Europäische Kommission

16. Bericht

der Artikel-29 -Datenschutzgruppe

Berichtsjahr 2012

Angenommen am 25. November 2014

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).

Weder die Europäische Kommission noch Personen, die im Namen dieser Kommission handeln, sind für die Verwendung der nachstehenden Informationen verantwortlich.

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

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2015

PDF	ISBN 978-92-79-44095-3	ISSN 2363-1015	doi: 10.2838/607091	DS-AA-15-001-DE-N

16. Bericht der Artikel-29-Datenschutzgruppe

Berichtsjahr 2012

Inhaltsverzeichnis

VORWORT DES VORSITZENDEN DER ARTIKEL-29-DATENSCHUTZGRUPPE

Das Jahr 2012 war ein äußerst wichtiges Jahr für den Datenschutz in der Europäischen Union und ein sehr interessantes Jahr für die Artikel-29-Datenschutzgruppe. Die Europäische Kommission hatte für das Jahr 2012 die Vorlage von Vorschlägen für einen neuen Rechtsrahmen für den Datenschutz innerhalb der EU geplant. In Anbetracht dessen, dass die Datenschutzgruppe bereits 2009 damit begonnen hat, die Kommission in Hinblick auf den neuen Rechtsrahmen zu beraten, sollte die Vorlage der Vorschläge ein äußerst bedeutender Augenblick werden.

Im Januar 2012 legte die Europäische Kommission schließlich tatsächlich ihren Vorschlag für einen neuen Rechtsrahmen für den Datenschutz in der EU vor, der eine allgemeinen Verordnung zum Datenschutz und eine Richtlinie für Strafverfolgungsbehörden umfasste.

Im Großen und Ganzen wurde der Vorschlag von der Datenschutzgruppe begrüßt. Die Tatsache, dass eine Verordnung als Instrument gewählt wurde, die unmittelbar für alle Mitgliedstaaten der EU gilt, ist ein großer Schritt nach vorne. Obwohl sich der Vorschlag aus zwei verschiedenen Instrumenten zusammensetzt, kann die umfassende Geltung dennoch durch die Gesetzgebung gewährleistet werden, und zwar unter der Voraussetzung, dass die Verordnung und die Richtlinie als Paket erachtet werden und die Grundsätze und Rechte in beiden Instrumenten übereinstimmen.

Es versteht sich von selbst, dass es auch nach wie vor einige Bedenken gibt. Die Datenschutzgruppe ist beispielsweise der Ansicht, dass der Grundsatz der Zweckbindung als einer der Grundsätze des Datenschutzes stark untergraben werden würde, wenn die Vorkehrung eingeführt wird, dass Daten zu einem anderen – und außerdem inkompatiblen – Zweck verwendet werden könnten, falls eine neue Rechtsgrundlage gefunden wird. Natürlich muss es gelegentlich möglich sein, Daten auch zu anderen Zwecken zu verwenden. Diese müssen jedoch mit dem Zweck, zu dem die Daten ursprünglich erfasst wurden, kompatibel sein. Einfach nach einer anderen Rechtsgrundlage zu suchen, reicht nicht aus.

Trotz der Aufgabe der Kommission, als Hüter der Verträge zu agieren, gibt es diesbezüglich starke Vorbehalte, da viele der Vorkehrungen zu einer Beeinträchtigung der Unabhängigkeit der Datenschutzbehörden führen könnten. Wenn eine Angelegenheit im Rahmen des Kohärenzverfahrens vom Europäischen Datenschutzausschuss (EDPB) gehandhabt wird oder wurde, sollte die Kommission zwar in der Lage sein, diese rechtlich zu beurteilen, jedoch grundsätzlich von einem Eingreifen absehen.

Des Weiteren kann es natürlich notwendig sein, bestimmte Angelegenheiten delegierten bzw. Durchführungsrechtsakten zu überlassen. Es sind jedoch nicht alle Angelegenheiten, für die delegierte bzw. Durchführungsrechtsakte vorgesehen sind, auch für solche Instrumente geeignet. In manchen Fällen ist die Angelegenheit ein wesentlicher Bestandteil und sollte daher im Text der Verordnung selbst aufgegriffen werden, während in anderen Fällen eine Anweisung durch den EDPB ein geeigneteres Instrument darstellen würde.

Nach der Vorlage des Vorschlags begannen das Europäische Parlament (EP) und der Rat ihre jeweiligen Gesetzgebungsverfahren. Zum Zeitpunkt der Abfassung hat der zuständige Ausschuss des Europäischen Parlaments (LIBE) seine Gespräche beendet und seinen Standpunkt eingenommen, auf dessen Grundlage das EP in die Verhandlungen gehen wird. Die Gespräche innerhalb des Rates dauern jedoch nach wie vor an.

Durch die technischen Entwicklungen und die zunehmende Globalisierung unserer Gesellschaft ist eine zukunftstaugliche Aktualisierung des Rechtsrahmens für den Datenschutz in der EU immer notwendiger geworden.

Die Gespräche innerhalb des Rates werden daher hoffentlich bald zu einem gemeinsamen Standpunkt der Mitgliedstaaten führen und dafür sorgen, dass die Verhandlungen – oder der Trilog – in Kürze beginnen können, damit der neue Rechtsrahmen im Sommer 2014 in Kraft treten kann.

Jacob Kohnstamm.

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

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

1.1 DATENÜBERMITTLUNG IN DRITTLÄNDER

1.1.1 Angemessenheit

Stellungnahme 7/2012 (WP198) zum Schutzniveau für personenbezogene Daten im Fürstentum Monaco

2009 bat das Fürstentum Monaco die Europäische Kommission zu bewerten, ob Monaco ein angemessenes Schutzniveau gemäß Artikel 25 Absatz 6 der Richtlinie 95/46/EG zum Schutz personenbezogener Daten gewährleistet, und diesbezüglich eine Entscheidung zu treffen. Im Zuge der Untersuchung ersuchte die Kommission die Artikel-29-Datenschutzgruppe um ihre Stellungnahme.

Wegen der historisch gewachsenen Verbindung zwischen Frankreich und Monaco weisen die datenschutzrechtlichen Bestimmungen Monacos enge Bezüge zum französischen Datenschutzrecht auf. Artikel 20 der Verfassung Monacos gewährleistet den Schutz des Rechts auf Privatsphäre und versichert: „Jedermann hat das Recht auf Achtung seines Privat- und Familienlebens sowie auf Wahrung des Brief-, Post- und Fernmeldegeheimnisses".

Der Schutz der personenbezogenen Daten ist in Monaco im Gesetz Nr. 1.165 vom 23. Dezember 1993 über den Schutz personenbezogener Daten (novelliert durch Gesetz Nr. 1.353 vom 4.Dezember 2008 sowie durch das Gesetz Nr. 1.353 vom 1.April 2009) und in der Fürstlichen Verordnung Nr. 2.230 vom 29. Juni 2009 zur Festlegung der Durchführungsbestimmungen für das Gesetz geregelt.

