt werden, die die Grundlage für die Einwilligung bilden.

iv. Eine Reihe von Vorschlägen in Bezug auf Minderjährige und sonstige Personen ohne Rechts- und Geschäftsfähigkeit.

Gesamtbeurteilung

Die Datenschutzgruppe ist der Ansicht, dass der derzeitige Datenschutzrechtsrahmen eine Reihe gut durchdachter Regeln enthält, die die zu erfüllenden Voraussetzungen festlegen, damit eine Einwilligung gültig ist und die Datenverarbeitung legitimiert wird. Diese Regeln gelten sowohl in der Offline- als auch der Online-Umgebung. Genauer gesagt:

Dem Rechtsrahmen gelingt die Balance zwischen einer Reihe von Anliegen. Einerseits garantiert er, dass nur eine echte Einwilligung in Kenntnis der Sachlage als Einwilligung angesehen wird. Diesbezüglich ist Artikel 2 Absatz h, der ausdrücklich fordert, dass die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt, einschlägig und zufriedenstellend. Andererseits ist diese Anforderung keine Zwangsjacke, sondern ermöglicht eine ausreichende Flexibilität und vermeidet spezifische technologische

Bestimmungen. Das veranschaulicht der vorgenannte Artikel 2 Absatz h, der Einwilligung als Willensbekundung der betreffenden Person definiert. Das lässt für die Art der Willensbekundung ausreichend Gestaltungsspielraum. Artikel 7 und 8, die eine Einwilligung ohne jeden Zweifel beziehungsweise eine ausdrückliche Einwilligung fordern, erfassen gut die Notwendigkeit der Ausgeglichenheit zwischen den beiden Anliegen. Dadurch gewähren sie Flexibilität und vermeiden zu strikte Strukturen, während sie gleichzeitig Schutz garantieren.

Das Ergebnis ist ein Rechtsrahmen, der bei der richtigen Anwendung und Umsetzung dazu in der Lage ist, mit der häufig aus technologischen Entwicklungen resultierenden großen Bandbreite an Datenverarbeitungsvorgängen Schritt zu halten.

In der Praxis ist es jedoch aufgrund der fehlenden Einheitlichkeit zwischen den Mitgliedstaaten nicht immer einfach zu entscheiden, wann eine Einwilligung erforderlich ist und insbesondere, welche Anforderungen für eine gültige Einwilligung erfüllt sein müssen und wie sie konkret umzusetzen sind. Die Umsetzung auf nationaler Ebene hat zu unterschiedlichen Ansätzen geführt. Die nachfolgend beschriebenen, spezifischen Schwachstellen wurden in den Diskussionen mit der Artikel-29-Datenschutzgruppe herausgearbeitet und haben zu der vorliegenden Stellungnahme geführt.

Mögliche Änderungen

- Der Begriff der Einwilligung ohne jeden Zweifel ist hilfreich, um ein System einzurichten, das nicht zu starr ist, aber dennoch guten Schutz bietet. Während er das Potential hat, zu einem angemessenen System zu führen, wird seine Bedeutung leider häufig missverstanden oder einfach ignoriert. Obwohl die oben dargelegten Hinweise und Beispiele eigentlich zu einer Stärkung der Rechtssicherheit und des Schutzes der Rechte des Einzelnen beitragen sollten, wenn die Einwilligung als Rechtsgrundlage genutzt wird, verlangt die geschilderte Situation ein paar Änderungen;

- Genauer gesagt, ist die Artikel-29-Datenschutzgruppe der Ansicht, dass die Formulierung selbst („ohne jeden Zweifel“) von weiteren Klarstellungen als Teil einer Überprüfung des allgemeinen Datenschutzrechtsrahmens profitieren würde. Mit der Klarstellung sollte betont werden, dass eine Einwilligung ohne jeden Zweifel die Nutzung von Mechanismen erforderlich macht, die keinen Zweifel an der Zustimmungsabsicht der betroffenen Person lassen. Gleichzeitig sollte deutlich gemacht werden, dass die Verwendung von Standardeinstellungen, welche die betroffene Person selbst ändern muss, um die Verarbeitung zu verhindern (auf Schweigen basierende Einwilligung), nicht in sich eine Einwilligung ohne jeden Zweifel darstellt. Das gilt insbesondere in der Online-Umgebung;

- Zusätzlich zu der oben beschriebenen Klarstellung schlägt die Artikel-29-Datenschutzgruppe Folgendes vor:

    i. *Erstens:* In die Definition von Einwilligung in Artikel 2 Absatz h sollte der Wortlaut „ohne jeden Zweifel“ (oder etwas Gleichwertiges) eingefügt werden, um die Ansicht zu stärken, dass nur eine Einwilligung, die auf Erklärungen oder Handlungen basiert, mit denen eine Zustimmung zum Ausdruck gebracht wird, auch eine gültige Einwilligung darstellt. Zusätzlich zu mehr Klarheit würde dies das Konzept der Einwilligung im Sinne von Artikel 2 Buchstabe h an das Erfordernis einer gültigen Einwilligung im Sinne von Artikel 7 angleichen. Außerdem könnte die Bedeutung von „ohne jeden Zweifel“ in einem Erwägungsgrund des zukünftigen Rechtsrahmens näher erläutert werden.

    ii. *Zweitens:* Im Kontext einer allgemeinen Rechenschaftspflicht sollten die für die Datenverarbeitung Verantwortlichen nachweisen können, dass sie die Einwilligung eingeholt haben. Wenn die Beweislast verstärkt wird, so dass die für die Datenverarbeitung Verantwortlichen nachweisen müssen, dass sie die Einwilligung der betroffenen Person

tatsächlich erhalten haben, sind sie dazu gezwungen, Standardpraktiken und -mechanismen einzuführen, um eine Einwilligung ohne jeden Zweifel einzuholen und sie auch nachweisen zu können. Die Art der Mechanismen ist kontextabhängig und sollte die Fakten und Umstände und insbesondere die Risiken der Verarbeitung berücksichtigen.

- Die Artikel-29-Datenschutzgruppe ist nicht überzeugt davon, dass der Rechtsrahmen grundsätzlich für jede Art der Verarbeitung, einschließlich der derzeit durch Artikel 7 der Richtlinie abgedeckten Verarbeitungen, eine ausdrückliche Einwilligung fordern sollte. Zwar ist sie ist der Ansicht, dass eine Einwilligung ohne jeden Zweifel der geforderte Standard bleiben sollte. Dies umfasst jedoch sowohl eine ausdrückliche Einwilligung als auch eine Einwilligung aus *Handlungen*, die keinen Zweifel an ihrer Absicht lassen. Diese Wahl gibt den für die Datenverarbeitung Verantwortlichen mehr Flexibilität beim Einholen der Einwilligung. Die Gesamtprozedur könnte so schneller und nutzerfreundlicher sein;

- Verschiedene, auf die Einwilligung Anwendung findende Aspekte des Rechtsrahmens werden aus dem Wortlaut oder der geschichtlichen Entwicklung geschlossen oder wurden durch Fallrecht oder die Stellungnahmen der Artikel-29-Datenschutzgruppe entwickelt. Die Rechtssicherheit wäre größer, wenn solche Aspekte ausdrücklich in den neuen Datenschutzrechtsrahmen integriert würden. Hierbei könnten die folgenden Punkte berücksichtigt werden:

  i. Das Einfügen einer ausdrücklichen Klausel, die den betroffenen Personen das Recht gibt, ihre Einwilligung zu widerrufen.

  ii. Die Betonung des Konzepts, dass die Einwilligung vor dem Beginn der Verarbeitung erteilt werden muss sowie vor der weiteren Nutzung der Daten für in der ursprünglichen Einwilligung nicht abgedeckte Zwecke, wenn kein anderer Rechtsgrund als die Einwilligung vorliegt.

  iii. Das Einfügen ausdrücklicher Erfordernisse bezüglich der Qualität (Pflicht, Informationen zur Datenverarbeitung in verständlicher Form und in einer klaren und einfachen Sprache zu geben) und der Zugänglichkeit der Information (Pflicht, die Informationen auffällig, markant und direkt zugänglich zu platzieren). Dies ist von größter Bedeutung, um den betroffenen Personen eine Einwilligung in voller Kenntnis der Sachlage zu ermöglichen.

- Schließlich könnte in Bezug auf Personen, die nur eine eingeschränkte Rechts- und Geschäftsfähigkeit haben, ein verstärkter Schutz vorgesehen werden. Dies umfasst unter anderem:

  i. Klarstellung, unter welchen Umständen die Einwilligung von den Eltern oder Vertretern einer Person gegeben werden muss, die nur eingeschränkt rechts- und geschäftsfähig ist. Dazu gehört auch die Altersgrenze, bis zu der eine solche Einwilligung verpflichtend ist.

  ii. Festlegen der Pflicht, Mechanismen zur Überprüfung des Alters zu nutzen. Diese können - abhängig von den Umständen, wie dem Alter des Kindes, der Art der Verarbeitung, der Frage, ob diese besonders riskant ist und ob die Informationen bei dem für die Datenverarbeitung Verantwortlichen verbleiben oder Dritten zur Verfügung gestellt werden - variieren.

  iii. Pflicht, die Informationen kindgerecht zu gestalten. Denn Kinder könnten so einfacher verstehen, was eine Verarbeitung ihrer personenbezogenen Daten bedeutet und folglich einwilligen.

  iv. Besondere Schutzmechanismen zur Identifizierung von Datenverarbeitungen, bei denen eine Einwilligung keine mögliche Basis für die Legitimierung der Verarbeitung personenbezogener Daten sein dürfte. Ein Beispiel hierfür ist verhaltensorientierte Werbung.

Die Artikel-29-Datenschutzgruppe wird das Thema der Einwilligung wieder aufgreifen. Insbesondere entscheiden nationale Datenschutzbehörden sowie die Datenschutzgruppe möglicherweise zu einem

späteren Zeitpunkt, Leitlinien abzufassen, um diese Stellungnahme weiter zu entwickeln und dabei weitere praktische Beispiele für die Art der Einwilligung zu geben.

Arbeitsdokument 1/2011 (WP184) über EU-Vorschriften betreffend Verstöße gegen Datenschutzvorschriften mit Empfehlungen für zukünftige politische Entwicklungen

Das vorliegende Dokument der Artikel-29-Datenschutzgruppe enthält eine Bestandsaufnahme der Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation und der Art und Weise, wie die Mitgliedstaaten die Vorschriften dieser Richtlinie über Verstöße gegen den Datenschutz in nationales Recht umsetzen[8].

Mit dieser Bilanz soll ein dreifaches Ziel verfolgt werden:

Erstens möchte die Artikel-29-Datenschutzgruppe umfassende Kenntnis über den aktuellen Stand der Dinge erlangen. Dazu gehören sowohl grundlegende Aspekte wie der Stand der Umsetzung als auch komplexere, wie beispielsweise die Ermittlung der Unterschiede in der Vorgehensweise in verschiedenen Bereichen (z. B. der Anwendungsbereich der Vorschriften; nationale Leitlinien, in denen einige Aspekte der Richtlinie weiterentwickelt werden; die zuständige Behörde des Mitgliedstaaten usw.). Durch das Aufzeigen etwaiger abweichender Entwicklungen in den Mitgliedstaaten kann diesen geholfen werden, selbst in dieser späten Phase noch ihre Positionen anzugleichen und eine fragmentierte Umsetzung zu vermeiden.

Zweitens: Die Bestandsaufnahme soll den nationalen Datenschutzbehörden helfen, bestimmte Ergebnisse zur Kenntnis zu nehmen. Sie wurden darauf aufmerksam gemacht, dass Folgemaßnahmen erforderlich sind, die in dem vorliegenden Arbeitsdokument beschrieben werden. Ein Ergebnis der Bestandsaufnahme ist, dass die zuständigen Behörden weiter darauf hinwirken sollten, dass interne Regeln und Verfahren festgelegt werden, nach denen die zuständigen Behörden und betroffenen Einzelpersonen von den für die Datenverarbeitung Verantwortlichen benachrichtigt werden. Wenn man in Betracht zieht, dass die für die Verarbeitung der Daten Verantwortlichen in zunehmendem Maße grenzüberschreitende Verstöße gegen den Schutz personenbezogener Daten melden werden, wird darüber hinaus deutlich, dass die Behörden gemeinsam Methoden der Zusammenarbeit besprechen müssen.

Drittens: Die Bestandsaufnahme hat der Artikel-29-Datenschutzgruppe die Gelegenheit gegeben, das Thema weiter zu vertiefen und einige Schlussfolgerungen bezüglich zukünftiger Politikentwicklungen im Bereich der Meldung von Verstößen zu ziehen. Diese Schlussfolgerungen ergänzen die Stellungnahmen, die die Artikel-29-Datenschutzgruppe bei anderen Gelegenheiten[9]zu diesem Thema abgegeben hat. Sie knüpfen an die gemeldeten Verstöße gegen den Datenschutz an, die diejenigen nationalen Datenschutzbehörden, die die Anzeigepflicht für Datenschutzverstöße bereits anwenden, gesammelt haben. Nach Ansicht der Artikel-29-Datenschutzgruppe sollten diese Ergebnisse bei künftigen Politikentwicklungen in Bezug auf Verstöße berücksichtigt werden. Politikentwicklungen werden insbesondere in den folgenden beiden Kontexten erwartet:

a) Ergänzung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation, die Datenschutzverletzungen betreffen. In Artikel 4 Absatz 5 der Richtlinie wird der Kommission die

[8] Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung, unter anderem, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt L 337 vom 18.12.2009, S.11.

[9] Siehe Papier der Artikel-29-Datenschutzgruppe „Die Zukunft des Datenschutzes: Gemeinsamer Beitrag zu der Konsultation der Europäischen Kommission zu dem Rechtsrahmen für das Grundrecht auf den Schutz der personenbezogenen Daten", angenommen am 1.12.2009 (WP 168); Stellungnahme 1/2009 über die Vorschläge zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), angenommen am 10.02.2009 (WP 159); Stellungnahme 2/2008 zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), angenommen am 15.05.2008 (WP 150).

Befugnis zur Annahme technischer Durchführungsmaßnahmen (gemäß Artikel 290 AEUV nach der Annahme des Vertrags von Lissabon als „übertragene Befugnisse" bezeichnet) übertragen, um eine einheitliche Umsetzung und Anwendung der Bestimmungen in genau festgelegten Bereichen zu gewährleisten (d. h. Umstände, Form und Verfahren der in den Bestimmungen vorgeschriebenen Informationen und Anzeigen).

b) Erweiterung der Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation, die Datenschutzverletzungen betreffen, im Zusammenhang mit der Überprüfung der Richtlinie 95/46. Die Kommission hat sich gegenüber dem Europäischen Parlament dazu verpflichtet, unverzüglich angemessene Vorbereitungsarbeiten einzuleiten. Dazu gehört auch die Konsultation interessierter Kreise mit dem Ziel, diesbezügliche Vorschläge – sofern anwendbar – bis Ende 2011 vorzulegen[10]. Diese Verpflichtung wurde in der Mitteilung der Kommission „Gesamtkonzept für den Datenschutz in der Europäischen Union" bekräftigt[11].

Die oben genannten Punkte werden wie folgt behandelt: Nach einer Zusammenfassung der wichtigsten Vorschriften zur Verletzung des Schutzes personenbezogener Daten in der Datenschutzrichtlinie für elektronische Kommunikation (Abschnitt II) werden die einschlägigen Rechtsvorschriften der Mitgliedstaaten zusammengefasst (Abschnitt III). Die Zusammenfassung basiert auf den Informationen, die von den nationalen Datenschutzbehörden bereitgestellt wurden. Sie werden hier jedoch nicht wiedergegeben, da die Umsetzung ein fortschreitender Prozess ist. In Abschnitt IV werden Maßnahmen aufgezeigt, die von den zuständigen Behörden und von der Artikel-29-Datenschutzgruppe mit Blick auf die Festlegung interner Prozesse und Kooperationsverfahren durchzuführen sind. In den Abschnitten V und VI wird insofern der Schwerpunkt auf die neuen Politikentwicklungen gelegt, als darin der Gesamtanwendungsbereich und die Verfahren für die erwarteten Aktionspläne in Bezug auf die Verletzung des Schutzes personenbezogener Daten in Erinnerung gerufen und Politikempfehlungen gegeben werden.

Die hier zum Ausdruck gebrachten Ansichten ergehen unbeschadet allfälliger speziellerer Leitlinien, die – auch im Zusammenhang mit der Annahme der technischen Durchführungsmaßnahmen gemäß Artikel 4 Absatz 5 der Datenschutzrichtlinie für elektronische Kommunikation durch die Kommission – in Zukunft veröffentlicht werden.

[10] Siehe die Erklärung, die die Kommission 2009 zur Anzeigepflicht für Datenschutzverstöße vor dem Europäischen Parlament im Zusammenhang mit der Reform des Rechtsrahmens für die elektronische Kommunikation abgegeben hat. Abrufbar auf http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-ta-2009-

[11] KOM(2010) 609 endgültig vom 4.11.2010.

Kapitel Zwei

Die wichtigsten Entwicklungen in den Mitgliedstaaten

BELGIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Cyberüberwachung am Arbeitsplatz

Die Überwachung der Internet- und E-Mail-Nutzung am Arbeitsplatz ist für die belgische Datenschutzbehörde seit geraumer Zeit ein Problem. Es gehen regelmäßig Fragen, Beschwerden und Anträge auf Empfehlungen und zu befolgende Richtlinien ein, um eine Unternehmenspolitik festzulegen, die sowohl rechtmäßig als auch anwendbar ist.

Die belgische Datenschutzbehörde hat deshalb darauf reagiert und eine Stellungnahme zu diesen Fragen herausgegeben. Zunächst wurde 2011 ein ausführlicher Bericht zum Thema veröffentlicht – eine Art Grünbuch mit Informationen, die als Grundlage einer Reihe von veröffentlichten praktischen Empfehlungen verwendet wurden. Darauf folgte im Mai 2012 eine ausführliche öffentliche Anhörung. Der Bericht ist auf der Website der belgischen Datenschutzbehörde einsehbar: http://www.privacycommission.be/fr/brochure-information-cybersurveillance

In diesem Bericht erklärt die belgische Datenschutzbehörde, dass diese Überwachungen dahingehend eine Rechtsgrundlage haben, dass Arbeitnehmer im Namen ihrer Arbeitgeber, mit denen sie in einen Beschäftigungsvertrag haben (vertragliches Unterstellungsverhältnis), ihrer Tätigkeit nachgehen. Im Rahmen des Beschäftigungsverhältnisses kommuniziert der Mitarbeiter mithilfe des vom Arbeitgeber bereitgestellten IT-Systems elektronisch mit Dritten. Die Ergebnisse der mithilfe von IT-Hilfsmitteln (einschließlich Internet und E-Mail-System des Arbeitgebers) verrichteten Arbeit müssen dem Arbeitgeber selbstverständlich bereitgestellt werden. Der Arbeitgeber sollte diese Informationen von dem entsprechenden Mitarbeiter erhalten können oder in der Lage sein, danach zu suchen und sie zu finden, um insbesondere im Falle der Abwesenheit, des Todes oder des Ausscheidens des Mitarbeiters die Kontinuität der Dienstleistung und den korrekten Betrieb des Unternehmens zu gewährleisten.

Diese Prüfungen müssen dennoch unter Einhaltung des geltenden Rechts erfolgen, darunter das *Gesetz zum Datenschutz bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz) vom 8. Dezember 1992*. Trotz dieser Anforderungen muss der Arbeitgeber stets in der Lage sein, seine rechtmäßigen Interessen (die Verwaltung und Organisation seiner Aktivitäten) effektiv zu schützen.

Mehr Transparenz bei Marketingumfragen

Wie schon mehrfach in der Vergangenheit hat die Marketingabteilung der belgischen Post (Bpost) auch 2011 eine umfangreiche Befragung mit mehreren Millionen belgischen Bürgern durchgeführt. Bpost wollte damit zu Direktmarketingzwecken ein Kundenprofil erstellen. Die Daten werden an Drittunternehmen verkauft, die diese für den Versand gezielter Werbemaßnahmen verwenden. Die Umfrage der belgischen Post wurde von der Datenschutzgruppe als aggressiv und nicht ausreichend transparent, wenn nicht sogar irreführend, bezeichnet. Bpost hat zum Beispiel nicht eindeutig angegeben, dass eine Teilnahme an der rein zu Marketingzwecken durchgeführten Befragung nicht verpflichtend sei. Die Umfrage wurde außerdem in einem braunen Umschlag verschickt, der dem Umschlag für den Versand von Steuererklärungen sehr ähnlich war und genau im selben Zeitraum verschickt wurde. Nachdem die belgische Datenschutzbehörde von der breiten Öffentlichkeit, insbesondere von Senioren, die sich von der Art dieses Fragebogens bedrängt fühlten, darauf aufmerksam gemacht wurde, begann die Behörde, mit der belgischen Post Gespräche aufzunehmen. Daraufhin sorgte Bpost für transparentere Fragebögen und klarere Informationen in jedermanns rechtmäßigem Interesse.

Alles Weitere ist im Jahresbericht 2011 der belgischen Datenschutzbehörde einsehbar: http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2011.pdf

Organisation	
Vorsitz und/oder Gremium	Name des Vorsitzenden, ggf. Zusammensetzung des Gremiums. Vorsitzender: W. Debeuckelaere (Vorsitzender) Stellvertretender Vorsitzender: S. Verschuere Gremiumsmitglieder: M. Salmon (Beraterin des Berufungsgerichts), S. Mertens de Wilmars (Dozent), A. Vander Donckt (Notarin), F. Robben (Geschäftsführer der Banque Carrefour de la Sécurité Sociale sowie der E-Health-Plattform), P. Poma (Vorsitzender), A. Junion (Anwältin). Um eine Übersicht über die stellvertretenden Mitglieder zu erhalten, besuchen Sie bitte die Website der Datenschutzbehörde auf (http://www.privacycommission.be) und lesen den Jahresbericht 2011. Vgl. außerdem Artikel 24, Abschnitt 4, Absätze 3 und 4: *„Die Kommission ist so aufgebaut, dass zwischen den verschiedenen sozio-ökonomischen Gruppen ein Gleichgewicht herrscht. Neben dem Vorsitzenden gehören der Kommission seine eigentlichen Mitglieder und stellvertretenden Mitglieder, jedoch mindestens die folgenden Personen an: eine Anwältin, eine IT-Fachkraft, eine Person mit einschlägiger Berufserfahrung im Bereich der Verwaltung personenbezogener Daten im Privatsektor sowie eine Person mit einschlägiger Berufserfahrung im Bereich der Verwaltung personenbezogener Daten im öffentlichen Sektor."*
Budget	Zugewiesenes und ausgegebenes Budget Zugewiesenes Budget: 5 516 000 EUR (2011)/5 684 000 EUR (2012)
Personal	Anzahl der Mitarbeiter (ggf. nach Beschäftigungsbereich): 52 Mitarbeiter (1 Vorsitzender – 1 stellvertretender Vorsitzender) Bereichsleiter: 3 Personal und Organisation (20): Buchhaltung (1), Übersetzer (5), Verwaltung (8), Statistiker (1), Personalleiter (1), Logistik (2), IT-Unterstützung (1), Kommunikationsleiter (1) Studien und Forschung (18): Rechtsberater (16), IT-Fachkraft (1), Forschungsassistent (1) Außenbeziehungen (Frontoffice) (11): Rechtsberater (4), Assistenten (7)

Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Stellungnahmen und zentralen Themen. Hier sollten sämtliche von der Datenschutzbehörde erstellten Dokumente aufgeführt werden, die Auswirkungen auf den Datenschutz im Allgemeinen, auf betroffene Personen oder auf für die Datenverarbeitung Verantwortliche haben. Stellungnahmen (auf Anfrage der Legislative oder Exekutive - siehe unten): 29 Stellungnahmen und Initiativempfehlungen: 14 Empfehlungen zur Weiterverarbeitung: 10
Meldungen	Ggf. Anzahl der Meldungen gemäß der in der nationalen Gesetzgebung enthaltenen Definition. 2011 wurden 7 169 Meldungen über den elektronischen Zugangspunkt erfasst. Dies entspricht einem Anstieg von 92 % im Vergleich zum Vorjahr. 2011 wurden 6 490 neue Datenverarbeitungsaktivitäten gemeldet: - Reguläre Meldungen (19 %) - Meldung durch den Datenschutzbeauftragten (z. B. eine Meldung durch eine Dachorganisation) - Meldungen von Weiterverarbeitungsaktivitäten (1 %) - Meldungen einer Installation und Nutzung von Überwachungskameras (52 %) 372 Meldungen von Änderungen bestehender Verarbeitungsaktivitäten 124 Berichtigungen bestehender Verarbeitungsaktivitäten 306 Beendigungen bestehender Verarbeitungsaktivitäten Die Meldungen erfolgten hauptsächlich in diesen Bereichen: „Überwachung und Kontrolle“ (2 850), „Überwachung und Kontrolle von Personen, die an einem überwachten Arbeitsplatz tätig sind“ (520), „allgemeine Zwecke“ (542), „Gesundheitswesen“ (104) und „Sonstige“ (2 043).
Vorabprüfungen	Ggf. Anzahl der Vorabprüfungen gemäß der in der nationalen Gesetzgebung enthaltenen Definition. Selbst wenn die Genehmigungsaktivitäten der Sektorausschüsse nicht exakt Art. 20 der Richtlinie 95/46/EG entsprechen, haben die

	verschiedenen Sektorausschüsse der Datenschutzbehörde die folgende Anzahl von Genehmigungen erteilt: - Sektorausschuss der Bundesbehörde: 108 (Einzelgenehmigungen und allgemeine Genehmigungen) - Sektorausschuss für Statistik: 35 (Einzelgenehmigungen) - Sektorausschuss für das Nationalregister: 286 (Einzelgenehmigungen und allgemeine Genehmigungen) - Sektorausschuss für soziale Sicherheit und Gesundheitswesen: - Gesundheitswesen: 1 Stellungnahme, 34 Beratungen - Soziale Sicherheit: 23 Stellungnahmen, 87 Beratungen
Anfragen betroffener Personen	Ggf. Anzahl der schriftlich oder telefonisch von Betroffenen erhaltenen Anfragen Die Statistiken der belgischen Datenschutzbehörde unterscheiden nicht zwischen Auskunftsersuchen von betroffenen Personen oder von für die Datenverarbeitung Verantwortlichen: Durch die Zentrale erteilte Auskünfte: 2011 wurden 3 042 „Fragen und Antworten“ bearbeitet (Recht an der eigenen Abbildung, Grundsätze des Datenschutzes, Konjunktur/Konsumentenkredit, Datenschutz am Arbeitsplatz und Behörden. Die belgische Datenschutzbehörde bearbeitete außerdem 2 866 Auskunfts- oder Vermittlungsanfragen (einschließlich Überprüfungen): Darunter: 2 447 Auskunftsanfragen sowohl von öffentlichen Stellen und derzeitigen oder zukünftigen für die Verarbeitung Verantwortlichen und betroffenen Personen, 296 Vermittlungsanfragen und 123 Überprüfungen.
Beschwerden betroffener Personen	Anzahl der berechtigten Beschwerden (ggf. nach Art): Siehe oben: 296 Vermittlungsanfragen: Vor jeder Vermittlung oder Auskunft überprüft die belgische Datenschutzbehörde stets die Zulässigkeit. Bei 153 Fällen wurde die Vermittlungsanfrage als nicht zulässig befunden, oftmals aufgrund mangelnder Informationen vonseiten der betroffenen Person (148 Fälle). 215 Anfragen (9 %) wurden fälschlicherweise an die Datenschutzbehörde geschickt, die stets darum bemüht war, die Ersuchenden an die richtige Stelle weiterzuleiten. Bei knapp 75 % der Fälle war die Datenschutzbehörde erfolgreich. Bei 75 % der bearbeiteten Fragen wurden Informationen zum Thema Datenschutz bereitgestellt. Bei 3,85 % der Fälle erwies sich die Beschwerde als unbegründet. Bei 5,01 % der Fälle wurde jedoch

	ein Verstoß gegen das Datenschutzgesetzes festgestellt und eine Korrektur vorgenommen.
Vom Parlament bzw. der Regierung angeforderte Beratung	Sämtliche auf Anfrage des Parlaments oder der Regierung oder in deren Auftrag erstellte Dokumente: Eine Auflistung der 2011 von der belgischen Datenschutzbehörde abgegebenen Stellungnahmen ist auf der Website der Behörde unter http://www.privacycommission.be einsehbar
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Anzahl der [von Datenschutzbehörden als nennenswert eingestufte Kategorie] Alle nennenswerten Zahlen, die die Aktivitäten der Datenschutzbehörde widerspiegeln, wie z. B. die Anzahl der verbindlichen unternehmensinternen Vorschriften, die die leitende Datenschutzbehörde genehmigt hat. Siehe Jahresbericht der belgischen Datenschutzbehörde, der einen umfangreichen Abschnitt mit Statistiken enthält. Der Jahresbericht ist auf der Website der Datenschutzbehörde einsehbar: http://www.privacycommission.be
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Ggf. Anzahl der Prüfungen bzw. Untersuchungen (ggf. nach zentralen Themen) gemäß der nationalen Gesetzgebung. 123 Prüfungen (siehe unten). Die häufigsten Bereiche (Auskunft, Vermittlung/Beschwerden und Prüfungen) lauten: • Umgang mit Aufnahmen, insbesondere Videoaufnahmen • Grundsätzliches zum Thema Datenschutz • Datenverarbeitung durch öffentliche Stellen • Gewerbliche Praktiken (vornehmlich Marketing)
Sanktionsmaßnahmen	
Sanktionen	Anzahl der von der Datenschutzbehörde beschlossenen Sanktionen (falls im nationalen Recht vorgesehen) Anzahl der von der Datenschutzbehörde begonnenen Verfahren gegen für die Datenverarbeitung Verantwortliche (falls im nationalen Recht vorgesehen) Die Datenschutzbehörde hat keine Sanktionsbefugnis. Sie kann jedoch Fälle, bei denen Verstöße ermittelt wurden, an die Staatsanwaltschaft weiterleiten.

Geldbußen	Amounts (indication on whether imposed by courts or DPAs): Die Datenschutzbehörde hat keine Sanktionsbefugnis. Sie kann jedoch Fälle, bei denen Verstöße ermittelt wurden, an die Staatsanwaltschaft weiterleiten.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Abhängig von den verfügbaren Daten in Mitgliedstaaten sind verschiedene Zahlen zulässig. Falls nicht im nationalen Recht vorgesehen, ist das Feld mit „k. A." zu markieren. Die Datenschutzbehörde verfügt nicht über diese Angaben.

B. Informationen zur Rechtsprechung

Google wird infolge des WLAN-Zwischenfalls im Zusammenhang mit Google Street View von der Staatsanwaltschaft strafrechtlich verfolgt

Die belgische Datenschutzbehörde hat nicht die Befugnis, für die Datenverarbeitung Verantwortlichen, die gegen das Datenschutzgesetz verstoßen, Bußgelder aufzuerlegen. Dennoch ist sie dazu verpflichtet, derartige Verstöße der Staatsanwaltschaft mitzuteilen, wenn sie von ihnen erfährt. Bezüglich des WLAN-Zwischenfalls im Zusammenhang mit Google Street View bzw. der Erfassung personenbezogener WLAN-Daten (Netzwerkbezeichnung, URL, vollständige E-Mails und manchmal sogar Passwörter) über ungeschützte Netzwerke durch „Google-Autos", die dazu ausgestattet sind, Panoramaaufnahmen zu machen, um Google Street View damit zu bestücken, hat die belgische Datenschutzbehörde die Staatsanwaltschaft eingeschaltet. Google hat den Fehler eingesehen und ein von der Staatsanwaltschaft auferlegtes Bußgeld in Höhe von 150 000 EUR akzeptiert.

BULGARIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
Vorsitz und/oder Gremium	Kommission zum Schutz personenbezogener Daten (CPDP), bestehend aus einer Leiterin – Veneta Shopova, und vier Mitgliedern – Krassimir Dimitrov, Valentin Enev, Mariya Mateva und Veselin Tselkov.
Budget	Zugewiesenes Budget – 2 560 000 BGN (Bulgarischer Lew), ausgegebene Haushaltsmittel – 2 344 993 BGN.
Personal	Anzahl der Mitarbeiter: 76
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2011 wurden 203 Beschlüsse erlassen, darunter 50 Stellungnahmen und 30 verbindliche Anweisungen, die in erster Linie die Verwaltungsverfahren Dritter betrafen. Außerdem war der Zeitraum zwischen dem Erlass und dem Inkrafttreten für den Verantwortlichen zu kurz, um in Bezug auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten die Empfehlungen der CPDP zu berücksichtigen und seine Arbeitsweise zu ändern und zu verbessern. Gegen Teile der Rechtsakte wurde vor Gericht Einspruch erhoben. Die Anhörungen werden derzeit fortgesetzt, wodurch sich deren Inkrafttreten verzögert.
Meldungen	42 911 für die Datenverarbeitung Verantwortliche
Vorabprüfungen	1 151
Anfragen betroffener Personen	Insgesamt 458 Anfragen, Beschwerden und Meldungen, davon 102 Anfragen und 15 Beschwerden. Unter den erhaltenen Anfragen stammten die meisten Anschuldigungen von Verletzungen des Datenschutzrechts aus den Bereichen Telekommunikation (15), Internet (12), staatliche Verwaltung (11) sowie Handel und Dienstleistungen (10). Deutlich geringer fallen die Anfragen aus den Bereichen Finanzen (5), Medien (2), Gesundheitswesen (2) und politische Parteien (2) aus.
Beschwerden betroffener Personen	341 – aus den Bereichen Telekommunikation und Informationsgesellschaft – 199; Medien – 8; Gesundheitswesen – 5; Bankwesen – 27; Versicherungsdienstleistungen – 11.
Vom Parlament bzw. der	Drei Stellungnahmen zur Wahl des Präsidenten und des Vizepräsidenten der Republik Bulgarien sowie von Stadträten und

Regierung angeforderte Beratung	Bürgermeistern im Jahr 2011; zwei Stellungnahmen zu Anträgen auf Zugang zu personenbezogenen Daten im NSIS sowie zur Beibehaltung des öffentlichen Spendenregisters durch das Innenministerium und die Möglichkeit, die personenbezogenen Daten von Spendern, die Privatpersonen sind, zu veröffentlichen; drei Stellungnahmen zu Anfragen vom Ministerium für auswärtige Angelegenheiten bezüglich der Rechtmäßigkeit einer Verarbeitung personenbezogener Daten und deren Übermittlung an ausländische Behörden sowie zur Erleichterung des Verfahrens für die Bereitstellung von Verwaltungsdiensten an bulgarische Bürger, die im Ausland bulgarische Dokumente erhalten.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Bezüglich der Übermittlung personenbezogener Daten sieht das Datenschutzgesetz ein Genehmigungsverfahren vor. Im Berichtszeitraum wurden 21 Anträge auf Genehmigung einer Übermittlung personenbezogener Daten an Drittländer bearbeitet. Im Hinblick auf verbindliche unternehmensinterne Vorschriften genehmigt die CPDP die federführende Behörde und koordiniert die Erstellung von Dokumenten zur Genehmigung unternehmensinterner Vorschriften gemäß des Verfahrens zur gegenseitigen Anerkennung. 2011 wurden neun Genehmigungsanträge eingereicht.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2011 wurden insgesamt 1 252 Prüfungen durchgeführt, darunter: *ex-ante* – 1 151; laufend – 74 und *ex-post* – 27, hauptsächlich in den Bereichen Gesundheitswesen – 612; Handel und Dienstleistungen – 153; Tourismus – 57; Rechts- und Beratungsdienstleistungen – 53; Transportwesen – 47; staatliche Verwaltung – 46 sowie soziale Angelegenheiten – 40.
Sanktionsmaßnahmen	
Sanktionen	Die CPDP hat 2011 45 Feststellungen von Verwaltungsdelikten vorgelegt und 27 Bußgeldbescheide erlassen.
Geldbußen	Die CPDP hat 2011 Bußgeldbescheide im Wert von 75 100 BGN erlassen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

1. Bezüglich der erlassenen verbindlichen Anweisungen und Bußgeldbescheide:

2011 wurden verbindliche Anweisungen in den folgenden Bereichen erlassen: Finanzwesen, staatliche Verwaltung, kommunale Dienste, Transportwesen, Medien, Handel und Dienstleistungen sowie Telekommunikation. Die Anweisungen betrafen in erster Linie Folgendes:

- Die nötigen organisatorischen und technischen Maßnahmen, um zu garantieren, dass das Schutzniveau nicht abnimmt – 36 %;
- Die Verarbeitung personenbezogener Daten zu Fremdzwecken, ohne die CPDP über diese Änderungen zu informieren – 21 %;
- Das Verbot der Verarbeitung bestimmter Kategorien personenbezogener Daten – 18 %;
- Keine festgelegte Aufbewahrungsfrist für personenbezogene Daten – 16 %;
- Verstoß gegen die Vorkehrungen zur Inkenntnissetzung von Einzelpersonen – 9 %.

Zu den häufigsten Verstößen gegen das Datenschutzgesetz, für die Stellungnahmen aufgrund von Ordnungswidrigkeiten abgegeben wurden, gehörten:

- Verstöße gegen die Registrierung von Verantwortlichen für die Verarbeitung personenbezogener Daten – wegen der Aktualisierung der Daten vor einer Änderung der eingereichten Daten; Verarbeitung von Daten vor dem Einpflegen der Register in das System der CPDP;
- Verstoß gegen die Vorschriften zu Maßnahmen zum Schutz personenbezogener Daten – die notwendigen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten wurden von den Verantwortlichen nicht umgesetzt (Artikel 23 Absatz 4 in Verbindung mit Absatz 1 des bulgarischen Datenschutzgesetzes);
- Verstoß gegen die Grundsätze einer rechtmäßigen Verarbeitung personenbezogener Daten – Daten, die rechtmäßig und auf gutgläubige Weise verarbeitet werden und dem Verarbeitungszweck entsprechen und nicht übersteigen (Artikel 2 Absatz 2 Ziffer 1 und 3 des bulgarischen Datenschutzgesetzes).

2. Im Hinblick auf Stellungnahmen, Meldungen und Anfragen:

Abgesehen von den in der Tabelle genannten Fälle, die von staatlichen Behörden eingegangen sind, sind die folgenden Stellungnahmen von großem Interesse:

2.1. Recht auf Zugriff auf Videoaufzeichnungen von Videoüberwachungsgeräten (in Krankenhäusern), einschließlich Informationen über Dritte sowie darüber, ob es sich bei Videoüberwachung um die Erfassung personenbezogener Daten handelt – die CPDP ließ in einer Stellungnahme verlauten, dass Videoaufzeichnungen zu Überwachungszwecken personenbezogene Daten darstellen, da sie Informationen über die körperliche Identität der aufgezeichneten Personen enthalten. In dieser Hinsicht hat jede natürliche Person das Recht, auf ihre personenbezogenen Daten zuzugreifen (einschließlich solcher, die durch Videoüberwachungsgeräte aufgezeichnet worden sind). Die von Videoüberwachungskameras aufgezeichneten personenbezogenen Daten bestimmter Einzelpersonen können bereitgestellt werden, wenn es technisch möglich ist, die personenbezogenen Daten Dritter zu löschen, die ansonsten im Falle einer Ausübung dieses Zugangsrechts offengelegt werden könnten. Falls es technisch nicht machbar ist, die Daten von Dritten vorübergehend zu löschen, läge die einzige Rechtsgrundlage für die Ausübung des Zugangsrechts in der ausdrücklichen Einwilligung aller weiteren Einzelpersonen, die von der jeweiligen Videoüberwachung betroffen sind.

2.2. Die Notwendigkeit einer Registrierung der für die Datenverarbeitung Verantwortlichen, die weder auf dem Gebiet der Republik Bulgarien noch auf dem Gebiet der anderen Mitgliedstaaten der Europäischen Union ansässig sind:

– Antrag auf eine Stellungnahme im Hinblick auf die Frage, ob Google/Google Inc. auf dem Gebiet der Republik Bulgarien Objekte für seinen Dienst Google Street View aufzeichnen darf. Die CPDP hat eine Stellungnahme bezüglich der Verarbeitung personenbezogener Daten für den Dienst Google Street View abgegeben. Der für die Verarbeitung Verantwortliche Google/Google Inc. muss einen rechtlichen Vertreter in Bulgarien ernennen.In der Stellungnahme gab die CPDP außerdem verbindliche Anweisungen, die vor, während und nach dem Aufzeichnungsprozess eingehalten werden müssen: bei der Aufzeichnung von Straßenansichten dürfen Kameras keine WLAN-Daten erfassen (Daten zu WLAN-Zugangspunkten); es müssen Maßnahmen ergriffen werden, die das Aufzeichnen von Nutzdaten und anderen direkt mit Einzelpersonen in Verbindung stehenden Daten (E-Mail-Adressen, Passwörter usw.) verhindern; die Öffentlichkeit muss über die Rechte des Einzelnen in Verbindung mit der Verarbeitung von personenbezogenen Daten für Google Street View informiert werden; es müssen weitere einschränkende Maßnahmen ergriffen werden, wie z. B. Technologie, die Bilder von Individuen an Orten, die mit der Verarbeitung spezieller Datenkategorien in Verbindung stehen oder stehen könnten, unscharf machen usw.

3. Weitere interessante Fälle bezüglich der Anträge auf Datenübermittlungen:

3.1. Antrag auf Genehmigung der Übermittlung gescannter biometrischer Daten an ein Unternehmen und eine weitere gemeinnützige Rechtsperson in den USA in Verbindung mit Computerprüfungen, die in Bulgarien für die Aufnahme von Studierenden in Wirtschaftshochschulen auf der ganzen Welt durchgeführt werden. Zu den Hauptgründen für das Scannen der Handabdrücke der Prüflinge gehören die Vermeidung von Betrug und die Aufrechterhaltung des Vertrauens in die Handelsschulen, zu denen der Zugang im Falle eines Bestehens der Prüfung gewährt würde. Die CPDP gab eine Stellungnahme heraus, die den für die Datenverarbeitung Verantwortlichen/regionalen Vertretern die Übermittlung gescannter Handabdrücke (biometrische Daten von Einzelpersonen) in die USA gewährt. Die Rechtsgrundlage für die Genehmigung der Datenübermittlung war in diesem Fall die ausdrückliche Einwilligung der Prüflinge, deren biometrische Daten der Gegenstand der Übermittlung war.

3.2. Antrag auf Genehmigung der Übermittlung von Bild- und Videoaufzeichnungen der Mitarbeiter und Besucher des für die Datenverarbeitung Verantwortlichen an die Muttergesellschaft in den USA. Während des Verwaltungsverfahrens stellte die CPDP die folgenden Schwachstellen fest: es gab keine Anzeichen der Zulässigkeit der Verarbeitung, die Notwendigkeit der Übermittlung von Besucherdaten war nicht gegeben, die Datenmenge war übermäßig hoch und die Verarbeitung war nicht mit dem spezifischen Zweck des Antrags – Personalverwaltung – kompatibel. Die CPDP lehnte diesen Antrag auf Genehmigung einer Datenübermittlung ab.

C. Sonstige wichtige Informationen

1. Bezüglich der Maßnahmen der CPDP zur Umsetzung der Richtlinie 2006/24/EG in bulgarisches Recht

Richtlinie 2006/24/EG (Richtlinie über die Vorratsdatenspeicherung) wurde 2010 mit Änderungen und Zusätzen in das bulgarische Gesetz für elektronische Kommunikation integriert. Nachdem diese Änderungen in Kraft getreten waren, wurden alle Parteien, die mit der Vorratsspeicherung von und dem Zugang zu Verkehrsdaten zu tun haben, rechtlich bestimmt und die CPDP zur Aufsichtsbehörde für Datensicherheit ernannt. Gemäß dem Gesetz für elektronische Kommunikation fasste die CPDP 2011

erstmals statistische Daten zusammen und stellte diese im Einklang mit dem Gesetz fristgerecht der Europäischen Kommission und der Nationalversammlung bereit.

In dieser Hinsicht wurden zwischen September und Dezember 2011 vier separate Treffen zwischen der CPDP und Interessengruppen organsiert, und zwar zu den folgenden Themen: zuständige Behörden nach dem Gesetz für elektronische Kommunikation, Anbieter elektronischer Kommunikationsnetzwerke bzw. -dienstleistungen, strafrechtliche Verfolgung und Gerichte.