Die Bewertung der Datenschutzgruppe stützt sich im Wesentlichen auf das Gesetz Nr. 1.165 in der geänderten Fassung von 2008 und 2009. Dabei bezieht sich die Datenschutzgruppe auf die wesentlichen Bestimmungen der Datenschutzrichtlinie unter Berücksichtigung der im Arbeitsdokument „Übermittlung von personenbezogenen Daten in Drittländer: Anwendung von Artikel 25 und 26 der EU-Datenschutzrichtlinie" vom 24. Juli 1998 (WP 12).

Mit dem Gesetz wurde die Datenschutzbehörde von Monaco (Commission de Contrôle des Informations Nominatives, CCIN) als unabhängige Behörde geschaffen. Die CCIN hat Leitlinien, Ausführungen und Jahresberichte sowie weitere Informationen zu verschiedenen Themenbereichen wie z. B. Biometrie, GPS-Chips und Videoüberwachung veröffentlicht, mit denen sie die Rechte und Pflichten für den Einzelnen, die Geschäftswelt und den Staat absteckt und Empfehlungen für die praktische Anwendung der Grundsätze zum Schutz der Privatsphäre gegeben hat.

Auf internationaler Ebene hat Monaco die folgenden Instrumente unterzeichnet und ratifiziert: die Europäische Menschenrechtskonvention im Jahr 2005, das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen 108) und dessen Zusatzprotokoll (in Kraft seit dem 1.4.2009) sowie den Internationalen Pakt über bürgerliche und politische Rechte am 28.8.1997.

Die Datenschutzgruppe kam zu dem Schluss, dass der Anwendungsbereich des monegassischen Datenschutzgesetzes dem der Richtlinie ähnlich ist, war jedoch der Auffassung, dass eine Umformulierung seine Anwendbarkeit auf juristische Personen präzisieren würde.

Die Datenschutzgruppe war der Auffassung, dass die Datenschutzvorschriften Monacos dem Grundsatz der Datenqualität und der Verhältnismäßigkeit, dem Grundsatz der Transparenz, dem Grundsatz der Sicherheit und, sofern die Ausnahmen hiervon eng ausgelegt werden, dem Recht auf Auskunft, Berichtigung und Widerspruch gerecht wird.

Darüber hinaus steht das Datenschutzgesetz von Monaco mit dem Grundsatz der Beschränkung der Weiterübermittlung personenbezogener Daten in Drittländer und im Allgemeinen mit den Anforderungen bezüglich besonderer Kategorien von personenbezogenen Daten in Einklang.

Obwohl die Bestimmungen bezüglich des Widerspruchsrechts bei Direktmarketing deutlicher hätten formuliert sein können, wird diesbezüglich ein ausreichender Schutz gewährleistet. Außerdem war man der

Auffassung, dass das Gesetz mit dem „Grundsatz für automatisierte Einzelentscheidungen“ in Einklang steht.

Die Datenschutzgruppe kam zu der Auffassung, dass das Ziel, ein hohes Maß an Übereinstimmung mit den einschlägigen Regelungen zu schaffen, nur zum Teil erreicht wird, und forderte die Behörden dazu auf, Vorschriften für eine effektivere Umsetzung der strukturellen und finanziellen Unabhängigkeit der CCIN zu erlassen und die auf diese Behörde übertragenen Durchsetzungsbefugnisse in Bezug auf die Befolgung der einschlägigen Regelungen durch den öffentlichen Sektor und allgemeiner in Bezug auf die Maßnahmen zu stärken, die den für die Verarbeitung Verantwortlichen, die sich nicht an Recht und Gesetz halten, auferlegt werden können, und zwar über die Verhängung strafrechtlicher Sanktionen durch die Justizbehörden hinausgehend.

Die Datenschutzgruppe kam zu der Auffassung, dass das Datenschutzgesetz von Monaco genügend Mechanismen bietet, um Einzelpersonen Hilfe und Unterstützung zu leisten, und dass das Recht der betroffenen Personen, Entschädigung zu erhalten für Schädigungen, die ihnen aus der Verletzung ihrer Rechte oder ihres Eigentums infolge einer rechtswidrigen Verarbeitung ihrer personenbezogenen Daten entstanden sind, in ausreichendem Maße gewährleistet.

Die Datenschutzgruppe kam zu dem Schluss, dass das Fürstentum Monaco ein angemessenes Datenschutzniveau im Sinne von Artikel 25 Absatz 6 der Richtlinie 95/46/EG gewährleistet. Sie forderte die Behörden jedoch auf, Begriffe wie „Datei“, „Dritter“, „Auftragsverarbeiter“ und „Einwilligung der betroffenen Person“ aufzunehmen; zu präzisieren, inwiefern das Gesetz auch auf juristische Personen Anwendung findet; zu präzisieren, dass betroffene Personen das Recht haben, rechtzeitig informiert zu werden (insbesondere wenn die Daten nicht direkt von der betroffenen Person eingeholt wurden) und Widerspruch gegen die Verarbeitung personenbezogener Daten zu Zwecken der kommerziellen Direktwerbung einzulegen. Die auf die Datenschutzbehörde übertragenen Durchsetzungsbefugnisse in Bezug auf die Befolgung der einschlägigen Regelungen durch den öffentlichen Sektor und auf die Maßnahmen, die den für die Verarbeitung Verantwortlichen auferlegt werden können, die sich nicht an das Gesetz halten, sollten ebenfalls gestärkt werden.

1.1.2 Verbindliche unternehmensinterne Vorschriften

Arbeitsdokument 2/2012 (WP 195) mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR) für Auftragsverarbeiter

Die Artikel-29-Datenschutzgruppe hat bereits Instrumente entwickelt, um die Anwendung verbindlicher unternehmensinterner Datenschutzregelungen (BCR) durch die für die Verarbeitung Verantwortlichen (BCR für die eigenen Daten) zu vereinfachen (WP 153). Mit diesen Regelungen sollten Vorgaben für die Übermittlung personenbezogener Daten gemacht werden, die ursprünglich von dem Unternehmen in seiner Funktion als für die Verarbeitung Verantwortlicher verarbeitet wurden (etwa Daten, die seine Kunden, seine Angestellten usw. betreffen).

Mit diesem Arbeitsdokument soll ein Instrumentarium zur Vereinfachung der Anwendung verbindlicher unternehmensinterner Datenschutzregelungen für Auftragsverarbeiter (BCR für die Daten Dritter) entwickelt werden, in dem die zu erfüllenden Bedingungen beschrieben werden.

Mit den BCR für Auftragsverarbeiter soll ein Rahmen für die Übermittlung personenbezogener Daten ins Ausland vorgegeben werden, die ursprünglich von dem Unternehmen in seiner Funktion als Auftragsverarbeiter in Einklang mit den externen Anweisungen eines für die Verarbeitung Verantwortlichen (etwa bei ausgelagerten Tätigkeiten) verarbeitet wurden. Nach Richtlinie 95/46/EG sollte zwischen einem für die Verarbeitung Verantwortlichen und einem Auftragsverarbeiter ein Vertrag abgeschlossen werden. Ein solcher Vertrag wird in dem Dokument als „Dienstleistungsvereinbarung“ bezeichnet.

Empfehlung 7/2012 (WP195a) für das Standardformular zur Beantragung der Genehmigung verbindlicher unternehmensinterner Vorschriften für die Übermittlung personenbezogener Daten zu Verarbeitungszwecken

In Verbindung mit dem Instrumentarium für verbindliche unternehmensinterne Datenschutzregelungen für Auftragsverarbeiter führte die Datenschutzgruppe mit dieser Empfehlung ein Standardformular zur Beantragung der Genehmigung einer Verarbeitung gemäß derartiger verbindlicher unternehmensinterner Vorschriften ein.

1.2 ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

Stellungnahme 6/2012 (WP 197) zum Entwurf des Beschlusses der Kommission über die Maßnahmen für die Benachrichtigung zu Verletzungen des Schutzes personenbezogener Daten gemäß Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation)

Diese Stellungnahme bezieht sich auf die Maßnahmen für die Benachrichtigung zu Verletzungen des Schutzes personenbezogener Daten gemäß Richtlinie 2002/58/EG (Datenschutzrichtlinie für elektronische Kommunikation), die aus technischen Gründen zunächst ein Entwurf des Beschlusses der Kommission war und anschließend in eine Verordnung umgewandelt wurde.

Die Datenschutzgruppe begrüßt in ihrer Stellungnahme die eingehenden Bemühungen der Kommission, die Bestimmungen über die Verletzungen des Schutzes personenbezogener Daten in der Richtlinie 2002/58/EC klarzustellen, hält jedoch in einigen Fällen eine präzisere Begriffsbestimmung für angebracht.

Bezüglich der Benachrichtigung der zuständigen Behörde begrüßt die Datenschutzgruppe die Tatsache, dass spezifische Fristen in die Verordnung aufgenommen wurden, und unterstützt ferner das zweistufige Benachrichtigungsmodell, durch das Reaktionsfähigkeit und Vollständigkeit der Benachrichtigungen kombiniert werden können.

Bezüglich der zu übermittelnden Informationen und Erstbenachrichtigungen sollte nach Auffassung der Datenschutzgruppe von den Betreibern verlangt werden, die zuständige Behörde bei der Erstbenachrichtigung über alle Einzelheiten zu informieren, die ihnen zu diesem Zeitpunkt bekannt sind, einschließlich der Art der betroffenen personenbezogenen Daten, die Umstände der Verletzung oder die Art der Gefährdung (Verlust, Diebstahl, Vervielfältigung usw.) sowie die Art und Weise, wie die Verletzung festgestellt wurde (verwendete Software zur Erkennung von Verletzungen, Auswertung der Protokolle, Meldung eines Vorfalls durch einen Mitarbeiter usw.), um Betreiber zu einer Implementierung einer hochwertigen Strategie zum Schutz personenbezogener Daten anzuregen.

Bezüglich der elektronischen Mittel unterstützt die Datenschutzgruppe die Initiative, derartige Mittel nach Möglichkeit zu fördern, warnt jedoch davor, dass diese elektronischen Mittel nicht umgehend in allen Mitgliedstaaten eingeführt werden: Zunächst muss ein einheitliches Format für elektronische Benachrichtigungen definiert werden und es müssen geeignete Sicherheitsmaßnahmen festgelegt und die elektronischen Mittel (Portal bzw. andere Systeme, wie z. B. sichere E-Mail) entwickelt und getestet werden, mit denen dieser Mechanismus in allen Mitgliedstaaten unterstützt wird.

Bezüglich der Benachrichtigung von anderen betroffenen nationalen Behörden begrüßt und unterstützt die Datenschutzgruppe die aktive Zusammenarbeit der Behörden und ist sich der Notwendigkeit einer Zusammenarbeit der zuständigen nationalen Behörden vollkommen bewusst, fordert die Kommission jedoch auf, den Anwendungsbereich der Bestimmung genauer zu beschreiben und die praktischen Methoden für die Zusammenarbeit der zuständigen Behörden zu benennen.

Bezüglich der Benachrichtigung der Teilnehmer oder der einzelnen Behörde begrüßt die Datenschutzgruppe die Tatsache, dass in der Verordnung ein Verfahren für Fälle beschrieben wird, in die Personen nicht direkt zu erreichen sind. Die Datenschutzgruppe begrüßt außerdem die Beschreibung der Umstände, die bei der Beurteilung der Frage zu berücksichtigen sind, ob durch die Verletzung des Schutzes

personenbezogener Daten die personenbezogenen Daten eines Teilnehmers oder einer Person oder deren Privatsphäre beeinträchtigt werden.

Bezüglich der **Beurteilung der Schwere und der nachteiligen Auswirkungen** hält die Datenschutzgruppe eine einheitliche und leicht verständliche Methodik zur Beurteilung des Schweregrades für Betreiber und zuständige Behörden in Europa für erforderlich. Detailliertere Leitlinien zu diesen Punkten würden zu einer wesentlichen Verbesserung des Beschlusses beitragen. Um diesem Erfordernis nachzukommen, unterstützt die Datenschutzgruppe ausdrücklich die Festlegung einer harmonisierten paneuropäischen Methodik zur Beurteilung des Schweregrades, die sich auf objektive Kriterien stützt.

Bezüglich der **technischen Schutzmaßnahmen und Unverständlichkeit der Daten** befürwortet die Datenschutzgruppe derartige Maßnahmen und ist der Meinung, dass die Beteiligten damit zu wirksameren Sicherheitsvorkehrungen angehalten werden und in allen Mitgliedstaaten gleichzeitig eine größere Rechtssicherheit in Bezug auf unverständliche Daten erreicht wird. Diese Verordnung darf bei den Betreibern jedoch nicht den Eindruck erwecken, dass bereits die Einführung von Verschlüsselung, Streuspeicherung (Hashing) oder sicherer Datenlöschung als ausreichend dafür gilt, dass Betreiber pauschal für sich in Anspruch nehmen können, die allgemeine Schutzpflicht gemäß Artikel 17 der Richtlinie 95/46/EG zu erfüllen – von den Betreibern sind außerdem geeignete organisatorische und technische Vorkehrungen zu treffen, um Verletzungen des Schutzes personenbezogener Daten vorzubeugen bzw. diese festzustellen und abzuwehren.

Ansonsten stellt die Datenschutzgruppe fest, dass der Entwurf der Verordnung keine Bestimmung bzw. keinen Erwägungsgrund in Bezug auf das in Artikel 4 Absatz 4 der Richtlinie erwähnte Verzeichnis enthält. Da das Verzeichnis im Zusammenhang mit den Benachrichtigungen eine wichtige Rolle spielt, schlägt die Datenschutzgruppe vor, in den Beschluss einen Erwägungsgrund aufzunehmen, der besagt, dass Betreiber sich bei der Festlegung des Formats für Verzeichniseinträge auch auf die Verordnung stützen können. Im Entwurf der Verordnung wird außerdem darauf hingewiesen, dass von den Behörden Statistiken über Verletzungen des Schutzes personenbezogener Daten geführt werden. Die Datenschutzgruppe schlägt vor, harmonisierte Indikatoren festzulegen, die statistisch erfasst werden.

Stellungnahme 5/2012 (WP 196) zu Cloud-Computing

In dieser Stellungnahme analysiert die Artikel-29-Datenschutzgruppe alle relevanten Fragen, die im Europäischen Wirtschaftsraum (EWR) tätige Cloud-Computing-Dienstanbieter und ihre Kunden betreffen. Dabei werden alle einschlägigen anzuwendenden Grundsätze aus der EU-Datenschutzrichtlinie 95/46/EG und der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG (in der durch die Richtlinie 2009/136/EG geänderten Fassung) aufgeführt.