Die CPDP schlug Diskussionen und Klarstellungen zu den folgenden Problemen vor: der Nutzen von Daten zur Erkennung und Verfolgung von Straftaten durch die Suche nach Personen sowie Daten zu Freisprüchen und Schuldsprüchen; der Umfang für das Einreichen von Daten über bestimmte, häufig auftretende Verbrechen oder Vergehen, zu Analysezwecken und deren Zusammenfassung, für die größtenteils der Zugang zu Verkehrsdaten erforderlich ist; der Umfang für die Zusammenfassung von Daten über die Rechtsgrundlagen und Zwecke, für die der Zugang in der Regel erforderlich ist; die Überwachung der Verpflichtung zu Registern für Zugangsanträge, Ablehnungen, gerichtliche Genehmigungen und Anfragen; der Umfang für Anträge mit langen (sechsmonatigen) Datenspeicherungen gemäß Artikel 250 (a) Absatz 5 des Datenschutzgesetzes; Fälle, bei denen Unternehmen das Einreichen von Daten verweigern; der Datenspeicherungszeitraum; Klarstellung der Frist, die Unternehmen gewährt wird, um der CPDP statistische Daten zu melden; Klärung der Frist, die Unternehmen gewährt wird, um der CPDP genauere Informationen zukommen zu lassen; Klarstellung der Verfahren für den Zugang zu Verkehrsdaten gemäß der Strafprozessordnung zu Zwecken vorgerichtlicher und gerichtlicher Verfahren.

2. Aktivitäten der CPDP im Zusammenhang mit der Schulung der für die Datenverarbeitung Verantwortlichen zur Einhaltung des Datenschutzgesetzes und zu spezifischen Fragen

2011 führte die CPDP ein Schulungskonzept ein und organisierte eine große Schulungskampagne. Bei der Vorbereitung und Organisation der Schulungskampagne wurden nationale Ziele und Prioritäten berücksichtigt. Dies führte zu einer Reihe von Schulungen zur Verbesserung der Professionalität von für die Verarbeitung personenbezogener Daten Verantwortlichen, die Zugang zum Schengen-Informationssystem (SIS) haben. Dies erfolgte im Hinblick auf den geplanten Beitritt der Republik Bulgarien zum Schengen-Raum. Neben den SIS-Schulungen wurden wie bereits im Jahr 2010 für Vertreter von Kommunalbehörden und die Verwaltung der Nationalversammlung der Republik Bulgarien Seminare abgehalten. Die CPDP nahm außerdem an Schulungen des Diplomatischen Instituts und der Universität der Bibliotheks- und Informationstechnologien teil.

2011 nahmen Verantwortliche für die Datenverarbeitung aus dem öffentlichen Sektor, dem privaten Sektor und der Wissenschaft an den Schulungen der CPDP teil. Es fanden 22 Seminare statt, darunter 12 für Mitarbeiter von Institutionen mit Zugang zum NSIS, drei Seminare für Kommunalbehörden und den Landesgemeindeverband der Republik Bulgarien, zwei Schulungen für Mitarbeiter der Nationalversammlung, eine für das Diplomatische Institut, eine für die Wissenschaft, zwei für Vertreter von Handelsunternehmen (NPP Kozloduy und EVN) und eine für Vertreter von Branchenverbänden (Verband der bulgarischen Pharmaindustrie). Insgesamt 106 Institutionen haben ihre Vertreter zur Teilnahme an Schulungen geschickt, darunter 47 öffentliche Institutionen, 55 Gerichte, zwei private Unternehmen und ein Branchenverband. Die Gesamtzahl der geschulten Personen besteht aus 481 für die Datenverarbeitung Verantwortlichen, von denen 333 an der Schulung von Verantwortlichen mit Zugang zum NSIS teilnahmen.

DÄNEMARK

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
Vorsitz und/oder Gremium	Für das Tagesgeschäft der Datenschutzbehörde 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	Rund 35
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	k. A. (in den folgenden Zahlen enthalten)
Meldungen	2 602
Vorabprüfungen	2 602
Anträge von Bürgern	1 965 (diese Zahl umfasst alle bei der dänischen Datenschutzbehörde eingegangenen Anträge und Beschwerden)
Beschwerden von Bürgern	Siehe oben
Vom Parlament bzw. der Regierung angeforderte Beratung	339
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	51 Fälle im Zusammenhang mit Sicherheitsfragen
Prüfmaßnahmen	
Prüfungen	54
Sanktionsmaßnahmen	
Sanktionen	Die dänische Datenschutzbehörde kritisiert jedes Jahr eine Reihe von Verantwortlichen für die Nichteinhaltung des Gesetzes über die Verarbeitung personenbezogener Daten.
Geldbußen	Verhängung von Geldbußen in 2 Fällen
Datenschutzbeauftragte (DPO)	

Zahlenangaben zu DPO	k. A. (im dänischen Recht nicht vorgesehen)

B. Informationen zur Rechtsprechung

Die Nutzung von Fingerabdrücken zur Registrierung der Teilnahme an einem verpflichtenden Kurs für den Erhalt von Sozialleistungen

Eine dänische Gewerkschaft wollte im Namen eines Mitglieds eine Beschwerde einreichen. Die Gemeinde vor Ort hatte ein Verfahren eingeführt, bei dem Arbeitslose an einem Kurs teilnehmen und zur Bestätigung ihrer Anwesenheit ihren Fingerabdruck registrieren mussten.

Die Gemeinde erklärte, dass der Zweck der Verarbeitung dieser Daten der Anwesenheitskontrolle diene, da die Arbeitslosen der Gemeinde an diesem Kurs teilnehmen mussten, um Sozialleistungen zu empfangen.

Ferner erklärte die Gemeinde, dass nur eine Nummer (Schablone) des Fingerabdrucks erfasst und vom System verarbeitet werde.

Zu guter Letzt erklärte die Gemeinde, dass es für sie nötig sei, Fingerabdrücke zu verwenden, um die Anwesenheit effizient zu kontrollieren und einen Missbrauch zu vermeiden. Außerdem habe die Gemeinde die Nutzung biometrischer Daten als mit dem dänischen Gesetz zur Verarbeitung personenbezogener Daten vereinbar befunden.

Die dänische Datenschutzbehörde stellte fest, dass die Verarbeitung der Fingerabdruckdaten aufgrund der Verpflichtungen der Gemeinde zur Umsetzung der Tätigkeit einer offiziellen Behörde nötig sei und die Behörde nichts gegen die Nutzung der Fingerabdrücke zur Registrierung der Teilnehmer ohne die Zustimmung der betroffenen Personen gemäß Abschnitt 6 Unterabschnitt 6 des dänischen Datenschutzgesetzes einzuwenden hatte.

Beratung für trauernde Kinder und Jugendliche

2011 erteilte die dänische Datenschutzbehörde einem Beratungszentrum für trauernde Kinder und Jugendliche eine Genehmigung.

Das Beratungszentrum kümmert sich hauptsächlich um Kinder und Jugendliche, die in ihrem unmittelbaren familiären Umfeld Erfahrungen mit Tod oder schweren Erkrankungen gemacht haben.

Das Beratungszentrum verarbeitete personenbezogene Daten sowohl der Kinder als auch der Jugendlichen, jedoch auch die der Angehörigen der Kinder/Jugendlichen. Die Daten der Kinder, die Beratungsdienste in Anspruch nehmen, wurden mit einer Einwilligung als Rechtsgrundlage verarbeitet. Bezüglich der Daten der Angehörigen, egal ob tot oder lebendig, war es nicht möglich, eine Einwilligung als Rechtsgrundlage heranzuziehen.

Die dänische Datenschutzbehörde kam zu dem Schluss, dass die Verarbeitung der personenbezogenen Daten der Angehörigen erlaubt werden sollte, und bezog sich erstmals auf Abschnitt 7 Absatz 7 des dänischen Datenschutzgesetzes, das Artikel 8 Absatz 4 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zugrunde liegt.

Die dänische Datenschutzbehörde war der Ansicht, dass der Zweck in diesem Fall gemäß Artikel 4 Abschnitt 4 der Richtlinie auf einem wichtigen öffentlichen Interesse beruht.

C. Sonstige wichtige Informationen

Internationaler Tag des Datenschutzes

Die dänische Datenschutzbehörde verbrachte den Internationalen Tag des Datenschutzes im nahegelegenen Einkaufszentrum und versuchte, die breite Öffentlichkeit zum Thema Datenschutz aufzuklären und zu informieren. Die Mitarbeiter beantworteten Fragen, verteilten Flugblätter mit einschlägigen Informationen an die Einkäufer und veranstalteten ein Online-Quiz zum Thema Datenschutz. Der Tag war ein großer Erfolg sowohl für die Mitarbeiter als auch für die Einkäufer, die viel über Datenschutz wussten und ein großes Interesse an dem Thema hatten.

Verbindliche unternehmensinterne Vorschriften in Dänemark

Die dänische Datenschutzbehörde schloss 2011 die ersten verbindlichen unternehmensinternen Vorschriften ab, die beim dänischen Unternehmen Novo Nordisk A/S zum Einsatz kommen. Die Arbeit an den Vorschriften für Novo begann 2007. Die dänische Datenschutzbehörde wird nach und nach von anderen dänischen Unternehmen kontaktiert, die ebenfalls verbindliche unternehmensinterne Vorschriften benötigen.

DEUTSCHLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

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 Bayern eine separate Aufsichtsbehörde für den privaten Sektor.

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

Organisation	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit
Vorsitz und/oder Gremium	Peter Schaar
Budget	EUR 8 765 000
Personal	85 insgesamt Hauptsitz: 4 Abteilung I: 4 Abteilung II: 13 Abteilung III: 8 Abteilung IV: 7 Abteilung V: 6 Abteilung VI: 9 Abteilung VII: 7 Abteilung VIII: 9 Abteilung IX: 4 Zentrale Dienste: 12 Pressebüro: 2
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	N/A

Meldungen	N/A
Vorabprüfungen	N/A
Anfragen betroffener Personen	9 143
Beschwerden betroffener Personen	5 161
Vom Parlament bzw. der Regierung angeforderte Beratung	N/A
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	N/A
Prüfmaßnahmen	
Prüfungen, Untersuchungen	N/A
Sanktionsmaßnahmen	
Sanktionen	N/A
Geldbußen	N/A
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	N/A

1. Beschäftigtendatenschutz

In Deutschland ist immer noch der Entwurf eines Beschäftigtendatenschutzgesetzes (Ergänzung des Bundesdatenschutzgesetzes) in der Beratung des Deutschen Bundestages. Angesichts des Artikels 82 des Entwurfs einer EU-Datenschutz-Grundverordnung ist aber zurzeit fraglich, ob das Gesetzesvorhaben noch verabschiedet wird.

2. Umsetzung der Richtlinie 2005/60/EG – Gesetz zur Optimierung der Geldwäscheprävention

Durch das Gesetz zur Geldwäscheprävention vom 22.12.2011 (BGBl. I 2011, 2959) fand eine umfangreiche Novelle des Geldwäschegesetzes (GwG) statt. Im Wesentlichen sind die Sorgfalts- und Meldepflichten, die Verpflichtetenkreise sowie die internen Sicherungsmaßnahmen verschärft und ausgeweitet worden. Die Novelle hat zu einer Absenkung der Eingriffsschwellen für allgemeine Sorgfaltspflichten geführt.

Die Ausweitung der Sorgfaltspflichten führt gleichermaßen zu einer Ausweitung der Datenspeicherungs- bzw. Datenerhebungspflichten der nach dem GwG Verpflichteten und damit auch zu einem höheren Verwaltungsaufwand. Durch die erheblichen Bußgeldandrohungen bei Verletzungen von Sorgfaltspflichten dürfte der Druck zudem erhöht werden, überobligatorisch Daten von Vertragspartnern zu sammeln und diese ggf. an das Bundeskriminalamt und die Strafverfolgungsbehörden weiterzuleiten, um drohenden Bußgeldern zu entgehen. Die Grundsätze der Datensparsamkeit und der Datenvermeidung werden damit

weitgehend ausgehebelt, da das Zusammenspiel von erweiterten Sorgfaltspflichten und Sanktionsmechanismus das Gegenteil bewirken dürfte. Auch die sukzessive Erweiterung des Verpflichtetenkreises auf immer mehr Wirtschaftszweige kann die Gefahr einer umfassenden Datenerhebung im Zahlungsverkehr mit sich bringen. Ferner sind die Schwellen für Verdachtsanzeigen merklich heruntergesetzt worden. Insgesamt bewirken die Verschärfungen der Sorgfaltspflichten und die Absenkung der Verdachtsstufen einen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung aus Article 2 Abs. 1 i.V.m. Article 1 Abs. 1 des Grundgesetzes (GG), da finanzielle Transaktionen zunehmend einer erzwungenen und flächendeckenden Transparenz unterworfen werden. Es besteht mithin die Gefahr, dass die gesetzlich intendierte umfangreiche Sammlung personenbezogener Daten – von Verdachtsstufen losgelöst – zu einer übermäßigen Überwachung des Geldverkehrs führt, da die Verpflichteten proaktiv überobligatorisch Daten sammeln und diese den Ermittlungsbehörden zuleiten.

B. Informationen zur Rechtsprechung

1. Das Bundesverfassungsgericht hat mit Beschluss vom 12. Oktober 2011, 2 BvR 236/08 zur Neuregelung strafprozessualer verdeckter Ermittlungsmaßnahmen entschieden. Diese enthält eine Differenzierung beim Schutz der Kommunikation mit Berufsgeheimnisträgern. Beispielsweise sind danach Gespräche mit Pressevertretern und Ärzten grundsätzlich schwächer geschützt als etwa Gespräche mit Seelsorgern. Die Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung bei der Telekommunikationsüberwachung hat das Gericht ebenfalls gebilligt. Die Neuregelungen waren zuvor auf erhebliche Kritik gestoßen.

2. Das Bundesverfassungsgericht hat in einem Beschluss vom 24. Januar 2012 klargestellt, dass bei einem Auskunftsersuchen zu Telekommunikationsdaten immer eine Ermächtigung zur Datenübermittlung und eine Anspruchsgrundlage für die Datenabfrage vorliegen müssen (Doppeltürenmodell). Aus diesem Grund wurde die Speicherung und Weitergabe von Telekommunikationsdaten an Ermittlungsbehörden als verfassungswidrig untersagt, weil diesen Behörden bislang der Zugriff auf Passwörter und PIN-Codes ermöglicht worden ist. Die Ermittlungsbehörden konnten dadurch bislang ein beschlagnahmtes Handy auslesen und gespeicherte Daten durchsuchen, ohne dass sichergestellt war, ob eine Nutzung durch die Behörden überhaupt erlaubt ist.

Darüber hinaus hat das Bundesverfassungsgericht klargestellt, dass ein Auskunftsersuchen zu den Anschlussinhabern hinter einer dynamischen IP-Adresse einen Eingriff in das Telekommunikationsgeheimnis begründet. Um eine dynamische IP-Adresse zu identifizieren, müssen die Telekommunikationsunternehmen die entsprechenden Verbindungsdaten ihrer Kunden sichten und somit auf konkrete Telekommunikationsvorgänge zugreifen, die dem Schutz des Artikels 10 Grundgesetz unterliegen. Der deutsche Gesetzgeber muss hierfür eine eindeutige Regelung schaffen, die den Schutz der äußerst sensiblen Telekommunikationsverkehrsdaten gewährleistet.

C. Sonstige wichtige Informationen

Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung (E-Governmentgesetz)

Derzeit wird der Entwurf eines Gesetzes zur Förderung der elektronischen Verwaltung, das sog. E-Governmentgesetz, beraten. Ziel des Gesetzes ist es, durch den Abbau rechtlicher Hindernisse die elektronische Kommunikation insbesondere zwischen dem Bürger und der Verwaltung zu erleichtern. Dies soll im Wesentlichen dadurch erreicht werden, dass sichere technische Verfahren zur Ersetzung der Schriftform zugelassen werden, u. a durch die Einbindung der Onlineausweisfunktion des Personalausweises sowie durch Bereitstellen sicherer und vertraulicher Kommunikationsmöglichkeiten im Internet. Weitere Kernpunkte des Gesetzentwurfs sind:

- Die Verpflichtung der Verwaltung zur Eröffnung eines elektronischen Zugangs;
- Eine einfache elektronischen Beibringung von Nachweisen in Verwaltungsverfahren;
- Einführung der elektronischen Akte in den Bundesbehörden sowie
- Bereitstellung von maschinenlesbaren Datenbeständen durch die Verwaltung („Open Government Data").

Bei den Beratungen des Gesetzentwurfes geht es auch darum, sicherzustellen, dass der Abbau von Hindernissen für die vollständige Abbildung medienbruchfreier elektronischer Verwaltungsprozesse nicht zu einem Abbau des in der öffentlichen Verwaltung erreichten Datenschutzniveaus führt. Im Vordergrund müssen deshalb eine datenschutzfreundliche Gestaltung der technischen Prozesse und deren datenschutzgerechte Organisation stehen.

ESTLAND

A: Zusammenfassung der Aktivitäten und Neuerungen:

Organisation	
Vorsitz und/oder Gremium	Estnische Datenschutzbehörde
Budget	592 446 EUR
Personal	18 (unterstützende Leistungen, wie z. B. IT und Buchhaltung, werden ausgelagert)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Beschlüsse: 354 Aufsichtsbeschlüsse (einschließlich 114 Verweigerungen und 38 Grundsätze), 58 Beschlüsse bezgl. Ordnungswidrigkeiten, 9 Berufungsbeschlüsse und 18 Genehmigungen (7 Genehmigungen wissenschaftlicher Forschungen und 11 Genehmigungen von Datenübermittlungen). Stellungnahmen (Leitlinien): **3** (Datenschutz im Arbeitsalltag; Leitlinien für Personalmitarbeiter: Personenbezogene Daten in Beschäftigungsverhältnissen und Informieren von Kindern, die Hilfe und Datenschutz benötigen). Empfehlungen: **130** für eine bessere Umsetzung von Datenschutz
Meldungen	327 (Verarbeitung vertraulicher Daten)
Vorabprüfungen	0
Anfragen betroffener Personen	**687** per E-Mail/Post (195 öffentlicher Sektor, 257 privater Sektor, 110 gemeinnütziger Sektor; 37 Medien, 53 soziale Netzwerke; 35 Spam und **615** Hotline-Anrufe
Beschwerden betroffener Personen	**413**
Vom Parlament bzw. der Regierung angeforderte Beratung	**2** (bzgl. der Gesetze über das Einwohnermeldewesen und über elektronische Kommunikation)
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	**41** Stellungnahmen zu Gesetzentwürfen auf Anfrage der Regierung
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Prüfungen: **77** vor Ort Untersuchungen: **7** (Prüfungen von Compliance

	und Angemessenheit) Vergleichende Kontrollen: 3 (unter Arbeitgebern; Sicherheitsmaßnahmen in Gemeinden; Direktmarketing)
Sanktionsmaßnahmen	
Sanktionen	**38** Zwangsgelder und Bußgelder für Ordnungswidrigkeiten
Geldbußen	3824 88 (durch die Datenschutzbehörde)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	**126** Meldungen neuer DPOs + **9** DPO-Änderungen

B. Informationen zur Rechtsprechung

Estnisch-lettische Zusammenarbeit – Gemeinsame Aufsicht über Stockmann

Die Datenschutzbehörden Estlands und Lettlands haben gemeinsam die Filialen der Kaufhauskette Stockmann in Estland und Lettland bezüglich des Schutzes personenbezogener Daten im Rahmen von Beschäftigungsverhältnissen und Kundenbeziehungen, einschließlich Direktmarketing, beaufsichtigt.

Die Aufseher legten nahe, dass Partner der Stockmann Group ihre Kunden besser über die Erfassung von Daten in Sachen Direktmarketing sowie die Schließung und Löschung von Kundendaten auf Anfrage informieren sollten. Des Weiteren schlugen die Datenschutzbehörden vor, dass Stockmann bei der Datenerfassung die Pflichtfelder abändere, die erforderlich seien, um ein Stockmann-Stammkunde zu werden. Die Behörden baten Stockmann, einen Bereich mit Informationen über die Möglichkeit einer Löschung personenbezogener Daten aus der Datenbank hinzuzufügen.

Darüber hinaus wiesen die Aufseher darauf hin, dass Stockmann bei der Zustellung vonWerbebotschaften, falls der Kunde diesbezüglich eine Einwilligung erteilt, lediglich das Recht habe, eine relevante Kontaktmethode (Post, E-Mail, Mobiltelefon usw.) zu erfassen.

Ein weiteres Problem, das gelöst werden müsse, beziehe sich auf das Erstellen von Kundenprofilen. Kunden müssten darüber informiert werden, um entscheiden zu können, ob sie Stockmann-Stammkunden werden.

C. Sonstige wichtige Informationen

Wir führten eine umfangreiche **interne Prüfung der Verwaltungsverfahren mit einer Analyse der Gerichtsurteile und Rechtsliteratur** durch. Die Prüfung hatte den Zweck, die Rechtspraxis der Aufsichtsbehörde zu harmonisieren, um zu garantieren, dass sie verständlich und gerechtfertigt ist und Verfahrensfehler reduziert werden. Wir haben detaillierte Leitlinien für Verwaltungsverfahren ausgearbeitet.

Der andere große Gegenstand der Analyse war das **Verhältnis zwischen Privatleben und freier Meinungsäußerung**. Nur wenige derartige Fälle kommen vor Gericht und beziehen sich in erster Linie auf Verleumdung. Eine Einschränkung des Rechts auf freie Meinungsäußerung muss eine gut durchdachte

Entscheidung sein. Wir führten eine gründliche Prüfung der Regelungen des Europäischen Gerichtshofs für Menschenrechte, der existierenden Literatur (die in Estland nur geringfügig vorhanden ist) sowie der Regelungen des Obersten Gerichtshofs durch. Dies bildet die Grundlage, auf die wir bei der Bearbeitung von Beschwerden und bei der Rechtfertigung unserer Beschlüsse zurückgreifen können. Des Weiteren organisierten wir gemeinsam mit der estnischen Zeitungsverlegerverbandes ein Seminar, das im April 2011 stattfand.

Der **Informationsaustausch mit dem Polizei- und Grenzschutzamt und dem Innenministerium zur Überwachung eines Missbrauchs der Polizeidatenbanken und des Bevölkerungsregisters** haben jeweils eine solide Grundlage. Der Missbrauch des Bevölkerungsregisters nahm zu. Daher diskutierten wir das Problem in den Medien und führten höhere Bußgelder ein.

Wir begannen außerdem mit einem **regelmäßigen Informationsaustausch mit der Estonian eHealth Foundation**, um den Missbrauch von Patientendaten zu überwachen.

FINNLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Schwerpunkt der Datenschutzbehörde lag auf vorbeugenden Maßnahmen. Gezielte Leitlinien und eine funktionale Integration in verschiedene Gruppen, Ausschüsse und ähnliche Organisationen sollten zu spürbareren Auswirkungen führen. Ein Vertreter vom Amt des Datenschutzbeauftragten beteiligte sich an der Arbeit von rund 80 Beratungsgremien, Arbeitsgruppen und ähnlichen Organen. Der Datenschutzbeauftragte ist ein Mitglied oder Expertenmitglied der Informationssicherheitsgruppe des Programms „Informationsgesellschaft im Alltag“, das am 28. Februar 2011 endete, sowie der Lenkungsgruppe für Informationssicherheit der finnischen Regierung (VAHTI). Außerdem ist er Mitglied einer Überwachungsgruppe der Kodifikation der Informationsgesellschaft, die am 9. Dezember 2011 vom Ministerium für Verkehr und Kommunikation ins Leben gerufen wurde. Die Überwachungsgruppe wird noch bis zum 31. Oktober 2014 fortbestehen. Am 14. Oktober 2011 lud das Justizministerium den Datenschutzbeauftragten zur Teilnahme an einem Gremium ein, das die Vorbereitung eines nationalen Aktionsprogramms für Menschenrechte unterstützen soll. Das Gremium war vom 14. Oktober 2011 bis zum 31. Januar 2012 aktiv.

Vertreter des Amtes beteiligten sich an mehreren, im Rahmen der Lenkungsgruppe für Informationssicherheit der finnischen Regierung (VAHTI) ins Leben gerufenen Arbeitsgruppen sowie an den rund 30 Arbeits- und Lenkungsgruppen verschiedener Verwaltungszweige. Die Zusammenarbeit hat u. a. zur Erstellung von Verhaltenskodizes oder anderer branchenspezifischer Leitlinien geführt.

Zum Ende des 24. Tätigkeitsjahres der Datenschutzbehörde kam es in Finnland zu einer beispiellosen Welle an Verstößen gegen das Datenschutzgesetz. Fast jede Woche gab es Nachrichten und Enthüllungen von offengelegten personenbezogenen Daten. Und dabei waren die öffentlich diskutierten Fälle laut Informationen der CERT-Einheit der finnischen Aufsichtsbehörde für Kommunikation nur ein kleiner Teil der Datenlecks desselben Zeitraums. Die Tatsache, dass die finnischen Vorschriften das Informieren der Personen, deren personenbezogene Daten offengelegt wurden, nicht zwingend vorsehen, wurde als besonders großes Problem erachtet. Das Vertrauen, das Bürger in die Dienste der Informationsgesellschaft gelegt haben, wurde auf eine harte Probe gestellt.

Die „Safer Internet Week“ hatte soziale Medien und Datenschutz im Internet zum Hauptthema.

Die Datenschutzbehörde beteiligte sich erneut an den Aktivitäten des Safer Internet Day am 8. Februar 2011 und der darauffolgenden Safer Internet Week. Der Safer Internet Day, der zum achten Mal stattfand, erfolgt im Rahmen der nationalen Strategie für Informationssicherheit. Dieses Jahr legte die Kampagne den Schwerpunkt auf Datenschutz im Internet. Informationssicherheit für soziale Medien wurde ebenfalls in einem breiteren Kontext diskutiert.

Soziale Medien haben dafür gesorgt, dass die Informationssicherheit im Internet auch für gewöhnliche Nutzer zunehmend zum Problem wird. Die sichere Nutzung von Online-Communities erfordert Sorgfalt und Aufmerksamkeit, und Datenschutz wird dabei immer wichtiger. Vor dem Safer Internet Day wurde die Website des Leitfadens für Informationssicherheit mit neuen Informationen zu betrügerischen Links, Datenschutz und die sichere Nutzung sozialer Medien aktualisiert.

Schulkinder und Teenager haben oftmals mehr Erfahrung in der Nutzung von Online-Communities als Erwachsene, benötigen jedoch mindestens genauso viele Ratschläge für ein sicheres Surfen im Internet und den Schutz ihrer Daten. Für Schulen wurden verschiedene Übungen zu dem Thema veröffentlicht, und

auf der Website der Online-Sicherheitsschule (www.tietoturvakoulu.fi) wurde ein Wettbewerb ausgeschrieben.

Darüber hinaus wurde die Sichtbarkeit des Safer Internet Day im Internet erhöht. Das Diskussionsforum Suomi24 beinhaltete während des gesamten Februars einen Spezialabschnitt über den Safer Internet Day, in dem Fachleute der Kampagne die Fragen der Benutzer zum Thema Informationssicherheit beantworteten.

In der folgenden Tabelle sind die wichtigsten Zahlen rund um das Amt des Datenschutzbeauftragten zusammengefasst.

Organisation	
Vorsitz und/oder Gremium	Reijo Aarnio ist seit dem 1. November 1997 der Datenschutzbeauftragte
Budget	Das Jahresbudget liegt bei rund 1 585 000 EUR
Personal	20
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2 630
Meldungen	377
Vorabprüfungen	siehe Meldungen
Anträge betroffener Personen	950
Beschwerden betroffener Personen	(Zugang und Korrekturen) 189
Vom Parlament bzw. der Regierung angeforderte Beratung	93
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Zusammenarbeit mit für die Datenverarbeitung Verantwortlichen in den folgenden Sektoren: Bildung, Gesundheitswesen, Soziales, Telekommunikation, Beschäftigung und Wirtschaft
Prüfmaßnahmen	
Prüfungen, Untersuchungen	654

Sanktionsmaßnahmen	75
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	>1 000

B. Informationen zur Rechtsprechung

– Ein Kläger, der von seinem Auskunftsrecht Gebrauch machte, hatte den für die Datenverarbeitung Verantwortlichen gebeten, ihm die Aufzeichnungen seiner an das Unternehmen gerichteten Kundenanrufe zukommen zu lassen.

Das Auskunftsrecht des Klägers gilt laut Abschnitt 26 des Datenschutzgesetzes für existierende Aufzeichnungen von Kundentelefonaten, es sei denn, es existiert ein Grund für eine Einschränkung des Auskunftsrechts gemäß Abschnitt 27 des Datenschutzgesetzes. In seiner Erklärung machte der für die Datenverarbeitung Verantwortliche für die betreffenden Aufzeichnungen keinen derartigen Grund zur Einschränkung des Auskunftsrechts des Klägers geltend. Daher war der Verantwortliche verpflichtet, dem Kläger gemäß Abschnitt 28.2 des Datenschutzgesetzes die entsprechenden Informationen zugänglich zu machen. Der Verantwortliche war verpflichtet, dem Kläger entweder die Möglichkeit zu geben, sich die Aufzeichnungen anzuhören, oder auf Anfrage des Klägers eine schriftliche Version der Aufzeichnungen zur Verfügung zu stellen.

– Eine Person rief den Datenschutzbeauftragten dazu auf, aufgrund einer Nachricht, die sie dem Städtebauamt geschickt hatte und fälschlicherweise auch an die Städteplanungsabteilung ging und somit öffentlich gemacht wurde, Maßnahmen zu ergreifen. Die Nachricht enthielt Informationen zur Straßenpflege und zum Parken auf Straßen.

Das Maß der Bekanntmachung eines Dokuments, das an einen Beamten geschickt wird, ist im Gesetz über die Öffentlichkeit von Verwaltungsaktivitäten (621/1999) festgelegt. Jeder Beamte trifft gemäß dem Gesetz über die Öffentlichkeit von Verwaltungsaktivitäten unabhängige Entscheidungen bezüglich der Vertraulichkeit von Dokumenten und anderen Verpflichtungen. Der Datenschutzbeauftragte ist generell nicht dazu verpflichtet, bezüglich der Einhaltung des Gesetzes über die Öffentlichkeit von Verwaltungsaktivitäten Ratschläge zu erteilen oder diese zu überwachen, und er hat auch nicht das Recht, in Entscheidungen von anderen Beamten, die gemäß dem Gesetz getroffen werden, einzugreifen.

– Das nationale Institut für Gesundheit und Wohlstand hat den Datenschutzbeauftragten um eine Anhörung gemäß Abschnitt 4, Unterabschnitt 1 des Gesetzes über nationale Kundenregister im Gesundheitswesen (556/1989, geändert in 38/1993) gebeten. Es wurde um eine Stellungnahme zu einer Gruppe von Forschern gebeten, um aus den Registern für sozialen Wohlstand und Gesundheit (HILMO), die vom nationalen Institut für Gesundheit und Wohlstand gepflegt werden, Informationen über deren Studie zu erlangen.

Wie die zusätzliche Erklärung gezeigt hat, war es nicht beabsichtigt, die Daten oder Stichproben, die von den Forschungsgegenständen mit deren Erlaubnis erfasst wurden, mit den angeforderten Registerdaten in

Verbindung zu bringen. Scheinbar gab es kein Hindernis für die Übermittlung der Daten, nachdem die Angemessenheit einiger Unklarheiten, die in dem Antrag angesprochen wurden, bestätigt worden war und andere Forschungsdaten auf rechtmäßige Weise erfasst worden waren.

– *Dem Datenschutzbeauftragten wurde eine Frage bezüglich der Rechtmäßigkeit von Kameraüberwachung im Außenbereich und in gemeinschaftlichen Innenbereichen eines Pflegeheims gestellt. In dem Pflegeheim wohnten auch die Mitarbeiter, die dort rund um die Uhr arbeiteten. Es gab keinerlei Anzeichen für eine Videoüberwachung. Eine Beschreibung der Datei existierte zwar, doch sie war in dem Heim nicht verfügbar. Eine Genehmigung für die Überwachung der Innenräume wurde ebenfalls nicht beantragt.*

Die primäre Frage lautete, ob die Kameraüberwachung im gemeinschaftlichen Wohnbereich des Pflegeheims im Hinblick auf die Grundrechte, das Strafrecht, das Kinderhilfegesetz und weitere bestimmte Gesetze generell erlaubt ist. Der Betrieb in Pflegeheimen ist gemäß dem Kinderhilfegesetz organisiert. Dies bedeutet, dass das Ministerium für Soziales und Gesundheit rechtlich dazu befugt ist, dahingehend Stellung zu beziehen, in welchen Situationen eine Kameraüberwachung für den betreffenden Betrieb gerechtfertigt ist. Der Datenschutzbeauftragte ist der Ansicht, dass die Frage, ob die Handhabung der personenbezogenen Daten der Einwohner und Mitarbeiter durch Kameraüberwachung gemäß dem Datenschutzgesetz (523/1999) oder dem Gesetz zum Schutz der Privatsphäre im Arbeitsleben rechtmäßig ist, in diesem Fall zweitrangig sei.

C. Sonstige wichtige Informationen

Erste Datenschutz-Folgenabschätzung ausgewertet

Ein großer finnischer Einzelhändler mit einer Stammkundendatenbank hat sein Bonuskartensystem geändert. Gleichzeitig wurden die Karten auf RFID-Technologie umgestellt. Aufgrund dieser Änderung führte das Unternehmen eine Datenschutz-Folgenabschätzung durch und reichte sie bei der Datenschutzbehörde zur Beurteilung ein.

In Finnland gab es außerdem eine Arbeitsgruppe, die die potenzielle Notwendigkeit eines Gesetzes für NFC-Technologie abschätzte. Die Arbeitsgruppe vertrat den Standpunkt, dass das allgemeine Datenschutzgesetz auch die NFC-Technologie ausreichend abdecke.

Maßnahmen zur Verbesserung des nationalen Informationsmanagements

Die finnische Regierung gab einen Grundsatzbeschluss zur Verfügbarkeit von öffentlichem Datenmaterial heraus. Dieser verfolgt das Ziel, die Möglichkeiten einer weitreichenderen Nutzung der nationalen Datenbestände (offene Daten) zu verbessern und dabei den Schutz personenbezogener Daten zu respektieren. Die Präsentation wurde außerdem durch das Datenverwaltungsgesetz gestützt, mit dem die Einführung einer nationalen Informationsarchitektur bestehend aus kompatiblen Elementen eingeführt werden soll.

Die Umsetzung einer Datenschutzverordnung auf Grundlage des Gesetzes über die Öffentlichkeit von Verwaltungsaktivitäten, das die angemessene Verwaltung öffentlichen Datenmaterials und Dateien mit personenbezogenen Daten regelt, wurde im Berichtsjahr ebenfalls vorangebracht. Damit soll gewährleistet werden, dass alle Einheiten der staatlichen Verwaltung ein ihren Aufgaben entsprechendes Maß an Informationssicherheit erreichen.

Datenschutz in verschiedenen Bereichen

Die Datenschutzbehörde hat u. a. in den Bereichen Bildung, Datenkommunikation, Gesundheits- und Sozialwesen, Marketing und Wissenschaft unter Aufsicht mit Interessengruppen zusammengearbeitet. Diese Arbeitsgruppen haben Probleme im Zusammenhang mit Themen wie das Wohl von Jugendlichen, Informationssysteme zu Bildungszwecken, mobile Zertifizierung und die Nutzung grundlegender Datenregister in der Forschung besprochen.

Es wurden branchenspezifische Befragungen durchgeführt, um in verschiedenen Sektoren das Datenschutzniveau zu untersuchen. Die Befragungen boten außerdem die Gelegenheit, den für die Datenverarbeitung Verantwortlichen Informationen und Ratschläge zu diesen Themen bereitzustellen.

FRANKREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Änderung der Richtlinie 95/46: erfolgreicher Datenschutz in Europa

Dieses Thema hat sowohl für die Europäische Kommission als auch für die französische Datenschutzbehörde CNIL, die sich mit den für die Konzeption des neuen Instruments verantwortlichen Ausschüssen der Europäischen Kommission getroffen hat, strategische Priorität. Auf Grundlage ihrer 30-jährigen Erfahrung unterstützt die CNIL ein partizipatorisches und dezentralisiertes Datenschutzsystem, das nach Meinung der CNIL am besten für das digitale Zeitalter und die verschiedenen Situationen auf diesem Gebiet gerüstet ist und verschiedene Bereiche der Gesetzgebung betrifft, wie z. B. das Arbeits-, Straf-, Steuer- oder Wirtschaftsrecht, mit denen vor allem die nationalen Behörden gut vertraut sind. Die Durchsetzung des europäischen Datenschutzrechts muss auf einer engen Zusammenarbeit zwischen kompetenten Regierungsbehörden basieren, um effektiv und demokratisch zu sein.

Die CNIL fand es nützlich, im Mai 2011 bezüglich des Entwurfs des Parlamentsberichts der Europäischen Kommission zum Thema Kommunikation mit mehreren MdEP zusammenzukommen. Zu guter Letzt traf sich der Vorsitzende der CNIL am 26. November 2011 in Paris mit Viviane Reding. Das Treffen war eine Gelegenheit für die CNIL, ihre Position im Hinblick auf die Ausrichtung des Verordnungsentwurfs zu bekräftigen.

Beobachtung der technischen Entwicklungen

Cloud

Im Oktober 2011 eröffnete die CNIL gemeinsam mit Fachleuten auf diesem Gebiet eine Konsultation zum Thema „Cloud-Computing“, um sich einen Überblick über die rechtmäßigen und technischen Lösungen zu verschaffen, die ein hohes Maß an Datenschutz gewährleisten und dabei die damit verbundenen wirtschaftlichen Herausforderungen berücksichtigen. Die Fragen deckten fünf Themenbereiche ab: Definition der Cloud, Qualifikation des Cloud-Anbieters, Festlegung des geltenden Rechts, Verwaltung der Übermittlungen sowie Cloud-Sicherheit. Am Ende der Konsultation wurden alle Beiträge auf der Website der CNIL (www.cnil.fr) veröffentlicht und können im Rahmen der Arbeit der G29 zu diesem Thema herangezogen werden.

Gütezeichen

Die ersten beiden Bezugsnormen, die es der CNIL ermöglichen, Gütezeichen für Prüfverfahren für die Verarbeitung von Daten sowie Schulungen zum Thema Datenschutz zu vergeben, wurden am 3. November 2011 veröffentlicht.

Jede Stelle, deren Prüfverfahren für die Datenverarbeitung oder Schulungen den Inhalten der von der CNIL angenommenen Bezugsnormen entspricht, kann nun einen Antrag auf ein Gütezeichen stellen. Dazu müssen lediglich das entsprechende Formular ausgefüllt und die erforderlichen Informationen bereitgestellt werden.

Das Gütezeichen ist daher eine zweifache Garantie für Qualität und Einhaltung der gesetzlich und von der CNIL vorgeschriebenen Anforderungen. Die Methode wird im eigens hierfür eingerichteten Bereich für CNIL-Gütezeichen auf der Website erläutert (www.cnil.fr). Eine Website für jedes Gütezeichen rundet die Erläuterung dieses Instruments ab.

Google

Zu guter Letzt hat die CNIL Google für die Massenerfassung technischer WLAN-Daten ohne Inkenntnissetzung der betroffenen Personen sowie sogenannter „Content"-Daten (Anmeldedaten, Passwörter, Verbindungsdaten, E-Mail-Kommunikation) ein Bußgeld auferlegt. Die CNIL hat Google im Mai 2010 dazu aufgefordert, die Situation aufzuklären. Angesichts der Tatsache, dass Google innerhalb der gesetzten Frist nicht auf die Aufforderungen reagiert hat, wurde dem Unternehmen von der Verwaltung des CNIL am 17. März 2011 ein Bußgeld in Höhe von 100 000 EUR auferlegt.

Prüfungen und Maßnahmen zur Sensibilisierung

Prüfungen aller Videoüberwachungssysteme

Mit dem LOPPSI-Gesetz für innerstaatliche Sicherheit vom 14. März 2011 erhielt die CNIL die Befugnis, alle auf öffentlichen Straßen oder Plätzen installierten Videoüberwachungssysteme zu überprüfen. Zuvor hatte die CNIL lediglich die Befugnis, Systeme zu überprüfen, die auf nicht frei zugänglichen Plätzen installiert waren. Diese lang erwartete Änderung ermöglicht nun die Umsetzung einer einheitlichen und unabhängigen Prüfung aller in Frankreich installierten Videoüberwachungssysteme.

Praktische Leitfäden

Des Weiteren hat die CNIL 2011 ihre Sensibilisierungsarbeit fortgesetzt und insbesondere zwei praktische Leitfäden (für Anwälte und medizinische Fachkräfte) sowie eine Empfehlung zu politischer Kommunikation veröffentlicht.

Organisation	
Vorsitz und/oder Gremium	Vorsitz: Isabelle FALQUE-PIERROTIN, Stellvertretende Vorsitzende: Emmanuel de GIVRY, Jean-Paul AMOUDRY Zusammensetzung des Gremiums: 4 Parlamentsabgeordnete, 2 Mitglieder des Wirtschafts- und Sozialrats, 6 Richter des obersten Gerichtshofs, 5 qualifizierte, vom Kabinett ernannte Persönlichkeiten (3), der Vorsitzende der Nationalversammlung (1) und der Vorsitzende des Senats (1).
Budget	Insgesamt für 2011: 15,8 Mio. EUR
Personal	Anzahl der Mitarbeiter: 159

Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	1 969 Beschlüsse (25,5 % mehr als 2010)/93 Stellungnahmen/1 Empfehlung
Meldungen	Bei der CNIL gingen 82 243 Meldungen ein, darunter: 5 993 Meldungen für Videoüberwachungssysteme (37 % mehr als 2010) 4 483 Meldungen für Ortungssysteme (33,5 % mehr als 2010)
Vorabprüfungen	Genehmigungen: 1 759 im Jahr 2011, darunter: 249 im Plenum angenommene Genehmigungen, 887 Genehmigungen von Datenübermittlungen an Nicht-EU-Staaten, 6 Rahmengenehmigungen, 744 Genehmigungen biometrischer Systeme (5,4 % mehr als 2010), 503 Genehmigungen von Datenverarbeitungen zu medizinischen Zwecken sowie 120 Genehmigungen von Datenverarbeitungen zu Zwecken der Beurteilung oder Analyse von Pflege- und Vorbeugungspraktiken oder -aktivitäten.
Anfragen betroffener Personen	Anträge aus der Öffentlichkeit: Bei der CNIL gingen 2011 32 743 schriftliche (10 % mehr als 2010) und 138 979 telefonische (4,6 % mehr als 2010) Anträge ein.
Beschwerden betroffener Personen	Bei der CNIL gingen 2011 5 738 Beschwerden ein (19 % mehr als 2010). Dies entspricht der höchsten Anzahl von Beschwerden, die jemals bei der CNIL eingegangen ist. Die Hauptanliegen der Beschwerden drehten sich um das Recht auf Vergessenwerden und Videoüberwachungssysteme. Anträge betroffener Personen: 2 099 Anträge auf indirekten Zugang in den Bereichen, wo eine Datenverarbeitung der Staatssicherheit, Verteidigung oder öffentlichen Sicherheit dient (12 % mehr als 2010).
Vom Parlament bzw. der Regierung angeforderte Beratung	2011 nahm die CNIL 92 Stellungnahmen zu nationalen Gesetzentwürfen an (d. h. 20 % aller vom Plenum angenommenen Stellungnahmen). Des Weiteren wurde die CNIL 23 Mal von Abgeordneten des französischen Parlaments konsultiert und nahm an 10 Sitzungen mit Abgeordneten des französischen Parlaments zum Austausch von Ansichten zu Datenschutzfragen teil.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	385 Untersuchungen (25 % mehr als 2010), davon 151 Untersuchungen bzgl. Videoüberwachungssystemen.

Sanktionsmaßnahmen	
Sanktionen	18 durch die CNIL im Jahr 2011 verhängte Sanktionen. Rechtsstreite gegen Verantwortliche von Datenverarbeitungen: 83 (65 Mahnungen, 5 Geldstrafen, 13 Verwarnungen), 2 Kündigungen.
Geldbußen	Die CNIL verhängte 2011 Geldbußen im Gesamtwert von 190 000 EUR.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	8 635 Behörden ernannten einen DPO (25 % mehr als 2010).

B. Informationen zur Rechtsprechung

Es folgt eine Auflistung der wichtigsten Urteile der französischen Justiz im Zusammenhang mit dem Schutz personenbezogener Daten.