Trotz der anerkannten Vorteile des Cloud-Computing zeigt die vorliegende Stellungnahme, wie die weit verbreitete Nutzung von Diensten des Cloud-Computing zu Datenschutzrisiken führen kann. Hier geht es in erster Linie um die fehlende Kontrolle über personenbezogene Daten und über unzureichende Informationen darüber, wie, wo und durch wen die Daten verarbeitet bzw. im Unterauftrag verarbeitet werden. Diese Risiken müssen von öffentlichen Einrichtungen und Privatunternehmen sorgfältig bewertet werden, wenn sie in Betracht ziehen, die Dienste eines Cloud-Anbieters in Anspruch zu nehmen.

Die vorliegende Stellungnahme untersucht Fragen hinsichtlich der gemeinsamen Nutzung von Ressourcen mit anderen Parteien, der fehlenden Transparenz in einer Outsourcing-Kette, die aus mehreren Auftragsverarbeitern und Unterauftragnehmern besteht, das Fehlen eines gemeinsamen, weltweiten Rahmens für die Datenportabilität und die Ungewissheit bezüglich der Zulässigkeit der Übermittlung personenbezogener Daten an Cloud-Anbieter, die außerhalb des EWR niedergelassen sind. Ebenso wird in der Stellungnahme hervorgehoben, dass die mangelnde Transparenz in Bezug auf die Informationen, die ein für die Verarbeitung Verantwortlicher der betroffenen Person über die Art der Verarbeitung ihrer personenbezogenen Daten geben kann, Anlass zu ernster Besorgnis ist. Die betroffenen Personen müssen

darüber informiert werden, wer ihre Daten zu welchen Zwecken verarbeitet, damit sie ihre diesbezüglichen Rechte ausüben können.

Eine wichtige Schlussfolgerung dieser Stellungnahme ist, dass Unternehmen und Verwaltungen, die Cloud-Computing nutzen wollen, eine umfassende und gründliche Risikoanalyse durchführen sollten. Alle Cloud-Anbieter, die Dienste im EWR anbieten, sollten dem Cloud-Anwender alle Informationen bereitstellen, die dieser benötigt, um die Vor- und Nachteile der Inanspruchnahme eines solchen Dienstes angemessen gegeneinander abwägen zu können. Beim Anbieten von Diensten des Cloud-Computing sollten Sicherheit, Transparenz und Rechtssicherheit für die Anwender die wichtigsten Aspekte sein.

Die Datenschutzgruppe begrüßt Artikel 26 des vorgeschlagenen Verordnungsentwurfs der Kommission, mit dem die Rechenschaftspflicht des Auftragsverarbeiters gegenüber dem für die Verarbeitung Verantwortlichen verstärkt wird, indem er diesen bei der Gewährleistung der Einhaltung insbesondere von Sicherheitsverpflichtungen und anderen, damit verbundenen Verpflichtungen unterstützt. Artikel 30 dieses Vorschlags führt die Pflicht für den Auftragsverarbeiter ein, geeignete technische und organisatorische Maßnahmen einzurichten. Der Vorschlagsentwurf stellt klar, dass ein Auftragsverarbeiter, der die Anweisungen des für die Verarbeitung Verantwortlichen nicht befolgt, als für die Verarbeitung Verantwortlicher gilt und spezifischen Bestimmungen als Mitverantwortlicher unterworfen ist.

Die Datenschutzgruppe ist der Ansicht, dass dieser Vorschlag in die richtige Richtung geht, um das Ungleichgewicht in der Cloud-Computing-Umgebung auszugleichen, in welcher der Anwender (insbesondere, wenn es sich um ein KMU handelt) Schwierigkeiten haben könnte, die in den Datenschutzvorschriften geforderte Kontrolle darüber auszuüben, wie der Anbieter die geforderten Dienste ausführt. Darüber hinaus wird angesichts der asymmetrischen Rechtsposition von betroffenen Personen und kleinen Unternehmen gegenüber großen Cloud-Computing-Anbietern eine proaktivere Rolle für Verbraucher- und Unternehmensschutzorganisationen empfohlen, um ausgewogenere allgemeine Geschäftsbedingungen solcher Anbieter auszuhandeln.

Die Datenschutzgruppe kommt zu dem Schluss, dass es den in der EU tätigen für die Verarbeitung Verantwortlichen im Interesse der Rechtssicherheit der betroffenen Personen, deren personenbezogene Daten in Datenzentren auf der ganzen Welt gespeichert werden, untersagt sein muss, personenbezogene Daten an Drittländer offenzulegen, wenn dies von einer Gerichts- oder Verwaltungsbehörde des Drittlandes gefordert wird, es sei denn, dies wird ausdrücklich in einer internationalen Vereinbarung oder einem Rechtshilfeabkommen gestattet oder von einer Aufsichtsbehörde genehmigt.

Öffentliche Behörden müssen erst prüfen, ob die Kommunikation, Verarbeitung und Speicherung der Daten außerhalb des innerstaatlichen Hoheitsgebiets die Sicherheit und Privatsphäre der Bürger sowie die nationale Sicherheit und Wirtschaft unannehmbaren Risiken aussetzen würde. Dies gilt insbesondere, wenn sensible Datenbanken (z. B. Zensusdaten) und Leistungen (z. B. Gesundheitsfürsorge) betroffen sind.Ausgehend davon könnten nationale Regierungen und Organe der Europäischen Union über eine weitere Prüfung des Konzepts einer Europäischen Regierungs-Cloud als einen supranationalen virtuellen Raum nachdenken, in dem einheitliche und harmonisierte Vorschriften angewendet werden könnten.

Die Datenschutzgruppe unterstützt die Strategie für eine Europäische Cloud-Partnerschaft, die eine öffentliche IT-Beschaffung zur Anregung eines europäischen Cloud-Marktes umfasst. Die Übermittlung personenbezogener Daten an einen europäischen Cloud-Anbieter, der sich an europäische Datenschutzvorschriften zu halten hat, könnte für die Kunden mit datenschutzrechtlichen Vorteilen verbunden sein, insbesondere durch die Förderung der Annahme allgemeiner Standards (vor allem in Bezug auf die Interoperabilität und die Datenportabilität), und könnte ihnen Rechtssicherheit geben.

Stellungnahme 4/2012 (WP 194) zur Ausnahme von Cookies von der Einwilligungspflicht

Artikel 5 Absatz 3 der Richtlinie 2002/58/EG, geändert durch Richtlinie 2009/136/EG, sieht für die Speicherung von Informationen oder den Zugriff auf Informationen auf dem Endgerät des Nutzers (oder Teilnehmers) eine Einwilligung in Kenntnis der Sachlage vor und stärkt damit den Schutz der Nutzer elektronischer Kommunikationsnetze und -dienste.

Dieses Erfordernis gilt für alle Arten von Informationen, die auf dem Endgerät des Nutzers gespeichert werden oder auf die dort zugegriffen wird. In dieser Stellungnahme wird erläutert, wie sich die Neufassung von Artikel 5 Absatz 3 auf die Verwendung von Cookies auswirkt, wobei der Begriff vergleichbare Technologien nicht ausschließt.

Nach Artikel 5 Absatz 3 ist für Cookies keine Einwilligung in Kenntnis der Sachlage erforderlich, wenn sie einem der folgenden Kriterien entsprechen: der Cookie wird verwendet, „wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist“, oder der Cookie wird verwendet, „wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann“.

Nachdem die Datenschutzgruppe die Anforderungen an die Einwilligung in Kenntnis der Sachlage bereits eingehend untersucht hat, sind die für Cookies und vergleichbare Technologien geltenden Ausnahmen von diesem Grundsatz Gegenstand der vorliegenden Stellungnahme.

Die von der Datenschutzgruppe durchgeführte Analyse hat gezeigt, dass folgende Cookies unter bestimmten Bedingungen von der Einwilligung in Kenntnis der Sachlage ausgenommen werden können, sofern sie nicht für weitere Zwecke verwendet werden: User-Input-Cookies für die Dauer einer Sitzung oder in bestimmten Fällen persistente Cookies, deren Gültigkeitsdauer auf wenige Stunden beschränkt ist; Authentifizierungscookies für Dienste, bei denen eine Authentifizierung erforderlich ist, für die Dauer einer Sitzung; nutzerorientierte Sicherheitscookies zur Erkennung von Authentifizierungsmissbrauch für eine begrenzte längere Dauer; Multimedia-Player-Sitzungscookies wie Flash-Player-Cookies für die Dauer einer Sitzung; Lastverteilungs-Sitzungscookies für die Dauer der Sitzung; persistente Cookies zur Anpassung der Benutzeroberfläche für die Dauer einer Sitzung (oder etwas länger) sowie Third-Party-Content-Sharing-Cookies sozialer Plug-Ins für angemeldete Mitglieder eines sozialen Netzwerks.

Im Zusammenhang mit sozialen Netzwerken weist die Datenschutzgruppe darauf hin, dass die Verwendung von Third-Party-Cookies in sozialen Plug-Ins, die anderen Zwecken als der Bereitstellung einer von den Mitgliedern des betreffenden Netzwerks ausdrücklich gewünschten Funktion dienen, der Einwilligung bedarf, insbesondere wenn es darum geht, das Verhalten von Nutzern über mehrere Websites hinweg zu verfolgen.

Die Datenschutzgruppe erinnert daran, dass Third-Party-Cookies, die Werbezwecken dienen, nicht von der Einwilligungspflicht ausgenommen werden können, und stellt weiter klar, dass eine Einwilligung auch erforderlich ist, wenn die Cookies für betriebliche Zwecke im Zusammenhang mit Werbung Dritter (wie Frequency Capping, Protokollierung von Finanzdaten, Affiliate-Marketing, Erkennen von Klickbetrug, Marktforschung und -analysen, Produktverbesserung und Fehlerbehebung) verwendet werden. Wenngleich bei manchen betrieblichen Zwecken sicherlich zwischen einzelnen Nutzern unterschieden wird, rechtfertigen diese Zwecke grundsätzlich nicht die Verwendung eindeutiger Kennungen. Dieser Aspekt ist vor allem vor dem Hintergrund der aktuellen Diskussion über die Umsetzung des Standards „Do Not Track“ in Europa von besonderer Bedeutung.

Diese Analyse zeigt auch, dass First-Party-Analysecookies nicht von der Einwilligungspflicht ausgenommen sind, aber nur ein begrenztes Datenschutzrisiko darstellen, sofern angemessene Sicherheitsvorkehrungen wie ausreichende Information der Nutzer, einfache Abwahlmöglichkeiten und umfassende Anonymisierungsmechanismen vorhanden sind.

Um abschließend entscheiden zu können, ob ein Cookie von der grundsätzlichen Pflicht zur Einholung einer Einwilligung in Kenntnis der Sachlage ausgenommen ist, muss sorgfältig geprüft werden, ob es einem der beiden Ausnahmekriterien entspricht, die der durch Richtlinie 2009/136/EG geänderte Artikel 5 Absatz 3 festlegt. Bestehen auch nach sorgfältiger Prüfung noch erhebliche Zweifel daran, ob eines der Ausnahmekriterien anwendbar ist, sollte der Websitebetreiber eingehend prüfen, ob es nicht praktisch möglich ist, die Einwilligung der Nutzer auf einfache und unaufdringliche Weise einzuholen und somit jegliche Rechtsunsicherheit zu vermeiden.

Stellungnahme 2/2012 (WP 192) zur Gesichtserkennung bei Online- und Mobilfunkdiensten

In den letzten Jahren hat sich die Gesichtserkennungstechnologie schnell verbreitet und ist genauer geworden. Darüber hinaus wurde diese Technologie für die Identifizierung, Authentifizierung/Verifizierung oder Kategorisierung von natürlichen Personen in Online- und Mobilfunkdienste integriert. Diese Technologie steht sowohl öffentlichen als auch privaten Organisationen zur Verfügung. Beispiele für ihre Verwendung im Bereich der Online- und Mobilfunkdienste umfassen soziale Netzwerke und Smartphone-Hersteller.

Die Datenschutzgruppe hat sich bereits im Arbeitspapier über Biometrie (WP80) und in Stellungnahme 03/2012 (WP193) zu den Entwicklungen im Bereich der biometrischen Technologien mit der Fähigkeit, Daten automatisch zu erfassen und ein Gesicht auf einem digitalen Bild zu erkennen, befasst. Die Gesichtserkennung wird als der Biometrie zugehörig betrachtet, da sie in vielen Fällen genügend Informationen enthält, um die eindeutige Identifizierung einer Person zu ermöglichen.

In dieser Stellungnahme prüfte die Datenschutzgruppe den Rechtsrahmen und gab Empfehlungen, die auf die Technologie zur Gesichtserkennung anzuwenden sind, wenn diese im Zusammenhang mit Online- und Mobilfunknetzen genutzt wird. Die Stellungnahme richtet sich an europäische und nationale Rechtsetzungsbehörden, für die Datenverarbeitung Verantwortliche und die Nutzer solcher Technologien und knüpft an die Grundsätze im Bereich der Online- und Mobilfunkdienste an, auf in Stellungnahme 03/2012 verwiesen wird.

Die Datenschutzgruppe kam zu dem Schluss, dass die Risiken eines Gesichtserkennungssystems von der Art der verwendeten Verarbeitung und dem jeweiligen Zweck bzw. den jeweiligen Zwecken abhängen, und gab Empfehlungen bezüglich spezieller Risiken ab.

Bilder dürfen in Online-Umgebungen nur dann erfasst werden, wenn dafür eine Rechtsgrundlage vorliegt.

Digitale Bilder und Templates dürfen nur zu dem angegebenen Zweck verwendet werden, für den sie zur Verfügung gestellt wurden. Außerdem sollten technische Kontrollen eingeführt werden, um das Risiko zu reduzieren, dass digitale Bilder durch Dritte zu Zwecken weiterverarbeitet werden, für die der Nutzer keine Einwilligung erteilt hat.