- Berufungsgericht Caen, 3. Kammer, Sektion Sozialfragen 1, Ausschuss für Sicherheit und Gesundheitsschutz am Arbeitsplatz (CHSCT) des Unternehmens Benoît GIRARD/Gewerkschaft (CFDT) für Mitarbeiter der Metallindustrie in der Region Caen, 0903336 (23. September 2011)

- Berufungsgericht Montpellier, Kammer 5, Sektion A, Marie-Cécile C/Google Inc, 1100832 (29. September 2011)

- Berufungsgericht Paris, Division 5, Kammer 11, SAS ANTIK BATIK/SA SAFETIC, 0920824 (9. September 2011)

- Kassationsgerichtshof, 1. Zivilkammer, Unternehmen NORD-OUEST u. a./Unternehmen DAILYMOTION, 0967896165 (17. Februar 2011)

- Kassationsgerichtshof, Kammer für Handelssachen, Ceramconcept/Administration des Impôts (Steuerbehörde), 1015014 (27. April 2011)

- Kassationsgerichtshof, Strafkammer, Movsar X und Zarea Y, 1084344 (11. May 2011)

- Kassationsgerichtshof, Strafkammer, Schering-Plough/DGCCRF (Generaldirektion Wettbewerb, Verbrauch und Betrugsbekämpfung) 1085479 (29. Juni 2011)

- Kassationsgerichtshof, Kammer für Soziales, M D/Unternehmen MOREAU Incendie, 1018036 (3. November 2011)

- Kassationsgerichtshof, Kammer für Soziales, M. X./Méditerranéenne de Nettoiement, Groupe Nicollin, 1014869 (21. September 2011)

- Kassationsgerichtshof, Kammer für Soziales, Frau T/Unternehmen UFIFRANCE Gestion, 1014685 (5. Juli 2011).

- EG, Association pour la Promotion de l'Image u. a., 317827 (26. Oktober 2011)

- Verwaltungsgericht Clermont-Ferrand, SA Notrefamille.com, 1001584 (13. Juli 2011)
- Verwaltungsgericht Straßburg, O A, C M, A Z/Präfektur Bas-Rhin, 0902015 (5. Oktober 2011)
- Verwaltungsgericht Straßburg, O A, C M, A Z/Präfektur Bas-Rhin, 0902016 (5. Oktober 2011)
- Handelsgericht Nanterre, Greenpeace/Thierry L EDF, (10. November 2011)
- Gericht erster Instanz Charleville-Mézières, Philippe D u. a./Jean-Luc P u. a., 10349000004 (24. Februar 2011)
- Gericht erster Instanz Coutances, René L/Stanislas L, 1000822 (6. Oktober 2011)

GRIECHENLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Das griechische Parlament hat vor Kurzem das Gesetz 4055/2012 verabschiedet, das bestimmte Vorkehrungen zur Regulierung von Angelegenheiten im Zusammenhang mit dem Betrieb der verfassungsrechtlich geschützten, unabhängigen Behörden im Allgemeinen und der Datenschutzbehörde im Speziellen umfasst. Das o. g. Gesetz stellt einen Vorentwurf des Parlamentsausschusses für Institutionen und Transparenz an die Konferenz der Präsidenten des Parlaments für die Wahl der Mitglieder und Präsidenten der Behörden für eine sechsjährige Amtszeit ohne Wiederernennung dar. Des Weiteren sieht es vor, dass der Status exklusiver Vollzeitbeschäftigung außerdem auf den stellvertretenden oder Vizepräsidenten jeder unabhängigen Behörde ausgeweitet wird, mit der Möglichkeit einer weiteren Ausweitung dieses Beschäftigungsstatus auf eine Reihe von Vorstandsmitgliedern der Behörden. Das Gesetz sieht außerdem vor, dass der Beschäftigungsstatus der wissenschaftlichen Mitarbeiter, die die Hauptaufgaben der Behörden ausführen, für alle Behörden gleich ist. Darüber hinaus hat das Gesetz 3917/2011 dazu geführt, dass a) die Richtlinie 2006/24/EG in nationales Recht umgesetzt wurde, b) Vorkehrungen bezüglich der Nutzung von Videoüberwachungssystemen in öffentlichen Bereichen getroffen wurden, und c) bestimmte Aspekte des Datenschutzgesetzes 2472/1997 abgeändert wurden. Die wichtigste Änderung gibt der Datenschutzbehörde das Recht, die zu bearbeitenden Beschwerden und Anträge nach Wichtigkeit und allgemeinem Interesse zu gewichten. Die restlichen Änderungen bezogen sich auf Angelegenheiten bezüglich der Zusammensetzung der Datenschutzbehörde und der Versetzung von Beamten in die Datenschutzbehörde. Zu guter Letzt wurde das Gesetz 3471/2006 im Hinblick auf die rechtswidrige Zusendung unerwünschter Kommunikation mit oder ohne menschlichem Zutun vorgenommen.

Zum wiederholten Mal konnte das Problem der Unterbesetzung der griechischen Datenschutzbehörde (HDPA) aufgrund der allseits bekannten prekären Finanzlage des Staates auch 2011 nicht gelöst werden.

Darüber hinaus beeinträchtigt die fortlaufende Reduzierung des Budgets, das der Datenschutzbehörde für betriebliche Zwecke zugeteilt wird, die Fähigkeit der Behörde, ihren Verpflichtungen nachzukommen.

Im Speziellen veröffentlichte die HDPA zwei Leitlinien: a) Leitlinie 1/2011 zur Nutzung von Videoüberwachungssystemen zum Schutz von Personen und Gütern in öffentlich zugänglichen Privatbereichen, und b) Leitlinie 2/2011 zur elektronischen Einwilligung im Zusammenhang mit elektronisch versandten kommerziellen Mitteilungen (siehe Rechtsprechung).

Des Weiteren erteilte die HDPA der Regierung, dem Parlament und anderen unabhängigen Behörden Ratschläge mittels folgender Stellungnahmen und Beschlüsse: a) auf Anfrage des Finanzministeriums und des Parlaments gab die HDPA ihre Stellungnahme zu einer Reihe von Steuerfragen ab, die sich insbesondere auf die Veröffentlichung von Steuerdaten im Internet bezogen (Stellungnahmen 1/2011, 4/2011, 7/2011 und 54/2011 – siehe Rechtsprechung), b) die HDPA beteiligte sich an einem Gesetzgebungsausschuss des Justizministeriums für die Umsetzung der Richtlinie 2009/136/EG in nationales Recht und die Änderung des Gesetzes 3471/2006 über den Schutz personenbezogener Daten und der Privatsphäre in der elektronischen Kommunikation, c) die HDPA beteiligte sich an der öffentlichen Konsultation zum Verordnungsentwurf der griechischen Behörde für die Sicherheit der Vertraulichkeit von Kommunikation (einer unabhängigen Verwaltungsbehörde) d) auf Anfrage des griechischen Parlaments brachte die HDPA ihre Ansicht zum „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Verwaltungszusammenarbeit durch das Interne Marktinformationssystem“ (die IMI-Verordnung) zum Ausdruck, e) die HDPA brachte ihre Ansicht zur Aufsichtsbehörde für Energie (einer weiteren unabhängigen Verwaltungsbehörde) im Zusammenhang mit den vorgeschlagenen Maßnahmen zur Verwaltung der Schulden von Kunden von Versorgungsunternehmen zum Ausdruck.

Außerdem gab die HDPA den Beschluss 50/2011 zu Verarbeitungsanträgen für die außergerichtliche Einigung von „Tiresias Bank Information Systems S.A.“, Beschluss 52/2011 zum Volkszählungs- und Unterbringungsverfahren der griechischen Statistikbehörde sowie Beschluss 53/2011 zum „Google-Maps-Service“ heraus (siehe Rechtsprechung).

Anlässlich des Europäischen Datenschutztages fügte die HDPA ihrer Website einen Sonderbereich zur Sensibilisierung von Schülern weiterführender Schulen bezüglich der sicheren Nutzung von Internetdiensten hinzu. Des Weiteren wurde ein Hilfs- und Selbstbeurteilungstool im Zusammenhang mit Identitätsdiebstahl für alle Altersgruppen eingerichtet. Das Bildungsministerium unterstützte diese Initiative, indem es weiterführende Schulen zur Nutzung des Materials zum Vorteil ihrer Schüler aufforderte. Darüber hinaus besuchten Fachkräfte der HDPA ausgewählte Schulen. Zu guter Letzt wurden auf der Website ein Bulletin und eine Pressemitteilung veröffentlicht.

Organisation	
Vorsitz und/oder Gremium	Christos Yeraris (Vorsitz) bis Mai 2011 Petros Christoforos (Vorsitz) seit August 2011
Budget	2 339 500 EUR
Personal	Abteilung Audit: 16 Juristen und 11 IT-Experten (davon befinden sich fünf im Mutterschutz, einer wurde für einen Teil des Jahres als nationaler Experte an europäische Gremien abgeordnet, einer ist im Bildungsurlaub und einer hat gekündigt); Abteilung Kommunikation und Öffentlichkeitsarbeit: 5 (davon 1 für ein halbes Jahr im Mutterschutz und Bildungsurlaub); Abteilung Personal und Finanzen: 16 und 1 von einem anderen öffentlichen Dienst abgeordnet.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die HDPA veröffentlichte 168 Beschlüsse, 7 Stellungnahmen und 2 Leitlinien. Davon hatten 6 Beschlüsse, 5 Stellungnahmen und 2 Leitlinien Auswirkungen auf den Datenschutz.
Meldungen	Die HDPA untersuchte 702 Meldungen (414 davon betrafen die Installation und den Betrieb von Überwachungskameras, 70 betrafen die Übermittlung von Daten in Drittländer).
Vorabprüfungen	Die HDPA bewilligte bzw. erneuerte 63 Genehmigungen zur Verarbeitung sensibler Daten, zur Verknüpfung von Akten sowie zur Datenübermittlung in Drittländer.
Anträge betroffener Personen und Verantwortlicher:	1 011
Beschwerden betroffener	812 (Strafverfolgungsbehörden und Ordnungsamt: 76, Verteidigungsministerium: 2, öffentliche Verwaltung und lokale

Personen	Behörden: 33, Steuerwesen/Finanzministerium: 4, Gesundheitswesen: 20, Sozialversicherung: 9, Bildung und Forschung: 5, Bankwesen: 51, Privatwirtschaft: 163, elektronische Kommunikation: 131, Arbeitsbeziehungen: 25, Massenmedien: 7, Sonstige: 286)
Vom Parlament bzw. der Regierung angeforderte Beratung	9 (Stellungnahme 1/2011, Stellungnahme 4/2011, Stellungnahme 7/2011, Beschluss 50/2011, Beschluss 52/2011 – siehe auch Abschnitt A – Zusammenfassung)
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	7 Prüfungen (davon 3: Bildungsministerium, 1: Nationale Eurodac-Einheit, 1: Behörde zur Bekämpfung von Geldwäsche, 1: soziale Sicherheit (Online-Verordnungssystem) und 1: private Wirtschaft.
Sanktionsmaßnahmen	
Sanktionen	22 Sanktionen (18 Verwarnungen, 4 Geldbußen), verhängt von der Datenschutzbehörde in den folgenden Bereichen: Gesundheitswesen (13), Sozialversicherung/Versicherungen (2), Spam (2), Überwachungskameras (2), Telekommunikation (1), Bankwesen (1), öffentlicher Sektor (1).
Geldbußen	Beträge: 3 000 EUR – 10 000 EUR (insgesamt 27 000 EUR), verhängt von der HDPA
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Leitlinie 1/2011

Die HDPA hat Leitlinie 1/2011 zur Nutzung von Videoüberwachungssystemen zum Schutz von Personen und Gütern in öffentlich zugänglichen Privatbereichen herausgegeben, die die vorherige ersetzt. Die Leitlinie enthält allgemeine und spezifische Aspekte verschiedener Kategorien von Verantwortlichen für die Datenverarbeitung. Besonderes Augenmerk kommt der Anwendung des Verhältnismäßigkeitsgrundsatzes zu.

Leitlinie 2/2011

Die HDPA hat Leitlinie 2/2011 zur elektronischen Einwilligung im Zusammenhang mit elektronisch versandten kommerziellen Mitteilungen herausgegeben. Die Leitlinie legt das gültige Verfahren für

Einwilligungen durch Nutzer fest und berät Verantwortliche im Hinblick auf die Verfahren und technischen Hilfsmittel, die sie für eine Validierung der erteilten elektronischen Einwilligung hinzuziehen sollten.

Stellungnahme 1/2011

Es wurde eine Stellungnahme bezüglich der Rechtmäßigkeit zweier verschiedener Anwendungen abgegeben, die das Generalsekretariat für Informationssysteme des Finanzministeriums zur Veröffentlichung von Steuerzahlerlisten im Internet geplant hatte. Im ersten Fall kam die Behörde zu dem Schluss, dass die Veröffentlichung von Steuerzahlerlisten in Steuerämtern, Gemeindeämtern, in den Medien und im Internet zur Bekämpfung von Steuerhinterziehung nicht mit dem Verhältnismäßigkeitsgrundsatz vereinbar sei. Bezüglich des zweiten Antrags kam die HDPA zu dem Schluss, dass der Datenvalidierungsdienst des Steuerregisters den Artikeln 9(a) und 25 Absatz 1 der Verfassung entspräche, da keine Informationen über das Einkommen der Steuerzahler und der entsprechenden Steuern offengelegt werden.

Stellungnahme 4/2011

Die HDPA kam zu dem Schluss, dass die Veröffentlichung der Schuldnerliste mit überfälligen Zahlungen an den griechischen Staat im Internet durch das Generalsekretariat für Informationssysteme des Finanzministeriums, die die griechische Gesetzgebung angesichts der derzeitigen kritischen Finanzlage des Staates als prinzipiell angemessene Maßnahme für die Erfüllung der steuerlichen Verpflichtungen der Bürger gegenüber dem Staat befunden hat, eine verfassungsrechtlich tolerierbare Datenverarbeitung darstelle und nicht die Grenzen des Verhältnismäßigkeitsgrundsatzes überschreite. In diesem Zusammenhang kam die Behörde zu dem Schluss, dass die oben genannte Veröffentlichung nicht gegen die höherrangigen Rechtsnormen verstoße, die das Recht des Einzelnen auf den Schutz personenbezogener Daten schützen, falls bestimmte, von der HDPA festgelegte Bedingungen erfüllt würden.

Stellungnahme 7/2011

Die HDPA gab auf Anfrage des griechischen Parlaments eine Stellungnahme zur Veröffentlichung von Vermögenserklärungen von Parlamentsabgeordneten im Internet ab. Unter Berücksichtigung des Gesetzeslage, die ausdrücklich die Veröffentlichung der Vermögenserklärungen der Parlamentsabgeordneten, einschließlich der Website des Parlaments, vorsieht, kam die HDPA zu dem Schluss, dass die Einschränkung des persönlichen Rechts der Rechtslage entspreche und durch ein ausreichendes öffentliches Interesse gerechtfertigt werde, da dies für Transparenz im politischen und öffentlichen Leben sorge und mit dem Verhältnismäßigkeitsgrundsatz vereinbar sei sowie einem übergeordneten rechtlichen Interesse diene.

Beschluss 50/2011

Auf eine Frage des Generalsekretariats für Verbraucherschutz hin kam die HDPA zu dem Schluss, dass Daten im Zusammenhang mit Anträgen auf außergerichtliche Einigungen gemäß dem griechischen Recht rechtmäßig auch ohne die Zustimmung der betroffenen Personen durch die Kreditauskunft TIRESIAS Bank Information Systems S.A. erfasst werden dürfe. Die Kreditinstitutionen können auf diese Daten nur mit der Einwilligung der Person zugreifen, die den Kredit beantragt hat.

Beschluss 52/2011

Die HDPA kam zu dem Schluss, dass der nationale Rechtsrahmen in Bezug auf das Volkszählungs- und Unterbringungsverfahren, das zur Zeit der Volkszählung 2011 in Kraft war, nicht die Bedingungen des griechischen Verfassungsgerichts und des Europäischen Gerichtshofs für Menschenrechte bezüglich der Einschränkung persönlicher Rechte erfülle, da die grundlegenden Probleme im Zusammenhang mit der allgemeinen Volkszählung und Unterbringung nicht eindeutig von einem Gesetz oder Präsidialdekret abgedeckt seien. Des Weiteren legte die HDPA die Spezifikationen der organisatorischen und technischen Maßnahmen dar, die für die Sicherheit solcher Daten erforderlich sind. Demzufolge wurde die Rechtslücke mit Gesetz 3995/2011 geschlossen.

Beschluss 53/2011

Im Jahr 2011 änderte Google Inc. den Zweck seiner ursprünglichen, noch ausstehenden Meldung an die HDPA betreffend „Google Street View" und ernannte außerdem Google Greece Applications Ltd. als regionalen Vertreter. Das Unternehmen gab die Straßenkartografierung griechischer Regionen als neuen ausschließlichen Zweck an, die darüber hinaus für weitere einschlägige Dienste, wie z. B. Navigationsdienste, verwendet werde. Die HDPA kam zu dem Schluss, dass der Dienst „Google Maps" die Verarbeitung personenbezogener Daten nach sich ziehe, und zwar in dem Maße, dass Aufnahmen von Gesichtern, Nummernschildern und Gebäuden gemacht würden. Diese Verarbeitung ist laut Datenschutzgesetz rechtmäßig, da der Einsatz wirtschaftlicher Aktivität prinzipiell einen rechtmäßigen Zweck darstellt. Nichtsdestotrotz muss der Dienst unter der Berücksichtigung, dass die betroffenen Personen, die direkt oder indirekt durch die Bilder identifiziert werden können, keine vorherige vertragliche oder sonstige Beziehung mit dem für die Datenverarbeitung Verantwortlichen hatten, unter bestimmten Bedingungen bereitgestellt werden, die da lauten: a) permanente Trübung von Bildern mit Gesichtern, Nummernschildern und Gebäuden innerhalb eines Jahres nach Aufnahmedatum, b) angemessene betriebliche und technische Sicherheitsmaßnahmen, um das Erfassen und weitere Verarbeiten von Bildern mit vertraulichen Daten zu vermeiden, d) angemessene vorherige Benachrichtigung der Öffentlichkeit mithilfe von angemessenen Ankündigungen in der Presse und auf der Website, und e) Gewährung des Rechtes auf Zugang, vorausgesetzt, dass die betroffenen Personen ausreichend Informationen bereitstellen, um den genauen Standort ihrer Daten ausfindig zu machen.

Beschluss 54/2011

Die HDPA kam zu dem Schluss, dass die Veröffentlichung einer Auflistung von Ärzten, die angeblich Steuern hinterzogen haben, auf der Website des Finanzministeriums rechtswidrig sei. Die Veröffentlichung widerspreche sogar dem gesetzlich vorgeschriebenen Steuergeheimnis, das nur in bestimmten rechtlichen Fällen umgangen werden kann. Die Behörde kam zu dem Schluss, dass die Veröffentlichung eine rechtswidrige Datenverarbeitung darstelle. Sie verwarnte den für die Datenverarbeitung Verantwortlichen und ordnete die Einstellung der Verarbeitung binnen fünfzehn (15) Tagen sowie die Entfernung der betreffenden Pressemitteilung von der Website des Finanzministeriums an.

IRLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

2011 eröffnete das Amt des Datenschutzbeauftragten 1 161 Verfahren zur Untersuchung formeller Beschwerden (viele Beschwerden werden informell bearbeitet, indem Beschwerdeführer angemessen über ihre Rechte informiert werden). Wie in vergangenen Jahren konnte ein Großteil der Beschwerden gütlich beigelegt werden; nur 17 Beschwerden gaben Anlass für formelle Beschlüsse. Informationen bezüglich strafrechtlicher Verfolgungen im Jahr 2011 sind in Abschnitt B dieses Berichts enthalten. Das Amt verzeichnete einen starken Anstieg der Meldungen von Verstößen gegen den Schutz personenbezogener Daten, hauptsächlich infolge der Einführung eines neuen Verhaltenskodex für Verstöße gegen den Schutz personenbezogener Daten im Juli 2010. Der Datenschutzbeauftragte tauschte sich auch weiterhin mit großen öffentlichen Organisationen über das Ausmaß des Datenaustausches im öffentlichen Sektor aus. Auf der Grundlage dieser Zusammenarbeit und einer Reihe von Prüfungen von Organisationen in dem Sektor stimmte der Datenschutzbeauftragte einer Reihe von Leitlinien für alle öffentlichen Organisationen mit Transparenz und Verhältnismäßigkeit als leitende Grundsätze zu. Zu weiteren veröffentlichten Leitlinien gehören die überarbeiteten Leitlinien zu Verstößen gegen den Schutz personenbezogener Daten, die überarbeiteten Leitlinien zum Datenschutz und die neuen Leitlinien zur Mitarbeiterkontrolle.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Billy Hawkes
Budget	1 458 000 EUR (1 516 404,20 EUR)
Personal	20
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	3 (Leitlinien)
Meldungen	2011 wurden rund 5 000 Meldungen registriert
Vorabprüfungen	k. A.
Anträge von Bürgern	15 000
Beschwerden von Bürgern	1 161 (Zugangsrechte – 48 %, elektronisches Direktmarketing – 22 %, Offenlegung – 10 %, unlautere Verarbeitung – 10 %, Sonstige – 10 %).
Vom Parlament bzw. der Regierung angeforderte Beratung	>100
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	1 167 Meldungen über Verletzungen des Schutzes personenbezogener Daten von 186 verschiedenen Einrichtungen

Prüfmaßnahmen	
Prüfungen	28 Audits (Prüfungen)
Sanktionsmaßnahmen	
Sanktionen	2011 wurden 54 strafrechtliche Verfolgungen gegen 6 Rechtssubjekte durchgeführt
Geldbußen	Kosten in Höhe von über 15 400 EUR (Geldbußen/von Gerichten verhängte Vergleichszahlungen)
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Im Laufe des Jahres 2011 beteiligte sich der Datenschutzbeauftragte an mehreren erfolgreichen strafrechtlichen Verfolgungen im Zusammenhang mit den Rechten betroffener Personen gemäß den Datenschutzgesetzen von 1988 und 2003 sowie gemäß der Rechtsverordnung 535 aus dem Jahr 2003 (Umsetzung der Richtlinie 2002/58/EG in irländisches Recht). 2011 kam es in sechs Fällen verschiedener Art zu strafrechtlichen Verfolgungen.

C. Sonstige wichtige Informationen

Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation

Am 1. Juli 2011 setzte Irland die überarbeitete Datenschutzrichtlinie für elektronische Kommunikation im Gesetz SI 336/2011 um.

Mit der Verordnung wurde die verpflichtende Meldung von Verstößen gegen den Datenschutz für Netzwerke und Anbieter elektronischer Kommunikation eingeführt. Außerdem setzte sie für all diese Stellen einen hohen Standard in Bezug auf zu ergreifende Sicherheitsmaßnahmen zum Schutz personenbezogener Daten, für die sie verantwortlich sind. Sie müssen u. a. dafür sorgen, dass solche personenbezogenen Daten gesichert und nur befugtem Personal nach dem Need-to-know-Prinzip zugänglich sind. Eine Nichteinhaltung kann strafrechtliche Folgen mit Geldbußen von bis zu 5 000 EUR und eine Anklage in Höhe von 250 000 EUR pro Verstoß nach sich ziehen.

Bei dieser Gelegenheit wurde im neuen Gesetz eine Reihe von Angelegenheiten im Zusammenhang mit Kundenkontakten über Direktmarketing klargestellt. Das Interessanteste war hierbei, dass nun eine vorherige Einwilligung benötigt wird, bevor eine Person zu Marketingzwecken auf dem Mobiltelefon angerufen werden kann, es sei denn, die Nummer wurde mit dem Wunsch, Marketinganrufe zu empfangen, in der nationalen Verzeichnisdatenbank hinterlegt – am 13. März 2012 waren ganze zwölf solcher Nummern hinterlegt!

Ebenfalls interessant ist, dass an eine nicht zu Marketingzwecken versandte SMS kein Marketingmaterial angehängt werden darf, es sei denn, der Empfänger hat seine vorherige Einwilligung für den Empfang

solcher Nachrichten erteilt. Außerdem werden diese Anforderungen auf alle Formen des Marketings ausgeweitet, die über einen öffentlich zugänglichen elektronischen Kommunikationsdienst durchgeführt werden – einschließlich das Erbitten von Spenden durch Wohltätigkeitsorganisationen oder politische Parteien.

ITALIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Neuerungen, Gesetzesänderungen:

2011 wurden am italienischen Datenschutzgesetz erhebliche Änderungen vorgenommen. Diese betrafen in erster Linie Folgendes:

- Verarbeitung der personenbezogenen Daten juristischer Personen: Das Gesetz über finanzielle Dringlichkeitsmaßnahmen (Mai 2011) schloss juristische Personen aus dem Anwendungsbereich des Datenschutzgesetzes aus, wenn die Datenverarbeitung zu sogenannten Verwaltungs- und Buchhaltungszwecken und im Rahmen von Geschäftsbeziehungen zwischen Unternehmen erfolgte (siehe Abschnitt 5(3) des Datenschutzgesetzes). Wenngleich dies später (im Dezember 2011) aufgehoben wurde, schloss eine neue Änderung des Gesetzes (Abschnitt 4) vom Mai 2012 juristische Personen endgültig aus der Definition des Begriffs „personenbezogene Daten" aus – wonach sich personenbezogene Daten lediglich auf „Daten im Zusammenhang mit einer natürlichen Person" beziehen. Dies bedeutet, dass die Verarbeitung personenbezogener Daten durch juristische Personen (einschließlich Verbänden, Stiftungen, Ausschüssen usw.) nicht unter das Datenschutzgesetz fällt. Die Datenschutzbehörde gab jedoch eine detaillierte Stellungnahme heraus (deren endgültige Fassung im Oktober 2012 veröffentlicht wurde), um klarzustellen, dass dies so auszulegen sei, dass juristische Personen „Nutzer" eines öffentlich zugänglichen elektronischen Kommunikationsdienstes seien, wie es im Datenschutzgesetz im Sinne der Datenschutzrichtlinie für elektronische Kommunikation (Abschnitt 4(2)f.) definiert ist;

- Telemarketing: Das Gesetz über finanzielle Dringlichkeitsmaßnahmen von 2011 dehnte die Rücktrittsoption für unerwünschte Postwurfsendungen und Telefonmarketing weiter aus. Auf Grundlage der zuletzt genannten Änderung können Direktmarketingbetreiber nun auf Anschriften zurückgreifen, die in Nutzerverzeichnissen enthalten sind, ohne dafür vorher die Einwilligung der Nutzer einholen zu müssen – vorausgesetzt, dass die Nutzer sich nicht durch Eintragung ihrer Telefonnummer und Anschrift in das Rücktrittsregister gegen diese Werbemaßnahme ausgesprochen haben;

- Sicherheitsdokument: Mit dem besagten Gesetz von 2011 wurde eine weitere Vereinfachung eingeführt, um Stellen, „die lediglich nicht sensible personenbezogene Daten oder sonstige sensible und Strafverfolgungsdaten verarbeiten, die sich auf die jeweiligen Mitarbeiter, einschließlich Nicht-EU-Bürger und/oder ihre Ehepartner und/oder Angehörigen, beziehen", von der Verpflichtung zur Vorlage eines sogenannten „Sicherheitsdokuments" (*Documento programmatico per la sicurezza*, DPS) bei der Datenschutzbehörde auszunehmen. Diese Verpflichtung wurde durch eine Änderung des Datenschutzgesetzes im Mai 2012 vollständig aufgehoben. Es muss daran erinnert werden, dass alle anderen Sicherheitsmaßnahmen auch weiterhin voll anwendbar sind;

- Das Gesetz von 2011 enthält weitere Änderungen, die Unternehmen und gewinnorientierte öffentliche Stellen davon ausnehmen, eine vorherige Einwilligung einzuholen, um die in Lebensläufen oder Biografien enthaltenen personenbezogenen Daten zu verarbeiten, wenn diese freiwillig von Bewerbern zugeschickt wurden, sowie um personenbezogene Daten innerhalb eines Konzerns weiterzugeben.

Haupttätigkeiten 2011:

Journalismus und Online-Informationen: Obwohl die Datenschutzbehörde anerkennt, dass die Veröffentlichung von Gerichtsprotokollen keine Einschränkung der Geheimhaltungspflicht im Rahmen der freien Meinungsäußerung darstellt, hat sie einer Website eine Unterlassungsanordnung auferlegt und somit die Verbreitung von Informationen untersagt, da diese übermäßig und für die spezifischen Informationszwecke irrelevant waren – obwohl dies auch in der gerichtlichen Anordnung zur Untersuchungshaft enthalten war.

Genetische Daten: Die allgemeine, von der Datenschutzbehörde erteilte Genehmigung der Verarbeitung genetischer Daten wurde infolge einer Stellungnahme an das italienische Gesundheitsministerium aufgewertet. In der neuen allgemeinen Genehmigung werden die gesammelten Erfahrungen sowie die Beiträge von Sachverständigen berücksichtigt; außerdem wurde sie gemäß der kürzlich erlassenen Rechtsvorschriften auch öffentlichen und privaten Vermittlungsorganisationen erteilt.

Datenverarbeitung zu wissenschaftlichen Forschungszwecken: 2011 wurde ein starker Anstieg der Genehmigungsanträge auf die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken ohne Einwilligung der betroffenen Personen verzeichnet, da es angeblich unmöglich sei, einen nennenswerten Teil der betroffenen Patienten darüber zu informieren. Die Datenschutzbehörde erteilte eine provisorische allgemeine Genehmigung und berücksichtigte dabei die häufigsten Fälle, die eine unterlassene Inkenntnissetzung der betroffenen Personen rechtfertigen würden – insbesondere wegen „ethischer Gründe“ und/oder der „Unmöglichkeit aufgrund von organisatorischen Vorkehrungen“.

Datenverarbeitung im Rahmen von Arbeitgeber-/Arbeitnehmerbeziehungen: Mehrere 2011 erlassene Beschlüsse wiesen auf die vielseitigen Situationen, in denen Arbeitgeber-/Arbeitnehmerbeziehungen entstehen können, sowie auf das Erfordernis einer sorgfältigen Erwägung der in diesem Zusammenhang genutzten personenbezogenen Daten hin. Die wichtigsten Beschlüsse betrafen die Überwachung der Internetaktivitäten von Arbeitnehmern; die Zulässigkeit von aus dem Internet bezogenen Informationen bei Disziplinarverfahren; die Nutzung von Fragebögen zur Erfassung der Charakterzüge von Arbeitnehmern; die Weitergabe von Informationen über eine angebliche Mehrfachbeschäftigung an die nationale Berufsunfähigkeitsversicherung; die Ortung von Arbeitnehmern usw.

Telemarketing: Die Datenschutzbehörde stellte klar, dass die Rolle von Unternehmen, die sich an Telemarketing-Aktivitäten beteiligen, unter Berücksichtigung der spezifischen Sachlage der Verarbeitung personenbezogener Daten festgelegt werden sollte. Prinzipiell ist der für die Datenverarbeitung Verantwortliche derjenige, in dessen Namen die Werbemaßnahmen durchgeführt werden. Dementsprechend ließ die italienische Datenschutzbehörde verlauten, dass jedes Unternehmen, das seine Werbemaßnahmen an externe Anbieter auslagert und dabei die betriebliche Kontrolle über solche Maßnahmen behält, die betreffenden Werbeagenturen, Agenten usw. offiziell als gemäß dem italienischen Datenschutzgesetz agierende Verantwortliche ernennen muss.

Unerwünschte Werbeanrufe infolge der Einrichtung eines „Rücktritts- oder Bitte-nicht-anrufen-Registers“ für Nutzer, die keine Werbeanrufe erhalten möchten, angesichts der relevanten Schwierigkeiten bei der Umsetzung;

„Stille“ Anrufe, d. h. solche Anrufe, die teilweise mehrmals am Tag erfolgen und für die es keine Schutzmechanismen und Abhilfen gibt, um der Stille am anderen Ende der Leitung zu entgehen. In diesem Zusammenhang hat die Datenschutzbehörde ein Unternehmen beauftragt, das durch ein wählerbasiertes System verschiedene Vorkehrungen und Maßnahmen implementiert, um wiederholten stillen Anrufen vorzubeugen und Anrufe derselben Nummer für mindestens 30 Tage zu unterbinden;

Unerbetene Faxe: Die Datenschutzbehörde kam zu dem Schluss, dass das italienische Datenschutzgesetz auf ein Unternehmen mit Sitz in einem Drittland anwendbar ist, das in diesem Land die personenbezogenen Daten (potenzieller) Kunden hielt und per Ferndatenverarbeitungsmechanismen exzessiv eine in Italien befindliche Datenübermittlungsausrüstung (Fax-Gateway) nutzte. Aus diesem

Grund wurden die ohne der Bereitstellung von geeigneten Informationsmeldungen und der Einholung der Einwilligung durch die Empfänger von besagtem Unternehmen verschickten Werbefaxe als rechtswidrig befunden und dementsprechend verboten.

Telefonie: Die wichtigsten Aktivitäten in diesem Bereich beziehen sich auf „Online-Nutzerverzeichnisse“: Es gingen mehrere Beschwerden gegen ein Unternehmen ein, das im Internet ein Nutzerverzeichnis veröffentlichte, das auch „vertrauliche“ Informationen enthielt. Die Datenschutzbehörde kam zu dem Schluss, dass die betreffende Verarbeitung insofern rechtswidrig ist, dass die in dem Verzeichnis enthaltenen personenbezogenen Daten nicht aus dem „Einheitlichen Telefonverzeichnis“ (Database Unico, DBU) stammten, welches laut italienischem Recht die einzig legitime Quelle für Telefonnutzerverzeichnisse ist.

Beziehungen zwischen dem Parlament und anderen Institutionen

Die Datenschutzbehörde wurde mehrmals vor parlamentarischen Ausschüssen und anderen parlamentarischen Foren zu parlamentarischen Angelegenheiten sowie im Zusammenhang mit Ermittlungsinitiativen oder vor der Verabschiedung von Gesetzentwürfen angehört. In allen Fällen wies die Datenschutzbehörde auf mögliche Folgen einer Verarbeitung personenbezogener Daten hin. Insbesondere kann dabei auf Folgendes verwiesen werden:

- Gesetzentwürfe, die Bestimmungen zur Verpflanzung von Embryonen enthalten, die in italienischen Zentren für medizinisch unterstützte Fortpflanzung gelagert werden;

- Änderungen des italienischen Datenschutzgesetzes (siehe oben); zusätzliche einschlägige Bestimmungen in der Verordnung Nr. 70/2011 (finanzielle Dringlichkeitsmaßnahmen);

- Betrieb des nationalen einheitlichen Kodierungssystems, das im Zusammenhang mit der Vergleichsstudie zur Effektivität, Qualität und Angemessenheit italienischer Gesundheitseinrichtungen genutzt wird;

- Tatsachenfeststellung in Bezug auf degenerative Erkrankungen mit besonderer gesellschaftlicher Bedeutung, insbesondere Brustkrebs, chronisch-rheumatische Erkrankungen und HIV/AIDS.

- Besonders erwähnenswert sind außerdem die von der Datenschutzbehörde in Bezug auf abgeleitetes Recht (von der Regierung initiierte Instrumente) und regionales Recht mit Auswirkungen auf den Schutz personenbezogener Daten (siehe Abschnitt 154(4) des Datenschutzgesetzes) abgegebene Stellungnahmen. Erwähnenswert seien an dieser Stelle die Stellungnahmen zu folgenden Angelegenheiten: das Register von Säugetierprothesen; eine Regulierung über die technischen Vorschriften für die Implementierung von IKT bei zivil- und strafrechtlichen Verfahren; technische Regelungen zur Identifizierung von Besitzern zertifizierter E-Mail-Konten auch über elektronische Netzwerke; die Verwaltung des Registers der Rechnungsprüfer und Wirtschaftsprüfungsunternehmen; die Leitlinien der Digit-PA [der öffentlichen Agentur zur Förderung von IKT in der öffentlichen Verwaltung] bezüglich des Katastrophenschutzes im öffentlichen Sektor; die ergänzenden Bestimmungen der italienischen Zivilprozessordnung zur Reduzierung und Vereinfachung der zivilrechtlichen Tatsachenfeststellung. Es ist jedoch darauf hinzuweisen, dass die Datenschutzbehörde in allen mit Datenschutz in Zusammenhang stehenden Fällen nicht um Rat gebeten wurde, obwohl dies gesetzlich vorgeschrieben ist.

Internationale Aktivitäten

Neben der aktiven Beteiligung an der Arbeit der Artikel-29-Datenschutzgruppe hat die italienische Datenschutzbehörde auch weiterhin die Entwicklungen der europäischen Datenschutzreform verfolgt – insbesondere durch Beteiligungen an der Future-of-Privacy-Untergruppe der WP29 zu vereinfachten Meldungsanforderungen, der Verarbeitung personenbezogener Daten und der Zusammenarbeit europäischer Datenschutzbehörden. Die italienische Datenschutzbehörde beteiligt sich außerdem an Arbeitsgruppen der OECD, die sich mit Datenschutzangelegenheiten befassen (insbesondere die Arbeitsgruppe zu Informationssicherheit und Datenschutz WPISP), sowie am Beratenden Ausschuss und Amt T-PD des Europarats (der momentan an einer Überarbeitung der Konvention Nr. 108/1981 arbeitet). Die Datenschutzbehörde ist Mitglied gemeinsamer Kontrollinstanzen, die für die Prüfung der gemeinsamen Informationssysteme (gemeinsame Kontrollinstanzen von Europol und Schengen, CIS, Eurodac-Koordinierungsgruppe) zuständig sind. Erwähnenswert seien außerdem die Aktivitäten im Zusammenhang mit der sogenannten Berlin Group (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation), in deren Rahmen die Datenschutzbehörde Mitberichterstatter des Arbeitsdokuments über das Recht auf Datenschutz und Vergessenwerden im Internet war, sowie die Beteiligung an der Diskussion beim Workshop der europäischen Datenschutzbehörden über die Bearbeitung von Fällen. Bezüglich der gerichtlichen und polizeilichen Zusammenarbeit bei Strafsachen setzte die Datenschutzbehörde ihre Aktivitäten zur Unterstützung der Arbeitsgruppe Polizei und Justiz fort – bis Letztere eingestellt wurde.

Sonstige Aktivitäten

Die Datenschutzbehörde setzte ihre Sensibilisierungsinitiativen fort und konzentrierte sich dabei insbesondere auf Jugendliche. Diesbezüglich wurden auf Ad-hoc-Basis Publikationsinitiativen zu sozialen Netzwerken, Schulen und Gesundheitswesen gestartet. Des Weiteren wurde der Wettbewerb „Privacy 2.0“ ausgerichtet. Jugendliche und neue Technologien“ ausgerichtet, der Schüler weiterführender Schulen dazu aufrief, Kurzfilme zum Thema Datenschutz zu drehen und sich somit als Drehbuchautoren, Darsteller, Regisseure usw. zu betätigen.

Organisation	Garante per la protezione dei dati personali
Vorsitz und/oder Gremium	Vorsitz: Prof. Francesco Pizetti Gremium: Giuseppe Chiaravalloti Mauro Paissan Giuseppe Fortunato
Budget	Ungefähr 8,5 Mio. EUR (von der Regierung bereitgestellt)
Personal	123
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Beschlüsse des Gremiums: etwa 540
Meldungen	1 218

Vorabprüfungen	22
Anfragen betroffener Personen	Anträge insgesamt: etwa 4 450 Auskunftsersuchen (*questiti*): 332 Im Jahr 2011 von Betroffenen eingereichte Berichte und Forderungen (*segnalazioni* und *reclami*): 4 022
Beschwerden betroffener Personen	(Durch das Datenschutzgesetz speziell geregelte formelle Beschwerden betreffend den Zugang zu personenbezogenen Daten einer Person) Rund 260
Vom Parlament bzw. der Regierung angeforderte Beratung	Stellungnahmen zu parlamentarischen Untersuchungen: 4 Stellungnahmen für Ministerien und das Amt des Premierministers: 32 Themen: Polizei, öffentliche Sicherheit: 2 Rechtsprechung: 2 E-Government und Datenbanken: 8 Aus- und Weiterbildung: 3 Beschäftigung in öffentlichen Behörden: 2 Gesundheitswesen: 6 Unternehmen: 5 Sozialhilfe: 2 Standesamt: 2
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	In der Zentrale der Datenschutzbehörde gingen im Jahr 2011 rund 32 000 Anrufe und E-Mails ein Nationale Genehmigungen für verbindliche unternehmensinterne Vorschriften: 1
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen und/oder Untersuchungen (vor Ort): etwa 450 (in 37 Fällen wurden Verstöße krimineller Natur bei den Justizbehörden zur Anzeige gebracht)
Sanktionsmaßnahmen	
Sanktionen	Etwa 400

Geldbußen	Betrag: etwa 3,1 Millionen EUR, im Namen der Datenschutzbehörde von der für Kontrollen zuständigen Finanzpolizei verhängt
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A. (im italienischen Rechtssystem sind keine Datenschutzbeauftragten vorgesehen)

B. Informationen zur Rechtsprechung

Das Verhältnis zwischen dem Recht auf Interessenverteidigung und dem Recht auf Datenschutz

Ein Urteil des Kassationsgerichts vom 8. Februar 2011 wurde viel diskutiert. Der vorliegende Fall betraf die Übermittlung – oder genauer, die rechtswidrige Verbreitung – personenbezogener Daten, die von einem Rechtsanwalt gehalten wurden, der Kundenakten selbst nach Ablauf der Aufbewahrungsfrist nicht vernichtet hatte, da er noch nicht bezahlt worden war. Die betreffenden Akten enthielten auch sensible Daten. Das Gericht entschied, dass man in diesem Fall „die tatsächlichen Merkmale des Verhältnisses zwischen Datenerfassung und dem zugrundeliegenden Zweck" berücksichtigen müsse, da die Daten zu dem Zweck, „einen Rechtsanspruch zu begründen oder geltend zu machen", erfasst wurden. Die Vorinstanz hätte jedoch der Frage nachgehen müssen, ob alle vom Anwalt gehaltenen Daten *de facto* notwendig gewesen seien, um die Ansprüche des Anwalts gegenüber seinen Kunden geltend zu machen. Kurzum: Das Kassationsgericht verwies auf den Grundsatz im Datenschutzgesetz, lediglich relevante Daten auf faire Weise und in gemäßigten Mengen zu erfassen, und bestätigte, dass sensible Daten auf keinen Fall verbreitet werden dürften (da dies das in Abschnitt 167 des Datenschutzgesetzes erwähnte Strafmaß nach sich ziehen würde).

Denselben Standpunkt vertrat das Kassationsgericht (Strafkammer) bei seinem Urteil vom 24. März 2011. Nach Ansicht der Richter sei „die Offenlegung eines aufgezeichneten Gesprächs zu anderen Zwecken als dem des Schutzes der eigenen Rechte oder der Rechte anderer" eine Straftat, die gemäß Abschnitt 167 des Datenschutzgesetzes zu ahnden sei. Im vorliegenden Fall war das Gespräch durch einen Privatdetektiv aufgezeichnet worden, dessen Stift ein Mikrofon und eine Mikrokamera enthielt, die für die anderen Parteien nicht sichtbar waren.

Was das Verhältnis zwischen dem Recht auf Informationsfreiheit im Hinblick auf die Geltendmachung von Rechtsansprüchen und der Datenschutzgesetzgebung betrifft, scheint der Standpunkt der Rechtsprechung darin zu liegen, dass das Recht auf Informationsfreiheit, wie ausdrücklich durch das entsprechende Recht vorgesehen, über Interessenkonflikten steht. Genauer gesagt, steht das Recht auf Informationsfreiheit über den Rechten Dritter auf Datenschutz, selbst wenn es sich um vertrauliche Daten handelt. Diese Sichtweise wurde von verschiedenen Verwaltungsgerichten gestützt: Regionales Verwaltungsgericht der Toskana, Urteil vom 12. Mai 2011; Regionales Verwaltungsgericht Ligurien, Urteil vom 1. Juni 2011 – bei dem entschieden wurde, dass „der Schutz des Rechts auf Datenschutz kein ausreichender Grund für eine Ablehnung der Erstellung von Dokumenten jeglicher Art ist"; Verwaltungsgericht Lombardei, Urteil vom 1. August 2011.

Überwachung am Arbeitsplatz

Mit dem Urteil vom 22. März 2011 entschied das Kassationsgericht (Kammer für Arbeitsrecht), dass für den Fall, dass in einem Unternehmen nach der Übereinkunft mit zuständigen Gewerkschaftsvertretern

audiovisuelle Geräte installiert werden, jegliche Aufzeichnungen, die das Verhalten des Mitarbeiters dokumentiert und dessen Entlassung rechtfertigt (wie z. B. Diebstahl von Unternehmenseigentum), im diesbezüglichen Gerichtsverfahren verwendet werden dürfen. Des Weiteren stellte ein Urteil des Kassationsgerichts (Strafkammer) vom 9. August 2011 klar, dass polizeiliche Aufzeichnungen innerhalb einer Gesundheitseinrichtung in einer Gerichtsverhandlung als Beweismaterial zulässig seien, da sie zeigten, dass ein Mitarbeiter die Stempeluhr manipuliert hatte. Nach Ansicht des Beklagten stehe der Arbeitsplatz einem Zuhause gleich, und demzufolge müssten audiovisuelle Aufzeichnungen von der zuständigen Justizbehörde gerechtfertigt und genehmigt werden. Das Gericht erklärte, dass der Begriff „Zuhause" sich auf eine bestimmte Beziehung zu einem Ort beziehe, an dem das Privatleben des Einzelnen auf eine Weise stattfinde, die externe Einwirkungen auf den Einzelnen unter allen Umständen verhindere. Dies treffe nicht auf eine öffentliche Stelle zu, ungeachtet dessen, ob eine solche Stelle der Arbeitsplatz des Beklagten sei. Dies sei beim Eingang einer Gesundheitseinrichtung umso weniger der Fall, da es sich dabei für alle Mitarbeiter sowie für die Patienten um einen Durchgangsbereich handele.