Der für die Datenverarbeitung Verantwortliche muss für die Sicherheit der Datenübermittlung zwischen der Bilderfassung und der weiteren Verarbeitungsschritte (z. B. dem Hochladen eines Bildes von einer Kamera auf eine Website für die Merkmalsextraktion und den Vergleich) sorgen, entweder durch Verschlüsselung der Kommunikationskanäle oder des erworbenen Bildes selbst.

Der für die Datenverarbeitung Verantwortliche muss dafür sorgen, dass von Systemen zur Gesichtserkennung erstellte Templates nur die Informationen enthalten, die für den angegebenen Zweck erforderlich sind, und so eine weitere Verarbeitung verhüten. Templates sollten nicht zwischen Gesichtserkennungssystemen übertragbar sein.

Da die Identifizierung und Authentifizierung/Verifizierung wahrscheinlich die Speicherung des Templates für die Verwendung bei einem späteren Vergleich erfordern, empfiehlt die Datenschutzgruppe, dass der für die Datenverarbeitung Verantwortliche prüft, wo die Daten am besten gespeichert werden, ob auf dem Gerät des Nutzers oder in den Systemen des für die Datenverarbeitung Verantwortlichen. Der für die Datenverarbeitung Verantwortliche muss die Sicherheit der gespeicherten Daten gewährleisten, indem er

das Template gegebenenfalls verschlüsselt, um unbefugten Zugang zum Template oder Speicherort zu verhindern. Im Fall der Gesichtserkennung zu Verifizierungszwecken werden biometrische Verschlüsselungstechniken empfohlen.

Schließlich empfiehlt die Datenschutzgruppe, dass der für die Datenverarbeitung Verantwortliche den betroffenen Personen geeignete Mechanismen zur Verfügung stellt, damit sie gegebenenfalls ihr Zugriffsrecht sowohl auf die Originalbilder als auch auf die im Zusammenhang mit der Gesichtserkennung generierten Templates ausüben können.

1.3 ÜBERARBEITUNG DES RECHTSRAHMENS FÜR DEN DATENSCHUTZ

Stellungnahme 1/2012 (WP 191) zu den Reformvorschlägen im Bereich des Datenschutzes

Insgesamt bietet die Verordnung mehr Klarheit. Sie stärkt die Rechte natürlicher Personen. Beispiele hierfür sind mehr Transparenz, bessere Kontrolle der Verarbeitung, Datenminimierung, besondere Vorschriften für die Verarbeitung personenbezogener Daten von Kindern, Stärkung des Rechts auf Auskunft über Daten, Stärkung des Widerspruchsrechts, Recht auf Datenportabilität, Stärkung des Rechts auf Löschung von Daten („Recht auf Vergessenwerden“) und Stärkung des Rechts auf Rechtsschutz durch die Datenschutzbehörden als auch auf gerichtlichen Rechtsschutz.

Für die für die Verarbeitung Verantwortlichen bringt die Verordnung Vereinfachung und mehr Kohärenz, eine stärkere Fokussierung auf ihre Rechenschaftspflicht für verarbeitete Daten und die Pflicht, dies anhand von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen, Datenschutz-Folgenabschätzungen, durch die Benennung eines Datenschutzbeauftragten, die Einhaltung der Meldepflichten für Verletzungen des Schutzes personenbezogener Daten und ein vorbeugendes Herangehen an grenzüberschreitende Datenübermittlungen nachzuweisen. Darüber hinaus werden verbindliche unternehmensinterne Vorschriften ausdrücklich als Instrument zur Handhabung grenzüberschreitender Datenübertragungen anerkannt.

Es wird eine Rechtsgrundlage für die für Auftragsverarbeiter geltenden Datensicherheitsvorschriften geschaffen. Außerdem werden Auftragsverarbeiter dazu verpflichtet, für bestimmte Verarbeitungsvorgänge die Pflichten des für die Verarbeitung Verantwortlichen zu übernehmen, wenn der Auftragsverarbeiter dabei über die Anweisungen des für die Verarbeitung Verantwortlichen hinausgeht (relevant für Cloud-Anbieter).

Die Verordnung stärkt die Unabhängigkeit und die Befugnisse von Datenschutzbehörden. Beispiele dafür sind die Befugnis zur Verhängung von Geldbußen, die Pflicht zur Zurateziehung bei legislativen Maßnahmen sowie Bestimmungen zur Gewährleistung einer einheitlichen Anwendung und nötigenfalls Durchsetzung der Rechtsvorschriften, insbesondere durch das Kohärenzverfahren.

Die Datenschutzgruppe hat ernsthafte Vorbehalte im Hinblick auf den Umfang der Befugnisse der Kommission, delegierte Rechtsakte und Durchführungsrechtsakte zu erlassen. Dies ist von besonderer Bedeutung, weil es um ein Grundrecht geht. Weitere Vorbehalte hat die Gruppe im Hinblick auf die Rolle der Kommission innerhalb des Europäischen Datenschutzausschusses.

Die Datenschutzgruppe empfiehlt eine unabhängige umfassende Abschätzung des Kostenanstiegs, der auf Grundlage der aktuellen Vorschläge auf die Datenschutzbehörden und den Europäischen Datenschutzbeauftragten (als Sekretariat des Europäischen Datenschutzausschusses) zukommt.

Im Allgemeinen deckt die Stellungnahme in Bezug auf den Verordnungsentwurf horizontale Fragen wie die Rolle der Kommission und der Europäischen Datenschutzbehörden in der Politikgestaltung, Schwellenwerte für KMU, Auswirkungen auf den Haushalt und die Mittel, allgemeine Bestimmungen (*Anwendungsbereich, betroffene Person und personenbezogene Daten, biometrische Daten, Hauptniederlassung, Pseudonymisierung, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen),* den Grundsatz des Zugangs der Öffentlichkeit zu Informationen, Weiterverarbeitung zu unvereinbaren Zwecken, Ausnahmen für Behörden, Minderjährige, das Recht auf Vergessenwerden, Direktwerbung,

Profiling, Vertreter, Rechenschaftspflicht, Meldung von Verletzungen des Schutzes personenbezogener Daten, Rolle und Funktionsweise der Datenschutzbehörden (*Unabhängigkeit, Befugnisse, Mittelausstattung, Ermessensspielraum)*, Zuständigkeit der Datenschutzbehörden (zentrale Kontaktstelle), Amtshilfe, Kohärenz (*Anwendung von einzelstaatlichem Recht (Kapitel IX), Fristen)*, zentrale Kontaktstelle für betroffene Personen, institutionelle Struktur des Europäischen Datenschutzausschusses, Datenübermittlungen ins Ausland, nach EU-Recht nicht zulässige Weitergabe von Daten, Recht auf Haftung und Schadenersatz, Geldbußen, Rechtsbehelfe sowie Kirchen und religiöse Vereinigungen.

Die Datenschutzgruppe nimmt zur Kenntnis, dass sich die Europäische Kommission ausdrücklich dafür entschieden hat, den Datenschutz nicht insgesamt in einem einzigen Rechtsinstrument zu regeln, sondern zur Regelung des Datenschutzes im Bereich der Polizei und Strafjustiz auf dem von ihr angestrebten einheitlich hohen Niveau eine Richtlinie vorzulegen.

Die Datenschutzgruppe bedauert, dass die Befugnisse der Datenschutzbehörden weder sehr ausführlich geregelt sind noch in Einklang mit den Bestimmungen der Verordnung stehen. Insbesondere enthält die Richtlinie im Gegensatz zur Verordnung keine Regelungen, die den Zugang zu Geschäftsräumen betreffen. Die Aufsichtsbehörde sollte in allen Bereichen die Möglichkeit haben, nötigenfalls Geschäftsräume des für die Verarbeitung Verantwortlichen zu betreten.

Die Datenschutzgruppe bedauert, dass die Richtlinie keine Bestimmungen zu Fristen, Überprüfungen und anderen Garantien (etwa die Beschränkung der Verwendung von Daten für schwere Straftaten usw.) enthält. Die Datenschutzgruppe stellt fest, dass zuständige Behörden, die Daten übermittelt haben, nicht verpflichtet sind, den Empfänger zu unterrichten, wenn die übermittelten Daten unrichtig waren oder unrechtmäßig übermittelt wurden.

Die Datenschutzgruppe bedauert schließlich auch, dass die Richtlinie keine Vorschriften zur Übermittlung von Daten an private Nutzer oder andere Behörden, die keine zuständigen Behörden im Sinne der Richtlinie sind, enthält. Die Datenschutzgruppe fordert deshalb den europäischen Gesetzgeber nachdrücklich auf, eine Bestimmung aufzunehmen, wonach Übermittlungen von Strafverfolgungsdaten an private Nutzer nur unter gesetzlich genau festgelegten Bedingungen zulässig sind.

Die angesprochenen Themen in Bezug auf die Richtlinie lauten Wahl des Instruments, Kohärenz, Anwendungsbereich, Datenverarbeitungsgrundsätze, Rechte der betroffenen Personen, Pflichten des für die Verarbeitung Verantwortlichen, Datenübermittlungen ins Ausland (*allgemeine Grundsätze für die Übermittlung und Weitergabe, negative Angemessenheitsbeschlüsse, Datenübermittlung auf der Grundlage geeigneter Garantien* und *Ausnahmen)* sowie die Befugnisse der Datenschutzbehörden und Zusammenarbeit.

Stellungnahme 8/2012 (WP 199) mit weiteren Beiträgen zur Diskussion der Datenschutzreform

In ihrer Stellungnahme vom 23. März 2012 reagierte die Artikel-29-Datenschutzgruppe zum ersten Mal allgemein auf die Vorschläge der Kommission, indem Problembereiche aufgezeigt und bestimmte Verbesserungsvorschläge gemacht wurden. Im Hinblick auf die laufenden Diskussionen sowohl im Europäischen Parlament als auch im Rat hat die Datenschutzgruppe beschlossen, diese Stellungnahme mit weiteren Leitlinien, insbesondere zu bestimmten wichtigen Datenschutzkonzepten, einer Analyse der Notwendigkeit und der Folgen der vorgeschlagenen delegierten Rechtsakte sowie gegebenenfalls Vorschlägen für geeignetere Alternativen anzunehmen.

Zentrale Begriffe waren personenbezogene Daten und Einwilligung.

Was die vorgeschlagenen delegierten Rechtsakte betrifft, brachte die Datenschutzgruppe ihre Ansichten zur eventuellen Notwendigkeit solcher Rechtsakte zum Ausdruck und bezog sich diesbezüglich auf spezifische vorgeschlagene Vorkehrungen.

In Bezug auf Artikel 14 Absatz 7 zur weiteren Festlegung verschiedener Kriterien für Kategorien von Empfängern, Meldung eventuellen Zugriffs, weiteren Informationen für spezifische Sektoren und Situationen sowie Bedingungen und geeignete Garantien im Hinblick auf die Ausnahmen räumte die Datenschutzgruppe ein, dass solche Bedingungen in einem delegierten Rechtsakt entwickelt werden

könnten, eine genauer detaillierte Orientierungshilfe durch den Europäischen Datenausschuss (European Data Protection Board, EDPB) allerdings bei der Beurteilung von Fällen, in denen die für die Verarbeitung Verantwortlichen auf der Grundlage einer Analyse der verschiedenen praktischen Situationen und Umstände die Ausnahmeregelung anwenden könnten, helfen könnte.

In Bezug auf Artikel 15 Absatz 3 zur Festlegung von Einzelheiten zu den Kriterien und Anforderungen bezüglich der Mitteilung über den Inhalt der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, sowie über jegliche verfügbaren Informationen über die Herkunft der Daten, an die betroffene Person erscheinen keine weiteren Rechtsvorschriften oder Orientierungshilfen notwendig.

In Bezug auf Artikel 17 Absatz 9 zur Festlegung von Kriterien und Anforderungen bezüglich des Rechts auf Vergessenwerden für bestimmte Sektoren und in speziellen Datenverarbeitungssituationen und der Bedingungen für die Löschung von Internet-Links, Kopien oder Replikationen von personenbezogenen Daten aus öffentlich zugänglichen Kommunikationsdiensten kam die Datenschutzgruppe zu der Übereinstimmung, dass ein delegierter Rechtsakt am besten geeignet ist, sofern er gleichzeitig mit Inkrafttreten der Verordnung verabschiedet wird. Gleiches gilt für Artikel 20 Absatz 5 zur näheren Regelung der Kriterien und Bedingungen für geeignete Maßnahmen zur Wahrung der berechtigten Interessen von betroffenen Personen, sofern der EDPB zusätzliche Orientierungshilfe gibt.

Für die Kriterien und Anforderungen in den Artikeln 8 (Anforderungen einer Einwilligung), 12 (unverhältnismäßige Entgelte und Anträge), 22 (allgemeine Pflichten), 26 (Auswahl eines Datenverarbeiters) und 28 (Dokumentation der Verarbeitungsvorgänge) schien es nicht notwendig, in einem delegierten Rechtsakt weitere Orientierungshilfen zu geben.

Für die Artikel 6 (Rechtmäßigkeit), 9 (sensible Daten), 23 und 30 (Sicherheit der Verarbeitung) und 34 (vorherige Anhörung) wurde weitere Orientierungshilfe durch den EDPB als bevorzugte Option zur näheren Regelung der Kriterien und Anforderungen erachtet.

Angesichts ihrer Bedeutung für alle betroffenen Interessenvertreter hätten zumindest die wesentlichen Merkmale der Kriterien und Anforderungen in den Artikeln 31 und 32 (Verpflichtung zur Meldung von Verletzungen des Schutzes personenbezogener Daten) sowie in Artikel 83 im Text der Verordnung selbst behandelt werden sollen. Für bestimmte Einzelheiten würde ein delegierter Rechtsakt ausreichen, sofern er gleichzeitig mit Inkrafttreten der Verordnung verabschiedet wird.

Delegierte Rechtsakte wurden mit weiterer Orientierungshilfe durch den EDPB zur Festlegung der Kriterien und Anforderungen in den Artikeln 33, 35, 37 und 44 Absatz 1 Buchstabe h als angemessen erachtet.

Die in den Artikeln 39 (Zertifizierung), 79 (Geldbußen), 81 und 82 (delegierte Rechtsakte) genannten Maßnahmen wurden als hinreichend erachtet.