Datenschutz und Journalismus

Mit dem Urteil vom 28. September 2011 bestätigte das Kassationsgericht (Zivilkammer) das Urteil eines Berufungsgerichts, das ein Zuschadenkommen durch die Veröffentlichung eines Zeitungsartikels ausgeschlossen hatte, da dieser lediglich Fakten enthielt, die der Wahrheit entsprachen. Nach Ansicht des Kassationsgerichts komme die Identität eines Individuums nicht zu Schaden, wenn ein Zeitungsartikel lediglich über Fakten berichtet, die wirklich stattgefunden haben.

LETTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Eine wichtige Entwicklung des Jahres 2011 bezog sich auf eine neue Befugnis, die der lettischen Datenschutzbehörde erteilt wurde: Die Umsetzung der Richtlinie 2009/136/EG über die Pflicht zur Anzeige von Verstößen. Es wurden Änderungen des Gesetzes über elektronische Kommunikation ausgearbeitet (das seit dem 8. Juni 2011 in Kraft ist), doch diese Befugnis wurde der Datenschutzbehörde ohne zusätzliche Ressourcen auferlegt, was für die Behörde eine große Herausforderung darstellt.

Die Verarbeitung vertraulicher personenbezogener Daten wurde 2011 in den Bereichen als Priorität festgelegt, in denen auch präventive Kontrollmaßnahmen vorhanden sind (z. B. in Bezug auf die Verarbeitung medizinischer Daten und die Nutzung von Videoüberwachung in Krankenhäusern und speziellen Pflegeeinrichtungen). 30 % aller Vorabprüfungen wurden im Zusammenhang mit der Datenverarbeitung im Gesundheitswesen durchgeführt. Folgendes ergab sich in vielen Fällen aus den Kontrollaktivitäten:

1. Es gab keine internen Verfahren für den Datenschutz, und es wurden keine Datenschutzprüfungen durchgeführt.

2. Zugangsrechte wurden nicht gemäß den Tätigkeiten der Mitarbeiter festgelegt.

3. Es gab keine Maßnahmen zur Kontrolle der Zugangsrechte.

Die Arbeit der Datenschutzbeauftragten wurde ebenfalls überwacht, da die Anzahl der Beauftragten in Lettland tendenziell steigt. Als Alternative zu Meldungen können Verantwortliche seit 2007 Datenschutzbeauftragte ernennen. Bezüglich der Arbeit der Datenschutzbeauftragten wurden keine nennenswerten Schwachstellen festgestellt. Ende 2011 hatten 40 Personen die Prüfung der Datenschutzbehörde bestanden und die Zertifizierung zum Datenschutzbeauftragten erhalten.

In Bezug auf die Sensibilisierung der Öffentlichkeit wurde eine Empfehlung zum Schutz der Daten von Kindern abgegeben. Diese Empfehlung fand bei den Mitarbeitern von Schulen und Vorschulen breite Anwendung. Die Datenschutzbehörde hielt mehrere Seminare für Lehrer, Schulleiter und andere Verwaltungsmitarbeiter zu Angelegenheiten rund um den Schutz personenbezogener Daten, wobei der Schutz der Daten sowohl von Schülern als auch von schulischen Mitarbeitern behandelt wurde. Die Zielgruppe hat bestätigt, dass solche praktischen Empfehlungen sehr hilfreich sind.

Maßnahmen zur Bewusstseinsbildung in der Öffentlichkeit wurden darüber hinaus in Zusammenarbeit mit anderen staatlichen Institutionen (wie z. B. CERT.LV) durchgeführt, um über Datenschutzfragen aufzuklären. Dies soll 2012 fortgesetzt werden.

Organisation	Datenschutzbehörde
Leiterin	Signe Plūmiņa
Budget	266 907 LVL (ungefähr 368 656,08 EUR)
Personal	19 (einschließlich Verwaltungs- und Wartungspersonal)
Allgemeine Aktivitäten	

Beschlüsse, Stellungnahmen, Empfehlungen	1 Empfehlung. Zu Beschlüssen und Stellungnahmen liegen keine Statistiken vor. Stellungnahmen werden regelmäßig bzgl. Gesetzentwürfen herausgegeben.
Meldungen	650.
Vorabprüfungen	Statistiken werden ab 2012 zur Verfügung stehen.
Anfragen betroffener Personen	
Beschwerden betroffener Personen	254
Vom Parlament bzw. der Regierung angeforderte Beratung	Regelmäßig bzgl. der Umsetzung bestimmter Rechtsakte und Probleme zu Datenschutzfragen.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	290 Untersuchungen.
Sanktionsmaßnahmen	
Sanktionen	Es wurden sowohl Verwarnungen ausgesprochen als auch Geldbußen verhängt.
Geldbußen	Der Betrag belief sich auf 23 100 LVL (31 906,08 EUR). Geldbußen wurden sowohl für Rechtswidrigkeiten als auch für die versäumte Bereitstellung von Informationen an die Datenschutzbehörde verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	40

B. Informationen zur Rechtsprechung

Die wirtschaftliche Situation des Landes hatte Auswirkungen auf die Beschwerden, die bei der Datenschutzbehörde in Zusammenhang mit der Verarbeitung personenbezogener Daten eingingen. Die Beschwerden bezogen sich hauptsächlich auf Folgendes:

1. Daten über Arbeitnehmer ohne offizielles Beschäftigungsverhältnis, die Arbeitgeber der staatlichen Steuerbehörde bereitgestellt haben (wodurch die betroffenen Personen keine Sozialleistungen vom Staat empfangen konnten, da lediglich ein Beschäftigungsverhältnis bestand, von dem man nichts wusste).

2. Die Verarbeitung personenbezogener Daten im Rahmen von Inkassoverfahren.

3. Die Verarbeitung personenbezogener Daten im Rahmen von Videoüberwachung;

4. Die rechtswidrige Veröffentlichung personenbezogener Daten im Internet.

LITAUEN

A: Zusammenfassung der Aktivitäten und Neuerungen

Die Änderung und Ergänzung des Gesetzes über elektronische Kommunikation (Amtsblatt 2004/69-2382) (nachfolgend „LEC“) trat am 1. August 2011 in Kraft und setzte die Bestimmungen der Datenschutzrichtlinie für elektronische Kommunikation in litauisches Recht um.

Am 4. Mai 2011 nahm die Regierung der Republik Litauen den Beschluss Nr. 522 „Zur Umsetzung des Beschlusses 2009/917/JI des Rates vom 30. November 2009 über den Einsatz von Informationstechnologie im Zollbereich“ an. Gemäß Artikel 1.2 dieses Beschlusses wurde die litauische Datenschutzbehörde (nachfolgend „SDPI“) zur Aufsichtsbehörde für die unabhängige Aufsicht der in das Zollinformationssystem eingegebenen Daten ernannt.

Am 9. November 2011 nahm die Regierung der Republik Litauen den Beschluss Nr. 1324 „Zur Genehmigung des Verfahrens für den grenzüberschreitenden Austausch von DNA-Daten, daktyloskopischen Daten, Daten von Fahrzeugen und deren Besitzer und Eigentümer sowie Informationen bezüglich großflächiger, grenzüberschreitender Ereignisse oder Terrorismusbekämpfung“ an, woraufhin der SDPI die Verantwortung für die Überprüfung der Rechtmäßigkeit von Offenlegungen und Zusendungen personenbezogener Daten übertragen wurde.

Am 17. Juni 2011 gab der Leiter der SDPI eine Anweisung „Zur Genehmigung des Verfahrens zur Umsetzung des Rechts auf Zugang zu personenbezogenen Daten betroffener Personen durch die litauische Datenschutzbehörde sowie der Berichtigung, Löschung oder Sperrung solcher Daten“, die das Gesetz zum Schutz personenbezogener Daten umsetzt, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.

Am 22. Juli 2011 gab der Leiter der SDPI eine Anweisung „Zur Genehmigung der Verfahren zur Meldung von Verstößen gegen den Schutz personenbezogener Daten“ heraus. Durch diese Anweisung wurden das Verfahren zur Meldung von Verstößen gegen den Schutz personenbezogener Daten und das Formular zur Meldung von Verstößen gegen den Datenschutz genehmigt, die diesbezüglich Leitlinien enthalten. Darüber hinaus wurden zahlreiche Seminare für Dienstleistungsanbieter veranstaltet.

Die SDPI, das Justizministerium und das Ministerium für Verkehr und Kommunikation starteten auf Websites von Regierungsinstitutionen und Kommunen eine Initiative zur praktischen Umsetzung der Anforderungen der Datenschutzrichtlinie für elektronische Kommunikation und Cookies. Außerdem wurden von der SDPI Diskussionen zur Abgabe von Empfehlungen vorbereitet.

Am 27. Januar 2011 wurde der Europäische Datenschutztag gefeiert. Im Seimas der Republik Litauen fanden eine Pressekonferenz und Aktivitäten zum Thema „Datenschutz im Cyberspace“ statt. Am 10. Februar 2011 wurde der Datenschutztag an der Universität Vilnius begangen. Ziel des Tages war es, auf die Bedrohungen für personenbezogene Daten bei der Datenverarbeitung im Cyberspace (soziale Netzwerke, Google, Kredite über das Internet und weitere elektronische Kanäle) aufmerksam zu machen. Die Hauptzielgruppe bestand aus Studierenden und Schülern weiterführender Schulen.

Die SDPI organisierte gemeinsam mit der Aktiengesellschaft Expozona die Konferenz „Datenschutz in Litauen: Neuerungen, Probleme und Perspektiven“, die am 19. Mai 2011 stattfand. Die Veranstaltung handelte vom Einsatz von Technologien und der Bereitstellung von Registerdaten und richtete sich an Unternehmen, Institutionen und Organisationen, Manager, Anwälte sowie an Fachkräfte für die Verarbeitung von Mitarbeiter- und Kundendaten.

Darüber hinaus organisierte die SDPI gemeinsam mit der Aktiengesellschaft Expozona die Konferenz „Datenschutz in Litauen: Neuerungen, Probleme und Perspektiven“, die am 24. November 2011 stattfand. Diesmal konzentrierte sich die Veranstaltung auf die rechtlichen Aspekte des Schutzes personenbezogener Daten und präsentierte Änderungen des Gesetzes über den rechtlichen Schutz personenbezogener Daten in der Republik Litauen sowie wichtige Gerichtsurteile, Diskussionen der Probleme der Justiz und weitere Angelegenheiten.

Organisation	
Vorsitz und/oder Gremium	Dr. Algirdas Kunčinas
Budget	Zugewiesen und ausgegeben: 1 881 Millionen LTL (546 484 EUR)
Personal	30
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	k. A.
Meldungen	998
Vorabprüfungen	257
Anträge von Bürgern	14
Beschwerden von Bürgern	256
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	3 356 Konsultationen; 88 öffentliche Mitteilungen; 6 Zusammenfassungen der Ergebnisse der Untersuchungen von Beschwerden und der Rechtsprechung; 5 Anträge betreffend die Verarbeitung von Daten im C.SIS; 63 Schlussfolgerungen zu Dokumenten der EU und des Europarates; 82 Antworten auf Anfragen von Parteien im Zusammenhang mit dem Übereinkommen (ETS Nr. 108); 234 koordinierte Rechtsakte und Dokumente von für die Datenverarbeitung Verantwortlichen; 6 vorbereitete Rechtsakte.
Prüfmaßnahmen	
Prüfungen	43 (Zulässigkeit der Speicherung von Internetverbindungsdaten bei der Bereitstellung von Internetdiensten, Zulässigkeit der Verarbeitung von Daten, Umfang von Internet-Shops und die Rechte von betroffenen Personen).
Sanktionsmaßnahmen	
Sanktionen	Die SDPI erstellte 24 Protokolle zu Verwaltungsverstößen.
Geldbußen	k. A.

Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Verarbeitung der personenbezogenen Daten eines Schuldners

Die SDPI erhielt eine Beschwerde bezüglich eines Inkassounternehmens, das die personenbezogenen Daten des Beschwerdeführers vom ursprünglichen Gläubiger einer Abtretungsvereinbarung erhalten hatte und diese Daten rechtswidrig an die konsolidierte Datei des Schuldners übermittelte. Die SDPI kam zu dem Schluss, dass der Beschwerdeführer die Schuld nicht aus zwingenden Gründen angefochten habe und dessen personenbezogene Daten rechtmäßig an die konsolidierte Datei des Schuldners übermittelt wurden. Der Beschwerdeführer legte am Bezirksverwaltungsgericht Vilnius gegen den Beschluss der SDPI Berufung ein und begründete dies damit, dass die SDPI nicht genauer darauf eingegangen sei, weshalb die Anfechtung des Beschwerdeführers nicht aus zwingenden Gründen erfolgt sei. Das Verwaltungsgericht Vilnius hob den Beschluss des SDPI auf und wies die SDPI an, den Fall erneut zu untersuchen. Die SDPI legte beim Obersten Verwaltungsgericht gegen dieses Urteil Berufung ein.

Das Oberste Verwaltungsgericht (nachfolgend „Gericht“) befand, dass das Gesetz über den rechtlichen Schutz personenbezogener Daten der Republik Litauen (nachfolgend „LLPPD“) keine Definition des Begriffs „aus zwingenden Gründen“ enthalte und es demnach keinen Grund gebe, dass eine Person, die eine Schuld einmal angefochten habe, dies regelmäßig wiederholen müsse. Andernfalls könnten ihre Daten nach mehreren schriftlichen Mahnungen des für die Datenverarbeitung Verantwortlichen 30 Tage nach der letzten Mahnung an die konsolidierte Datei des Schuldners übermittelt werden (Artikel 21, Absatz 2.3 des LLPPD). Bei dem Beschluss, wie der Begriff „aus zwingenden Gründe“ auszulegen sei, berücksichtigte das Gericht zahlreiche Aspekte, darunter die Frage, ob die betroffene Person den für die Datenverarbeitung Verantwortlichen, in diesem Fall den Gläubiger, in Bezug auf die Würdigung des Beweismaterials, das dieser Entscheidung zugrunde liegt, angemessen angefochten hat. Aufgrund der fehlenden Einigung kann eine Partei keine Entscheidung treffen, die für die andere Partei verbindlich ist. Das Berufungsgesuch der SDPI wurde abgewiesen und das Urteil des Bezirksverwaltungsgerichts Vilnius unverändert beibehalten.

LUXEMBURG

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetzesänderungen

Das Gesetz vom 28. Juli 2011 setzt durch eine Änderung des Gesetzes vom 30. Mai 2005 zu speziellen Regelungen für den Datenschutz im Sektor für elektronische Kommunikation die Bestimmungen der Richtlinie 2009/136/EG in luxemburgisches Recht um. Es umfasst eine Definition des Begriffs „Verstoß gegen den Datenschutz" sowie eine diesbezügliche Meldepflicht, die eine Benachrichtigung der Datenschutzbehörde und der betroffenen Personen vorsieht, falls Letztere durch den Verstoß in Mitleidenschaft gezogen werden. Eine wichtige Entwicklung des luxemburgischen Rechts ist das Recht, dem für die Datenverarbeitung Verantwortlichen bei wiederholten Verstößen gegen den Datenschutz ein Bußgeld aufzuerlegen. Das Gesetz enthält außerdem einige geringfügige Änderungen des Gesetzes von 2005 sowie das abgeänderte Gesetz vom 2. August 2002.

Wichtige Themen

Die *Commission nationale pour la protection des données (CNPD)* hat der luxemburgischen Regierung 2011 zu vielen verschiedenen, die Gesetzgebung betreffenden Themen Ratschläge erteilt. Der wichtigste bezog sich auf den Gesetzentwurf zur Einrichtung einer nationalen Schülerdatenbank durch das Bildungsministerium. Die luxemburgische Datenschutzbehörde hat seine Zusammenarbeit mit verschiedenen Ministerien und der öffentlichen Verwaltung an einer Reihe von Projekten fortgesetzt, die Auswirkungen auf den Datenschutz haben, wie z. B. elektronische Krankenakten, die Reform des Strafregisters, die Einführung einer biometrischen Aufenthaltsgenehmigung und die Europäische Bürgerinitiative.

Neuerungen

Die CNPD und das „Interdisciplinary Centre for Security, Reliability and Trust (SnT)" der Universität Luxemburg haben eine Übereinkunft im Hinblick auf eine strategische Partnerschaft getroffen. Das gemeinsame Forschungsprogramm umfasst drei Hauptbereiche: neue Entwicklungen des europäischen Datenschutzrechts, neue technologische Herausforderungen, wie z.B. Cloud-Computing und dessen Auswirkungen auf den Standort Luxemburg, sowie das Konzept des eingebauten Datenschutzes („Privacy by Design").

Wichtige Veranstaltungen und Sensibilisierung

Die CNPD feierte den Europäischen Datenschutztag mit der Organisation der Konferenz „Keine Privatsphäre mehr im Netz?" mit Alexander Dix (Berliner Beauftragter für Datenschutz und Informationsfreiheit). Richard Allan von Facebook nahm ebenfalls an dieser Konferenz teil, auf die eine Diskussionsrunde mit Vertretern aus der Politik und dem Bereich Jugendschutz folgte. Neben dieser Veranstaltung, die für die breite Öffentlichkeit ausgerichtet wurde, nahm die CNPD außerdem an zahlreichen Seminaren und Schulungen teil, um auch das Fachpublikum auf das Thema Datenschutz aufmerksam zu machen.

Organisation	Commission nationale pour la protection des données (CNPD)
Vorsitz und/oder Gremium	Herr Gérard Lommel – Präsident Herr Thierry Lallemang – Beauftragter Herr Pierre Weimerskich – Beauftragter
Budget	1 494 000 EUR
Personal	Gremium: 3 Rechtsabteilung: 4 Meldungen und Vorabprüfungen: 2 Allgemeine Verwaltung: 3 Kommunikation und Dokumentation: 1 Gesamt: 13
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	492
Meldungen	401
Vorabprüfungen	429
Anfragen betroffener Personen	314
Beschwerden betroffener Personen	115
Vom Parlament bzw. der Regierung angeforderte Beratung	14
Treffen und Konsultationen (öffentlicher/privater Sektor)	140
Informationssitzungen und Konferenzen	15
Verbindliche unternehmensinterne Vorschriften als leitende Datenschutzbehörde	2
Prüfmaßnahmen	
Prüfungen	17

Sanktionsmaßnahmen	
Sanktionen	0
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Im Laufe des Jahres 2011 ernannte DPO: 10 (Zum Zeitpunkt der Erstellung des Berichts) insgesamt ernannte DPO: 48

B. Informationen zur Rechtsprechung

Zivil- und strafrechtliche Rechtsprechung

Berufungsgericht Luxemburg (8. Kammer für Arbeitsrecht) zur Verhältnis- und Rechtmäßigkeit der Überwachung eines Mitarbeiters am Arbeitsplatz, 3. März 2011

Ein Mitarbeiter wurde des unlauteren Wettbewerbs bezichtigt. Er wurde mit der Begründung entlassen, es sei ein Dokument auf seinem Computer und dem eines weiteren Mitarbeiters gefunden worden, das den Plan enthalten habe, ein Konkurrenzunternehmen zu gründen. Dieses Dokument wurde von einem privaten E-Mail-Account des entlassenen Mitarbeiters an den private E-Mail-Account seines Kollegen geschickt, jedoch auf dem Rechner des Arbeitgebers gespeichert. Das Berufungsgericht befand, dass das Abfangen und die Übermittlung dieses Dokuments keinen Verstoß gegen das Briefgeheimnis darstelle. Das Gericht berücksichtigte die Tatsache, dass die besagte E-Mail an mehrere Mitarbeiter adressiert war und keine Angaben dazu enthielt, dass der Inhalt vertraulich oder schutzwürdig sei.

MALTA

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Berichtszeitraum ergriff die Datenschutzbehörde Rechtsmaßnahmen zur Einführung von Änderungen der nachgeordneten Rechtsvorschrift 440.01, welche die Verarbeitung personenbezogener Daten im Sektor für elektronische Kommunikation regelt. Diese Änderungen waren für die Umsetzung der Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 u. a. zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation erforderlich.

Eingeführt wurden die Änderungen aufgrund des im Amtsblatt vom 24. Juni 2011 veröffentlichten rechtlichen Hinweises 239/2011. Die Vorschrift soll 2012 in Kraft treten und wird außerdem durch eine Reihe von Leitlinien ergänzt, welche die für die Datenverarbeitung Verantwortlichen mit den nötigen Informationen zur Umsetzung der neuen Anforderungen, insbesondere zur Meldung von Verstößen gegen den Datenschutz und den Einsatz von Cookies, ausstatten.

Verantwortliche stellten Anträge auf Vorabprüfungen bezüglich der Einführung biometrischer Systeme und der Installation von Überwachungskamerasystemen am Arbeitsplatz und auch in anderen Bereichen, in denen die Verarbeitung von Daten besondere Risiken von Verstößen gegen die Rechte und Freiheiten der betroffenen Personen gemäß Artikel 34 des Datenschutzgesetzes birgt. Auf einen Antrag des Ministeriums für auswärtige Angelegenheiten bezüglich der Verarbeitung biometrischer Daten im Rahmen des neuen VIS beurteilte die Datenschutzbehörde die einschlägigen Auswirkungen auf den Datenschutz, bevor ähnliche, durch die Verordnungen 767/2001/EG und 810/2009/EG vorgesehene Verarbeitungen genehmigt wurden. Diese Beurteilung erfolgte im Rahmen einer Sitzung mit Interessenvertretern sowie von zwei Vor-Ort-Beurteilungen zur Untersuchung der Funktionalitäten des Systems und zur Implementierung der nationalen Komponente.

Im November führte die Datenschutzbehörde zwei Vor-Ort-Prüfungen in den maltesischen Konsulaten in Moskau (Russland) und Kairo (Ägypten) durch. Der Zweck der beiden Prüfungen war die Beurteilung der Verarbeitung personenbezogener Daten durch beide Ämter bei der Ausstellung von Visa für Drittstaatsangehörige. Darüber hinaus sollten dabei bestimmte etablierte Verfahren im Hinblick auf die Anforderungen des Datenschutzgesetzes und weiterer Rechtsinstrumente überprüft werden. Mitarbeiter der Datenschutzbehörde nahmen an einer Schulung zur Sensibilisierung in Sachen Datenschutz teil, die auf die Rechte, die Bürgern gemäß dem Datenschutzgesetz zustehen, sowie auf die relativen VIS-Regulierungen und das Schengen-Abkommen in Bezug auf die Ausstellung von Visa aufmerksam machte.

Am 28. Januar feierte die maltesische Datenschutzbehörde gemeinsam mit anderen Datenschutzbehörden aus aller Welt den Datenschutztag. Auf regionaler Ebene verteilte die Behörde zur Feier des Tages Informationsmaterial und Schreibwarenartikel an die Schüler aller staatlichen, privaten und kirchlichen Schulen. Die Datenschutzbehörde ist seit jeder fest davon überzeugt, dass fortlaufend in Bildung investiert und die junge Generation sensibilisiert werden müsse, um einen effektiven kulturellen Austausch zu ermöglichen.

Mit der zunehmenden Verfügbarkeit von Anwendungen zur sozialen Vernetzung und der damit einhergehenden Verwässerung der Grenzen der Privatsphäre wollte die Datenschutzbehörde durch diese Aktion ein Zeichen setzen und auf die Datenschutzrisiken aufmerksam machen, denen betroffene Personen im Internet begegnen. Die diesjährige Botschaft bezog sich auf die Nutzung des Internets und die Notwendigkeit, über potenzielle Datenschutzrisiken, denen personenbezogene Daten von Einzelpersonen bei der Veröffentlichung im Internet ausgesetzt sein können, Bescheid zu wissen. Die

Datenschutzbehörde wies nachdrücklich darauf hin, dass die Identität betroffener Personen wertvoll und deren Schutz daher unerlässlich sei.

Zu weiteren Sensibilisierungsmaßnahmen der Datenschutzbehörde im Berichtszeitraum gehörten Vorträge vor verschiedenen Verantwortlichen aus verschiedenen Bereichen der maltesischen Gesellschaft, die Teilnahme an regionalen Fernseh- und Radioprogrammen mit telefonischen Zuschaltungen sowie die regelmäßige Aktualisierung des Portals der Datenschutzbehörde mit den neuesten Entwicklungen im Bereich des Datenschutzes. Die Datenschutzbehörde ist fest davon überzeugt, dass eine Aufklärung durch die Medien eine wirkungsvolle Methode darstellt, um die breite Öffentlichkeit auf ihre Belange aufmerksam zu machen.

Organisation	
Vorsitz und/oder Gremium	Informations- und Datenschutzbeauftragter
Budget	Ungefähr 300 000 EUR
Personal	Beauftragter – 1 Fachpersonal – 3 Technische Unterstützung – 2 Administrative Unterstützung – 3
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Hinsichtlich der beim Datenschutzbeauftragten eingegangenen Beschwerden wurden 38 Beschlüsse veröffentlicht. Darüber hinaus wurden 26 Stellungnahmen/Empfehlungen herausgegeben. Hierbei handelte es sich um Stellungnahmen in Form von Zeitungsartikeln, die sich sowohl an die Allgemeinheit als auch an für die Datenverarbeitung Verantwortliche richteten, sowie um sonstige Stellungnahmen/Empfehlungen, die den für die Datenverarbeitung Verantwortlichen zu spezifischen Themen bereitgestellt wurden.
Meldungen	154 neue Meldungen
Vorabprüfungen	5 Anträge auf Vorabprüfung
Anfragen betroffener Personen	Anfragen per Telefon – durchschnittlich 7 Anrufe pro Tag Anfragen per E-Mail – 135
Beschwerden betroffener Personen	70 Beschwerden
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.

Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	17 Prüfungen wurden in Bezug auf Untersuchung von Beschwerden betroffener Personen, die maltesische Konsularvertretung im Ausland sowie Strafverfolgungsbehörden im Rahmen koordinierter Übungen der gemeinsamen Kontrollinstanz durchgeführt.
Sanktionsmaßnahmen	
Sanktionen	Gerichtsverfahren gegen einen für die Verarbeitung Verantwortlichen, der den Anordnungen des Datenschutzbeauftragten nicht Folge geleistet hat.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Es wurden 15 Datenschutzbeauftragte ernannt.

B. Informationen zur Rechtsprechung

Im Berichtszeitraum gab es keine neue Rechtsprechung.

NIEDERLANDE

A: Zusammenfassung der Aktivitäten und Neuerungen

Die niederländische Datenschutzbehörde überwacht die Einhaltung der Vorschriften zum Schutz personenbezogener Daten. Die niederländische Datenschutzbehörde konzentriert sich im Allgemeinen auf die strategische Durchsetzung, um eine bessere Einhaltung zu gewährleisten. Falls nötig, werden Sanktionen verhängt.

Die Prioritäten werden auf der Grundlage einer fortlaufenden Risikoeinschätzung festgelegt, für die Signale aus verschiedenen Quellen innerhalb der Gesellschaft, wie z. B. Telefonanrufe, E-Mails oder Medienberichte, eingesetzt werden. 2011 wurde ein neues Signalregistrierungssystem eingeführt, das eine Erfassung von Signalen nach Sektoren ermöglicht. Die Risikoeinschätzung berücksichtigt die Schwere des mutmaßlichen Vergehens, die Anzahl der Betroffenen, die Eindeutigkeit des Verstoßes und die rechtliche Umsetzbarkeit einer Durchsetzungsmaßnahme. Des Weiteren werden die Auswirkungen des großflächigen Einsatzes neuer Technologien berücksichtigt. Die Schwerpunkte der niederländischen Datenschutzbehörde lagen 2011 u. a. auf folgenden Bereichen: Einwilligung, Datenschutz, Zweckbindung und Aufbewahrungsfristen.

Ein Beispiel für die zahlreichen Untersuchungen, die die Datenschutzbehörde 2011 durchgeführt hat, ist der Umgang mit Jugendkriminalität in sogenannten *Veiligheidshuizen,*[12] auf denen Strafverfolgungs- und Sozialbehörden zusammenarbeiten, um kriminelles Verhalten zu vermeiden und zu unterbinden. Die Untersuchung hat ergeben, dass alle beteiligten Parteien die personenbezogenen Daten von Kindern unter zwölf Jahren erfassten und bei regulären Treffen untereinander austauschten. Die *Veiligheidshuizen* waren jedoch nicht in der Lage zu zeigen, nach welchen Kriterien die personenbezogenen Daten ausgetauscht wurden. Darüber hinaus war der Austausch der Daten nicht mit dem Zweck der regulären Treffen vereinbar und stand daher im Widerspruch mit der Rechtslage. Während der Durchsetzungsphase der Überprüfung durch die niederländische Datenschutzbehörde änderten die *Veiligheidshuizen* ihre Strategien und setzten bei den Treffen Kriterien für den Austausch personenbezogener Daten auf.

Die niederländische Datenschutzbehörde überprüfte außerdem die folgenden Datenverarbeitungsaktivitäten:

- Den Austausch personenbezogener Daten von Studierenden (z. B.: Geburtsland und Ethnie);
- Die Verlinkung personenbezogener Daten ohne die Genehmigung des sozialen Informations- und Suchdienstes;
- Den Austausch personenbezogener Daten durch die niederländische Steuerbehörde mit rund 900 Help- und Informationsdesks, ohne dabei die Genehmigung der anfragenden Institution zu prüfen;
- Die Erfassung von WLAN-Daten durch Google-Street-View-Fahrzeuge;
- Die Erfassung der Standortdaten von Kunden durch TomTom.

Einige Situationen erforderten Durchsetzungsmaßnahmen vonseiten der Datenschutzbehörde, wie z. B. im Falle des zu Rotterdam gehörenden Bezirks Charlois, der Daten über die Ethnie oder Rasse minderjähriger

[12] *Veiligheidshuizen* sind Plattformen, auf denen die Polizei, der Staatsanwalt und das Kinder- und Jugendamt zusammenarbeiten, um der Rückfälligkeit von Jugendstraftätern vorzubeugen.

Minderheitsgruppierungen erfasste. Die niederländische Datenschutzbehörde verhängte eine bedingte Geldbuße, um eine Verarbeitung solcher personenbezogenen Daten zu unterbinden. Charlois legte Berufung ein. Ein weiteres Beispiel ist das Versprechen der niederländischen Bahn und Trans Link Systems – dem Herausgeber von Chipkarten für öffentliche Verkehrsmittel – von kürzeren Aufbewahrungsfristen für die Reisedaten von Schülern. Dies hätte bis spätestens Mai 2012 geschehen sollen. Als die Frist für die Einführung kürzerer Aufbewahrungsfristen tatenlos verstrichen war, verhängte die niederländische Datenschutzbehörde im Juli 2012 eine Geldbuße über die niederländische Bahn.

Neben den Untersuchungen berät die niederländische Datenschutzbehörde die Regierung im Hinblick auf Gesetzentwürfe, bevor diese dem Parlament vorgelegt werden. Auf die Ratschläge der niederländischen Datenschutzbehörde hin werden die Entwürfe (manchmal) abgeändert, um Verstößen gegen das Datenschutzgesetz vorzubeugen. U. a. der Minister für Sicherheit und Justiz hat die niederländische Datenschutzbehörde bezüglich der Einführung eines Systems, das dafür sorgt, dass die Telefonnummern von Anwälten nicht erkannt und demzufolge Gespräche nicht abgehört werden können, um Rat gebeten. Die niederländische Datenschutzbehörde begrüßte die Einführung eines solchen Systems, um das Anwaltsgeheimnis zu schützen, riet jedoch dazu, Klarstellungen und Spezifikationen hinzuzunehmen.

Organisation	Niederländische Datenschutzbehörde
Vorsitz und/oder Gremium	Jacob Kohnstamm, Vorsitzender Madeleine McLaggan, Mitglied des Gremiums; stellvertretende Vorsitzende Jannette Beuving, Mitglied des Gremiums (bis zum 1. September 2011) Wilbert Tomesen, Mitglied des Gremiums (ab dem 1. Dezember 2011)
Budget	Zugewiesen: 7 631 000 EUR Ausgegeben: 7 731 000 EUR
Personal	80,5 Vollzeitbeschäftigte (83 Angestellte)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	298 (Untersuchungen, Leitlinien, Verhaltensregeln, Vorabprüfungen, Sanktionen und Beratung zu Gesetzgebungsverfahren)
Meldungen	3 939
Vorabprüfungen	170
Signale[13] betroffener Personen	Der Datenschutzbehörde über die Website signalisierte Fälle: k. A. Eingehende E-Mails: k. A.

[13] Seit April 2011 werden alle Bürgerkontakte als Signale registriert. Diese Signale dienen der Priorisierung unserer Aufgaben. Demnach werden Signale nicht anhand des Eingangsdatums, sondern anhand von Sektoren registriert.

	Eingehende Anrufe: k. A. Von all diesen eingegangenen Signalen traten die Sektoren Handel und Dienstleistungen (1 871), öffentliche Verwaltung (954) sowie Gesundheit und Pflege (686) besonders hervor.
Signale betroffener Personen –gesamt–	Anzahl der bearbeiteten berechtigten Signale: 5 790
Vom Parlament bzw. der Regierung angeforderte Beratung	35
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	85
Sanktionsmaßnahmen	
Sanktionen	6
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Der Datenschutzbehörde wurden 264 DPO gemeldet (Stand: 8. August 2012)

B: Informationen zur Rechtsprechung

Berechtigtes Interesse; Verhältnismäßigkeit und Subsidiarität

Das Büro für Kreditregistrierung (Bureau Krediet Registratie, BKR) registriert Verbraucherkredite. Das BKR pflegt Datenbanken mit den personenbezogenen Daten von Verbrauchern, zu denen u. a. Name, Anschrift und die Höhe der Schulden und Kredite zählen. Diese Datenbanken des BKR sind all seinen Mitgliedern zugänglich.

Im vorliegenden Fall stand von Herrn X eine überfällige Rate seines Kredits bei der Santander Bank aus. Selbst nach der Tilgung des Kredits war Herr X weiterhin bei der BKR als Schuldner registriert. Herr X stellte beim BKR einen Antrag auf Löschung seiner personenbezogenen Daten, der jedoch abgelehnt wurde.

Herr X zog vor Gericht, um die Löschung seiner personenbezogenen Daten aus dem BKR-System durchzusetzen. Im vorliegenden Fall kam der Oberste Gerichtshof der Niederlande zu dem Urteil, dass die Verarbeitung personenbezogener Daten nur dann zulässig sei, wenn dies rechtlich und ausdrücklich festgelegt sei und ein berechtigtes Interesse bestehe. Des Weiteren fügte der Oberste Gerichtshof diesen Kriterien ergänzend hinzu, dass im Falle einer rechtlich zulässigen Verarbeitung personenbezogener Daten

aufgrund eines berechtigten Interesses individuell abgewogen werden solle, ob eine Verarbeitung dieser Daten notwendig sei, um ein berechtigtes Interesse zu erreichen. Im vorliegenden Fall entschied der Oberste Gerichtshof, dass kein legitimes Interesse mehr daran bestehe, Herrn X als Schuldner zu registrieren, nachdem er seinen Kredit zurückgezahlt hat. Demnach mussten die personenbezogenen Daten von Herrn X aus der Datenbank gelöscht werden.

Der Oberste Gerichtshof verweist außerdem auf Artikel 8 der Europäischen Menschenrechtskonvention. Eine Datenverarbeitung sei in diesem Zusammenhang nur dann erlaubt, wenn die Interessen der betroffenen Person im Verhältnis zu den verfolgten Interessen nicht unverhältnismäßig verletzt würden (Verhältnismäßigkeit) und der Zweck nicht auf andere Weise erfüllt werden könne (Subsidiarität). Im vorliegenden Fall seien die Interessen der betroffenen Person unverhältnismäßig verletzt worden.

ÖSTERREICH

A. Neue Entwicklungen und Aktivitäten

Im Berichtszeitraum wurde die Regierungsvorlage einer **Verwaltungsgerichtsbarkeits-Novelle 2012** beschlossen.[14] Diese Novelle sieht vor, dass bestimmte weisungsfreie Verwaltungsbehörden (darunter auch die Datenschutzkommission) mit Ende 2013 aufgelöst werden, wobei deren rechtsprechende Tätigkeit auf neu zu schaffende Verwaltungsgerichte übergehen soll. Die Datenschutzkommission hat sich wiederholt kritisch zum Vorhaben ihrer Auflösung geäußert. Im Fall der Auflösung der Datenschutzkommission muss schon aufgrund des Art. 28 der Richtlinie 95/46/EG eine neue Datenschutzbehörde gegründet werden, der die Aufgaben der Datenschutzkommission übertragen werden. Der ursprünglich angedachte Übergang rechtsförmlicher Entscheidungen an ein Verwaltungsgericht scheint einerseits schon im Hinblick auf die in Art. 28 der Richtlinie 95/46/EG genannten „wirksamen Eingriffsbefugnisse", andererseits auch im Hinblick auf den im Entwurf einer „Datenschutz-Grundverordnung" ablesbaren Trend zu einer Stärkung der Datenschutzbehörden und einer Vereinheitlichung der Kompetenzen der europäischen Datenschutzbehörden problematisch. Denkbar wäre ein Rechtszug von der Datenschutzbehörde an ein Verwaltungsgericht.

Im Berichtszeitraum wurde vom Bundesministerium für Gesundheit der Entwurf eines **„Elektronische Gesundheitsakte-Gesetzes" (ELGA-G)** versendet, zu dem die Datenschutzkommission eine umfangreiche Stellungnahme[15] abgegeben hat. Eine wesentliche Rolle bei der Erstellung des Gesetzesentwurfes spielte dabei das Arbeitspapier der Art. 29 Gruppe WP 131 zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA) aus dem Jahr 2007. Der Entwurf erfuhr in weiterer Folge zahlreiche Überarbeitungen.[16]

Die Datenschutzkommission hat im Berichtszeitraum an einem **Datenschutz-Twinning-Projekt in Montenegro** mitgewirkt. Im Rahmen von EU-Twinning-Projekten wird unter anderem Know How etablierter Behörden zum Auf- und Ausbau öffentlicher Strukturen in Ländern, die Beitrittskandidaten sind oder werden sollen, weitergegeben. Im gegenständlichen Fall stellten Mitglieder der Datenschutzkommission bzw. Mitarbeiter ihrer Geschäftsstelle im Rahmen von Short Term Projekten ihre Expertise zur Verfügung. Das geschäftsführende Mitglied der Datenschutzkommission übernahm in den letzten Monaten des Projekts auch die Projektleitung auf österreichischer Seite. Im Jahr 2011 fand eine „study visit" von Vertretern der montenegrinischen Datenschutzbehörde bei der Datenschutzkommission in Wien statt.

Zum **Europäischen Datenschutztag 2011** wurde – inzwischen schon einer Tradition folgend – gemeinsam mit dem Datenschutzrat und dem Bundeskanzleramt eine Veranstaltung abgehalten, die vor allem der Zukunft des Datenschutzes in Zeiten des Internets gewidmet war. Ein besonderes Thema stellte bei dieser Veranstaltung auch die Strategie der Europäischen Kommission für einen neuen Datenschutz-Rechtsrahmen dar.

Organisation	Österreichische Datenschutzkommission
Vorsitz und/oder Gremium	Vorsitz: Dr. Anton SPENLING Geschäftsführendes Mitglied: Dr. Eva SOUHRADA-KIRCHMAYER

[14] Inzwischen von Nationalrat und Bundesrat beschlossen und im BGBl I 51/2012 veröffentlicht.
[15] Siehe http://www.dsk.gv.at/DocView.axd?CobId=42793
[16] Im Oktober 2012 wurde die Regierungsvorlage eines "„ELGA-Gesetzes"" beschlossen.

	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 werden aus dem Budget des Bundeskanzleramts gedeckt.
Personal	20 Vollzeitstellen (18 Vollzeit- und vier Teilzeitbeschäftigte)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	84 formale Beschlüsse (Beschwerden), 220 Fälle für den Bürgerbeauftragten, 43 Genehmigungen (Datenübermittlung in Drittländer, Forschung und Gutachten), 155 formale Beschlüsse im Meldungsverfahren und drei formale Empfehlungen.
Meldungen	12 542
Vorabprüfungen	2 167
Anfragen betroffener Personen	Schriftlich: 1 327 Telefonisch: ca. 25 000
Beschwerden betroffener Personen	Beschwerden, denen eine formale Entscheidung folgte: 84
Vom Parlament bzw. der Regierung angeforderte Beratung	Beschwerden, denen eine Klärung oder Empfehlung folgte: 220
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Diese Aufgabe fällt in die Zuständigkeit zweier anderer Institutionen: des Datenschutzrats und der Rechtsabteilung der Regierung im Bundeskanzleramt.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	13. Die meisten Fälle stehen im Zusammenhang mit Videoüberwachung.
Sanktionsmaßnahmen	
Sanktionen	Keine. Die österreichische Datenschutzbehörde kann keine Sanktionen auferlegen.
Geldbußen	Keine. Die österreichische Datenschutzbehörde kann keine Geldbußen auferlegen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Keine. Das österreichische Recht sieht keine Datenschutzbeauftragten vor.

B. Fallrecht

Im Berichtsjahr wurde das 2010 neu aufgerollte Meldeverfahren zu **Google Street View** abgeschlossen. Die Datenschutzkommission hat die Registrierung von Google Street View verfügt und gleichzeitig drei Empfehlungen an Google Inc. ausgesprochen. Der Registerauszug und die Empfehlungen wurden am 21. April 2011 an Google Inc. zugestellt. Mit der Registrierung wurde das Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts betreffend die durch Google Inc. registrierten Datenanwendung „Google Street View" (Datenverwendung für Kartographiezwecke und zur Veröffentlichung in „Google Street View„) beendet. Google Inc. hat in diesem Verfahren die verlangten Verbesserungen der Meldung vorgenommen.

Ergänzend zu den von Google Inc. bereits im Rahmen des Meldeverfahrens bzw. Prüfverfahrens getätigten Zusagen (z.B: Unkenntlichmachung der Gesichter und Autokennzeichen vor Veröffentlichung der Daten im Internet und Information der Öffentlichkeit) sind an Google Inc. folgende Empfehlungen ergangen:

a) Bei Aufnahmen von Personen in besonders sensiblen Bereichen sind jedenfalls nicht nur die Gesichter, sondern auch die Gesamtbilder der Personen unkenntlich zu machen. Dazu zählen insbesondere die Eingangsbereiche von Kirchen, Gebetshäusern, Krankenhäusern, Frauenhäusern und Gefängnissen.

b) Bildaufnahmen privater, für einen Spaziergänger nicht einsehbarer Immobilien, wie insbesondere umzäunter Privatgärten und -höfe, sind vor einer Veröffentlichung im Internet unkenntlich zu machen.

c) Gemäß § 28 Abs. 2 DSG 2000 steht dem Betroffenen ab dem Zeitpunkt der Ermittlung der Daten ein Widerspruchsrecht zu. Um den Betroffenen auch vor Veröffentlichung der Bilddaten diese Möglichkeit zum Widerspruch gegen die Veröffentlichung von Gebäuden einzuräumen, sind geeignete Werkzeuge zur Verfügung zu stellen, die ein einfaches und unbürokratisches Geltendmachen des Widerspruchrechts ermöglichen. Auf dieses (bereits vor Veröffentlichung bestehende) Widerspruchsrecht und das Werkzeug zur Ausübung des Widerspruchsrechts ist auch auf der Website der Google Inc. hinzuweisen.

Die Empfehlungen a. und b. sind bis spätestens zur Veröffentlichung der Daten im Internet umzusetzen. Das Werkzeug sowie der Hinweis darauf gemäß Empfehlung c. sind mindestens zwölf Wochen vor Veröffentlichung der Daten im Internet zur Verfügung zu stellen.

Google hat bislang seine zuvor erhobenen Street View Daten nicht ins Internet gestellt. Soweit feststellbar, fanden auch keine weiteren Street View Fahrten in Österreich statt.

Die Datenschutzkommission hat sich im Rahmen einer Beschwerde mit der **Identitätsprüfung bei der Ausübung des Auskunftsrechts** auseinandergesetzt. Einem Auskunftswerber, der seine Identität bereits durch Übermittlung einer Ausweiskopie samt Faksimile-Wiedergabe seiner eigenhändigen Unterschrift (zusätzlich zum eigenhändig unterschriebenen Auskunftsbegehren) nachgewiesen hatte, war vom Auftraggeber aufgetragen worden, auch noch die Vornamen seiner Eltern anzugeben, um die gewünschte Auskunft zu erhalten. Die Datenschutzkommission erachtete den bereits stattgefundenen Identitätsnachweis für hinreichend. Indem der Beschwerdegegner, trotz eines erbrachten Identitätsnachweises, auf die Übermittlung der Vornamen der Eltern des Beschwerdeführers bestanden und die datenschutzrechtliche Auskunft nicht erteilt hat, hat er den Beschwerdeführer in seinem Recht auf Auskunft über eigene Daten verletzt.

POLEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Die wichtigste Veranstaltung im Zusammenhang mit den Aktivitäten des Datenschutzbeauftragten (nachfolgend „GIODO“) war das Inkrafttreten des abgeänderten Gesetzes zum Schutz personenbezogener Daten am 7. März 2011 – nach fast drei Jahren intensiver Arbeit. Die Bestimmungen, die am 7. März in Kraft traten, erteilten dem GIODO die Befugnis einer Durchsetzungsbehörde mit den folgenden Aufgaben: Verwaltungsvollstreckung immaterieller Verpflichtungen (Artikel 12 Punkt 3); das Recht, an staatliche Behörden, territoriale Selbstverwaltungsbehörden, staatliche und kommunale Organisationseinheiten, sowie an natürliche und rechtliche Personen im Hinblick auf einen effizienten Schutz personenbezogener Daten heranzutreten; sowie das Recht, zuständige Behörden aufzufordern, legislative Initiativen durchzuführen und Rechtsakte im Zusammenhang mit dem Schutz personenbezogener Daten zu verabschieden oder zu ändern. Die Stelle, die eine Aufforderung oder einen Antrag des GIODO erhält, muss innerhalb von 30 Tagen nach Erhalt schriftlich darauf reagieren. Des Weiteren wird eine Behinderung der Prüfer des GIODO mit einer Geldbuße und einer Freiheitseinschränkung von bis zu zwei Jahren geahndet.

Der GIODO war 2011 erneut am Gesetzgebungsverfahren des Gesetzentwurfs zum Austausch von Informationen unter Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union beteiligt, bei dem es sich aus der Perspektive des Datenschutzes um einen wichtigen Rechtsakt handelt. Des Weiteren wurden Stellungnahmen zum Gesetzentwurf herausgegeben. Das Gesetz wurde am 16. September 2011 verabschiedet und trat am 1. Januar 2012 in Kraft. Am Gesetz zum Austausch von Informationen unter Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union ist die Einführung von Änderungen des Gesetzes zum Schutz personenbezogener Daten hervorzuheben: Dem Artikel 43, Absatz 1 des Gesetzes zum Schutz personenbezogener Daten wurde Punkt 2c hinzugefügt, der Verantwortliche, die solche Daten verarbeiten, von der Verpflichtung zur Registrierung von Dateien mit personenbezogenen Daten ausnimmt, die von zuständigen Behörden auf der Basis der Bestimmungen zum Informationsaustausch unter Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union verarbeitet werden. Dem Artikel 26(a) Absatz 1 zur Abgabe von Beschlüssen zu Einzelfällen betroffener Personen auf Grundlage der automatischen Verarbeitung personenbezogener Daten wurde eine neue gesetzliche Bestimmung zur Gestattung solcher Maßnahmen hinzugefügt, die Maßnahmen zum Schutz des berechtigten Interesses betroffener Personen enthält. Die Abänderung von Artikel 47 Absatz 1 sieht vor, dass die Übermittlung personenbezogener Daten an Drittländer nur dann erfolgen darf, wenn das Zielland auf seinem Staatsgebiet ein angemessenes Datenschutzniveau gewährleisten kann. Gemäß dem hinzugefügten Absatz 1(a) dieses Artikels ist eine Angemessenheit des in Absatz 1 genannten Schutzniveaus unter Berücksichtigung aller Umstände einer Datenübermittlung zu beurteilen, insbesondere die Art der Daten, der Zweck und die Dauer der jeweiligen Datenverarbeitung, das Ursprungsland und das Zielland der Daten sowie die geltenden rechtlichen Vorkehrungen, Sicherheitsmaßnahmen und Standesregeln des jeweiligen Drittlandes. Absatz 2 von Artikel 47 wurde klargestellt und besagt, dass die Bestimmungen von Absatz 2 nicht gelten, falls die Übermittlung personenbezogener Daten durch einen Verantwortlichen aufgrund gesetzlicher Bestimmungen oder durch ein ratifiziertes internationales Abkommen, das ein angemessenes Schutzniveau garantiert, erfolgt.

Zu wichtigen Veranstaltungen gehören die Ernennung einer neuen Organisationseinheit der polnischen Datenschutzbehörde – die Verwaltungsvollstreckung – sowie die Festlegung der Standorte und der gebietsbezogenen Zuständigkeit lokaler Zweigstellen der Datenschutzbehörde (gemäß der Verordnung des Präsidenten der Republik Polen vom 10. Oktober 2011 in Bezug auf die Einräumung der Rechtsstellung der polnischen Datenschutzbehörde).

Organisation	Amt des Generalinspektors für den Schutz personenbezogener Daten (GIODO)
Vorsitz und/oder Gremium	Dr. Wojciech Rafał Wiewiórowski, Generalinspektor für den Schutz personenbezogener Daten
Budget	14 700 000 PLN
Personal	131
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden 1 110 Beschlüsse herausgegeben.
Meldungen	Es wurden 11 845 Dateien mit personenbezogenen Daten gemeldet.
Vorabprüfungen	Als Folge der Anmeldeverfahren (Vorabprüfungen) wurden 2 298 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.
Anfragen betroffener Personen	Es gingen 3 935 Rechtsfragen per E-Mail und per Post ein (nicht nur von betroffenen Personen, sondern auch von Personen, die Interesse an Angelegenheiten zum Thema Verarbeitung personenbezogener Daten haben). Insgesamt wurden 2 796 Stellungnahmen und Empfehlungen herausgegeben. Über die Informations-Hotline der GIODO wurden außerdem 4 118 Erklärungen bereitgestellt.
Beschwerden betroffener Personen	Beschwerden über Verletzungen des Schutzes personenbezogener Daten, unter anderem in folgenden Bereichen: • Öffentliche Verwaltung (80 Beschwerden); • Gerichte, Staatsanwaltschaft, Polizei, Gerichtsvollzieher (32 Beschwerden); • Banken und andere Finanzinstitute (94 Beschwerden); • Internet (78 Beschwerden); • Marketing (18 Beschwerden); • wohnungsbezogen (69 Beschwerden); • Sozial-, Sach- und Personenversicherungen (13

	Beschwerden); • Schengener Informationssystem (4 Beschwerden); • Telekommunikation (48 Beschwerden); • Beschäftigung (35 Beschwerden); • Sonstige (178 Beschwerden).
Vom Parlament bzw. der Regierung angeforderte Beratung	Dem GIODO wurden 592 Gesetzentwürfe zur Prüfung vorgelegt.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	55 – Anzahl der durch den GIODO durchgeführten Schulungen zu den Bestimmungen zum Schutz personenbezogener Daten, insbesondere für öffentliche Einrichtungen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	199 Prüfungen, davon 104 sektorspezifische Prüfungen und 95 Prüfungen im Zusammenhang mit Beschwerden, die gegen die Verarbeitung personenbezogener Daten und gemeldeten Dateien mit personenbezogenen Daten gerichtet waren sowie infolge einer Bereitstellung von Daten an den GIODO durch externe Stellen erhoben wurden. Sektorspezifische Prüfungen wurden in den folgenden Sektoren durchgeführt: • öffentliche Verwaltung (21 Prüfungen); • 10 Prüfungen im Zusammenhang mit der Verarbeitung personenbezogener Daten durch das SIS, das VIS und das nationale Informationssystem; • Steuer- und Finanzberatung (15 Prüfungen); • Gesundheitswesen (5 Prüfungen); • Personalvermittlung (17 Prüfungen); • Organisation von Massenveranstaltungen in Stadien (14 Inspektionen); • Betreiber öffentlicher Telekommunikationsnetzwerke und Anbieter von öffentlich verfügbaren Telekommunikationsdiensten (10 Prüfungen); • Kindererziehung (12 Prüfungen). Infolge der Prüfungen wurden 66 Verwaltungsverfahren eingeleitet, um es dem GIODO zu ermöglichen, Verwaltungsbeschlüsse

	herauszugeben und die Rechtsstaatlichkeit wiederherzustellen.
Sanktionsmaßnahmen	
Sanktionen	2011 erstattete der GIODO 10 Meldungen wegen des Verdachts auf Zuwiderhandlungen, von denen vier den Verdacht auf Zuwiderhandlungen im Zusammenhang mit der Internetnutzung betrafen. Im Vergleich zu 2010 ging die Anzahl der Meldungen um mehr als die Hälfte zurück (23 Meldungen im Jahr 2010).
Geldbußen	
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Das Urteil des Obersten Verwaltungsgerichts vom 19. Mai 2011 war für das Berichtsjahr aus Sicht der Verarbeitung personenbezogener Daten im Internetsektor von entscheidender Bedeutung. Demnach sollen gemäß Artikel 6 Absatz 1 und 2 des Datenschutzgesetzes alle Fälle, in denen die IP-Adresse eine indirekte Identifikation natürlicher Personen zulässt, als Verarbeitungen personenbezogener Daten erachtet werden. Anderweitige Interpretationen wären mit den verfassungsrechtlichen Bestimmungen der Artikel 30 und 47 der Verfassung der Republik Polen nicht vereinbar. Das Gericht entschied einstimmig, dass IP-Adressen (Internet-Protocol-Adressen) personenbezogene Daten darstellen.

Im Urteil vom 24. Oktober 2011 teilte das Verwaltungsgericht der Woiwodschaft Warschau die Ansicht des GIODO bezüglich der Löschung personenbezogener Daten aus dem nationalen polizeilichen Informationssystem (KSIP). Laut dem Gericht gelten im Falle einer Löschung der im KSIP gespeicherten personenbezogenen Daten die Bestimmungen des Datenschutzgesetzes und nicht die Bestimmungen des Polizeigesetzes, das die Polizei zur Einrichtung eines KSIP berechtigt.

C. Sonstige wichtige Informationen

Ein wichtiger Aspekt des GIODO ist die Abgabe von Stellungnahmen zu Gesetzentwürfen. Unter den Gesetzentwürfen, die dem GIODO 2011 zur Prüfung vorgelegt wurden, sind die Gesetzentwürfe im Hinblick auf IKT-Datenbanken besonders hervorzuheben. Die polnische Datenschutzbehörde ließ verschiedenen Gesetzentwürfen zur Regulierung der Funktionsweise von Datenbanken besondere Aufmerksamkeit zukommen, darunter: Bildungsinformationssysteme (SIO), Informationssysteme im Gesundheitswesen und das Zentrale Register juristischer Personen – nationales Register der Steuerzahler (CRP KEP). Des Weiteren ließ der GIODO bezüglich der Ausrichtung der UEFA EURO 2012 mit Ausnahme der oben genannten IKT-Datenbanken dem Gesetzentwurf zur Änderung des Gesetzes zur Sicherheit bei Massenveranstaltungen und bestimmten weiteren Gesetzen besondere Aufmerksamkeit zukommen. Der GIODO konzentrierte sich außerdem auf die Fortführung des Gesetzgebungsverfahrens im Hinblick auf den Gesetzentwurf zum Informationsaustausch zwischen EU-Mitgliedstaaten sowie zu Leitlinien zum Gesetzentwurf zur Reduzierung der Informationsverpflichtungen und administrativer Lasten für Bürger und Unternehmer. Außerdem ist zu erwähnen, dass der GIODO seine Ansichten zur vorgeschlagenen Änderung des Datenschutzgesetzes zum Ausdruck brachte. Neben den Gesetzentwürfen – einschließlich derer, die oben als wichtigste Beispiele genannt wurden – gab der GIODO eine Reihe von Stellungnahmen zu

Vorschriftenentwürfen im Zusammenhang mit allgemeinen Fragen zur Verarbeitung personenbezogener Daten heraus.

Im Berichtszeitraum setzte sich der zunehmende Trend bei der Anzahl der gemeldeten Speichersysteme für persönliche Daten im Vergleich zu den Vorjahren fort (2009: 6 465, 2010: 9 921, 2011: 11 845). Dies war u. a. auf die Tatsache zurückzuführen, dass die Erklärungen nicht so sehr mit Fehlern behaftet waren, wie es in den Vorjahren der Fall war. Zweifelsohne wurde dieses Ergebnis von den gesetzgeberischen, bildungstechnischen, organisatorischen und technischen Aktivitäten des GIODO im Jahr 2011 und in vorherigen Jahren beeinflusst, die zu einer beträchtlichen Reduzierung der herausgegebenen Beschlüsse zu Registrierungsverweigerungen führten (2010: 453, 2011: 105), während die Anzahl der registrierten Dateien zunahm.

Anlässlich des Europäischen Datenschutztages am 31. Januar 2011 organisierte die Datenschutzbehörde in der Hauptgeschäftsstelle für alle Bürger einen Tag der offenen Tür sowie eine Konferenz mit dem Titel „Datenspeicherung in einem demokratischen Rechtsstaat". Außerdem wurde der Europäische Datenschutztag wie üblich auch in Brüssel gefeiert.

Am 21. September 2011 organisierte der polnische Innenminister und der Datenschutzbeauftragte in Warschau im Rahmen der polnischen Ratspräsidentschaft mit der Internationalen Datenschutzkonferenz eine der wichtigsten Veranstaltungen auf diesem Gebiet. Zu den Partnern der Konferenz gehörten der ungarische Beauftragte für Datenschutz und Informationsfreiheit, das ungarische Ministerium für öffentliche Verwaltung und Justiz, der Europarat, die Akademie für europäisches Recht und das spanische Justizministerium.

Am 15. Juni 2011 organisierte der Datenschutzbeauftragte in der Hauptgeschäftsstelle in Zusammenarbeit der französischen Datenschutzbehörde (CNIL) den Workshop für Datenschutzbehörden der EU-Mitgliedstaaten mit dem Titel „Verbindliche unternehmensinterne Vorschriften in der Praxis – ein Erfahrungsaustausch unter Datenschutzbehörden". Ziel dieses Workshops war der Austausch von Erfahrungen und Fachwissen aus der praktischen Anwendung verbindlicher unternehmensinterner Vorschriften. Zu den Fragen, die im Rahmen des Workshops angesprochen wurden, gehörte u. a. die Methodik einer Analyse von Anwendungen verbindlicher unternehmensinterner Vorschriften.

Vom 4. bis zum 5. Oktober 2011 fand in Warschau der vom GIODO organisierte Workshop über die Bearbeitung von Fällen statt. An der Veranstaltung nahmen Vertreter von sowohl nationalen als auch regionalen Datenschutzbehörden sowie Vertreter des Europäischen Datenschutzbeauftragten teil. Der Workshop war auf den praktischen Erfahrungsaustausch zwischen Mitarbeitern bestimmter Datenschutzbehörden ausgerichtet, die mit der Bearbeitung von Fällen und der Durchführung von Prüfungen befasst sind. Während der Plenar- und Breakout-Sitzungen wurden u. a. die folgenden Themen angeschnitten: die Bearbeitung grenzüberschreitender Fälle, der Schutz personenbezogener Daten im Zusammenhang mit Websites zur sozialen Vernetzung und anderen Online-Diensten, Prüfungsmethoden sowie Datenschutz am Arbeitsplatz.

Der GIODO veröffentlichte 2011 erneut Informationsbroschüren der Reihe „Das ABC des Datenschutzes" sowie die folgenden Leitfäden:

- Leitfaden zum Schutz personenbezogener Daten bei Wahlkampagnen;

- Leitfaden zum Schutz personenbezogener Daten in der orthodoxen Kirche, eine gemeinsame Erklärung des Oberhauptes der polnisch-orthodoxen Kirche und Metropoliten Sawa und des GIODO;

- Der Leitfaden mit dem Titel „Ausgewählte Themen zum Datenschutz. Ein Handbuch für Unternehmer" wurde im Rahmen des Partnerprojektes „Bewusstseinsbildung zu

Datenschutzfragen bei innerhalb der EU tätigen Unternehmern“ der polnischen, tschechischen und ungarischen Datenschutzbehörden herausgegeben (erhältlich in polnischer, englischer, tschechischer und ungarischer Sprache).

PORTUGAL

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2011 war durch einen Anstieg der Aktivitäten der Datenschutzbehörde gekennzeichnet. Dies kam auch in der Anzahl der Verfahren zum Tragen, die einen Rekordwert erreichten.

Einer der wichtigsten Aspekte war die Einführung des elektronischen Meldesystems für Meldungen aller Art im Rahmen des fortlaufenden papierlosen Verfahrens, das es der Datenschutzbehörde ermöglicht, ihre internen Abläufe erheblich zu beschleunigen und ihre Reaktionszeit zu erhöhen. Dies soll es den für die Datenverarbeitung Verantwortlichen ermöglichen, ihren Meldeverpflichtungen schneller und unkomplizierter nachzukommen.

Auf institutioneller Ebene ist außerdem die gute Zusammenarbeit mit anderen nationalen Aufsichtsbehörden zur Diskussion konvergierender Angelegenheiten hervorzuheben, sowie die Zusammenarbeit mit einigen Ministerien zur genauen Nachverfolgung neuer Projekte mit Auswirkungen auf den Datenschutz sowie zur Erteilung von Ratschlägen bei Diskussionen auf europäischer Ebene.

Die portugiesische Datenschutzbehörde hat auch weiterhin durch die Unterstützung zahlreicher Initiativen zur Bewusstseinsbildung in Sachen Datenschutz beigetragen, wie z. B. durch ein Kolloquium, das gemeinsam mit dem Verband für Direktmarketing zu den Themen Datenschutz und Marketing organisiert wurde, oder die Aktivitäten für Kinder des Projektes DADUS, das sich an 20 Sitzungen in Schulen mit 1 500 Schülern beteiligte, sowie die Förderung eines zweiten Wettbewerbs „Ein Slogan für den Datenschutz“.

Was Prüfungen betrifft, erhöhte die Datenschutzbehörde die Anzahl an Vor-Ort-Prüfungen und prüfte Strafverfolgungsbehörden und Telekomanbieter.

Organisation	
Vorsitz und/oder Gremium	Gremium bestehend aus 7 Mitgliedern: Filipa Calvão (Vorsitzender), Ana Roque, Carlos Campos Lobo, Helena Delgado António, Luís Barroso, Luís Paiva de Andrade, Vasco Almeida
Budget	Zugewiesenes Budget: 3 326 388,13 EUR Staatliches Budget: 1 308 280,00 EUR Aus den eigenen Einnahmen der Datenschutzbehörde: 2 018 108,13 EUR Ausgegebene Haushaltsmittel: 1 719 550,60 EUR
Personal	23 (Generalsekretär: 1; Abteilung für internationale Beziehungen und Kommunikation: 1; Rechtsabteilung: 9; Prüfabteilung: 3; Zentrale: 2; Verwaltungs- und Finanzabteilung: 7.

Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	14 913 verbindliche Beschlüsse (darunter 13 307 Genehmigungen von Datenverarbeitungen und 75 Stellungnahmen zu Gesetzesentwürfen. Der Rest bezog sich auf Verstoßverfahren, Beschwerden, Anträge Dritter auf Datenzugriff, Schengen-Zugriffsrechte usw.
Meldungen	16 141
Vorabprüfungen	14 852
Anfragen betroffener Personen	k. A.
Beschwerden betroffener Personen	489 (224 betreffend Videoüberwachungssysteme und 86 betreffend der Datenverarbeitung in Beschäftigungsverhältnissen).
Vom Parlament bzw. der Regierung angeforderte Beratung	72 Stellungnahmen zu Gesetzentwürfen zum Thema Datenschutz
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	18 023 neue Verfahren (Meldungen, Beschwerden, Stellungnahmen, Verstöße, Zugang durch Dritte); 181 Anträge auf Zugang zu und Löschung von Daten im Schengener Informationssystem (ein Recht, das indirekt über die Datenschutzbehörde in Anspruch genommen werden kann); 303 Anträge auf Stellungnahmen durch Telekommunikationsanbieter bezüglich einer Aufhebung des Vertraulichkeitsschutzes bei störenden Anrufen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	984 begonnene Prüfungen (Verstoßverfahren), darunter 249 Prüfungen vor Ort
Sanktionsmaßnahmen	
Sanktionen	197 von der Datenschutzbehörde verhängte Geldbußen
Geldbußen	Die Datenschutzbehörde verhängte Geldbußen in Höhe von ± 333 000 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B: Informationen zur Rechtsprechung

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

C: Sonstige wichtige Informationen

www.cnpd.pt

RUMÄNIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	**Nationale Aufsichtsbehörde für den Schutz personenbezogener Daten**
Vorsitz und/oder Gremium	Georgeta Basarabescu
Budget	3 320 000 RON (ungefähr 772 093 EUR)
Personal	41 sowie Präsidentin und Vizepräsident der Datenschutzbehörde
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	1 214 (davon 1 normativer Beschluss)
Meldungen	11 223
Vorabprüfungen	1
Anfragen betroffener Personen	90
Beschwerden betroffener Personen	404
Vom Parlament bzw. der Regierung angeforderte Beratung	58
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	214 (vor Ort)
Sanktionsmaßnahmen	
Sanktionen	50 Geldbußen in Höhe von insgesamt 61 300 RON (ungefähr 14 222 EUR)
Geldbußen	41 Verwarnungen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Rechtsprechung 1

Die Aufsichtsbehörde wurde über zwei Fälle bezüglich der Verarbeitung biometrischer Mitarbeiterdaten zur Überwachung von deren Arbeitsstunden informiert. Diesbezüglich wurden bestimmte Untersuchungen mit den folgenden Ergebnissen durchgeführt:

die Einführung elektronischer Systeme zur Überprüfung der Arbeitsstunden mittels der Speicherung von Fingerabdrücken. Alle Mitarbeiter waren dazu verpflichtet, bei jedem Betreten/Verlassen der Einheit das biometrische Erfassungsgerät zu benutzen, um ihre effektiven Arbeitsstunden zu registrieren;

die Umsetzung eines solchen Beschlusses durch die Geschäftsleitung öffentlicher Institutionen (ein Krankenhaus und ein Rathaus) mit der Absicht einer Mitarbeiterbeobachtung zur Erfassung der Arbeitsstunden, wobei zuvor ein Anwesenheitsregister geführt wurde und damit die Verspätungen und Abwesenheiten einiger Mitarbeiter registriert oder für andere Kollegen abgezeichnet wurden;

die Mitarbeiter wurden über den Beschluss zur Einführung des neuen Zeiterfassungssystems kurz vor dessen Umsetzung benachrichtigt;

nur in einem der beiden untersuchten Fälle wurde diesbezüglich die ausdrückliche Einwilligung der Mitarbeiter eingeholt. Als die Mitarbeiter jedoch erstmals über das System informiert wurden, warnte man sie, dass sie im Falle einer Verweigerung der Nutzung dieses biometrischen Zeiterfassungssystems nur für die Stunden bezahlt würden, die über das System erfasst werden, was einer Beendigung des Beschäftigungsverhältnisses gleichkommt;

obwohl das elektronische System das alte System, bei dem die Mitarbeiter das Anwesenheitsregister abzeichnen mussten, ersetzen sollte, erlaubten beide untersuchten Stellen bestimmten Mitarbeitern oder Abteilungen jedoch nach wie vor die Nutzung der alten Anwesenheitsregister;

da die Meldepflicht für die Verarbeitung personenbezogener (biometrischer) Daten zur Erfassung der Arbeitsstunden innerhalb von 30 Tagen vor Beginn der Datenverarbeitung nicht eingehalten wurde, verstößt dies gegen die Bestimmungen des Gesetzes Nr. 667/2001 und gegen den Beschluss Nr. 11/2011 des Präsidenten der Aufsichtsbehörde.

Auf der Grundlage dieser Ergebnisse ergriff die Aufsichtsbehörde die folgenden Maßnahmen:

gegen die überprüften Stellen wurden gemäß Artikel 31 (Nichteinhaltung der Meldepflicht), Artikel 32 (übermäßige Verarbeitung biometrischer Daten gemessen am Zweck der Verarbeitung sowie die ausbleibende Reaktion auf die Beschwerde innerhalb der gesetzlich vorgeschrieben Frist) und Artikel 33 (unterlassene Erstellung eines Sicherheits-Backups) des Gesetzes Nr. 677/2001 Sanktionen verhängt;

der Aussetzungsbeschluss infolge eines Beschlusses zur Beendigung der Verarbeitung biometrischer Mitarbeiterdaten zur Erfassung der Arbeitsstunden.

Bei ihren Beschlüssen berücksichtigte die Aufsichtsbehörde Folgendes:

Der angegebene Zweck der Datenverarbeitung, nämlich die Erfassung der Arbeitsstunden der Mitarbeiter, hätte auch durch andere, weniger die Privatsphäre verletzende Methoden, wie z. B. die Nutzung des Anwesenheitsregisters, oder durch andere Funktionen des implementierten elektronischen Systems

erfolgen können. Es wurde festgestellt, dass die Anwesenheit einiger Mitarbeiter nach wie vor über das Anwesenheitsregister erfasst wurde. Die Nutzung unterschiedlicher Methoden für den gleichen Zweck ist den Mitarbeitern derselben Einrichtung gegenüber potenziell diskriminierend. Des Weiteren kann im Zusammenhang der Arbeitgeber-/Arbeitnehmerbeziehung die schriftliche Einwilligung der Mitarbeiter in einem der Fälle zur Legitimierung der Verarbeitung unmöglich als freiwillig und in Kenntnis der Sachlage gelten, vor allem in Anbetracht der Konsequenzen einer Verweigerung der Systemnutzung.

Demnach kann die Verarbeitung der biometrischen Mitarbeiterdaten gemäß Art. 4 Abs. 1 Buchst. c des abgeänderten Gesetzes Nr. 677/2001 im Vergleich zu dem Zweck, zu dem sie erfasst und später verarbeitet wurden, als übermäßig gelten. Infolge der Untersuchungen befolgten die beiden Stellen die Beschlüsse der Aufsichtsbehörde und beendeten die Verarbeitung biometrischer Mitarbeiterdaten zur Erfassung der Arbeitsstunden.

Rechtsprechung 2

Eine weitere Situation, auf die die Aufsichtsbehörde aufmerksam gemacht wurde, bezog sich auf die Verarbeitung der personenbezogenen Daten von Ausweisen beim Kauf und Aufladen von Prepaid-Karten. Aufgrund der fehlenden Rechtsgrundlage würde eine Verweigerung der Vorlage eines Ausweises dem Kunden/Einzelnen den Zugang zu einem Mobiltelefondienst verwehren.

Infolge der durchgeführten Untersuchungen wurden die für die Datenverarbeitung Verantwortlichen dazu aufgefordert, ihre Methode zur Bereitstellung von Prepaid-Karten zu ändern, da das Erstellen einer Ausweiskopie beim Kauf einer Prepaid-Karte nur mit der schriftlichen Genehmigung der betroffenen Personen erfolgen könne. Was das Aufladen der Prepaid-Karten betrifft, kam die Aufsichtsbehörde zu dem Schluss, dass dieser Service nicht auf der Vorlage eines Ausweises beruhen sollte.

Rechtsprechung 3

Die Aufsichtsbehörde erhielt von Studierenden Informationen bezüglich der Tatsache, dass die Websites ihrer Universitäten Profile von Studierenden hielten, die ein persönliches Konto erstellt hatten. Der Zugang zu den Profilseiten, die die personenbezogenen Daten der Studierenden und ihrer Eltern enthielten (Vor- und Nachname, Nachname nach Heirat, Geburtsdatum, Geburtsort, Geschlecht, Religionszugehörigkeit, Ausweisnummer, persönliche Identifikationsnummer, Familienstand und Militärrang sowie weitere schulische Informationen), erfolgte mit einer persönlichen Identifikationsnummer.

Infolge einer Überprüfung wurde festgestellt, dass diese Art der Profilerstellung im Rahmen einer Bewerbung (über das Verwaltungssystem der Universität, UMS) an höhere Bildungsinstitutionen erfolge und die Authentifizierung technisch gesehen mit einer persönlichen Identifikationsnummer und dem Geburtsdatum geschehe.

Der angegebene Zweck der Verarbeitung im Rahmen dieser Anwendung war die Pflege zentralisierter Datensätze aller Studierenden sowie deren schulischer und finanzieller Situation, bei denen es sich um Daten handelt, die vom Ministerium für Bildung, Forschung, Jugend und Sport angefordert werden, um auf nationaler Ebene ein einzigartiges Register aufzubauen.

In diesen Fällen empfahl die Aufsichtsbehörde, für den Zugang zu den Studierendenprofilen einen eindeutigen Identifikationscode zu wählen, der nicht der persönlichen Identifikation entspricht.

SCHWEDEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Aufsicht

E-Government

Die Datenschutzbehörde hat ein spezielles Informationsblatt zur Verarbeitung personenbezogener Daten und E-Government veröffentlicht. Darüber hinaus wurden auf der Website Informationen über eingebauten Datenschutz („Privacy by Design“) veröffentlicht, die in diesem Zusammenhang relevant sind. Außerdem wurden in dieser Sache Stellungnahmen zu Gesetzentwürfen herausgegeben, und im Zusammenhang mit dem elektronischen Datenaustausch zwischen Behörden wurde ein spezielles Prüfprojekt durchgeführt. Weitere Prüfungen im Bereich E-Government wurden im Gesundheitswesen und in Wohlfahrtseinrichtungen in die Wege geleitet.

Cloud-Computing

Zur Klarstellung der Anforderungen, die im Gesetz zum Schutz personenbezogener Daten in Sachen Cloud-Computing festgelegt sind, hat die Datenschutzbehörde eine Reihe von Kommunalbehörden und Unternehmen geprüft, die solche Dienste nutzen. Das Projekt führte zur Erstellung eines Informationsblattes, das eine Checkliste mit den Datenschutzanforderungen an Cloud-Computing-Dienste enthält.

Kameraüberwachung

Im Zusammenhang mit der Kameraüberwachung am Arbeitsplatz sowie in Wohngebäuden und Schulen wurde ein großes Prüfprojekt durchgeführt. Daraus entstanden Informationsblätter mit Checklisten der Erwägungen, die im Hinblick auf Kameraüberwachung gezogen werden müssen.

Sensibilisierung

Die Sensibilisierung der Bevölkerung in Sachen Datenschutz und Privatsphäre ist ein wichtiger Bestandteil unserer Strategie. Wir arbeiten auch weiterhin proaktiv an der Sichtbarkeit von Privatsphäre und Datenschutz. Die Anzahl der Besucher unserer Website stieg 2011 um 24 %. Die Datenschutzbehörde verzeichnete außerdem einen erheblichen Anstieg der bei unserem Helpdesk eingehenden Fragen. Des Weiteren hat die Datenschutzbehörde zum vierten Mal in Folge das jährlich erscheinende Infoblatt „Jahr des Datenschutzes“ (2011) herausgegeben, das die Gesetzgebung, Gesetzentwürfe, Beschlüsse und weitere Aspekte enthält, die während des Jahres Auswirkungen auf den Datenschutz gehabt haben.

Sonstige Aktivitäten

Ein Vertreter der Datenschutzbehörde war im Zusammenhang mit dem Entwurf eines Arbeitsdokuments zu epSOS (Intelligente offene Dienste für europäische Patienten), WP 189, Berichterstatter der Untergruppe zu Gesundheitsdaten der Artikel-29-Datenschutzgruppe.

Im Hinblick auf das Inkrafttreten des neuen Gesetzes über polizeiliche Daten im März 2012 wurde der Schwerpunkt vermehrt auf Datenschutzfragen im Strafverfolgungsbereich gelegt.

Organisation	
Vorsitz und/oder Gremium	Göran Gräslund (Generaldirektor)
Budget	37 Millionen SEK = 4,2 Millionen EUR
Personal	47
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2011 wurden 247 Prüfungen eingeleitet 107 Stellungnahmen zu Gesetzgebungsvorschlägen 61 Stellungnahmen in Absprache mit Datenschutzbeauftragten 13 Leitlinien, Empfehlungen und Berichte
Meldungen	215
Vorabprüfungen	238
Anfragen betroffener Personen	206 formelle Anträge Per Telefon und E-Mail bei unserem Helpdesk eingegangene, informelle Fragen: 4 700 (E-Mail) 7 500 (Telefon)
Beschwerden betroffener Personen	312
Vom Parlament bzw. der Regierung angeforderte Beratung	107 Stellungnahmen zu Gesetzgebungsvorschlägen
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Vorträge, Seminare und Konferenzen: 42 Pressemitteilungen: 67
Prüfmaßnahmen	
Prüfungen, Untersuchungen	43 Vor-Ort-Prüfungen 134 Dokumentenprüfungen 70 Prüfungen per Fragebogen Wichtige Themen: Cloud-Computing, Kameraüberwachung, GPS-

	Systeme zur Ortung von Mitarbeitern, Zuverlässigkeitsüberprüfungen durch Personalvermittlungsagenturen, E-Government
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Die Gesamtzahl der 2011 gemeldeten Datenschutzbeauftragten belief sich auf 6 621. Die Datenschutzbehörde nahm 61 formale Konsultationen von Datenschutzbeauftragten in Anspruch und hielt 9 Vorträge speziell für Datenschutzbeauftragte.

B. Informationen zur Rechtsprechung

Das Oberste Verwaltungsgericht bestätigte die Entscheidung der Datenschutzbehörde, in Eingangsbereichen von Wohngebäuden keine Kameraüberwachung zu gestatten. Die Datenschutzbehörde hatte einem Wohnungsbauunternehmen angeordnet, die Nutzung von Überwachungskameras in den Eingangsbereichen ihrer Wohngebäude einzustellen, da es dem Unternehmen dadurch möglich war, die Gewohnheiten und Bekanntschaften der Mieter zu beobachten und aufzuzeichnen. Gegen den Beschluss der Datenschutzbehörde wurde beim Verwaltungsgericht und beim Berufungsgericht Berufung eingelegt, wo man jeweils den Beschluss der Datenschutzbehörde bestätigt hat. Im Dezember 2011 bestätigte das Oberste Verwaltungsgericht diesen Beschluss. In einem Interessenausgleich befand das Gericht, dass es keine Anzeichen dafür gebe, dass die Gebäude besonders anfällig für Kriminalität seien. Noch habe man einen anderen triftigen Grund für die Überwachung feststellen können. Demnach solle die Überwachung als Verstoß gegen die Privatsphäre und das Gesetz zum Schutz personenbezogener Daten erachtet werden.

SLOWAKEI

A. Zusammenfassung der Aktivitäten und Neuerungen

2011 setzte die Datenschutzbehörde der Slowakischen Republik (nachfolgend „Datenschutzbehörde“) ihre Maßnahmen zur Sensibilisierung der breiten Öffentlichkeit fort, indem neue Entwicklungsaspekte in verschiedenen Bereichen des Datenschutzes in den Medien verbreitet wurden. Die Mitarbeiter der Datenschutzbehörde produzierten anlässlich des Datenschutztages sowie zu bestimmten Themen Fernsehankündigungen, wie z. B. zum Online-Datenschutz für Kinder. Die Fachleute der Datenschutzbehörde empfingen außerdem eine Delegation des serbischen Datenschutzbeauftragten und hielten Vorträge zu ausgewählten Themen.

Darüber hinaus initiierte die Datenschutzbehörde eine wichtige Änderung des Gesetzes über Zahlungsdienste, das eine Inkenntnissetzung betroffener Personen über die eventuelle Verarbeitung ihrer Ausweisnummer vorsieht, wenn der per Kreditkarte zu zahlende Betrag eine festgesetzte Höhe übersteigt. Diese Vereinbarung wurde nach mehreren Verhandlungsrunden mit dem slowakischen Bankenverband abgeschlossen. Beide Parteien einigten sich auf den Text eines Informationsstickers, der an den Verkaufspunkten aufgeklebt werden soll.

Des Weiteren stand die Datenschutzbehörde einer Budgetkürzung in Höhe von 10 % gegenüber, die unter dem Vorwand einer Reduzierung der Gesamtausgaben der öffentlichen Verwaltungsbehörden erwirkt wurde.

Diese Situation wirkte sich negativ auf die nationale Überwachung des Schutzes personenbezogener Daten und die Ausübung der Aufgaben der Datenschutzbehörde aus und führte sogar zur Entlassung von Mitarbeitern. Demzufolge wurde die negative finanzielle Situation auf die Initiative der Datenschutzbehörde von der Europäischen Kommission im Zusammenhang mit einem möglichen Verstoßverfahren untersucht. Die Verfahren blieben das ganze Jahr 2011 über in der anfänglichen Pilotphase.

Organisation	Behörde für den Schutz personenbezogener Daten der Slowakischen Republik
Vorsitz	Herr Gyula Veszelei
Budget	684 349 EUR
Personal	34 im ersten HJ 2011, 29 zum 31.12.2011
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	714 + 24 auf der Grundlage des Gesetzes über den Zugang der Öffentlichkeit zu Informationen
Meldungen	33; sowie Meldungen der PDPO (Beauftragten für den Schutz personenbezogener Daten) – 881
Vorabprüfungen	8 (besondere Meldungen)

Anträge von Bürgern	714+24
Beschwerden von Bürgern Beschwerden anderer	176; 6 wiederholte Beschwerden 33
Vom Parlament bzw. der Regierung angeforderte Beratung	77
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Prüfungsverfahren insgesamt – 266 Prüfung von Beschwerden insgesamt – 290 An einzelne für die Datenverarbeitung Verantwortliche gerichtete verbindliche Anordnungen – 102 Beschlüsse der Präsidenten zur Erhebung von Einsprüchen gegen Entscheidungen der Behörde – 12 Grenzübergreifende Datenströme – 20 Beschlüsse zu Genehmigungen von Datenübermittlungen an Drittländer, für die kein angemessenes Datenschutzniveau garantiert werden konnte Strafanzeigen – 6
Prüfmaßnahmen	
Prüfungen	125 bzgl. der Beschwerden; 57 Prüfungen von Amts wegen 36 Anträge auf Erläuterungen; Wichtige Themen und Fragen: Volkszählung: unzureichende Informationen für die Bürger bezüglich der Anonymität der im Rahmen der Volkszählung erhobenen personenbezogenen Daten; Treuekarten: falsche Rechtsgrundlage, rechtswidrige Kombination personenbezogener Daten, deren Verarbeitung über den eigentlichen Zweck hinausgeht; Videoüberwachung: unangemessene Markierung der überwachten Bereiche; Nichtlöschung von Aufzeichnungen innerhalb der vorgegebenen Frist; rechtswidrige Bereitstellung von Aufzeichnungen an Massenmedien; unzulängliche Informationen von Personen mit Zugang zu Kamerasystemen; Schengen-Informationssystem: Umsetzung der vom nationalen Schengen-Aktionsplan ausgehenden Verpflichtung; Prüfung der Ausgabe von Schengen-Visa im Konsulat der slowakischen Botschaft in Wien (Österreich); Prüfung des nationalen SIRENE-

	Büros des Innenministeriums der Slowakischen Republik bezüglich der gründlichen Anwendung der Artikel 95, 96 und 99 des Schengener Abkommens.
Sanktionsmaßnahmen	
Sanktionen	9
Geldbußen	34 300 EUR; Bis Ende 2011 wurde eine Summe von 16 600 EUR bezahlt, der Rest wurde an Beitreibungsverfahren übergeben.

B. Informationen zur Rechtsprechung

2011 gab es keine Gerichtsurteile im Zusammenhang mit Berufungen gegen Beschlüssen der Datenschutzbehörde. Das Bezirksgericht Bratislava ging der Klage einer Aktiengesellschaft nach, die aufgrund eines angeblich rechtswidrigen Beschlusses der Datenschutzbehörde Schadenersatz forderte. Das Verfahren wurde 2008 eröffnet. Die Datenschutzbehörde wurde jedoch nicht über die Klage informiert und trat als Mitbeklagte neben der Slowakischen Republik auf, die bis zum 14. Juli 2011 durch das Justizministerium der Slowakischen Republik vertreten wurde. Das Gericht kam diesbezüglich 2011 zu keinem Urteil.

SLOWENIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Datenschutzbeauftragte ist gemäß dem slowenischen Gesetz zum Schutz personenbezogener Daten (DSG) die Aufsichtsbehörde im Bereich Datenschutz. 2011 eröffnete der Datenschutzbeauftragte 682 Fälle bzgl. vermuteter Verstöße gegen das Datenschutzgesetz, 246 davon im öffentlichen Sektor und 436 im privaten Sektor. In beiden Sektoren bezogen sich die meisten vermuteten Verstöße auf eine ungenehmigte Offenlegung personenbezogener Daten durch die Übertragung von Daten an Dritte oder durch die rechtswidrige Veröffentlichung von Daten. Im privaten Sektor wären darüber hinaus die rechtswidrige Nutzung von Daten zu Zwecken des Direktmarketings und rechtswidrige Videoüberwachung zu nennen. Der Datenschutzbeauftragte leitete 136 Ordnungswidrigkeitsverfahren ein. Die Anzahl der Prüfungsverfahren stieg im Vergleich zum Vorjahr an.

Neben den Kompetenzen als Behörde für Prüf- und Ordnungswidrigkeitsverfahren gibt der Datenschutzbeauftragte zu Datenschutzfragen von Einzelpersonen, von den für die Datenverarbeitung Verantwortlichen sowie von öffentlichen und internationalen Stellen unverbindliche Stellungnahmen und Klarstellungen heraus. 2011 gab der Datenschutzbeauftragte 2 143 Stellungnahmen und Klarstellungen heraus. Dies entspricht einem starken Anstieg im Vergleich zum Vorjahr (1 859) und könnte auf die transparente Arbeit und die intensiven öffentlichen Kampagnen des Datenschutzbeauftragten zurückzuführen sein. Der Datenschutzbeauftragte ist gemäß dem Datenschutzgesetz außerdem für die Durchführung von Vorabprüfungen im Zusammenhang mit biometrischen Messungen, die Übermittlung von Daten an Drittländer und die Anbindung von Dateien zuständig. Die für die Datenverarbeitung Verantwortlichen müssen in solchen Fällen zunächst die Genehmigung des Datenschutzbeauftragten einholen.

Im Rahmen seiner Sensibilisierungsmaßnahmen hat der Datenschutzbeauftragte seine Präventivarbeit fortgesetzt (Vorträge, Konferenzen, Workshops für verschiedene öffentliche Gruppen). Gemeinsam mit dem slowenischen Zentrum für sicherere Internetnutzung führte die Datenschutzbehörde Sensibilisierungsmaßnahmen durch (Vorträge an Schulen, Publikationen). Die Datenschutzbehörde erweiterte den Umfang ihrer Hilfsmittel zur Sensibilisierung und änderte das Format der Sonderberichte: Der erste bezog sich auf Treuekarten. Die Behörde veröffentlichte außerdem *Leitlinien zu Hilfsmitteln für den Online-Datenschutz*. Anlässlich des Europäischen Datenschutztages organisierte die Datenschutzbehörde eine Veranstaltung, um mit der Premiere des Dokumentarfilms „Erasing David“ auf die Bedeutung des Datenschutzes in der modernen IKT-Gesellschaft aufmerksam zu machen. Bei dieser Gelegenheit zeichnete die Datenschutzbehörde drei für die Datenverarbeitung Verantwortliche für vorbildliche Verfahren in Bezug auf den Schutz personenbezogener Daten aus – eine der Auszeichnungen wurde im Zusammenhang mit eingebautem Datenschutz („Privacy by Design“) verliehen. All diese Aktivitäten haben dazu geführt, dass die Datenschutzbehörde einen sehr guten Ruf und öffentliches Vertrauen genießt, was sich in den Ergebnissen der repräsentativen öffentlichen „*Politbarometer*“-Befragung niederschlägt. Aus diesen geht hervor, dass der Datenschutzbeauftragte in Sachen Vertrauen der slowenischen Bürger in verschiedene Institutionen an erster Stelle steht.

Die Datenschutzbehörde beteiligte an einer Reihe von ressortübergreifenden Arbeitsgruppen zu E-Government-Projekten, wie z. B. zu sichereren und benutzerfreundlicheren elektronischen Identitäten sowie zur Entwicklungsstrategie der Informationsgesellschaft von 2011 bis 2015. Die Datenschutzbehörde wurde vom Gesetzgeber und von zuständigen Behörden zu 27 Rechtsakten und anderen Gesetzestexten in den Bereichen minderjährige Straftäter, Immobiliendaten, Maut, eCommerce und elektronische Signaturen, Hochschulwesen, Kinder mit besonderen Bedürfnissen, Parlamentswahlen, Steuern, Strafverfahren und Strafgesetzbuch usw. konsultiert.

Die Datenschutzbehörde beteiligte sich aktiv an einer Reihe von internationalen Gremien: an der Artikel-29-Datenschutzgruppe, der gemeinsamen Kontrollinstanz von Europol und Schengen sowie für den Zoll, EURODAC, WPPJ, der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation sowie am Beratenden Ausschuss des Europarates zur Konvention über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (T-PD). Die Datenschutzbeauftragte setzte ihre Arbeit als Vizepräsidentin der gemeinsamen Kontrollinstanz von Europol fort.

Organisation	Informationsbeauftragte der Republik Slowenien
Vorsitz und/oder Gremium	Frau Nataša Pirc Musar
Budget	1 468 000 EUR
Personal	30 Angestellte: Kabinett (6 – 2 der Mitarbeiter sind auch Datenschutzbeauftragte und 2 Rechtsberater), Verwaltung (3), Rechtsberater für den Zugang zu öffentlichen Informationen (10), Datenschutzforscher und -berater (4), Datenschutzbeauftragte (10)
Allgemeine Aktivitäten	Datenschutz und Zugang zu öffentlichen Informationen
Beschlüsse, Stellungnahmen, Empfehlungen	261 Stellungnahmen und Empfehlungen auf der Grundlage von betroffener Personen und für die Datenverarbeitung Verantwortlichen
Meldungen	Rund 200 Meldungen zu Dateien mit personenbezogenen Daten.
Vorabprüfungen	25 Vorabprüfungen: 8 betreffend Biometrik, 4 betreffend die Übermittlung von Daten an Drittländer, 6 betreffend die Verknüpfung von Dateien mit personenbezogenen Daten.
Anfragen betroffener Personen	2 143 Anträge auf Stellungnahmen/Klärungen von betroffenen Personen.
Beschwerden betroffener Personen	Insgesamt 617 Beschwerden betroffener Personen, davon 444 berechtigt. Bereiche: 218 betreffend die unrechtmäßige Übermittlung oder Offenlegung von Daten, 128 betreffend die unrechtmäßige Datenerfassung, 79 betreffend Direktmarketing, 89 betreffend Videoüberwachung, 43 betreffend Datensicherheit, 60 sonstige. Darüber hinaus 85 Beschwerden betreffend den Umgang mit Rechten betroffener Personen.
Vom Parlament bzw. der Regierung angeforderte Beratung	Der Gesetzgeber und die für die Erarbeitung von Gesetzentwürfen zuständigen Behörden konsultierten die Datenschutzbeauftragte zu 27 Gesetzen und sonstigen Rechtstexten, unter anderem betreffend das Gesetz für Datenbanken im Gesundheitswesen, das Gesetz zum Umgang mit jugendlichen Straftätern, das Gesetz zur Mauterhebung, das Gesetz für Immobiliendaten, die Strafprozessordnung usw.
Sonstige Informationen zu nennenswerten allgemeinen	Weitere Tätigkeiten der Datenschutzbeauftragten im Jahr 2011:

Aktivitäten	Fortsetzung der Präventivarbeit (Vorträge, Konferenzen) gemeinsam mit dem slowenischen Zentrum für sichereres Internet; Beteiligung an einer Reihe von ressortübergreifenden Arbeitsgruppen im Bereich E-Government, u. a. auch im Bereich elektronische Identität; Veröffentlichung von Leitlinien zum Online-Datenschutz sowie ein Sonderbericht zum Thema Treuekarten; Konsultationen bzgl. einer Reihe von Gesetzen; Fortsetzung der starken internationalen Beteiligung.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	682 Prüfungen: 246 im öffentlichen Sektor, 436 im privaten Sektor.
Sanktionsmaßnahmen	
Sanktionen	Es wurden 136 Verfahren eingeleitet (43 im öffentlichen, 66 im privaten Sektor, 27 zu Privatpersonen), davon wurden 30 Verwarnungen und 52 Ermahnungen ausgesprochen sowie 12 Geldbußen und 7 Zahlungsanordnungen verhängt.
Geldbußen	Die Datenschutzbehörde verhängte Geldbußen in Höhe von 50 035 EUR (netto ohne Verwaltungssteuern).
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Die Datenschutzbehörde erhielt zahlreiche Beschwerden in Bezug auf **Veterinärsämter**, die Hundebesitzern Impferinnerungen zuschickten und ihnen gleichzeitig weitere Dienstleistungen anboten. Man fand heraus, dass die Veterinärämter die personenbezogenen Daten der Hundebesitzer aus dem nichtöffentlichen zentralen Hunderegister entnommen hatten, die lediglich für rechtskräftig festgestellte Zwecke verwendet werden dürfen (Pflege des Hunde- und Hundebesitzerregisters, Kontrolle über reguläre Impfungen und Überwachung von Bissen sowie zu statistischen Zwecken). Die Veterinärämter hätten diese Daten trotz des rechtmäßigen Zugangs nicht zu Direktmarketingzwecken verwenden dürfen. Zu Direktmarketingzwecken dürfen lediglich die personenbezogenen Daten der Hundebesitzer verwendet werden, die Kunden eines bestimmten Amtes sind, sowie die Daten aus öffentlich zugänglichen Quellen. Die Datenschutzbehörde verhängte eine Sanktion über das Veterinäramt.

Die Datenschutzbehörde hat in einem Fall entschieden, bei dem es um das **Direktmarketing geodätischer Dienste** ging, die Einzelpersonen angeboten wurden, deren Immobilien nicht in das Register des Portals Prostor (dt.: Raum) eingetragen waren. Obwohl die Daten aus einer öffentlich zugänglichen Quelle stammten, verstieß der für die Datenverarbeitung Verantwortliche gegen das Datenschutzgesetz, da nur die folgenden Daten zu Direktmarketingzwecken verwendet werden dürfen: der Name der Person, die

Anschrift ihres ständigen oder vorübergehenden Wohnsitzes, Telefonnummer und Faxnummer. Um die Information, dass Besitzer ihre Immobilien noch nicht in das Register eingetragen haben, nutzen zu können, hätte der für die Datenverarbeitung Verantwortliche die ausdrückliche Einwilligung benötigt.

Die Datenschutzbehörde erhielt eine Beschwerde, dass eine **Online-Dating-Website** die Namen, E-Mail-Adressen und Passwörter ihrer Nutzer im Internet offengelegt habe. Wie sich herausstellte, hatte der Betreiber der Website deren Design einem indischen Auftragnehmer anvertraut. Das Produkt enthielt keinerlei Maßnahmen zur Rückverfolgbarkeit der Datenverarbeitung, und eine mangelhafte Programmierung sorgte dafür, dass die Täter sich Zugang zu den Daten von 7 000 Website-Nutzern verschaffen konnten. Der Websitebetreiber wurde außerdem des Verstoßes gegen die Bestimmungen der vertraglichen Datenverarbeitung für schuldig befunden, da kein Vertrag mit dem Datenverarbeiter abgeschlossen worden war. Des Weiteren wurde eine Datenübermittlung in Drittländer ohne Rechtsgrundlage festgestellt. Die Datenschutzbehörde wies den Websitebetreiber an, die Datenverarbeitung einzustellen und alle Nutzer über den Zwischenfall zu informieren.

Die Datenschutzbehörde stellte fest, dass auf der Website der **Nationalen Wahlkommission** personenbezogene Daten offengelegt werden: sowohl die der Kandidaten der vergangenen Parlamentswahlen als auch die der Kandidaten der vergangenen Kommunalwahlen. Die Veröffentlichung der personenbezogenen Daten der Kandidaten wird durch sektorale Vorschriften nur im Hinblick auf den Zeitraum vor einer Wahl geregelt, jedoch nicht im Hinblick auf die Zeit nach der Wahl. Die Datenschutzbehörde befand, dass die personenbezogenen Daten der Kandidaten veröffentlicht wurden, um Wählern eine informierte und unabhängige Wahlentscheidung zu ermöglichen. Da der Zweck der Verarbeitung der personenbezogenen Daten für die vergangene Wahl bereits erfüllt war, hätte der für die Datenverarbeitung Verantwortliche die Daten der Kandidaten löschen müssen.

Die Datenschutzbehörde bearbeitete einen Fall, bei dem es um **räumliche Fotografien mit identifizierbaren Personen** ging, die ein professioneller Fotograf auf seiner Website veröffentlicht hatte. Bei dem Verfahren wurden räumliche Fotografien im Zusammenhang mit dem Zweck der Veröffentlichung und der Identifizierbarkeit der Personen auf den Bildern betrachtet. Die Datenschutzbehörde kam zu dem Schluss, dass der Zweck der Abbildung von Natur- und Kulturerbe auch ohne die Abbildung identifizierbarer Passanten erzielt werden könne. Das Interesse des Fotografen an der Veröffentlichung steht in diesem Fall nicht über dem Interesse der Passanten, entscheiden zu können, ob sie auf einem Bild zu identifizieren sind oder nicht. Daher müssen solche Bilder vor der Veröffentlichung im Internet anonymisiert werden, damit die Personen nicht mehr zu identifizieren sind. In der dazugehörigen Stellungnahme wies die Datenschutzbehörde außerdem auf den Unterschied zwischen Straßenfotografie und räumlicher Fotografie hin.

C. Sonstige wichtige Informationen

In Sachen **internationale Zusammenarbeit** war die Datenschutzbehörde außerdem im Bereich der bilateralen internationalen Zusammenarbeit tätig. 2011 begrüßte sie Vertreter zahlreicher Länder, darunter Kroatien, Serbien, Kosovo, Montenegro und Mazedonien. Als Juniorpartner setzte sie gemeinsam mit dem Projektleiter, dem Ludwig-Boltzmann-Institut für Menschenrechte aus Österreich, die Umsetzung des Partnerschaftsprojekts IPA 2009 Nr. MN/09/IB/JH/03 – Umsetzung einer Strategie zum Schutz personenbezogener Daten in Montenegro – fort, für das sie 2010 den Zuschlag erhalten hatte. Im November 2011 wurde die Datenschutzbehörde von der Europäischen Kommission zur Umsetzung des Partnerschaftsprojekts SR/2009/IB/JH/01 zur Verbesserung des Datenschutzes bestimmt, das sich mit der Verbesserung des Datenschutzes in Serbien befasst. Die Datenschutzbehörde führte außerdem eine Prüfung der Botschaften der Republik Slowenien in Pristina und Kairo durch und überprüfte dabei u. a. die Rechtmäßigkeit der Datenverarbeitung bei Verfahren für den Erhalt von Schengen-Visa sowie innerhalb des Visa-Informationssystems (VIS).

In Sachen **politische Angelegenheiten**, mit denen sich die Datenschutzbehörde weitreichend befasst hat, sei der vermehrte Einsatz von Videoüberwachung in Bereichen wie Saunen, Umkleideräumen, Spielplätzen und einigen anderen öffentlichen Bereichen, wie z. B. auf Wanderwegen, zu nennen. Die Datenschutzbehörde stellte außerdem einen Anstieg von Fällen in Bezug auf Online-Marketing und unerwünschte E-Mails fest, deren Absender oftmals nicht nachweisen können, dass sie die Einwilligung der Empfänger erhalten haben, oder aber die Rücktrittsoptionen nicht beachten und Empfänger nicht über ihre Rechte informieren. Bezüglich der Sicherheit der Datenverarbeitung stellte die Datenschutzbehörde fest, dass Sicherheit häufig nicht ausreiche, um die Bedingungen des Datenschutzgesetzes zu erfüllen. In zahlreichen Fällen seien im Internet offen zugängliche personenbezogene Daten festgestellt worden.

Darüber hinaus stellte die Datenschutzbehörde fest, dass zahlreiche für die Datenverarbeitung Verantwortliche vor dem Dilemma stünden, ob sie **Cloud-Computing** einsetzen sollen oder nicht. Dies führe zu bestimmten Fragen bezüglich der Übereinstimmung mit den Vorschriften im Bereich des Schutzes personenbezogener Daten und der Privatsphäre. Organisationen, die sich für den Einsatz von Cloud-Computing entscheiden, sind häufig nicht ausreichend darüber informiert, wo ihre personenbezogenen Daten gespeichert und wie diese geschützt werden. Ohne solche Informationen ist es jedoch schwierig, vor einer diesbezüglichen Entscheidung angemessene Risikoeinschätzungen durchzuführen. Die Datenschutzbehörde hat einige Stellungnahmen zum Thema Cloud-Computing herausgegeben und zum Ende des Jahres 2011 außerdem damit begonnen, Entscheidungshilfen für den Einsatz dieses Produkts durch die für die Datenverarbeitung Verantwortlichen zu erstellen.

SPANIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Bürgerinformationen und Schutz ihrer Rechte

Die Aktivitäten der AEPD in direktem Bezug auf die Bereitstellung von Informationen an Bürger sowie deren Schutz haben 2011 stark zugenommen. Die Anzahl der Auskunftsersuchen über die Bürger-Hotline stieg um 30 % (mit rund 135 000 Ersuchen). Die Website verzeichnete insgesamt drei Millionen Besucher. In gleicher Weise stieg die Anzahl der Klagen[17] 2011 um 35 % auf insgesamt 2 230 Anträge. Mehr als 60 % der Beschlüsse der AEPD infolge dieser Anträge bezogen sich auf das Recht auf Löschung oder Widerspruch. Dieser Trend findet sich auch bei den Anklagen bezüglich des „Rechts auf Vergessenwerden" wieder, wo sich die Zahlen von nur drei Klagen im Jahr 2007 auf 160 Klagen im Jahr 2011 erhöht haben. Darüber hinaus war die Anzahl der Beschwerden[18] mit knapp 5 500 um die Hälfte höher als 2010.

Der Schutz von Kindern ist für die AEPD besonders wichtig. 2011 stellten alle Datenschutzbehörden Spaniens (die AEPD sowie die substaatlichen Behörden Kataloniens, Madrids und des Baskenlandes) ein Schulungstool namens „Registrieren, eingeben, abmelden. Rechte schützen und Daten kontrollieren" zur Verfügung. Das Tool ist eine Anpassung des Originalmaterials der irischen Datenschutzbehörde an die Situation in Spanien. Auf diese Bildungsressource wird 2013 ein umfangreicheres Tool folgen.

Förderung der Gesetzesanwendung

In bestimmten komplizierten Fällen kann es vorkommen, dass die für die Datenverarbeitung Verantwortlichen um Klärung der einschlägigen Bestimmungen des Datenschutzgesetzes bitten. Die AEPD gab 2011 knapp 500 Berichte heraus. Außerdem hat die AEPD über 100 Berichte zu Gesetzentwürfen und Regulierungen herausgegeben. Die Berichte sind für die Regierung verpflichtend, und obwohl sie nicht rechtsverbindlich sind, nehmen sie Einfluss auf das Gesetzgebungsverfahren.

Im April 2011 führte die AEPD ein neues Informationssystem (RENO) ein, das die betriebliche Effizienz im Zusammenhang mit Meldungen, Dateiregistrierungen und Genehmigungen internationaler Datenübermittlungen verbessern soll. Die Anwendung umfasst individuelle Signaturen und elektronische Siegelsysteme u. a. zur Vereinfachung der Herausgabe und Meldung von Beschlüssen.

Gesetzliche Änderungen

Im März wurde das spanische Datenschutzgesetz aufgrund des Gesetzes 2/2011 über eine nachhaltige Wirtschaft abgeändert. Die Änderungen betreffen das Sanktionssystem in vielerlei Hinsicht. Einerseits hat sich die Klassifizierung von Verstößen geändert. Die Kategorien (nicht schwerwiegend, schwerwiegend und äGraphical layout and design of the brochure ußerst schwerwiegend) bleiben zwar unverändert, doch die den Kategorien zugrundeliegenden Maßnahmen sind angepasst worden. Die Mindest- und Höchstbeträge der möglichen Geldbußen sind ebenfalls in jeder Kategorie leicht abgeändert worden. Dies ist dahingehend

[17] Anträge auf einen Beschluss der Datenschutzbehörde zur Wahrung der Datenschutzrechte der Kläger in Fällen von Verstößen durch die für die Datenverarbeitung Verantwortlichen

[18] Anträge auf eine Erklärung der Datenschutzbehörde zum Vorliegen eines Gesetzesverstoßes, die die Anweisung einer Einstellung des Verstoßes und das Verhängen einer Sanktion enthält.

äußerst relevant, als dass die abgeänderten Bestimmungen objektive Kriterien für die Modulation von Sanktionen aufgestellt haben sowie die Möglichkeit einer Reduzierung der Sanktionen vorsehen, falls präventive/proaktive Maßnahmen ergriffen wurden, und eine „präventive Verwarnung" einführen, die in bestimmten Fällen (z. B. erster „nicht schwerwiegender" Verstoß, falls weitere Kriterien erfüllt sind) Geldbußen ersetzen können.

Internationale Zusammenarbeit

Im Juni 2009 erhielt die AEPD den Zuschlag für die Leitung eines Partnerprojekts in Kroatien. Das Projekt setzt die Rahmenbedingungen der Zusammenarbeit zwischen der spanischen und der kroatischen Datenschutzbehörden zur Vorbereitung des EU-Beitritts Kroatiens fest. 2011 haben die AEPD und die kroatische Datenschutzbehörde gemeinsam an dem Projekt weitergearbeitet, das 2012 abgeschlossen werden soll.

Organisation	Spanische Datenschutzbehörde
Vorsitz und/oder Gremium	Herr José Luis Rodríguez
Budget	14 437 970,00 EUR
Personal	156 (154 Beamte – 2 Nichtbeamte) sowie ein Datenschutzbeauftragter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Beschlüsse zu Anfragen: 7 233; Berichte: 140
Meldungen	638 533 Registrierungen (öffentliche und private Dateien) Insgesamt gemeldete Dateien zum 31.12.2011: 2 609 471
Vorabprüfungen	k. A.
Anfragen betroffener Personen	134 635 Anfragen über die Hotline (schriftlich, telefonisch, online sowie über die Zentrale) 484 Anforderungen von Berichten an die Rechtsabteilung (246 aus der öffentlichen Verwaltung und 238 von Bürgerinnen und Bürgern bzw. Unternehmen).
Beschwerden betroffener Personen	5 389 Beschwerden betroffener Personen. Sektoren: Telekommunikation und Videoüberwachung verzeichneten erhebliche Zugänge (jeweils 17,78 % und 6,35 %). Zu weiteren relevanten Sektoren gehörten Internet, Werbung usw.
Vom Parlament bzw. der Regierung angeforderte Beratung	Die AEPD gab rechtliche Stellungnahmen zu insgesamt 110 allgemeinen Gesetzentwürfen oder Änderungen bestehender Gesetze heraus, unter anderem zum Transparenzgesetz, zum Gesetz über die Beaufsichtigung privater

	Versicherungsunternehmen, zum allgemeinen Telekommunikationsgesetz und zum Anti-Doping-Gesetz.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	2 892 516 Zugriffe auf die Website (durchschnittlich 7 923 pro Tag) 3 500 883 Konsultationen des öffentlichen Registers 175 Genehmigungen des Direktors für internationale Datenübermittlungen
Prüfmaßnahmen	
Prüfungen, Untersuchungen	5 389 Voruntersuchungen und 2 230 Verfahren zum Schutz von Rechten. 7 233 Beschlüsse aus Prüfungen, davon 1 939 betreffend den Schutz von Rechten (Zugang, Berichtigung, Löschung und Widerspruch) und 5 294 Verfahren betreffend die Sanktionsbefugnis. Die Prüfungsabteilung führte außerdem in verschiedenen BereichenUntersuchungen von Amts wegen durch: • Cloud-Computing; • Übermittlung von Unternehmensdaten – Prüfungen betreffend den Verkauf von Schulden durch Telekommunikationsanbieter und Finanzinstitute (andauernd); • Europäische Haftbefehle in Spanien Analyse der Vertragsbestimmungen von Telekommunikationsanbietern.
Sanktionsmaßnahmen	
Sanktionen	898 Sanktionsbeschlüsse: 96,46 % zum Datenschutzgesetz, 3,02 % zum Gesetz über Dienste der Internetgesellschaft (Spam) und nur 0,52 % zum allgemeinen Telekommunikationsgesetz (Werbung per Fax)
Geldbußen	19 597 905,97 EUR (+12 % im Vergleich zu 2010)
Datenschutzbeauftragte (DPO)	k. A.
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Die „präventive Verwarnung", die mit der Änderung des Datenschutzgesetzes eingeführt wurde, wird seit 2011 umfassend genutzt. Knapp 40 % aller Erklärungen von Verstößen wurden mit einer Verwarnung anstelle einer Geldbuße geschlossen. Zu den Fällen, bei denen die „präventive Verwarnung" zum Einsatz kommt, gehören in der Regel unbeabsichtigte Fehler, Verstöße durch Privatpersonen aufgrund unzureichender Kenntnisse des Datenschutzgesetzes sowie Verstöße gegen formelle oder administrative Anforderungen. Aspekte, wie z. B. die Kooperationsbereitschaft des für die Datenverarbeitung Verantwortlichen bei der Berichtigung des Verstoßes, die Vertraulichkeit der betreffenden Daten, die wirtschaftlichen Auswirkungen des Verstoßes oder das Verhältnis der Datenverarbeitung zur Hauptaktivität des für die Datenverarbeitung Verantwortlichen, werden regelmäßig bei Beschlüssen, ob Verwarnungen ausgesprochen oder Geldbußen verhangen werden, berücksichtigt.

Rechtsprechung des Nationalen Gerichtshofs:

2011 waren zahlreiche Urteile besonders relevant, mit denen ein Ausgleich zwischen dem Recht auf Datenschutz und anderen Grundrechten und -freiheiten beschlossen wurde.

- Im Hinblick auf das Auskunftsrecht erklärte der nationale Gerichtshof in seinem Urteil vom 29. September die Veröffentlichung eines Fotos in den Medien, auf dem ein Opfer des Terrorangriffs vom März 2004 in Madrid abgebildet war, als mit dem Datenschutzgesetz vereinbar. Das Gericht befand, dass solche Bilder im Zusammenhang mit den Informationen, die Medien anzubieten beabsichtigen, relevant seien.

- Das Recht auf Freiheit einer Gewerkschaft wurde in Fällen, bei denen die Offenlegung von Daten für die Arbeiter von Bedeutung ist und die Veröffentlichung auf den Arbeitsplatz selbst beschränkt ist, gegenüber dem Recht auf Datenschutz als vorrangig betrachtet.

Rechtsprechung des Obersten Gerichtshofs:

Der Gerichtshof der EU erklärte in seinem Urteil vom 24. November, dass Artikel 7(f) der Richtlinie 45/96 nicht in einer Art und Weise interpretiert werden kann, wie das spanische Datenschutzgesetz (*Ley Orgánica* 15/1999, *de Protección de Datos*) es tut. Das Urteil beantwortet eine Frage, die der Oberste Spanische Gerichtshof im Zusammenhang mit einer Berufung gestellt hatte, in deren Rahmen einige Unternehmen mehrere Artikel der Verwaltungsvorschrift angefochten haben, die den Artikel des Datenschutzgesetzes umsetzt, durch den wiederum Artikel 7(f) der Richtlinie in spanisches Recht umgesetzt wurde. Obwohl der Fall die Verwaltungsvorschrift betraf, fragte der Oberste Gerichtshof den Europäischen Gerichtshof, ob der Artikel des Gesetzes, auf dem die Vorschrift beruht, mit der Europäischen Richtlinie kompatibel sei. Das Urteil des Europäischen Gerichtshofs besagt, dass Artikel 7(f) unmittelbare Wirkung habe und demnach der entsprechende Artikel des spanischen Datenschutzgesetzes nichtig sei. Darüber hinaus erklärte der Oberste Spanische Gerichtshof einige der angefochtenen Bestimmungen der Vorschrift für nichtig.

TSCHECHISCHE REPUBLIK

A. Zusammenfassung der Aktivitäten und Neuerungen

Die Überwachungsaktivitäten basierten teilweise auf dem Prüfplan der Datenschutzbehörde und wurden teilweise von Beschwerden betroffener Personen angestoßen. Es folgt eine Zusammenfassung der typischen oder interessantesten Fälle. Im Allgemeinen war der Prüfplan auf Informationssysteme der Regierung (solche Datenbanken treten seit einigen Jahren vermehrt auf), Informationssysteme von Unternehmen (z. B. Kundenkarten, Treuekarten) und Datenverarbeitungen zum Zweck der Verbrechensbekämpfung und des Kampfs gegen den Terrorismus ausgerichtet. Beschwerden von Bürgern bezogen sich größtenteils auf Videoüberwachung, personenbezogene Daten im Internet und Datenverarbeitungen von Finanzinstitutionen oder Anbietern elektronischer Dienste.

Im Sommer schloss das Amt gemeinsam mit den ungarischen und polnischen Datenschutzbehörden das internationale Projekt „Raising awareness of data protection issues among the entrepreneurs operating in the EU“ ab, das vom Leonardo-da-Vinci-Partnerschaftsprogramm unter der Nummer CZ/09/LLP-PS/P/LdV/061 finanziert wurde. Das Projekt war dem Datenschutz am Arbeitsplatz und dem Schutz von Arbeitnehmerdaten aus der Sicht der Arbeitgeber gewidmet. Die wichtigsten Ergebnisse waren ein umfangreiches Handbuch und eine Reihe von Verteilungsaktivitäten.

Zwei Mitarbeiter waren im Rahmen des technischen Hilfsprojekts „Support to the Directorate for Personal Data Protection“ (EuropeAid/128570/S/CER/FYR) bei mehreren Gelegenheiten als kurzfristige Experten in Skopje (EJRM) tätig.

Organisation	Amt für Datenschutz
Vorsitz und/oder Gremium	Igor Němec (Präsident des Amtes für Datenschutz)
Budget	262 175 040 CZK (10 487 001 EUR, Wechselkurs 1 EUR = 25 CZK) – davon 3 073 800 EUR aus EU-Strukturfonds, insbesondere für ein Projekt zur Schaffung eines staatlichen Zentralregisters.
Personal	99
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	3 Stellungnahmen (alle zur Datenverarbeitung im Privatsektor)
Meldungen	4 421 Meldungen (davon 3 856 registriert und 1 002 laufend oder ausgesetzt)
Vorabprüfungen	82
Anfragen betroffener Personen	2 294 (davon 110 aus dem Ausland)
Beschwerden betroffener Personen	1 119 (und weitere 4 613 bezüglich Spam)

Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	23 Anträge unter Berufung auf das Informationsfreiheitsgesetz. 75 Gesetzentwürfe und 91 Durchführungsverordnungen, zu denen im Rahmen des interministeriellen Stellungnahmeverfahrens Stellung genommen wurde Genehmigung internationaler Übermittlungen: 9 Anträge, davon 3 gestattet und 6 aus verfahrensrechtlichen Gründen ausgesetzt
Prüfmaßnahmen	
Prüfungen, Untersuchungen	179 (davon 144 abgeschlossen) und 157 Untersuchungen bzgl. Spam (davon 137 abgeschlossen)
Sanktionsmaßnahmen	
Sanktionen	ca. 70 Sanktionen Anmerkung: Unter Sanktionen wird eine nichtfinanzielle Abhilfemaßnahme verstanden, die einem für die Datenverarbeitung Verantwortlichen auferlegt wird. Im Rahmen einer Untersuchung wird eine Reihe unterschiedlicher Sanktionen (Abhilfemaßnahmen) verhängt, doch zum Zweck dieser Informationen gilt eine Reihe von Sanktionen im Rahmen einer bestimmten Untersuchung als Sanktion. Der Durchschnitt pro Aktion liegt bei etwa 2,7.
Geldbußen	ca. 105 Geldbußen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Die Tschechische Republik führte 2011 eine **Volkszählung** durch. Einer der Prüfer des Amtes für Datenschutz führte dabei im Tschechischen Statistikamt eine Prüfung durch. Dies folgte auf zahlreiche Beschwerden von Bürgern, die sich über die Methodik der Volkszählung sowie über die Aufbewahrung anonymisierter Formulare im Nationalarchiv (und die Aufbewahrung der Ergebnisse der Volkszählung im Tschechischen Statistikamt) beschwert hatten. Die Prüfung begann Mitte 2011 und war bis zum Ende des Jahres nicht abgeschlossen.

Das Amt **prüfte die Online-Version des Handelsregisters**, das zum E-Government-System gehörte. Über dieses Portal (das vom Justizministerium betrieben wird) werden personenbezogene Daten verarbeitet. Aufgrund der Online-Umgebung entsteht ein höheres Missbrauchsrisiko. Der Prüfer wies darauf hin, dass es für jede Datenverarbeitung einen Verantwortlichen geben müsse, der für die Einhaltung der gesetzlichen Vorschriften zuständig ist. Außerdem sei laut Prüfer der Umfang der erfassten Daten (oder Dokumente) durch die Richtlinie 2009/101/EG vorgeschrieben, und das Einstellen anderer Dokumente

müsse sorgfältig auf den Grundsatz der Zweckbindung hin geprüft werden. Gleichermaßen muss die Aufbewahrungsfrist dieser personenbezogenen Online-Daten in einem angemessenen Verhältnis zum Zweck stehen (Verfügbarkeit geeigneter Daten für Dritte). Ein weiteres Problem, das bei der Prüfung zutage geführt wurde, war die Offenlegung von Geburtsnummern (d. h. Identifikationsnummern, die Neugeborenen zugeteilt werden). Da man dank der Prüfung auf das Problem aufmerksam wurde, konnte das Amt in der abgeänderten Version des Handelsgesetzbuches die Vorkehrung treffen, dass Geburtsnummern weder im Auszug des Handelsregisters noch im Handelsamtsblatt veröffentlicht werden.

Viele Gemeinden nutzen Videokameras, um ihre Sitzungen aufzuzeichnen oder in Echtzeit zu übertragen. Das Problem der **Videoaufzeichnungen und Übertragungen** von Gemeinderatssitzungen wird sowohl von der Öffentlichkeit als auch von Journalisten genau beobachtet. Das Amt hat demzufolge mehrere Vor-Ort-Prüfungen durchgeführt und anschließend einige Grundsätze herausgegeben: Der Gemeinderat muss stets den genauen Zweck der Audio- oder Videoaufzeichnung angeben. Falls eine Sitzung komplett und ohne Bearbeitung aufgezeichnet wird, unterliegt das Dokument dem Gesetz über Archive. Ein solches Dokument darf nur dann als Quelle für Sitzungsprotokolle herangezogen und muss nach Fertigstellung der Protokolle vernichtet werden. Falls der Gemeinderat das Online-Streaming einer Sitzung bereitstellt (ohne sie aufzuzeichnen), stellt dies keine Verarbeitung personenbezogener Daten dar. Demzufolge greift auch nicht das Datenschutzgesetz.

Bezüglich der rasch zunehmenden elektronischen Kommunikation über staatliche Informationssysteme konzentrierte sich das Amt auf das für **elektronische Vorgänge durch staatliche Stellen mithilfe von Datenboxen** garantierte Sicherheitsniveau. Datenboxen werden innerhalb des Datenbox-Informationssystems unter Einhaltung des Gesetzes für elektronische Vorgänge und autorisierte Konvertierungen betrieben. Das Amt begann mit einer Prüfung des Innenministeriums, das für die Verarbeitung personenbezogener Daten verantwortlich war, sowie der Tschechischen Post, die dieses System betrieb. Es wurde als notwendig befunden, diese Prüfung auf das Justizministerium auszuweiten. Die Anzahl der Beschwerden stieg 2010 und 2011 in Bezug auf die Zusendung gerichtlicher, an Rechtsanwälte adressierter Dokumente an die Datenboxen natürlicher Personen, die ein Geschäft führen. Aus einer Stellungnahme des Justizministeriums ging hervor, dass Dokumente von zahlreichen Gerichten fälschlicherweise versandt wurden. Dies ergab eine Prüfung durch den Anbieter von Informationssystemen. Darüber hinaus gingen beim Justizministerium Beschwerden von Einzelpersonen ein. Auf Grundlage dieser Informationen wurde eine Prüfung angestoßen (auch im Einklang mit den Prioritäten des Prüfplans). Die Prüfung bezog sich in erster Linie auf die Systembedingungen, die für die Pflichterfüllung der Verwalter bei der Verarbeitung personenbezogener Daten innerhalb des sogenannten Datenbox-Informationssystems erstellt wurden, mit besonderem Augenmerk auf die Pflichterfüllung bei der Sicherung personenbezogener Daten. Unter der Berücksichtigung, dass das Hauptziel einer Prüfung darin besteht, eine Lösung zu finden und Systembedingungen zur Beseitigung menschlicher Fehler zu schaffen, konzentrierten sich drei Vor-Ort-Prüfungen auf die Mitarbeiter des Innenministeriums, die für die Installation und Verwaltung der Datenboxen verantwortlich waren. Mitarbeiter des Innenministeriums wurden außerdem zur Abschlussprüfung eingeladen, vor allem deshalb, da alle Beschwerden Gerichte betrafen. Gemäß den Stellungnahmen von Vertretern beider Ministerien sollte ab dem Tag, an dem die Einrichtung von Datenboxen für Anwälte Pflicht ist, ein separates Warnsignal für Anwälte eingeführt werden.

C. Sonstige wichtige Informationen

Am Rande der Konferenz der Datenschutzbeauftragten, die im Oktober in Mexiko-Stadt stattfand, führte einer der tschechischen Delegierten mit Prüfbefugnis eine **Prüfung der tschechischen Botschaft** in Mexiko durch. Der Zweck der Prüfung war die Pflichterfüllung im Rahmen des Schengenevaluierungsprozesses. Ebenfalls in diesem Jahr wurden ähnliche Prüfungen der tschechischen Botschaften in Mazedonien und Moldau durchgeführt.

Der im Januar stattfindende Europäische Datenschutztag bietet seit jeher die Gelegenheit, eine Veranstaltung zur Sensibilisierung zu organisieren. Dieses Jahr veranstaltete das Amt bereits zum fünften Mal den erfolgreichen Wettbewerb für Kinder und Jugendliche mit dem Titel „This is my privacy! Don't look, don't poke about!" Bei der Vorbereitung der Veranstaltung arbeitete das Amt erneut mit dem Tschechischen Radio Prag, dem Internationalen Filmfestival für Kinder und Jugendliche in Zlín und diesmal auch mit dem Verband für Bibliotheks- und Datenfachleute zusammen. In mehr als 100 Bibliotheken in der gesamten Tschechischen Republik traten Kinder im Alter von sieben bis zehn Jahren beim Spiel „Durch die Wild Web Woods" gegeneinander an, das ihnen auf witzige Weise beibringt, wie man sich sicher und respektvoll im Internet verhält. Für die Bereitstellung der tschechischen Version des Spiels arbeitete das Amt mit dem Europarat zusammen, der diese unterhaltsame Bildungsmaßnahme für sicheres Verhalten im Internet entwickelt hat.

Die Fachleute des Amtes nahmen als Dozenten an rund 40 regionalen Veranstaltungen für akademische und rechtliche Institutionen, Unternehmen sowie Einrichtungen des öffentlichen Rechts zum Thema Datenschutz teil.

UNGARN

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Beauftragte für Datenschutz und Informationsfreiheit erstellte als für das Jahr 2011 verantwortliche Datenschutzbehörde keinen Jahresbericht und keine Statistik zu seinen Aktivitäten im Jahr 2011. Die nationale Behörde für Datenschutz und Informationsfreiheit, die im Januar 2012 gegründet wurde, stellt die folgenden Zahlen für das Berichtsjahr 2011 auf Grundlage der vom Amt des Beauftragten erstellten Register zur Verfügung.

Organisation	Beauftragter für Datenschutz und Informationsfreiheit
Vorsitz und/oder Gremium	Dr. András Jóri
Budget	352 381 000 HUF
Personal	49
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	5 461 (Anzahl der Fälle einschließlich Meldungen von Einträgen ins Datenschutzregister) 71 Empfehlungen sind auf der offiziellen Website des Datenschutzbeauftragten für das Jahr 2011 einsehbar.
Meldungen	k. A.
Vorabprüfungen	14 (alle bzgl. Meldungen von Einträgen ins Datenschutzregister)
Anfragen betroffener Personen	3 162 (Meldungen von Einträgen ins Datenschutzregister)
Beschwerden betroffener Personen	949
Vom Parlament bzw. der Regierung angeforderte Beratung	290 (Stellungnahmen zu Gesetzentwürfen bzgl. Datenschutz oder Informationsfreiheit)
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	797 Konsultationen, 112 internationale Fälle (bzgl. Datenschutz oder Informationsfreiheit)
Prüfmaßnahmen	
Prüfungen, Untersuchungen	309 (im Zusammenhang mit abgeschlossenen und berechtigten Beschwerden)
Sanktionsmaßnahmen	

Sanktionen	Der Datenschutzbeauftragte ist nicht dazu befugt, Sanktionen zu verhängen.
Geldbußen	Der Datenschutzbeauftragte ist nicht dazu befugt, Sanktionen zu verhängen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Zwei wichtige Beispiele:

a) *Rechtswidrige Datenverarbeitung – Anbieter der Websites* (www.ingatlandepo.com und www.ingatlanbazar.com)

Der Datenschutzbeauftrage (nachfolgend „DBA") untersuchte den Fall eines Websiteanbieters (nachfolgend Verantwortlicher genannt). Für die Inserate von Immobilien im Namen der betroffenen ungarischen Personen auf der Website des Verantwortlichen wurden zwischen den beiden Parteien Verträge abgeschlossen.

Sobald die Immobilien verkauft waren, verfielen die Inserate, und die betroffenen Personen wollten diese einfach löschen – oder sie vom Verantwortlichen löschen lassen. Dies geschah jedoch nicht. Trotz der nachdrücklichen und wiederholten Anfragen wurden die Inserate vom Verantwortlichen nicht gelöscht. Außerdem gab der für die Datenverarbeitung Verantwortliche die personenbezogenen Daten der betroffenen Personen u. a. an Forderungsmanagementunternehmen weiter.

Diesbezüglich gingen beim DBA zahlreiche Beschwerden ein. Demzufolge eröffnete der DBA ein Ermittlungsverfahren und rief den Verantwortlichen dazu auf, innerhalb einer festgelegten Frist zu seinem Verhalten Stellung zu nehmen.

Nach dem Verfahren kam der DBA zu dem Schluss, dass der Verantwortliche mehrfach gegen das Recht auf Datenschutz der betroffenen Personen verstoßen habe. Der Verantwortliche verstieß u. a. gegen den Verhältnismäßigkeitsgrundsatz, das Auskunftsrecht, das Recht der betroffenen Personen auf die Löschung ihrer personenbezogenen Daten sowie den Grundsatz der Zweckbindung. Darüber hinaus vernachlässigte der Verantwortliche die zahlreichen Einwände der betroffenen Personen im Hinblick auf die Datenverarbeitung durch den Verantwortlichen. Daher fehlte dem Verantwortlichen die rechtliche Grundlage für verschiedene Datenverarbeitungsaktivitäten.

Demzufolge veröffentlichte der DBA eine Pressemitteilung und eine Erklärung, in der er die Weitergabe von Immobilieninseraten und somit die Andeutung der Verarbeitung personenbezogener Daten gegen den Willen der Kunden als rechtswidrig erklärte. Des Weiteren können diese Methoden nicht als Entschädigung einer ausstehenden Forderung an den Kunden eingesetzt werden. Der DBA rief Kunden dazu auf, vor der Preisgabe personenbezogener Daten die Datenschutzerklärung des Anbieters genau zu prüfen.

b) biometrische Identifikation im Zusammenhang mit Eintrittspässen für öffentliche Bäder

Ein Kunde stellte einen Antrag auf eine offizielle Erklärung des DBA zu der Frage, ob die Datenverarbeitung eines Betreibers eines öffentlichen Bades/Spas rechtmäßig sein könne, falls dieser für seine Eintrittspässe ein biometrisches Identifikationssystem einführen würde. Den Absichten des Betreibers zufolge würde ein biometrisches System die Fingerabdrücke von Kunden speichern und so für den Anbieter zu einem effektiveren und kundenspezifischeren Identifikationssystem werden.

Der Antragsteller wollte wissen, ob Fingerabdrücke personenbezogene Daten darstellen, die nur auf Einwilligung der betroffenen Person erfasst werden dürfen. Außerdem wollte der Kunde wissen, ob es im Zusammenhang mit der Verarbeitung von Fingerabdruckdaten genauere – und eventuell strengere – Vorschriften gebe.

Im Hinblick auf die einschlägigen nationalen und EU-Vorschriften wurde dem Kunden Folgendes mitgeteilt:

Die Fingerabdrücke einer natürlichen Person stellen personenbezogene Daten und deren Speicherung eine Verarbeitung ebendieser dar. Nicht nur die einschlägige nationale Gesetzgebung, sondern auch die EU-Datenschutzrichtlinie enthält wesentliche rechtliche Grundsätze, die bei der Datenverarbeitung berücksichtigt werden müssen. Hierzu gehört u. a. der Grundsatz der Verhältnismäßigkeit und der Notwendigkeit.

Die Datenschutzgruppe (WP 29) betonte, dass geprüft werden müsse, ob der Einsatz des biometrischen Identifikationssystems notwendig sei, um die Ziele des Anbieters zu erreichen. In dieser Hinsicht müssen die folgenden Aspekte durchdacht werden:

- Ist die Installation eines solchen Systems unvermeidbar oder einfach nur kostengünstig und bequem?
- Ist der Einsatz eines solchen Systems wirkungsvoll, und falls ja, in welchem Ausmaß?
- Steht die Einschränkung der Privatsphäre im Verhältnis zu den voraussichtlichen Vorteilen?
- Können die Ziele des Anbieters auch durch weniger einschränkende Maßnahmen erreicht werden?

Schlussendlich kam der DBA zu dem Schluss, dass ein biometrisches System – zur Erfassung und Speicherung der Fingerabdrücke von Kunden nach dem Betreten des öffentlichen Bades/Spas – für den Zweck einer besseren und wirkungsvolleren persönlichen Identifizierung nicht dem Verhältnismäßigkeitsgrundsatz entspreche. Eine bessere Identifikation könnte auch durch andere – harmlosere und weniger auf Kosten der Privatsphäre gehende – Methoden erzielt werden, wie z. B. durch Eintrittspässe mit Passfoto usw. Demzufolge wäre die Einführung eines solchen Eintrittssystems nicht mit dem Datenschutzgesetz vereinbar.

C. Sonstige wichtige Informationen

Wichtige Gesetzesänderungen in Ungarn

Aufgrund fundamentaler Änderungen der ungarischen Verfassungsstruktur infolge einer Entscheidung der ungarischen Nationalversammlung im Jahr 2011 wurde die Arbeit des ehemaligen Datenschutzbeauftragten beendet. Die neu gegründete nationale Behörde für Datenschutz und Informationsfreiheit hat zum 1. Januar 2012 ihren Dienst aufgenommen. Das neue Rechtsinstrument für den Bereich des Datenschutzes und der Informationsfreiheit (Gesetz CXII von 2011 über das Recht auf informationelle Selbstbestimmung und Informationsfreiheit) wurde am 11. Juli 2011 vom Parlament verabschiedet.

VEREINIGTES KÖNIGREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Entwicklungen im Bereich öffentliche Ordnung

Das ICO wirkte maßgeblich bei der Verabschiedung des Protection of Freedoms Act mit, indem es beim Parliamentary Public Bill Committee vorsprach. Das neue Gesetz stärkt den Datenschutz in Bereichen wie z. B. Videoüberwachung und biometrische Daten, sorgt für ein erhöhtes Maß an Transparenz und garantiert eine noch größere Unabhängigkeit des ICO. Das ICO war außerdem einer der frühen Zeugen der Leveson-Untersuchung der Kultur, Praxis und Ethik der Presse und sagte über unsere Berichte aus, die zunächst den rechtswidrigen Handel mit personenbezogenen Daten betonten und zur Einführung von Freiheitsstrafen drängten.

Stärker und technisch versierter

Das ICO hat neue Befugnisse erhalten, die es ihm ermöglichen, für schwerwiegende Verstöße gegen das Gesetz über Datenschutz und elektronische Kommunikation Geldbußen von bis zu 500 000 GBP zu verhängen. Dies bedeutet mehr Gleichheit in Bezug auf die Befugnisse, von denen wir bislang Gebrauch gemacht haben, um die abschreckende Wirkung im Hinblick auf schwerwiegende Verstöße gegen das Datenschutzgesetz von 1998 zu erhöhen. Wir bemühen uns auch weiterhin um mehr Befugnisse und haben dem Justizministerium einen Business-Case vorgelegt, um unsere Befugnisse in Sachen Prüfungen des NHS und der Kommunalregierungen auszuweiten.

Im Hinblick auf die Relevanz von Technologie und Datenschutz hat das ICO Verstärkung in Form eines Technologieberaters erhalten, der für die Arbeit des Datenschutzbeauftragten im Zusammenhang mit politischen Entwicklungen, Untersuchungen und der Bearbeitung von Beschwerden eine Führungsrolle übernehmen wird.

Leitlinien

Wir starteten mit der Feier des Europäischen Datenschutztages in das Jahr 2011 und führten ein neues „Toolkit für personenbezogene Daten“ ein, um britische Organisationen zu einem besseren Umgang mit Zugangsanträgen zu verhelfen.

Außerdem gaben wir zwei neue Leitlinien zu WLAN-Sicherheitseinstellungen heraus, da eine Umfrage gezeigt hatte, dass 40 % nicht wissen, wie dies zu bewerkstelligen ist. Wir legten die Datenschutzleitlinien für politische Parteien und Kandidaten im Wahlkampf für das britische Referendum sowie für Kommunal- und Parlamentswahlen neu auf und verschickten Erinnerungen an den Gesundheitsdienst, um personenbezogene Patientendaten zu sichern, nachdem gegen fünf Gesundheitsorganisationen infolge von Verstößen gegen das Datenschutzgesetz Durchsetzungsmaßnahmen ergriffen worden waren. Des Weiteren gaben wir Leitlinien für Studierende heraus, um sie über ihre Datenschutzrechte bezüglich des Zugangs zu ihren Klausurnoten aufzuklären.

Wir stellten britischen Website-Betreibern als Reaktion auf Änderungen des EU-Rechts, nach denen sie die Einwilligung zur Erfassung von Laden- oder Zugangsdaten auf den Computern von Verbrauchern einholen müssen, detaillierte Leitlinien bereit.

Wir regten auch weiterhin zu Diskussionen im Bereich Datenschutz an, indem wir in Cardiff, Belfast und Glasgow für Organisationen aus dem öffentlichen, dem Wohltätigkeits- und dem Freiwilligensektor Veranstaltungen zum Thema Datenaustausch organisierten, um die Bedeutung eines effizienten Datenaustauschs zu diskutieren. Wir veranstalteten in London ein Seminar zur Datenanonymisierung mit über 100 Delegierten, darunter Fachleute aus einer Reihe von Sektoren. Außerdem richteten wir in Nordirland eine Konferenz mit über 100 Delegierten aus, um den Business-Case für den Datenschutz zu besprechen.

Bildung, Bildung, Bildung

Dafür zu sorgen, dass Einzelpersonen ihre Auskunftsrechte kennen und diese in das britische Bildungssystem integrieren, ist von entscheidender Bedeutung. Wir starteten ein Forschungsprojekt, um Mittel und Wege zu finden, um dies in die Praxis umzusetzen. Wir haben uns außerdem mit Studierenden von 15 Universitäten im gesamten Vereinigten Königreich zusammengetan, um junge Menschen auf ihre Datenschutzrechte und auf die Arbeit des ICO aufmerksam zu machen.

Organisation	
Vorsitz und/oder Gremium	Christopher Graham (Datenschutzbeauftragter)
Budget	19 695 000 GBP (Meldegebühren 15 600 000 GBP und Zuschüsse in Sachen Informationsfreiheit in Höhe von 4 500 000 GBP)
Personal	Gesamt: 378 Erste Kontaktaufnahme – 72 Kundenproblemlösung – 102 Durchsetzung – 34 Strategische Zusammenarbeit – 18 Umsetzung politischer Maßnahmen – 11 Meldung – 20 Prüfungen – 32 Verwaltung – 10 Interne Steuerung – 14 Rechtliches – 6 Geschäftliches – 22 Einrichtungen – 4 Finanzen – 7

	IT – 9 Lernen und Entwicklung – 3 Regionale Zweigstellen – 10
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Toolkit für personenbezogenen Daten Leitlinien zur Informationsfreiheit Konsultation zum Verhaltenskodex für Anonymisierung
Meldungen	Gesamtzahl der Meldungen von Verantwortlichen 355 292
Vorabprüfungen	k. A.
Anfragen betroffener Personen	Anrufe bei der Hotline: 217 183
Beschwerden betroffener Personen	Zum Thema Datenschutz eingegangene Beschwerden: 12 985 Zum Thema Informationsfreiheit eingegangene Beschwerden: 4 633 Zum Gesetz über den Schutz der Privatsphäre in der elektronischen Kommunikation eingegangene Beschwerden: 7 095
Vom Parlament bzw. der Regierung angeforderte Beratung	17 Konsultationen
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Anzahl der [von Datenschutzbehörden als nennenswert eingestufte Kategorie] Alle nennenswerten Zahlen, die die Aktivitäten der Datenschutzbehörde widerspiegeln, wie z. B. die Anzahl der verbindlichen unternehmensinternen Vorschriften, die die leitende Datenschutzbehörde genehmigt hat.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	42 Prüfungen
Sanktionsmaßnahmen	
Sanktionen	2 Vollzugsmitteilungen 8 Durchsuchungsbefehle 76 Vereinbarungen 15 Verfahren (1 Fall führte zu konfiszierten Mitteln in Höhe von

	insgesamt 73 000 GBP, die zurückgezahlt werden müssen)
Geldbußen	Wir verhängten 10 zivile Geldbußen in Höhe von 1 171 000 GBP.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

Alle oben genannten Zahlen beziehen sich auf das Geschäftsjahr 2011/2012

B. Informationen zur Rechtsprechung

Anonymisierte Daten und personenbezogene Daten

Im Februar 2005 beantragte die ProLife Alliance gemäß dem Gesetz über Informationsfreiheit (Freedom of Information Act, FOIA) von 2002 beim Gesundheitsministerium detaillierte statistische Daten zu Abtreibungen im Jahr 2003. Das Gesundheitsministerium wies den Antrag auf die Bereitstellung der Abtreibungsstatistik für das Jahr 2003 ab und bezog sich dabei auf eine Reihe von FOIA-Ausnahmeregelungen in Bezug auf eine Offenlegung, einschließlich der Ausnahmeregelung in Abschnitt 40 zu personenbezogenen Daten.

Auf eine Beschwerde über die verweigerte Offenlegung an den Datenschutzbeauftragten und eine Berufung beim Information Tribunal wurde die Angelegenheit dem High Court und Richter Cranston im Fall *R (auf Antrag des Gesundheitsministeriums) gegen den Datenschutzbeauftragten [2011] EWHC 1430 (Verw)* vorgelegt. Der zentrale Aspekt des Falles war die Frage, ob es sich bei der detaillierten Abtreibungsstatistik um personenbezogene Daten im Sinne des Datenschutzgesetzes von 1998 handelt.

Hierzu wurden die im Datenschutzgesetz enthaltene Definition des Begriffs „personenbezogene Daten“ sowie teilweise der 26. Erwägungsgrund der Richtlinie, der besagt, dass „die Grundsätze des Datenschutzes nicht für Daten gelten [sollten], die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann“, genau betrachtet. Das Gericht berücksichtigte außerdem die Stellungnahme 4/2007 der Artikel-29-Datenschutzgruppe zum Begriff „personenbezogene Daten“ und verwies auf das Fazit der Stellungnahme, laut dessen anonyme Daten im Sinne der Richtlinie folgendermaßen definiert sind: „Informationen, die sich auf eine natürliche Person beziehen, wobei die Person von dem für die Verarbeitung Verantwortlichen oder einem Dritten nicht bestimmt werden kann, wenn alle Mittel berücksichtigt werden, die vernünftigerweise eingesetzt werden, um die betreffende Person zu bestimmen“.

Richter Cranston befand nach der Ausführung von Lord Hope des Obersten Gerichtshofs im Fall *Common Services Agency gegen Scottish Information Commissioner* [2008] UKHL 47, dass die Tatsache, dass der für die Datenverarbeitung Verantwortliche Zugang zu allen Daten habe, auf denen die Statistik beruht, ihn nicht davon abhalte, die Daten auf eine Weise zu verarbeiten, dass sie gemäß dem 26. Erwägungsgrund der Richtlinie zu Daten werden, mit denen kein lebendes Individuum mehr identifiziert werden könne. Sollten die zugrundeliegenden Daten auf diese Weise zu Statistiken verarbeitet werden können, stehe dem für die Datenverarbeitung Verantwortlichen der Weg offen, die Daten in statistischer Form offenzulegen, da diese nicht mehr als personenbezogene Daten gelten würden. Richter Cranston kam zu dem Schluss, dass die Offenlegung der detaillierten Abtreibungsstatistik durch das Gesundheitsministerium nicht einer Offenlegung personenbezogener Daten gleichkomme. Das Urteil stellt in Bezug auf das Verhältnis zwischen personenbezogenen Daten und anonymisierten Daten im Sinne des 26. Erwägungsgrundes der Richtlinie eine hilfreiche Klarstellung dar.

ZYPERN

A. Zusammenfassung der Aktivitäten und Neuerungen

Im September 2011 wurde Herr Yiannos Danielides zum Datenschutzbeauftragten ernannt. Er übernahm das Amt von Frau Panayiota Polychronidou, die im Juni zurückgetreten war.

Im Rahmen der Sensibilisierungsmaßnahmen des Datenschutzamtes und der Aktivitäten rund um den Europäischen Datenschutztag gab das Amt am 28. Januar ein Budget von 4 878 EUR für Infoblätter für Besucher eines Einkaufszentrums, Maßbänder und CD-Schutzhüllen aus. Die Botschaft des Tages lautete „Schutzmaßnahmen".

Die Datenschutzbehörde hat in Zusammenarbeit mit der Polizei Zyperns ein Arbeitsdokument (Gesetzentwurf) über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, vorbereitet.

Im Dezember 2010 reichte ein anerkannter Flüchtling eine Beschwerde gegen eine journalistische Website ein, die Kopien seines Ausweises und Sozialhilfedokumente veröffentlichte, auf denen Namen, Adressen und die monatlichen Beträge der Sozialhilfeleistungen von ihm und anderen asylsuchenden Flüchtlingen zu lesen waren. Auf die Untersuchung der Beschwerde kam das Kommissionsmitglied unter Berücksichtigung der Ansichten des Rechtsanwalts der Websitebetreiber und des dem Beschwerdeführer entstandenen Schadens zu dem Schluss, dass die fortlaufende Veröffentlichung der oben genannten Daten einen Gesetzesverstoß darstelle, und verhängte zwei Verwaltungssanktionen über die Website (ein Bußgeld in Höhe von 3 000 EUR sowie die Vernichtung der Daten und das Einstellen deren Verarbeitung). Da die Website dem Beschluss nicht nachkam, meldete das Kommissionsmitglied gemäß seiner in Abschnitt 23 Buchst. a des Gesetzes festgelegten Befugnis den Fall dem Polizeipräsident zur Ermittlung eines möglichen Vergehens vonseiten der Website gemäß Abschnitt 26 des Gesetzes.

Die Datenschutzbehörde untersuchte eine Beschwerde gegen die Zypriotische Telekommunikationsbehörde (CYTA), die von einem Mitarbeiter stammte, dem das Recht auf Zugang zu Daten eines Disziplinarverfahrens, das infolge einer Anschuldigung gegen ihn eingeleitet wurde, und insbesondere den Zugang zum Namen des Anklägers verwehrte. Die CYTA kam zu dem Schluss, dass die Anschuldigung nicht gerechtfertigt sei, dass es kein Disziplinarverfahren gegeben und der Beschwerdeführer alle einschlägigen Dokumente erhalten habe. Sie verweigerte jedoch, die Identität des Anklägers preiszugeben, gegen den der Beschwerdeführer rechtliche Schritte einleiten wollte. Das Kommissionsmitglied kam zu dem Entschluss, dass alle Daten, einschließlich die eines Anklageschreibens, personenbezogene Daten der betroffenen Person darstellen und dass in diesem Fall dem Antrag auf Zugang teilweise nachgekommen wurde. Die CYTA wurde hinzugezogen, um dem Beschwerdeführer eine Kopie des Schreibens des Anklägers zugänglich zu machen und seine Identität offenzulegen.

Angesichts des kommenden Vorschlags bzw. der Vorschläge der Kommission zur europäischen Datenschutzgesetzgebung hat die Datenschutzbehörde den Antrag des Justizministeriums und des Ordnungsamts auf die Vertretung der Republik in der Arbeitsgruppe des Rates DAPIX stattgegeben, die den Vorschlag bzw. die Vorschläge während der polnischen Ratspräsidentschaft diskutieren sollte. Eine Reihe von Beamten nahm in der Akademie für öffentliche Verwaltung an speziellen Schulungen teil, die sie bei ihren neuen Verantwortlichkeiten im Rat und bei der kommenden Ratspräsidentschaft unterstützen sollten. Des Weiteren fanden Gespräche mit dem Ministerium und der Polizei statt, um ein Verfahren für die Annahme gemeinsamer Standpunkte auszuarbeiten.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Herr Yiannos Danielides
Budget	Zugewiesenes Budget: 297 033 EUR; ausgegebene Haushaltsmittel: 28 472 EUR
Personal	Verwaltungsbedienstete: 7 Fachkräfte für Informationstechnologie: 2 Bürofachkräfte: 6 Hilfskräfte: 2
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Stellungnahmen: 11 Anzahl der Beschlüsse: 7 Anzahl der Empfehlungen: 4
Meldungen	Anzahl der Meldungen: 162
Vorabprüfungen	Anzahl der Vorabprüfungen: k. A.
Anfragen betroffener Personen	Anzahl der schriftlich oder telefonisch eingegangenen Anträge betroffener Personen: k. A.
Beschwerden betroffener Personen	Anzahl der berechtigten Beschwerden: 469
Vom Parlament bzw. der Regierung angeforderte Beratung	In acht Fällen wurde das Amt vom zypriotischen Parlament zu Konsultationen und zur Teilnahme an Sitzungen der zuständigen parlamentarischen Ausschüsse eingeladen.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	Anzahl der Genehmigungen für die Verknüpfung von Speichersystemen: 18 Anzahl der Genehmigungen für Übermittlungen an Drittländer: 48
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen bzw. Untersuchungen: 22 2009 wurden Prüfungen des Bankensektors durchgeführt. 2010 veröffentlichte die Datenschutzbehörde wichtige Leitlinien und führte eine erneute Compliance-Prüfung der Banken durch, die 2011 abgeschlossen wurde. Der Bericht der Folgeprüfung zeigte, dass 16 von 18 in Zypern aktiven Geschäftsbanken die Leitlinien

	einhielten. Die anderen vier Prüfungen, die im Rahmen der Untersuchung von Beschwerden durchgeführt wurden, bezogen sich auf die Installation von Überwachungskamerasystemen.
Sanktionsmaßnahmen	
Sanktionen	Anzahl der von der Datenschutzbehörde beschlossenen Sanktionen: 7 Anzahl der von der Datenschutzbehörde begonnenen Rechtsstreite gegen Verantwortliche zur Eintreibung von Bußgeldern: 2
Geldbußen	Wert der von der Datenschutzbehörde erhobenen Bußgelder: 13 000 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

Kapitel Drei

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. EUROPÄISCHE KOMMISSION

Europäischer Datenschutztag 2011, 28.1.2011

Der Schutz personenbezogener Daten ist ein Grundrecht der EU. Am 28. Januar 2011 feierten die Kommission und die Mitgliedstaaten des Europarates den fünften 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.

Anlässlich des Datenschutztages 2011 wurden nicht nur in Europa, sondern auf der ganzen Welt Veranstaltungen organisiert, um Aufklärungsarbeit zum Thema Datenschutz zu leisten und die Bürger über ihre Rechte und bewährte Methoden zu informieren. Somit sollen sie in die Lage versetzt werden, auf effektivere Weise von diesen Rechten Gebrauch zu machen.

Die bedeutendste Veranstaltung des Datenschutztages 2011 war eine hochrangige Konferenz zum Thema Datenschutz mit dem Titel "Datenschutz (30 Jahre später): Von europäischen zu internationalen Normen".

Neben Ansprachen des Generalsekretärs des Europarates, einer Vizepräsidentin der Europäischen Kommission und des Generaldirektors der GD Justiz der Europäischen Kommission fand eine Podiumsdiskussion zu neuen europäischen Vorschriften zum Datenschutz statt, an der der Vorsitzende des Beratenden Ausschusses zur Konvention Nr. 108, der Europäische Datenschutzbeauftragte und der Vorsitzende der Artikel-29-Datenschutzgruppe teilnahmen.

Konsultation zum Gesamtkonzept der Kommission für den Datenschutz in der Europäischen Union vom 15. Januar 2011

Zur Einholung von Stellungnahmen zu den Vorstellungen der Kommission – nachzulesen in der dieser Konsultation beigefügten Mitteilung – bezüglich des Umgangs mit neuen Herausforderungen für den Schutz personenbezogener Daten (z. B. sich rasant entwickelnde Technologien oder Globalisierung) zur Gewährleistung eines effektiven und umfassenden Schutzes personenbezogener Daten innerhalb der EU.

Die Kommission erhielt 305 Reaktionen auf die öffentliche Konsultation: 54 von Bürgern, 31 von öffentlichen Stellen und 220 von privaten Organisationen.

Sonderstudie des Eurobarometers – Ansichten zu den Themen Datenschutz und elektronische Identität in der Europäischen Union, Juni 2011

Die Sonderstudie des Eurobarometers ist die größte Studie, die jemals bezüglich des Verhaltens und der Ansichten von Bürgern in Bezug auf Identitätsmanagement, Datenschutz und Privatsphäre durchgeführt wurde, und spiegelt die Ansichten und das Verhalten der Europäer zu diesen Themen wider.

Die wichtigsten Ergebnisse der Studie lauten:

- 74 % der Europäer sind der Ansicht, dass *die Offenlegung personenbezogener Daten* zunehmend Teil des modernen Lebens ist.

- Daten, die als personenbezogen erachtet werden, sind vor allem finanzielle Daten (75 %), medizinische Daten (74 %) sowie nationale Identifikationsnummern oder Ausweise und Reisepässe (73 %).

- Bei Nutzern von Websites zur sozialen Vernetzung ist die Wahrscheinlichkeit größer, dass sie ihren Namen (79 %), ihr Foto (51 %) und ihre Nationalität (47 %) preisgeben. Zu den *Daten*, die Online-Shopper *tatsächlich bei Online-Käufen offenlegen*, gehören in erster Linie ihr Name (90 %), ihre Anschrift (89 %) und ihre Mobiltelefonnummer (46 %).

- Sowohl für Nutzer von Websites zur sozialen Vernetzung (61 %) als auch für Online-Shopper (79 %) ist der wichtigste Grund für die Preisgabe von Daten der Zugang zu Online-Diensten.

- 43 % der Internetnutzer gaben an, für den Zugang oder die Nutzung eines Online-Dienstes mehr personenbezogene Daten als nötig angeben zu müssen.

- Ein Großteil der Europäer hat Bedenken bezüglich der Ausspähung ihres Verhaltens durch die Nutzung von Kartenzahlungen (54 % vs. 38 %), Mobiltelefonen (49 % vs. 43 %) oder mobilem Internet (40 % vs. 35 %).

- Knapp 60 % der Internetnutzer lesen für gewöhnlich Datenschutzerklärungen (58 %), und der Großteil derer, die sie lesen, passt sein Surfverhalten dementsprechend an (70 %).

- Über die Hälfte der Internetnutzer ist über den Status quo der Datenerfassung und die weitere Nutzung ihrer Daten informiert, wenn sie sich bei einer Website zur sozialen Vernetzung oder für einen Online-Dienst registrieren (54 %).

- Nur ein Drittel der Europäer ist sich der Existenz einer nationalen Behörde bewusst, die für den Schutz ihrer Rechte bezüglich ihrer personenbezogenen Daten verantwortlich ist (33 %).

- Nur knapp über ein Viertel der Nutzer sozialer Netzwerke (26 %) und sogar noch weniger Online-Shopper (18 %) sind der Ansicht, *volle* Kontrolle zu haben.

- Europäer nutzen die folgenden Arten von Identitätsnachweisen: größtenteils Kredit- und Bankkarten (74 %), Ausweise oder Aufenthaltsgenehmigungen (68 %), Berechtigungskarten der Regierung (65 %) oder Führerscheine (63 %). 34 % der Befragten verfügen über einen Account, den sie im Internet nutzen, wie z. B. für E-Mail, soziale Netzwerke oder Online-Shopping.

- Um ihre Identität im öffentlichen Leben zu schützen, geben 62 % der Europäer lediglich ein Mindestmaß an erforderlichen Informationen preis.

- Die häufigsten Strategien zum Schutz ihrer Identität im Internet liegen im technischen oder verfahrensorientierten Bereich, wie z. B. Hilfsmittel und Strategien zur Einschränkung unerwünschter E-Mails bzw. Spam (42 %), Überprüfung der Sicherheit von Transaktionen oder der Sicherheitslogos auf Websites (40 %) sowie Anti-Spy-Software (39 %).

- Behörden und Institutionen – darunter die Europäische Kommission und das Europäische Parlament (55 %) – wird dabei mehr vertraut als gewinnorientierten Unternehmen.

- Weniger als ein Drittel vertraut Telefon- und Mobiltelefonunternehmen oder Internetserviceanbietern (32 %), und nur knapp über ein Fünftel vertraut Internetunternehmen wie z. B. Suchmaschinen, Websites zur sozialen Vernetzung und E-Mail-Diensten (22 %).

- 70 % der Europäer haben dahingehend Bedenken, dass ihre von Unternehmen gehaltenen personenbezogenen Daten für Zwecke verwendet werden, für die sie ursprünglich nicht erfasst wurden.

- 28 % sind bereit, für den Zugang zu ihren bei öffentlichen oder privaten Stellen gespeicherten personenbezogenen Daten zu bezahlen.

- Was das „Recht auf Vergessenwerden" betrifft, möchte eine eindeutige Mehrheit der Europäer (75 %) dazu in der Lage sein, ihre von Websites gehaltenen personenbezogenen Daten jederzeit zu löschen.

- Obwohl die Mehrheit der europäischen Internetnutzer sich persönlich für den sicheren Umgang mit ihren personenbezogenen Daten verantwortlich fühlt, befürworten alle Europäer die gleichen Rechte auf Datenschutz innerhalb der gesamten EU (90 %).

- Mehr als 40 % der Europäer würden eine Durchsetzung der Vorschriften auf europäischer Ebene bevorzugen (44 %); etwas weniger würden sich dagegen eine Durchsetzung auf nationaler Ebene wünschen (40 %).

- Auf die Frage, welche Art von Vorschriften eingeführt werden sollen, um Unternehmen davon abzuhalten, personenbezogene Daten ohne das Wissen der Eigentümer zu verwenden, waren die meisten Europäer der Ansicht, dass solche Unternehmen eine Geldstrafe erhalten sollten (51 %), ihnen eine Nutzung solcher Daten in der Zukunft verboten werden sollte (40 %) oder sie den Opfern eine Entschädigung zahlen sollten (39 %).

- Die Mehrheit ist der Ansicht, dass ihre personenbezogenen Daten in großen Unternehmen besser geschützt wären, wenn diese Unternehmen zur Ernennung eines Datenschutzbeauftragten verpflichtet wären (88 %).

- Die Meinungen der Europäer gehen im Hinblick auf die Umstände, unter denen die Polizei Zugang zu personenbezogenen Daten haben sollte, auseinander. Im Gegensatz dazu sind fast alle der Meinung, dass Minderjährige vor der Offenlegung personenbezogener Daten geschützt (95 %) und davor gewarnt (96 %) werden sollten. Eine große Mehrheit sprach sich für einen besonderen Schutz genetischer Daten aus (88 %).

3.2. EUROPÄISCHER GERICHTSHOF

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

Die Kommission leitete ein Vertragsverletzungsverfahren 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 unmittelbarer oder mittelbarer, Einflussnahme durch alle öffentlichen Behörden sicher sein müssten, nicht nur vor der Einflussnahme seitens Einrichtungen, die kontrolliert werden. 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.

Urteil des Gerichts für den öffentlichen Dienst (Erste Kammer) vom 28. Juni 2011 – AS/Europäische Kommission (Rechtssache F-55/10)

Der ärztlichen Schweigepflicht unterliegen unter anderem Daten, die einer medizinischen Fachkraft bei der Ausübung ihrer Tätigkeiten zu Ohren kommen oder ihr von Patienten anvertraut werden. Bei dem Recht auf die Wahrung der ärztlichen Schweigepflicht, die ein Aspekt des Rechts auf Datenschutz ist, handelt es sich um ein unter dem Rechtsschutz der Europäischen Union stehendes Grundrecht. Diese beiden Rechte können beschränkt sein, vorausgesetzt, dass diese Beschränkungen tatsächlich den Zielen des allgemeinen Interesses der Gemeinschaft entsprechen und keine unverhältnismäßige und unannehmbare Einmischung bedeuten, durch die die eigentliche Substanz der garantierten Rechte beeinträchtigt wird.

Im Hinblick auf das in Artikel 8 der Europäischen Menschenrechtskonvention verankerte Recht auf Achtung des Privatlebens, das außerdem das Recht auf die Geheimhaltung des Gesundheitszustandes enthält, kann das Eingreifen durch eine öffentliche Stelle gerechtfertigt sein, vorausgesetzt, es ist „gesetzlich vorgeschrieben" und verfolgt eines der in Absatz 2 dieses Artikels aufgeführten Ziele, wie z. B. „wirtschaftliches Wohlergehen" und „Gesundheitsschutz", und ist notwendig, „um diese Ziele zu erreichen".

Dies ist nicht der Fall bei der Verwendung von Elementen, die in den Behandlungsunterlagen der Einzelperson enthalten sind, durch eine Institution für den alleinigen Zweck der Entwicklung eines Arguments, das ihr Desinteresse am Agieren zeigen würde.

Urteil des Gerichts für den öffentlichen Dienst (Erste Kammer) vom 5. Juli 2011 – V/Europäisches Parlament (Rechtssache F-46/09)

Das in Artikel 8 der Europäischen Menschenrechtskonventionen verankerte Recht auf Achtung des Privatlebens, das sich aus den gemeinsamen Verfassungstraditionen der Mitgliedstaaten herleitet, stellt ein von der Gemeinschaftsrechtsordnung geschütztes Grundrecht dar. Es umfasst insbesondere auch das Recht einer Person, ihren Gesundheitszustand geheim zu halten.

Die Übermittlung von personenbezogenen Daten über den Gesundheitszustand einer Person, die von einem Organ erhoben worden sind, an einen Dritten, auch an ein anderes Organ, stellt als solche einen Eingriff in das Privatleben der betreffenden Person dar, unabhängig von der späteren Verwendung der übermittelten Informationen.

Gemäß Artikel 8 Absatz 2 der Konvention kann der Eingriff einer Behörde in das Privatleben gerechtfertigt sein, soweit er „gesetzlich vorgesehen" ist, mit ihm ein oder mehrere – abschließend aufgezählte – Ziele verfolgt werden und er für die Erreichung dieser Ziele „notwendig" ist.

Aufgrund des überaus intimen und sensiblen Charakters medizinischer Daten ist die Möglichkeit, solche Informationen ohne Einwilligung der betroffenen Person einem Dritten zu übermitteln oder mitzuteilen, auch wenn es sich dabei um ein anderes Organ oder eine andere Einrichtung der Union handelt, besonders streng zu prüfen.

Urteil des Gerichts (Zweite Kammer) vom 23. November 2011 – Gert-Jan Dennekamp/Europäisches Parlament (Rechtssache T-82/09)

Die Verordnung Nr. 1049/2001 soll, wie sich aus ihrem vierten Erwägungsgrund und Art. 1 ergibt, der Öffentlichkeit ein größtmögliches Recht auf Zugang zu den Dokumenten der Organe gewähren (Vgl. Urteil vom 1. Juli 2008 *Schweden und Turco/Rat*, C-39/05 P und C-52/05 P, Slg. 2008, I-4723, Randnr. 33).

Wird beim Rat die Verbreitung eines Dokuments beantragt, muss er in jedem Einzelfall prüfen, ob es unter die in Art. 4 der Verordnung Nr. 1049/2001 genannten Ausnahmen vom Recht der Öffentlichkeit auf Zugang zu Dokumenten der Organe fällt (vgl. diesbezüglich *Schweden und Turco/Rat*, Randnr. 21 oben, Randnr. 35). Angesichts der mit der Verordnung Nr. 1049/2001 verfolgten Ziele sind diese Ausnahmen eng auszulegen und anzuwenden (*Schweden und Turco/Rat*, Randnr. 36).

Zweitens ist aus der Rechtsprechung ersichtlich, dass bei der Prüfung des Verhältnisses zwischen den Verordnungen Nrn. 1049/2001 und 45/2001 im Hinblick auf die Anwendung der Ausnahme des Art. 4 Abs. 1 Buchst. b der Verordnung Nr. 1049/2001 – nämlich den Schutz und die Integrität des Einzelnen – auf den vorliegenden Fall zu beachten ist, dass diese Verordnungen unterschiedliche Ziele haben. Verordnung Nr. 1049/2010 zielt darauf ab, die größtmögliche Transparenz des Entscheidungsprozesses staatlicher Stellen und der Informationen, auf denen ihre Entscheidungen beruhen, zu gewährleisten. Sie soll also die Ausübung des Rechts auf Zugang zu Dokumenten so weit wie möglich erleichtern und eine gute Verwaltungspraxis fördern. Verordnung Nr. 45/2001 dient dem Schutz der Grundrechte und Grundfreiheiten der natürlichen Personen und insbesondere deren Recht auf die Privatsphäre bei der Verarbeitung personenbezogener Daten (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 49).

Da die Verordnungen Nrn. 1049/2001 und 45/2001 keine Bestimmungen enthalten, die ausdrücklich den Vorrang der einen gegenüber der anderen vorsähen, ist ihre volle Anwendung zu gewährleisten (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 56).

Art. 4 Abs. 1 Buchst. b der Verordnung Nr. 1049/2001 enthält eine spezifische, verstärkte Schutzregelung für Personen, deren personenbezogene Daten gegebenenfalls veröffentlicht werden könnten (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 60).

Wenn ein nach der Verordnung Nr. 1049/2001 gestellter Antrag auf die Gewährung des Zugangs zu Dokumenten gerichtet ist, die personenbezogene Daten enthalten, werden die Bestimmungen der Richtlinie Nr. 45/2001 einschließlich ihres Art. 8 in vollem Umfang anwendbar (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 60).

Drittens sollte angemerkt werden, dass im vorliegenden Fall der Kläger den Antrag auf Zugang gestellt hat, um die Namen der MdEP, die zum Zeitpunkt der ersten Antragstellung oder zum 1. September 2005 an der Ruhegehaltsergänzungsregelung teilgenommen haben, sowie die Namen derer, die zum Zeitpunkt der ersten Antragstellung an dieser Regel teilgenommen und vom Europäischen Parlament einen monatlichen Beitrag erhalten haben, in Erfahrung zu bringen. Die Namen der MdEP stellen gemäß Art. 2 Buchst. a der Verordnung Nr. 45/2001 personenbezogene Daten dar (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 68).

Des Weiteren fällt, wie das Europäisches Parlament im angefochtenen Urteil zutreffend festgestellt hat, die Weitergabe solcher Daten unter die in der Verordnung Nr. 45/2001 verwendeten Definition von „Verarbeitung" (*Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 69).

Demzufolge trat im Hinblick auf den Antrag auf Zugang zu Dokumenten mit personenbezogenen Daten des Klägers Art. 8 Buchst. b der Verordnung Nr. 45/2001 in Kraft. Die Argumentation des Klägers, dass die von ihm angefragte „Verarbeitung" gemäß Art. 5 Buchst. b der Verordnung Nr. 45/2001 rechtmäßig gewesen sei und dies ausreiche, da Art. 8 Buchst. b dieser Verordnung Artikel 5 nicht berühre, ist daher unmöglich.

Um eine Offenlegung der in den Dokumenten enthaltenen personenbezogenen Daten zu erwirken, hätte der Kläger die Notwendigkeit der Übermittlung dieser personenbezogenen Daten darlegen müssen, damit das Europäisches Parlament anschließend die verschiedenen Interessen der Beteiligten gegeneinander abwägen und gemäß Art. 8 Buchst. b der Verordnung Nr. 45/2001 hätte prüfen können, ob ein Grund für die Annahme, dass durch diese Übermittlung möglicherweise die berechtigten Interessen der MdEP beeinträchtigt werden konnten, bestand oder nicht (vgl. *Kommission/Bavarian Lager*, Randnr. 13 oben, Randnr. 78).

Urteil des Gerichtshofs (Dritte Kammer) vom 24. November 2011 – Scarlet Extended SA/Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (Rechtssache C-70/10)

Richtlinien 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft und 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums in Verbindung mit den Richtlinien 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) und 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr), die im Licht der Artikel 7, 8, 11 und 52 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie der Artikel 8 und 10 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten ausgelegt wurden, dass sie dem nationalen Richter erlauben, in einem Verfahren zur Hauptsache allein aufgrund der Vorschrift, dass „[die nationalen Gerichte] … ebenfalls eine Unterlassungsanordnung gegen Vermittler erlassen [können], deren Dienste von einem Dritten zur Verletzung eines Urheberrechts oder verwandter Rechte genutzt werden", gegen einen Anbieter von Internetzugangsdiensten die Anordnung zu erlassen, auf eigene Kosten zeitlich unbegrenzt für sämtliche Kunden generell und präventiv ein Filtersystem für alle eingehenden und ausgehenden elektronischen Kommunikationen, die mittels seiner Dienste insbesondere unter Verwendung von „Peer-to-Peer"-Programmen durchgeleitet werden, einzurichten, um in seinem Netz den Austausch von Dateien zu identifizieren, die ein Werk der Musik, ein Filmwerk oder audiovisuelles Werk enthalten, an denen der Kläger Rechte zu haben behauptet, und dann die Übertragung dieser Werke entweder auf der Ebene des Abrufs oder bei der Übermittlung zu sperren".

Urteil des Gerichtshofs (Dritte Kammer) vom 24. November 2011 – Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) und Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10)/Administración del Estado. (Verbundene Rechtssachen C-468/10 und C-469/10)

Mit seiner ersten Frage möchte das vorlegende Gericht wissen, ob Art. 7 Buchst. f der Richtlinie 95/46 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für die Verarbeitung personenbezogener Daten, die zur Verwirklichung des berechtigten Interesses, das von dem für diese Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen diese Daten übermittelt werden, erforderlich ist, ohne Einwilligung der betroffenen Person nicht nur verlangt, dass deren Grundrechte und Grundfreiheiten nicht verletzt werden, sondern auch, dass diese Daten in öffentlich zugänglichen Quellen enthalten sind.

Art. 1 der Richtlinie 95/46 verpflichtet die Mitgliedstaaten, den Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten zu gewährleisten (vgl. in diesem Sinne Urteil vom 16. Dezember 2008, *Huber*, C-524/06, Slg. 2008, I-9705, Randnr. 47).

Gemäß den Bestimmungen des Kapitels II („Allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten“) der Richtlinie 95/46 muss jede Verarbeitung personenbezogener Daten – vorbehaltlich der in Art. 13 zugelassenen Ausnahmen – den in Art. 6 der Richtlinie aufgestellten Grundsätzen in Bezug auf die Qualität der Daten und einem der sechs in Art. 7 der Richtlinie aufgeführten Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung von Daten genügen (vgl. in diesem Sinne Urteil vom 20. Mai 2003, *Österreichischer Rundfunk u. a.*, C-465/00, C-138/01 und C-139/01, Slg. 2003, I-4989, Randnr. 65, sowie Urteil *Huber*, Randnr. 48).

Aus dem siebten Erwägungsgrund der Richtlinie 95/46 ergibt sich, dass die Errichtung und das Funktionieren des Binnenmarkts durch die in den nationalen Regelungen über die Verarbeitung personenbezogener Daten bestehenden Unterschiede in schwerwiegender Weise beeinträchtigt werden können (vgl. Urteil vom 6. November 2003, *Lindqvist*, C-101/01, Slg. 2003, I-12971, Randnr. 79).

In diesem Zusammenhang ist darauf hinzuweisen, dass die Richtlinie 95/46, wie sich insbesondere aus ihrem achten Erwägungsgrund ergibt, bezweckt, in allen Mitgliedstaaten ein gleichwertiges Schutzniveau hinsichtlich der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten herzustellen. Der zehnte Erwägungsgrund der Richtlinie ergänzt, dass die Angleichung der nationalen Rechtsvorschriften in dem entsprechenden Bereich nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen darf, sondern im Gegenteil darauf abzielen muss, in der Union ein hohes Schutzniveau sicherzustellen (vgl. in diesem Sinne Urteile *Lindqvist*, Randnr. 95, und *Huber*, Randnr. 50).

So wurde entschieden, dass die Harmonisierung dieser nationalen Rechtsvorschriften nicht auf eine Mindestharmonisierung beschränkt ist, sondern zu einer grundsätzlich umfassenden Harmonisierung führt. Im Hinblick darauf will die Richtlinie 95/46 den freien Verkehr personenbezogener Daten sicherstellen, wobei sie zugleich ein hohes Niveau des Schutzes der Rechte und Interessen der von diesen Daten betroffenen Personen gewährleistet (vgl. Urteil *Lindqvist*, Randnr. 96).

Daher ergibt sich aus dem Ziel, ein gleichwertiges Schutzniveau in allen Mitgliedstaaten sicherzustellen, dass Art. 7 der Richtlinie 95/46 eine erschöpfende und abschließende Liste der Fälle vorsieht, in denen eine Verarbeitung personenbezogener Daten als rechtmäßig angesehen werden kann.

Diese Auslegung wird durch die Formulierung „lediglich erfolgen darf, wenn eine der folgenden Voraussetzungen erfüllt ist“ in Art. 7 der Richtlinie 95/46 bestätigt, die den erschöpfenden und abschließenden Charakter der in diesem Artikel enthaltenen Liste unterstreicht.

Folglich dürfen die Mitgliedstaaten weder neue Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten neben Art. 7 der Richtlinie 95/46 einführen, noch zusätzliche Bedingungen stellen, die die Tragweite eines der sechs in diesem Artikel vorgesehenen Grundsätze verändern würden.

Die vorstehende Auslegung wird auch durch Art. 5 der Richtlinie 95/46 nicht in Frage gestellt. Dieser Artikel erlaubt nämlich den Mitgliedstaaten lediglich, nach Maßgabe des Kapitels II und damit des Art. 7 dieser Richtlinie die Voraussetzungen näher zu bestimmen, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist.

Von dem Ermessen, über das die Mitgliedstaaten nach diesem Art. 5 verfügen, kann also nur im Einklang mit dem von der Richtlinie 95/46 verfolgten Ziel Gebrauch gemacht werden, ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren (vgl. Urteil *Lindqvist*, Randnr. 97).

Die Richtlinie 95/46 enthält Vorschriften, die durch eine gewisse Flexibilität gekennzeichnet sind, und überlässt es in vielen Fällen den Mitgliedstaaten, die Einzelheiten zu regeln oder zwischen Optionen zu wählen (vgl. Urteil *Lindqvist*, Randnr. 83). Es ist somit wichtig, zwischen nationalen Maßnahmen, die zusätzliche Bedingungen vorsehen, mit denen die Tragweite eines in Art. 7 der Richtlinie 95/46 enthaltenen Grundsatzes verändert wird, einerseits und nationalen Maßnahmen, die nur einen dieser Grundsätze näher bestimmen, andererseits zu unterscheiden. Die zuerst genannte Art von nationalen Maßnahmen ist verboten. Nur im Rahmen der zweiten Art von nationalen Maßnahmen verfügen die Mitgliedstaaten nach Art. 5 der Richtlinie 95/46 über einen Ermessensspielraum.

Folglich dürfen die Mitgliedstaaten nach Art. 5 der Richtlinie 95/46 auch keine anderen Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten als die in Art. 7 dieser Richtlinie aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in diesem Art. 7 vorgesehenen Grundsätze verändern.

Im vorliegenden Fall sieht Art. 7 Buchstlit. f der Richtlinie 95/46 vor, dass die Verarbeitung personenbezogener Daten rechtmäßig ist, wenn sie „erforderlich [ist] zur Verwirklichung des berechtigten Interesses, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person, die gemäß Artikel 1 Absatz 1 geschützt sind, [überwiegen]“.

Dieser Art. 7 Buchst. f sieht zwei kumulative Voraussetzungen vor, damit eine Verarbeitung personenbezogener Daten rechtmäßig ist, nämlich zum einen, dass die Verarbeitung personenbezogener Daten zur Verwirklichung des berechtigten Interesses erforderlich ist, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, und zum anderen, dass nicht die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

Demnach steht Art. 7 Buchst. f der Richtlinie 95/46 hinsichtlich der Verarbeitung personenbezogener Daten jeder nationalen Regelung entgegen, die bei Fehlen der Einwilligung der betroffenen Person neben den beiden in der vorstehenden Randnummer genannten kumulativen Voraussetzungen zusätzliche Erfordernisse aufstellt.

Jedoch ist zu berücksichtigen, dass die zweite dieser Voraussetzungen eine Abwägung der jeweiligen einander gegenüberstehenden Rechte und Interessen erfordert, die grundsätzlich von den konkreten

Umständen des betreffenden Einzelfalls abhängt und in deren Rahmen die Person oder die Einrichtung, die die Abwägung vornimmt, die Bedeutung der Rechte der betroffenen Person, die sich aus den Art. 7 und 8 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta) ergeben, zu berücksichtigen hat.

Gemäß Art. 8 Abs. 1 der Charta hat „[j]ede Person ... das Recht auf Schutz der sie betreffenden personenbezogenen Daten". Dieses Grundrecht steht in engem Zusammenhang mit dem in Art. 7 der Charta verankerten Recht auf Achtung des Privatlebens (Urteil vom 9. November 2010, *Volker und Markus Schecke und Eifert*, C-92/09 und C-93/09, Slg. 2010, I-0000, Randnr. 47).

Nach der Rechtsprechung des Gerichtshofs erstreckt sich die in den Art. 7 und 8 der Charta anerkannte Achtung des Privatlebens hinsichtlich der Verarbeitung personenbezogener Daten auf jede Information, die eine bestimmte oder bestimmbare natürliche Person betrifft (vgl. Urteil *Volker und Markus Schecke und Eifert*, Randnr. 52). Allerdings geht aus den Art. 8 Abs. 2 und 52 Abs. 1 der Charta hervor, dass dieses Recht unter bestimmten Voraussetzungen Beschränkungen unterworfen werden kann.

Außerdem ist es Sache der Mitgliedstaaten, bei der Umsetzung der Richtlinie 95/46 darauf zu achten, dass sie sich auf eine Auslegung derselben stützen, die es ihnen erlaubt, ein angemessenes Gleichgewicht zwischen den verschiedenen durch die Unionsrechtsordnung geschützten Grundrechten und Grundfreiheiten sicherzustellen (vgl. entsprechend Urteil vom 29. Januar 2008, *Promusicae*, C-275/06, Slg. 2008, I-271, Randnr. 68).

Bei der nach Art. 7 Buchst. f der Richtlinie 95/46 erforderlichen Abwägung kann berücksichtigt werden, dass die Grundrechte der betroffenen Person durch diese Datenverarbeitung unterschiedlich stark beeinträchtigt sein können, je nachdem, ob die in Rede stehenden Daten bereits in öffentlich zugänglichen Quellen enthalten sind oder nicht.

Denn im Unterschied zur Verarbeitung von Daten, die in öffentlich zugänglichen Quellen enthalten sind, impliziert die Verarbeitung von Daten aus nicht öffentlich zugänglichen Quellen zwangsläufig, dass der für die Verarbeitung Verantwortliche und gegebenenfalls der bzw. die Dritten, denen die Daten übermittelt werden, von Informationen über die Privatsphäre der betroffenen Person Kenntnis erlangen. Diese schwerere Beeinträchtigung der in den Art. 7 und 8 der Charta verbürgten Rechte der betroffenen Person ist gebührend zu berücksichtigen, indem sie gegen das berechtigte Interesse, das von dem für die Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen die Daten übermittelt werden, abgewogen wird.

Insoweit ist darauf hinzuweisen, dass nichts dagegen spricht, dass die Mitgliedstaaten in der Ausübung ihres Ermessens nach Art. 5 der Richtlinie 95/46 Leitlinien für diese Abwägung aufstellen.

Es handelt sich jedoch nicht mehr um eine nähere Bestimmung im Sinne dieses Art. 5, wenn eine nationale Regelung die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließt, indem sie für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen abschließend vorschreibt, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt.

Unbeschadet des Art. 8 der Richtlinie 95/46 über die Verarbeitung besonderer Kategorien personenbezogener Daten, der für den Rechtsstreit des Ausgangsverfahrens nicht einschlägig ist, verbietet daher Art. 7 Buchst. f der Richtlinie 95/46, dass ein Mitgliedstaat kategorisch und verallgemeinernd die Verarbeitung bestimmter Kategorien personenbezogener Daten ausschließt, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen.

Aufgrund dieser Erwägungen ist auf die erste Vorlagefrage zu antworten, dass Art. 7 Buchst. f der Richtlinie 95/46 dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für die

Verarbeitung personenbezogener Daten, die zur Verwirklichung des berechtigten Interesses, das von dem für diese Verarbeitung Verantwortlichen oder von dem bzw. den Dritten wahrgenommen wird, denen diese Daten übermittelt werden, erforderlich ist, ohne Einwilligung der betroffenen Person nicht nur verlangt, dass deren Grundrechte und Grundfreiheiten nicht verletzt werden, sondern auch, dass diese Daten in öffentlich zugänglichen Quellen enthalten sind, und damit kategorisch und verallgemeinernd jede Verarbeitung von Daten ausschließt, die nicht in solchen Quellen enthalten sind.

Zur zweiten Vorlagefrage

Mit seiner zweiten Frage möchte das vorlegende Gericht wissen, ob Art. 7 Buchst. f der Richtlinie 95/46 unmittelbare Wirkung hat.

Insoweit ist zu beachten, dass sich nach ständiger Rechtsprechung des Gerichtshofs der Einzelne in all den Fällen, in denen die Bestimmungen einer Richtlinie inhaltlich unbedingt und hinreichend genau sind, vor den nationalen Gerichten gegenüber dem Staat auf diese Bestimmungen berufen kann, wenn der Staat die Richtlinie nicht fristgemäß oder unzulänglich in nationales Recht umgesetzt hat (vgl. Urteil vom 3. März 2011, *Auto Nikolovi*, C-203/10, Slg. 2011, I-0000, Randnr. 61 und die dort angeführte Rechtsprechung).

Es ist festzustellen, dass Art. 7 Buchst. f der Richtlinie 95/46 so genau ist, dass sich ein Einzelner darauf berufen und ein nationales Gericht ihn anwenden kann. Im Übrigen räumt zwar die Richtlinie 95/46 den Mitgliedstaaten unbestreitbar ein mehr oder weniger großes Ermessen bei der Umsetzung einiger ihrer Bestimmungen ein, doch begründet Art. 7 Buchst. f eine unbedingte Verpflichtung (vgl. entsprechend Urteil *Österreichischer Rundfunk u. a.*, Randnr. 100).

Die Verwendung des Ausdrucks „sofern“ in Art. 7 Buchst. f der Richtlinie 95/46 reicht für sich nicht aus, um die Unbedingtheit dieser Bestimmung im Sinne dieser Rechtsprechung in Frage zu stellen.

Dieser Ausdruck zielt nämlich auf das Vorliegen einer der beiden in Art. 7 Buchst. f der Richtlinie 95/46 vorgesehenen kumulativen Voraussetzungen ab, von deren Einhaltung die Möglichkeit abhängt, personenbezogene Daten ohne Einwilligung der betroffenen Person zu verarbeiten. Da dieses Element festgelegt ist, nimmt es Art. 7 Buchst. f nicht seine Genauigkeit und Unbedingtheit.

Daher ist auf die zweite Frage zu antworten, dass Art. 7 Buchst. f der Richtlinie 95/46 unmittelbare Wirkung hat.

3.3. EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Laufe des Jahres 2011 setzte der EDSB in verschiedenen Tätigkeitsbereichen neue Maßstäbe. Bei der **Aufsicht über die Organe und Einrichtungen der EU** hinsichtlich der Verarbeitung personenbezogener Daten hat der EDSB mit mehr behördlichen Datenschutzbeauftragten in mehr Organen und Einrichtungen zusammengearbeitet als jemals zuvor. Darüber hinaus zeigt die neue **Durchsetzungspolitik** des EDSB Wirkung: Die meisten Organe und Einrichtungen der EU verzeichnen bei der Einhaltung der Datenschutzverordnung gute Fortschritten, wenngleich an manchen Stellen noch verstärkte Anstrengungen unternommen werden sollten.

Bei der **Beratung zu neuen Rechtsetzungsmaßnahmen** gab der EDSB die bislang größte Anzahl an Stellungnahmen zu einer breiten Themenvielfalt heraus. Die **Überarbeitung des EU-Rechtsrahmens für den Datenschutz** stand dabei ganz oben auf der Prioritätenliste. Doch auch die Umsetzung des **Stockholmer Programms** für den Raum der Freiheit, der Sicherheit und des Rechts sowie die **Digitale Agenda** als Eckpfeiler der Strategie Europa 2020 hatten Auswirkungen auf den Datenschutz. Gleiches gilt für Themen im Bereich des Binnenmarktes, des Gesundheitswesens, des Verbraucherschutzes und der grenzüberschreitenden Durchsetzung.

Des Weiteren erhöhte der EDSB die **Zusammenarbeit** mit anderen Aufsichtsbehörden und vertiefte die Effizienz und Wirksamkeit seiner **Einrichtung** und **Kommunikation**.

Für das Jahr 2012 hat sich der EDSB unter anderem folgende Hauptziele gesetzt:

- **Bewusstseinsbildung**: Der EDSB wird Zeit und Ressourcen investieren, um Organen und Einrichtungen der EU Hilfestellungen in Form von thematischen Richtlinien, Fortbildungen, Workshops und einer speziellen Sektion für behördliche Datenschutzbeauftragte auf der EDSB-Website zu geben.

- Die **Festlegung von Vorgehensweisen** für den Umgang mit Meldungen für Standardverwaltungsverfahren und für bereits laufende Datenverarbeitungen.

- Eine Umfrage zum Stand der Dinge für **behördliche Datenschutzbeauftragte** in Organen und Einrichtungen der EU durchzuführen, um ihre Rolle gemäß dem Prinzip der Verantwortlichkeit zu **stärken**.

- **Besuche und Inspektionen** bei Organen und Einrichtungen, nicht nur zur Durchsetzung, sondern auch zur Schaffung eines Bewusstseins für Datenschutzfragen und die Rolle des EDSB.

- In seiner Rolle als Berater wird der EDSB 2012 einen Schwerpunkt auf die Arbeit am **Rechtsrahmen für den Datenschutz in der EU** legen.

- **Technische Entwicklungen**, insbesondere im Internet und damit verbundenen Politikbereichen, werden ein weiterer Schwerpunkt sein. Dies beinhaltet Pläne für einen gesamteuropäischen Rahmen für elektronische Identifizierung, Authentifizierung und Signaturen, den Themenbereich Überwachung des Internets (z. B. Durchsetzung von Rechten an geistigem Eigentum und Verfahren zur Entfernung von Inhalten), Cloud-Computing, und elektronische Gesundheitsdienste. Der EDSB wird zudem seine technischen Fachkompetenzen stärken und Technologien zum besseren Schutz der Privatsphäre („privacy-enhancing technologies“) erforschen.

- Der **Raum der Freiheit, der Sicherheit und des Rechts** (z. B. EUTFTS und intelligente Grenzen) und die Reform des Finanzsektors sollen weiter ausgebaut werden, sofern sie sich auf das Recht auf Privatsphäre und Datenschutz auswirken.

- Der EDSB wird zudem weiterhin seine Aufgaben im Bereich der **koordinierten Aufsicht** wahrnehmen und die Kontakte mit nationalen Datenschutzbehörden und internationalen Organisationen ausbauen, um ein Datenschutzbewusstsein zu schaffen und bewährte Praktiken auszutauschen.

Organisation	**Europäischer Datenschutzbeauftragter**
Vorsitz und/oder Gremium	Peter Hustinx, Europäischer Datenschutzbeauftragter Giovanni Buttarelli, Stellvertretender Europäischer Datenschutzbeauftragter
Budget	7 564 137 EUR
Personal	52 Mitarbeiter (37 EU-Beamte)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden **24 legislative Stellungnahmen** u. a. zu Initiativen im Raum der Freiheit, der Sicherheit und des Rechts sowie in den Bereichen technologische Entwicklungen, internationale Zusammenarbeit, Datenübermittlungen und Binnenmärkte abgegeben. Es wurden **12 formelle Kommentare** u. a. zu den Themen geistiges Eigentum, Sicherheit der Zivilluftfahrt, EU-Kriminalpolitik und Energieeffizienz sowie zum System zum Aufspüren der Terrorismusfinanzierung und zum Programm „Grundrechte und Unionsbürgerschaft“ abgegeben.
Meldungen	Es gingen **164 Meldungen** zu Datenverarbeitungsvorgängen der Institutionen und Organe der EU ein, die spezielle Risiken beinhalteten.
Vorabprüfungen	Es wurden **71 Stellungnahmen im Rahmen einer Vorabkontrolle** durchgeführt, insbesondere zu Gesundheitsdaten, zu Beurteilungen und zur Einstellung von Personal, zum Verdacht auf Verstöße und zu elektronischer Überwachung durchgeführt.
Anfragen betroffener Personen	Es gingen **196 schriftliche Auskunftsersuche bzw. Anforderungen von Beratungen** aus der allgemeinen Öffentlichkeit ein, hauptsächlich zu den Themen Online-Datenschutz, internationale Datenübermittlungen, Rechtsrahmen des EU-Datenschutzes und Datenspeicherung.

Beschwerden betroffener Personen	**107 eingegangene Beschwerden, 26 davon zulässig** Vorrangige Arten vermuteter Verstöße: Datenzugang und -berichtigung, Einspruch und Löschung, Verletzung der Vertraulichkeit von Daten, unverhältnismäßige Erfassung von Daten und Datenverlust.
Vom Parlament bzw. der Regierung angeforderte Beratung	Von den 24 oben genannten legislativen Stellungnahmen wurden **20** auf Anfrage der Europäischen Kommission abgegeben (Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001).
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	**34 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	**4 Vor-Ort-Inspektion** beim CEDEFOP, beim OLAF und bei der EZB **Nachbereitung** von Empfehlungen, die bei früheren Prüfungen abgegeben wurden **Sicherheitsprüfung** des Visa-Informationssystems (VIS)
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	**Überwachung der Umsetzung der Verordnung (EG) Nr. 45/2001**: Die dritte Bestandsaufnahme hat zu einem Bericht geführt, der die von den Einrichtungen und Organen erzielten Fortschritte bei der Umsetzung der Verordnung sowie die Schwachstellen herausarbeitet. Eintägige Besuche bei der Europäischen Eisenbahnagentur, beim Gemeinschaftlichen Sortenamt, bei der Europäischen Stiftung zur Verbesserung der Lebens- und Arbeitsbedingungen sowie bei der Agentur für das Europäische GNSS.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	54 DPO in EU-Einrichtungen und -Organen.

B. Informationen zur Rechtsprechung

Beteiligungen des EDSB an Gerichtsverhandlungen

In der **Rechtssache V./Europäisches Parlament (F-46/09)** wurde der EDSB vom Gericht für den öffentlichen Dienst aufgefordert, dem Verfahren als Streithelfer beizutreten. Gegenstand des Verfahrens war die vermeintlich rechtswidrige Übermittlung medizinischer Daten durch den Ärztlichen Dienst der Kommission an den Ärztlichen Dienst des Europäischen Parlaments. Der EDSB vertrat die Sache der Klägerin und brachte vor, die Übermittlung sei nicht mit den Datenschutzbestimmungen vereinbar gewesen, da sie nicht notwendig gewesen sei und keine ordnungsgemäße Rechtsgrundlage gehabt habe. In seinem Urteil vom 5. Juli 2011 folgte das Gericht für den öffentlichen Dienst der Argumentation des EDSB und entschied zugunsten der Klägerin.

In seinem Urteil vom 7. Juli 2011 in der **Rechtssache Valero Jordana/Kommission (T-161/04)** befand das Gericht, die Kommission habe einen Antrag auf Zugang zu bestimmten personenbezogenen Daten zu Unrecht nicht nach Maßgabe der Datenschutzbestimmungen gewürdigt. Diese Schlussfolgerung entsprach dem Vorbringen des EDSB zu den Argumenten des Gerichts.

In seinem Urteil vom 23. November 2011 in der **Rechtssache Dennekamp/Europäisches Parlament (T-82/09)** stellte das Gericht fest, dass der Kläger – ein Journalist, der sich nach den Namen der Parlamentsmitglieder erkundigte, die an einer Ruhegehaltsergänzungsregelung teilnahmen – nicht die Notwendigkeit nachgewiesen hatte, die Daten öffentlich zu machen. Der EDSB hatte die gegenteilige Auffassung vertreten, da ein Ausgleich der unterschiedlichen beteiligten Interessen zu einer Weitergabe der Daten an den Journalisten hätte führen sollen.

In der **Rechtssache Egan & Hackett/Europäisches Parlament (T-190/10)** ist noch kein Urteil des Gerichtes ergangen. Gegenstand der Rechtssache war ein Antrag auf Zugang zu den Namen der Assistenten von Mitgliedern des Europäischen Parlaments.

Der EDSB trat außerdem einem Vertragsverletzungsverfahren – **Kommission/Österreich (C-614/10)** – als Streithelfer bei, in dem die unzureichende Unabhängigkeit der österreichischen Datenschutzkommission verhandelt wurde. Der EDSB reichte einen Streithilfeschriftsatz ein, in dem er sich den Schlussfolgerungen der Kommission anschloss, dass die Unabhängigkeit der österreichischen Datenschutzkommission infolge ihrer Ansiedlung beim Bundeskanzleramt nicht hinreichend gewahrt sei.

Schließlich befasste die ENISA das Gericht mit einer Entscheidung des EDSB zu einer **Beschwerde (T-345/11)**. Die Klage wurde aus Verfahrensgründen für offenkundig unzulässig erklärt.

Rechtsprechung im Datenschutzbereich

In der **Rechtssache Deutsche Telekom (C-543/09)** wurde die Frage erörtert, ob nach der Datenschutzrichtlinie für elektronische Kommunikation ein Unternehmen, das Endnutzern Telefonnummern zuweist, berechtigt ist, Daten über diese Endnutzer an ein anderes Unternehmen weiterzugeben, das öffentlich zugängliche Auskunftsdienste oder Teilnehmerverzeichnisse anbietet, ohne dass von den betroffenen Teilnehmern eine erneute Zustimmung erteilt worden ist. Der Gerichtshof vertrat in seinem Urteil vom 5. Mai 2011 die Auffassung, dass eine erneute Einwilligung nicht erforderlich sei, da die Teilnehmer bereits zuvor ordnungsgemäß über diese Möglichkeit unterrichtet wurden.

In seinem Urteil vom 24. November 2011 in der **Rechtssache ASNEF und FECEMD (verbundene Rechtssachen C-648/10 und C-469/10)** antwortete der Gerichtshof einem spanischen Gericht, das um Klärung einer Bestimmung der Datenschutzrichtlinie ersucht hatte, die die Verarbeitung

personenbezogener Daten ermöglicht, wenn sie der Verwirklichung eines berechtigten Interesses dient und nicht das Interesse der betroffenen Person überwiegt. Nach spanischem Recht war dies nur bei bereits öffentlich zugänglichen personenbezogenen Daten möglich. Nach Auffassung des Gerichtshofes entspricht diese einzelstaatliche Einschränkung nicht den Vorgaben der Richtlinie, die in diesem Punkt unmittelbare Wirkung hat.

Am 24. November 2011 erließ der Gerichtshof in einem belgischen Fall eine Vorabentscheidung in Bezug auf die Verpflichtung eines Internetdienstanbieters (Scarlet Extended), das Surfverhalten seiner Kunden zu überwachen, um die Verletzung von Rechten des geistigen Eigentums zu verhindern (C-70/10). Nach Auffassung des Gerichtshofes entsprach die Verpflichtung einer allgemeinen Überwachungspflicht, die nach den EU-Vorschriften für den elektronischen Geschäftsverkehr verboten ist. Der Gerichtshof stellte zudem fest, dass eine derartige Verpflichtung kein angemessenes Gleichgewicht zwischen der Durchsetzung des Rechts am geistigen Eigentum und verschiedenen in der Charta der Grundrechte verankerten Grundrechten und Grundfreiheiten darstelle, zu denen auch das Recht auf Datenschutz zähle.

Kapitel Vier

Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

ISLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Eines der wichtigsten Themen im Jahr 2011 war die Verarbeitung personenbezogener Daten im Zusammenhang mit anonymen Meldungen an Verwaltungsbehörden bezüglich angeblicher Rechtsverstöße. Auf den Websites sowohl des Arbeitsministeriums als auch des Finanzamtes erhielten Bürgerinnen und Bürger die Möglichkeit, ihre Verdächtigungen in Bezug auf Steuerhinterziehung und damit zusammenhängende Straftaten anonym zu melden. Die Datenschutzbehörde beschloss, die Zulässigkeit der Verarbeitung personenbezogener Daten im Zusammenhang mit diesem anonymen Meldungsverfahren zu untersuchen. Das Ergebnis dieser Untersuchung wurde im Rahmen von an die entsprechenden Behörden gerichteten Beschlüssen veröffentlicht, laut derer die Verwendung von Formularen zur anonymen Meldung u. a. zu einer unsachgemäßen Erfassung personenbezogener Daten führen könnte. Des Weiteren befand die Datenschutzbehörde Anonymitätsgarantien als unzuverlässig, da Telekommunikationstechnologien die Möglichkeit bieten, den Absender von Meldungen ausfindig zu machen, z. B. falls eine polizeiliche Ermittlung falscher Anschuldigungen in die Wege geleitet wird. Auch wenn eine Verwaltungsbehörde Bürger nie gänzlich davon abhalten kann, anonyme Meldungen einzusenden, sollte ihnen angesichts der oben dargelegten Lage nicht ausdrücklich die Möglichkeit gegeben werden, auf solche Weise Meldungen zu machen. Folglich kam die Datenschutzbehörde zu dem Schluss, dass die auf den Websites der entsprechenden Behörden bereitgestellten Formulare für solche Meldungen nicht mit dem Datenschutzgesetz vereinbar sind.

Ein weiteres wichtiges Thema war der vom nationalen Verfassungsausschuss vorgelegte Entwurf einer neuen Verfassung für Island. Der Ausschuss war nach den Wahlen 2010 ins Leben gerufen worden. Der Entwurf enthielt eine Bestimmung über das Recht auf Datenschutz, das mit der Bestimmung über dieses Recht in der existierenden Verfassung von 1944 identisch ist. In einer Stellungnahme zu dem Entwurf verwies die Datenschutzbehörde auf Bestimmungen in neueren Verfassungen und Menschenrechtschartas, darunter die Charta der Grundrechte der Europäischen Union, in der das Recht auf den Schutz personenbezogener Daten gesondert erwähnt wird. Die Datenschutzbehörde forderte die nationale verfassungsgebende Versammlung dazu auf, eine solche Erklärung in ihren Entwurf aufzunehmen. Darüber hinaus wies die Datenschutzbehörde darauf hin, dass eine Bestimmung in dem Entwurf, nach der jeder das Recht auf die Erfassung und Verbreitung von Daten habe, sorgfältig durchdacht werden müsse, da eine uneingeschränkte Erfassung personenbezogener Daten nirgendwo sonst in der westlichen Welt erlaubt sei.

2011 wurden eine Reihe von Rechtsakten verabschiedet, die Bestimmungen zur Verarbeitung personenbezogenen Daten enthielten. Der bedeutendste davon ist Gesetz Nr. 68/2011 über Sonderuntersuchungsausschüsse. Laut diesem Gesetz kann das Parlament Kommissionen zur Untersuchung bestimmter Angelegenheiten ernennen. Diese Kommissionen haben laut dem Gesetz weitreichende Befugnisse – darunter die Befugnis zur Verarbeitung personenbezogener Daten. 2008 wurde ein Gesetz zu einem solchen Ausschuss verabschiedet: Gesetz Nr. 142/2008 über eine Untersuchung der Ereignisse und der Gründe für den Niedergang der isländischen Banken im Jahr 2008 sowie damit in Zusammenhang stehender Ereignisse. Die Bestimmungen in Gesetz Nr. 68/2011 stehen mit den Bestimmungen dieses vorhergehenden Gesetzes im Einklang. Eine Erläuterung des Letzteren ist im Kapitel zu Island des 12. Jahresberichtes der Artikel-29-Datenschutzgruppe zu finden.

Organisation	
Vorsitz und/oder Gremium	Sigrún Jóhannesdóttir, Kommissionsmitglied; Páll Hreinsson, Vorstandsvorsitzender bis November 2011, danach Björg Thorarensen.
Budget	69 Millionen ISK (ca. 434 000 EUR zum 31. Dezember 2011)
Personal	Fünf Rechtsberater, eine Sekretärin.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Etwa 100
Meldungen	470
Vorabprüfungen	110 Genehmigungen zur Verarbeitung von Daten.
Anfragen betroffener Personen	Etwa 400
Beschwerden betroffener Personen	139
Vom Parlament bzw. der Regierung angeforderte Beratung	Etwa 50
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	2011 wurden insgesamt 1 397 neue Fälle registriert.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	14
Sanktionsmaßnahmen	
Sanktionen	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.
Geldbußen	2011 wurden keine Geldbußen in Form von Tagessätzen verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung:

Am 20. Oktober 2011 fällte der Oberste Gerichtshof Islands ein Urteil (Rechtssache Nr. 706/2010) betreffend der Veröffentlichung eines Berichts über einen Unfall mit Todesfolge. In dem Bericht erläuterte die Unfalluntersuchungsgruppe ihre Ergebnisse bezüglich des Unfallhergangs, bei dem die fahrende Person ums Leben kam. Der überlebende Partner der fahrenden Person reichte eine Klage ein, in der er Schadenersatz für Personenschäden durch die Veröffentlichung des Berichts der Gruppe forderte, da der Name der fahrenden Person aus dem Bericht hervorging, obwohl dieser zuvor nicht bekannt gegeben worden war. Die Klage war zuvor bereits von der Datenschutzbehörde bearbeitet worden, die zu dem Schluss kam, dass die Identität der fahrenden Person aus dem Bericht hervorging und dessen Veröffentlichung einer Verarbeitung personenbezogener Daten entsprochen hätte. Angesichts der eindeutigen rechtlichen Bestimmungen, die die Veröffentlichung des Berichts der Gruppe vorsehen, und da die Gruppe in ihrem Bericht nur die nötigsten Informationen veröffentlicht hatte, konnte die Datenschutzbehörde keinen Verstoß gegen das Datenschutzgesetz feststellen. Sowohl das Bezirksgericht Reykjavík als auch der Oberste Gerichtshof gelangten beide zu dem Schluss, dass die Gruppe gesetzlich dazu verpflichtet war, den Bericht zu veröffentlichen, und dass die offengelegten Informationen keinen Rechtsverstoß darstellten. Demzufolge wurde die Klage auf Entschädigung abgewiesen.

LIECHTENSTEIN

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetz über Zentrales Personenregister

In der Landesverwaltung wird seit Jahren ein Register geführt, in dem insbesondere zahlreiche Daten aller Einwohner des Landes erfasst werden. Die Datenschutzstelle forderte seit Jahren die Schaffung einer gesetzlichen Grundlage für diese wichtige Datenbank. Dem wurde 2011 nachgekommen. Endlich wurde ein Gesetz geschaffen, in dem auch das Verfahren zur Neuregelung der Zugriffsberechtigung durch die einzelnen Behörden geregelt wird. Die Datenbank muss auch gewissen technischen Korrekturen unterworfen werden, insbesondere zur Gewährleistung der Verhältnismässigkeit bei den Zugriffsberechtigungen.

Schengen

2011 fand die Datenschutzevaluation statt. Die Datenschutzstelle (DSS) wurde dabei auf die Erfüllung verschiedener Aspekte wie die Unabhängigkeit, Struktur, gesetzliche Aufgaben und Kompetenzen sowie die Rechte der betroffenen Personen geprüft. Die Prüfung war positiv. Liechtenstein ist seit Dezember 2011 Mitglied von Schengen. Auf Grund mangelnder Ressourcen ist aber eine Teilnahme an den Sitzungen des Gemeinsamen Kontrollausschusses Schengen kaum möglich. Ein Ausbau der Ressourcen der DSS war zwar bei der Evaluation gefordert worden. Dies wurde jedoch nicht umgesetzt.

Öffentlichkeitsarbeit

Anlässlich des Europäischen Datenschutztages lud die DSS in Zusammenarbeit mit dem Institut für Wirtschaftsinformatik der Universität Liechtenstein zu einer öffentlichen Veranstaltung mit dem Titel „Schau mal, wer da spricht – Was Handys, Notebooks & Co alles erzählen". Handys, Notebooks und Tablet-PCs sind heutzutage aus unserem Alltag nicht mehr wegzudenken. Dank kompakter Geräte und schneller drahtloser Netzwerke kann überall kommuniziert und gearbeitet werden. Damit stand die Datenbearbeitung im Rahmen von mobilen Geräten im Zentrum.

Auf Einladung der privaten Universität im Fürstentum Liechtenstein nahmen wir an einer Podiumsdiskussion zum Thema „Der Zugriff des Staates auf private Daten am Beispiel der Vorratsdatenspeicherung" teil. Während in Deutschland die Vorratsdatenspeicherung durch das Bundesverfassungsgericht abgeschafft und sie in Österreich noch nicht eingeführt wurde, werden in Liechtenstein die Verkehrs- und Standortdaten aller Personen bei jeder Nutzung von Telefon oder Internet auf Vorrat gespeichert. Diesen erheblichen Eingriff in das Recht auf Privatsphäre aller Bürger bezeichnet der Europäische Datenschutzbeauftragte als die stärkste Massnahme, die je in der EU für einen Eingriff in die Privatsphäre geschaffen wurde.[19] In der Diskussion ging es um die Vor- und Nachteile einer solchen Speicherung.

[19] Vgl. Newsletter Januar 2011: „Angesichts des Anwendungsbereichs der Richtlinie und der Zahl der von ihr betroffenen Menschen hält der EDSB sie deshalb für die am stärksten in die Privatsphäre eingreifende Rechtsvorschrift, die jemals in der EU angenommen wurde": http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Newsletters/Newsletter_27_DE.pdf und Tätigkeitsbericht 2010.

Am Networking Day der Universität Liechtenstein wurden wir zur Podiumsdiskussion zum Thema *Cloud Computing* eingeladen.

2009 wurde die Möglichkeit geschaffen einen behördlichen oder betrieblichen Datenschutzverantwortlichen zu benennen als Ersatz der Meldepflicht von Datensammlungen. Zur Schaffung von Synergien in einem noch jungen Bereich luden wir die bereits bestehenden Verantwortlichen sowie Interessierte zu einem Gedankenaustausch mit dem Thema „Aufgaben und Stellung eines Datenschutzverantwortlichen ein.

Die Internetseite der DSS ist die Hauptinformationsquelle für die Öffentlichkeit.[20] Hier wurden unter anderem Informationen zum Thema *Cloud Computing* oder zum *Outsourcing* im Allgemeinen veröffentlicht wie auch eine Empfehlung zur Umsetzung von *technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit*.

Organisation	
Vorsitz und/oder Gremium	Dr. Philipp Mittelberger
Budget	682 000 CHF
Personal	2,2 Recht, 1,0 Technik, 0,8 Administration
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	11 Bewilligungen von Videoüberwachungsanlagen
Meldungen	k. A., sehr wenige neue Meldungen
Vorabprüfungen	k. A.
Anfragen betroffener Personen	64
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	24 Stellungnahmen zu Gesetzesentwürfen[21]
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	559 Anfragen[22]
Prüfmaßnahmen	
Prüfungen, Untersuchungen	verschiedene Kontrollen in Vorbereitung

[20] http://www.dss.llv.li/
[21] Vgl. Tätigkeitsbericht 2011 der DSS, unter 3., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.
[22] S. Statistik der DSS, Tätigkeitsbericht 2011 der DSS, unter 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2011.pdf.

Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	25 gemeldete Datenschutzverantwortliche bis Ende 2011

B. Informationen zur Rechtsprechung

2011 wurden durch die Datenschutzkommission keine Entscheide veröffentlicht. Dies kann damit zusammen hängen, dass nach wie vor unklar ist, ob und inwiefern der Rechtsmittelhinweis nach Artikel 34 Buchstabe b des Datenschutzgesetzes in der Praxis überhaupt verwendet wird.

In einem Fall vor dem Staatsgerichtshof (Verfassungsgericht) wurde das Auskunftsrecht auf den verstorbenen Ehemann geltend gemacht. Rechtsgrundlage dieses Anspruchs war Article 1 Abs. 7 der Datenschutzverordnung. Diese Regelung im Zusammenhang mit dem Auskunftsrecht lautet: *„Wird Auskunft über Daten von verstorbenen Personen verlangt, so ist sie zu erteilen, wenn der Gesuchsteller ein Interesse an der Auskunft nachweist und keine überwiegenden Interessen von Angehörigen der verstorbenen Person oder von Dritten entgegenstehen. Nahe Verwandtschaft, Ehe oder eingetragene Partnerschaft mit der verstorbenen Person begründen ein Interesse."*

Der Staatsgerichtshof stellte einleitend fest, dass der Datenschutz bzw. der Schutz der „informationellen Integrität" einen Teilaspekt des Schutzes der Privatsphäre gemäß Artikel 32 der Landesverfassung und Artikel 8 EMRK darstellt.

In der Sache entschied er, dass diese Bestimmung kein eigenständiges Auskunftsrecht begründet, sondern als ein verfahrensrechtliches Akteneinsichtsrecht zu qualifizieren ist. Das Auskunftsrecht beziehe sich auf die eigenen Daten. Dies sei bei der Verordnungsbestimmung nicht der Fall. Somit handle es sich um eine datenschutzrechtlich zentrale Frage, die grundsätzlich auf Gesetzesebene zu regeln sei. Die Bestimmung sei somit verfassungskonform restriktiv zu interpretieren und stelle nur (aber immerhin) ein schutzwürdiges Interesse an der Akteneinsicht in einem konkreten Verfahren dar (StGH 2011/11).

NORWEGEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Die Strategie der Datenschutzbehörde für das Gesundheitswesen.

Seit 2010 gibt es ein internes Strategieprogramm. Im Herbst 2011 wurde die „Datenstrategie für eine bessere Vorgehensweise im Gesundheitswesen" auf den Weg gebracht. Die Datenschutzbehörde hat sich langfristig Ziele gesetzt, wie sie zu einer besseren Strategie im Gesundheitswesen beitragen wird. Hierzu gehören Maßnahmen im Hinblick auf Zugangskontrolle (sowohl intern als auch extern), Modernisierung und Verwaltung von Krankenakten (zentrale Krankenakten und andere wichtige Akten) sowie eine Bewertung der Art und Weise, wie die Behörde in der Lage ist, für die Selbstbestimmung und Autonomie der Menschen zu sorgen. Die Strategie behandelt außerdem, wie die Behörde mit den lokalen Aufzeichnungen, Abteilungen, dem Gesundheitsdirektorat sowie wichtige Interessengruppen im Bereich Gesundheit und anderen Bereichen im Gesundheitssektor zusammenarbeiten wird.

Organisation	Norwegische Datenschutzbehörde
Vorsitz und/oder Gremium	Bjørn Erik Thon, Direktor
Budget	32 Millionen NOK
Personal	40 insgesamt, Direktor: 1, Rechtsabteilung: 16, Untersuchung und Sicherheit: 9, Informationsabteilung: 4, Verwaltung und Archiv: 10.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	Neu 2011: 4 010, insgesamt 11 211 Ende 2011.
Vorabprüfungen	Insgesamt 2011: 143
Anfragen betroffener Personen	Insgesamt gingen in der Zentrale der norwegischen Datenschutzbehörde 5 196 Anrufe und 2 632 E-Mails ein.
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu nennenswerten allgemeinen Aktivitäten	k. A.

Prüfmaßnahmen	
Prüfungen, Untersuchungen	Adressenvermittlung 1 Beschäftigung 3 Kundenkarte 5 Versicherung 4 Forschung 2 Internetunternehmen 4 Kameraüberwachung 9 Sozialhilfe 4 Webcast 5 Bildung 1 INSGESAMT 38
Sanktionsmaßnahmen	
Sanktionen	4 Geldbußen und 1 Zwangsmaßnahme, alle von der Datenschutzbehörde verhängt
Geldbußen	Geldbußen in Höhe von insgesamt 135 000 NOK, Zwangsmaßnahmen 380 000 NOK
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Einordnung von Facebook

Im Dezember 2010 veröffentlichten wir den Bericht „Soziale Netzwerkdienste und Datenschutz – eine Fallstudie zu Facebook“. Der Bericht zeigte, dass die Daten, die Nutzer über sich preisgeben, nur einen kleinen Teil des gesamten von Facebook erfassten Datenvolumens darstellen. Der gleiche Bericht brachte zahlreiche Unklarheiten bezüglich der Datenerfassung durch Facebook und der Nutzung personenbezogener Daten zutage. Auf dieser Grundlage schickte die nordische Datenschutzbehörde auf Initiative der norwegischen Datenschutzbehörde Facebook eine Reihe spezifischer Fragen, um herauszufinden, wer über Facebook Daten erfasst und darauf zugreift und was mit den erfassten personenbezogenen Daten passiert.

Richtlinie über die Vorratsdatenspeicherung

Das norwegische Parlament setzte im April 2011 die Richtlinie über die Vorratsdatenspeicherung in norwegisches Recht um. Die Richtlinie wird in die Vorschriften für elektronische Kommunikation, in die Strafprozessordnung und in die Vorschriften zum Schutz personenbezogener Daten umgesetzt.

Die Datenschutzbehörde wird im Zusammenhang mit der Richtlinie eine Reihe neuer Verpflichtungen erhalten, darunter Aufsichtspflichten in Bezug auf die Verpflichtung zur Löschung von Daten und zur

Bereitstellung von Lizenzen mit Sicherheitsanforderungen. Die Datenschutzbehörde hat sich nachdrücklich gegen die Richtlinie ausgesprochen, jedoch die Entscheidung des Parlaments zur Kenntnis genommen. Die Behörde arbeitet nun mit der norwegischen Post- und Telekommunikationsbehörde zusammen, um eine bestmögliche Umsetzung zu garantieren. Die Richtlinie war zum Ende des Jahres noch nicht in Kraft getreten.

App-Bericht

Im September 2011 veröffentlichte die Datenschutzbehörde den Bericht „Was weiß die App über Sie? Datenschutzfragen im Zusammenhang mit mobilen Anwendungen". Mobile Anwendungen, kurz „Apps" genannt, nehmen rasant zu. Der Grund für eine Prüfung dieses Marktes liegt darin, dass zahlreiche Anwendungen große Mengen personenbezogener Daten verarbeiten, ohne dass sich die Nutzer dessen überhaupt bewusst sind. Einige Anwendungen erfordern den Zugang zu personenbezogenen Daten, die viel über den Nutzer preisgeben, wie zum Beispiel Standortdaten sowie Daten über Freunde oder persönliche Interessen.

Der Fall RMI

Im Jahr 2010 überprüfte die Datenschutzbehörde das Institut für Rechtsmedizin (Rettsmedisinisk Institutt, RMI) der Universität Oslo. Die Prüfung ergab, dass das Institut große Mengen sensibler Daten über seine Aktivitäten speichert, ohne dass es weder im norwegischen Recht noch aufgrund von Vereinbarungen mit Kunden eine Rechtsgrundlage für eine solche Speicherung gäbe. Die Datenschutzbehörde fand außerdem heraus, dass in Sachen Informationssicherheit große Defizite herrschten und die Universität im Allgemeinen nur geringe Sicherheitsvorkehrungen für gespeicherte Daten ergreift. Im Laufe des Jahres gab die Datenschutzbehörde ihren Beschluss bekannt, die Daten zu löschen.

„Nettby"

Im Dezember 2010 wurde die Social-Networking-Website „Nettby" der norwegischen Tageszeitung VG geschlossen. Nettby war zur damaligen Zeit die größte Online-Community und speicherte beträchtliche Datenmengen, einschließlich privater Kommunikation. Nach der Schließung waren alle Daten, die von VG gespeichert wurden, weder den ehemaligen Nutzern noch der breiten Öffentlichkeit zugänglich. VG und die Nationalbibliothek waren der Ansicht, dass die Daten bis auf Weiteres gespeichert werden müssten, um sie gegebenenfalls zu einem späteren Zeitpunkt zu Forschungszwecken heranziehen zu können. Der ursprüngliche Zweck von Nettby bestand jedoch darin, Mitgliedern die Teilnahme an einer Online-Community zu ermöglichen – einschließlich der Möglichkeit, privat mit anderen Mitgliedern zu kommunizieren. Demzufolge verordnete die Datenschutzbehörde die Löschung der Daten.

Branchenstandard für elektronische Tickets

Auf Initiative öffentlicher Verkehrsbetriebe nahm die Datenschutzbehörde an einem Gemeinschaftsprojekt zu datenschutzfreundlichen Lösungen für elektronische Tickets und der Herausarbeitung eines Branchenstandards teil. Ein Branchenstandard für elektronische Tickets soll dafür sorgen, dass jeder anonym mit Bus, Zug oder Schiff reisen kann, und verpflichtet die Branche dazu, elektronische Tickets anzubieten, die Reisenden ein hohes Maß an Datenschutz bieten. Die breite Öffentlichkeit muss in der Lage sein, öffentliche Verkehrsmittel zu nutzen, ohne dabei preiszugeben, wer oder wo sie sind, und dabei dennoch die gleichen Vorteile und Dienstleistungen in Anspruch nehmen können wie Pendler, die mit einem Verkehrsbetrieb einen persönlichen Vertrag abschließen. Der Kodex wurde im Dezember 2011 eingeführt.

Zollkontrollstandards für Einzelpersonen

Das Königliche Zollamt hat ein Verfahren entwickelt, um im Zusammenhang mit Fremdwährungsgeschäften die Daten von Einzelpersonen aus dem Register abzurufen und sie alphabetisch zu speichern und zu registrieren. Die betroffenen Personen wurden aufgefordert, die betreffenden Transaktionen sowie ggf. deren Zusammenhang mit Zollangelegenheiten zu dokumentieren. Die Datenschutzbehörde kam zu dem Schluss, dass es sich hierbei um eine Überprüfung von Einzelpersonen ohne rechtliche Befugnisse handelt, und wies die Zollbehörde an, dies zu unterlassen.

Kapitel Fünf

Mitglieder und Beobachter der Artikel-29-Datenschutzgruppe

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE IM JAHR 2011

Belgien	Bulgarien
Herr Willem Debeuckelaere Datenschutzkommission (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue Haute 139 - BE - 1000 Brüssel Tel: +32(0)2/213.85.40 Fax: +32(0)2/213.85.65 E-Mail: commission@privacycommission.be Website: http://www.privacycommission.be/	Herr Krassimir Dimitrov Kommission für den Schutz personenbezogener Daten (CPDP) (Комисия за защита на личните данни) 15 Acad. Ivan Evstratiev Geshov blvd. Sofia 1431 Republik Bulgarien Tel. + 359 2 915 35 31 Fax: + 359 2 915 35 25 E-Mail: kzld@cpdp.bg Website: http://www.cdpd.bg
Dänemark	**Deutschland**
Frau Janni Christoffersen Dänische Datenschutzbehörde (Datatilsynet) Borgergade 28, 5th floor - DK - 1300 Koebenhavn K Tel: +45 3319 3200 Fax: +45 3319 3218 E-Mail: dt@datatilsynet.dk Website: http://www.datatilsynet.dk	Herr Peter Schaar Bundesbeauftragter für Datenschutz und Informationsfreiheit (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

	(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
Estland	**Finnland**
Herr Viljar Peep Estnische Datenschutzbehörde (Andmekaitse Inspektsioon) 19 Väike-Ameerika St., 10129 Tallinn Tel: +372 627 4135 Fax: +372 627 4137 E-Mail: info@aki.ee oder international@aki.ee Website: http://www.aki.ee	Herr Reijo Aarnio Amt des Datenschutzbeauftragten (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	**Griechenland**
Herr Alex Türk Vorsitzender Präsident der französischen Datenschutzbehörde (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 Französische Datenschutzbehörde	Herr Christos Yeraris Griechische Datenschutzbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 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

(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	
Irland	**Italien**
Herr Billy Hawkes Kommissionsmitglied für Datenschutz (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 Pizetti Italienische Datenschutzbehörde (Garante per la protezione dei dati personali) Piazza di Monte Citorio, 121 - IT - 00186 Rom 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 Plūmiņa Lettische Datenschutzbehörde (Datu valsts inspekcija) Blaumana street 11/13-15 Riga, LV-1011 Lettland E-Mail: info@dvi.gov.lv Website: www.dvi.gov.lv Tel: + 371 67223131	Herr Algirdas Kunčinas Estnische Datenschutzbehörde (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 Schutz personenbezogener Daten (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 Informations- und Datenschutzbeauftragter (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	**Österreich**
Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Besucheradresse (nur mit Termin): Juliana van Stolberglaan 4-10 2595 CL DEN HAAG Anschrift: P.O. Box 93374 2509 AJ DEN HAAG Tel: +31 70 8888500 Fax: +31 70 8888501 E-Mail: info@cbpweb.nl Website: http:// www.cbpweb.nl http://www.mijnprivacy.nl	Frau Eva Souhrada-Kirchmayer (ab 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/

Polen	Portugal
Herr Wojciech Rafał Wiewiórowski Generalinspektor für den Schutz personenbezogener Daten (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	Herr Luís Novais Lingnau da Silveira Nationale Datenschutzkommission (Comissão Nacional de Protecção de Dados - CNPD) Rua de São Bento, 148, 3º PT - 1 200-821 Lissabon Tel: +351 21 392 84 00 Fax: +351 21 397 68 32 E-Mail: geral@cnpd.pt Website: http://www.cnpd.pt
Rumänien	**Schweden**
Frau Georgeta Basarabescu Nationale Aufsichtsbehörde für den Schutz personenbezogener Daten (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	Herr Göran Gräslund Schwedische Datenschutzbehörde (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
Slowakei	**Slowenien**
Herr Gyula Veszelei Slowenische Datenschutzbehörde (Úrad na ochranu osobných údajov Slovenskej republiky) Odborárske námestie 3 - SK - 81760 Bratislava 15 Tel: +421 2 5023 9418 Fax: +421 2 5023 9441	Frau Natasa Pirc Musar Datenschutzbeauftragte (Informacijski pooblaščenec) Vošnjakova 1, SI - 1000 Ljubljana Tel: +386 1 230 97 30 Fax: +386 1 230 97 78

E-Mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	E-Mail: gp.ip@ip-rs.si Website: http://www.ip-rs.si rs.si
Spanien	**Tschechische Republik**
Herr José Luis Rodriguez Álvarez Spanische Datenschutzbehörde (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 Igor Nemec Amt für Datenschutz (Úřad pro ochranu osobních údajů) Pplk. Sochora 27 - CZ - 170 00 Prag 7 Tel: +420 234 665 111 Fax: +420 234 665 501 E-Mail: posta@uoou.cz Website: http://www.uoou.cz/
Ungarn	**Vereinigtes Königreich**
Herr András Jóri Ungarisches Kommissionsmitglied für Datenschutz und Informationsfreiheit (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	Herr Christopher Graham Amt des Datenschutzbeauftragten (Information Commissioner's Office) Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel: +44 1625 545700 Fax: +44 1625 524510 E-Mail: Nutzen Sie bitte das Kontaktformular auf der website Website: http://www.ico.gov.uk
Zypern	**Europäischer Datenschutzbeauftragter**
Frau Panayiota Polychronidou Kommissionsmitglied für den Schutz personenbezogener Daten (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str.	Herr Peter Hustinx Europäischer Datenschutzbeauftragter – EDSB Anschrift: 60, rue Wiertz, BE - 1047 Brüssel Amt: rue Montoyer, 63, BE - 1047 Brüssel Tel: +32 2 283 1900

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	Fax: +32 2 283 1950 E-Mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE IM JAHR 2011

Ehemalige jugoslawische Republik Mazedonien	Kroatien
Herr Dimitar Gjeorgjievski Datenschutzbehörde (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	Herr Franjo Lacko Direktor Frau Sanja Vuk Leiterin der Abteilung für EU- und Rechtsfragen Kroatische Datenschutzbehörde (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
Island	**Liechtenstein**
Frau Sigrun Johannesdottir Isländische 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 Philipp Mittelberger Datenschutzbeauftragter Datenschutzstelle 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
Norwegen	
Kim Ellertsen Direktor, Leiter der Rechtsabteilung Datenschutzbehörde	

(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	

Sekretariat der Artikel-29-Datenschutzgruppe
Frau Marie-Hélène Boulanger
Geschäftsführende Referatsleiterin
Europäische Kommission
Generaldirektion Justiz
Referat Datenschutz
Amt: MO59 02/13 - BE - 1049 Brüssel
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E-Mail: JUST-ARTICLE29WP-SEC@ec.europa.eu
Website: http://ec.europa.eu/justice/data-protection/index_en.htm

WO ERHALTE ICH EU-VERÖFFENTLICHUNGEN?

Kostenlose Veröffentlichungen:

- Einzelexemplar:

  über EU Bookshop (http://bookshop.europa.eu);

- mehrere Exemplare/Poster/Karten:

  bei den Vertretungen der Europäischen Union (http://ec.europa.eu/represent_de.htm),
  bei den Delegationen in Ländern außerhalb der Europäischen Union (http://eeas.europa.eu/delegations/index_de.htm),
  über den Dienst Europe Direct (http://europa.eu/europedirect/index_de.htm)
  oder unter der gebührenfreien Rufnummer 00 800 6 7 8 9 10 11 (*).

  (*) Sie erhalten die bereitgestellten Informationen kostenlos, und in den meisten Fällen entstehen auch keine Gesprächsgebühren (außer bei bestimmten Telefonanbietern sowie für Gespräche aus Telefonzellen oder Hotels).

Kostenpflichtige Veröffentlichungen:

- über EU Bookshop (http://bookshop.europa.eu).

DS-AA-14-001-DE-N

Amt für Veröffentlichungen

doi: 10.2838/10635

DE