1.4. PERSONENBEZOGENE DATEN

1.4.1. epSOS

Arbeitspapier 1/2012 (WP 189) zu epSOS

Ziel dieses Arbeitspapiers der Artikel 29-Datenschutzgruppe ist es, eine Orientierungshilfe zu Datenschutzfragen im Zusammenhang mit dem Projekt epSOS (European Patients Smart Open Services) zu bieten, die wichtigsten Grundsätze der Richtlinie 95/46/EG zu erläutern und zu erklären, wie das Arbeitspapier zur Verarbeitung von Patientendaten in elektronischen Patientenakten (WP 131) auf das Projekt epSOS angewendet wird.

epSOS ist ein Pilotgroßprojekt zu elektronischen Speichersystemen für Patientendaten im Zusammenhang mit zwei grenzüberschreitenden Diensten, und zwar der Patienten-Kurzakte und elektronischen Verschreibungen (e-Rezept).

Die Datenschutzgruppe kam in ihrer Beurteilung zu einer Reihe von Schlussfolgerungen.

Alle in medizinischen Unterlagen, elektronischen Patientenakten und EPA-Systemen gespeicherten Daten sind „sensible personenbezogene Daten" und unterliegen damit Artikel 8 der Richtlinie. Für die Verarbeitung von Daten im Bereich der Gesundheitsversorgung muss eine klare Rechtsgrundlage gegeben sein.

Eine der Hauptvoraussetzungen für die Gültigkeit einer Einwilligung besteht darin, dass die der betroffenen Person gegebenen Informationen den Anforderungen von Artikel 10 und 11 der Richtlinie genügen.

Die Verarbeitung personenbezogener Daten ist strikt auf das Mindestmaß zu beschränken, das für das Erreichen der Zwecke von epSOS erforderlich ist, die wiederum genau festgelegt, eindeutig und rechtmäßig sein müssen. Um zu gewährleisten, dass Daten nicht länger als erforderlich im epSOS-System gespeichert werden, sollte eine Höchstspeicherfrist beschlossen und ein gemeinsames Verfahren für den Umgang mit den Daten nach Ablauf dieser Speicherfrist festgelegt werden.

Jeder Abfrage von personenbezogenen Daten aus dem epSOS-System sollte ein tatsächlicher Bedarf an spezifischen Daten zu der zu erbringenden medizinischen Versorgungsleistung oder Behandlung oder zu dem zu verschreibenden oder abzugebenden Medikament in einem bestimmten Fall zugrunde liegen.

Aufgrund des grenzüberschreitenden Charakters der epSOS-Verarbeitung wird eine Zusammenarbeit zwischen den Datenschutzbehörden bei der Kontrolle von epSOS nachdrücklich empfohlen.

Alle für die Verarbeitung Verantwortlichen, die mit epSOS-Daten umgehen, müssen die nationale Kontrollstelle gemäß den nationalen Rechtsvorschriften benachrichtigen, unabhängig davon, ob die betroffene Person Staatsangehöriger ist oder ihren Wohnsitz in einem anderen Mitgliedstaat hat und unabhängig davon, ob die betreffenden Daten von für die Verarbeitung Verantwortlichen in anderen Mitgliedstaaten stammen.

epSOS benötigt ein hohes Maß an IT-Sicherheit. Hierfür sind beispielsweise die folgenden Maßnahmen und Regelungen erforderlich: Mitarbeitern, die mit der Durchführung des Projekts befasst sind, sollten eindeutige schriftliche Weisungen für eine ordnungsgemäße Nutzung des epSOS-Systems an die Hand gegeben werden, um Sicherheitsrisiken und Verletzungen der Sicherheit zu verhindern; durch entsprechende Vorkehrungen bei der Verwendung von Systemen zur Speicherung und Archivierung der Patienten-Kurzakten und Verschreibungen ist dafür zu sorgen, dass die Daten gegen unbefugten Zugriff, Diebstahl bzw. vor dem teilweisen/völligen Verlust des Speichermediums geschützt sind; für den Datenaustausch sind auf Grundlage von Verschlüsselungsstandards für eine sichere elektronische Kommunikation sichere Kommunikationsprotokolle und ein Verschlüsseln der Daten von Endstelle zu Endstelle vorzusehen; besondere Aufmerksamkeit ist dem Aufbau von zuverlässigen und wirksamen elektronischen Identifizierungssystemen mit eindeutiger Authentisierung (sowohl der teilnehmenden Fachkräfte als auch der teilnehmenden Patienten) zu widmen; das System muss in der Lage sein, in nachprüfbarer Weise die einzelnen Vorgänge, die die Datenverarbeitung insgesamt ausmachen, korrekt aufzuzeichnen und rückzuverfolgen; bei der Übermittlung bzw. Speicherung der Back-up-Daten sollte (z. B. durch Verschlüsselung) ein unbefugter Zugriff auf die Daten bzw. ihre unbefugte Änderung verhindert werden; im Hinblick auf das System der elektronischen Verschreibungen sollten zusätzliche Maßnahmen ergriffen werden, damit im pharmazeutischen Bereich Tätige Zugang zu digitalen Rezepten nur erhalten, um die verschriebenen Medikamente abzugeben; und in Notfällen sollte jeder Zugriff aufgezeichnet und nachgeprüft werden.

Alle für die Verarbeitung der Daten Verantwortlichen, die mit epSOS-Daten umgehen, müssen betroffenen Personen das Recht auf Auskunft und das Recht auf Berichtigung, Löschung oder Sperrung der eigenen Daten einräumen. Des Weiteren sollte eine betroffene Person allen für die Verarbeitung Verantwortlichen sowie allen anderen am Informationsaustausch im Rahmen von epSOS Beteiligten Fragen zu ihrem Auskunftsrecht sowie zu Anträgen auf Berichtigung/Löschung/Sperrung stellen können. Ein Antrag auf Auskunft oder auf Berichtigung/Löschung/Sperrung von Daten, der bei einem epSOS-Partner eingereicht wird, der die Daten über die betroffene Person nicht verarbeitet, ist an den zuständigen für die Verarbeitung Verantwortlichen innerhalb des epSOS-Systems weiterzuleiten, auch wenn dieser seinen Sitz in einem anderen Mitgliedstaat hat.

epSOS sollte prüfen, ob betroffenen Personen nicht (auf elektronischem Wege) ein direkter Lesezugriff auf ihre jeweiligen Daten gewährt werden kann. Es sollte eine gemeinsame epSOS-Website eingerichtet werden, auf der die betroffenen Personen über ihre Rechte aufgeklärt werden, die sie gemäß den jeweiligen Rechtsvorschriften der einzelnen teilnehmenden Länder besitzen.

1.4.2 Entwicklungen im Bereich biometrische Technologien

Stellungnahme 3/2012 (WP193) zu Entwicklungen im Bereich biometrische Technologien

Die Datenschutzgruppe hat in ihrem Arbeitspapier über Biometrie (WP80) bereits Fragen des Datenschutzes im Zusammenhang mit der Nutzung aufkommender Technologien zum elektronischen Lesen und Verarbeiten biometrischer Daten untersucht.

In den darauf folgenden Jahren haben diese Technologien stark zugenommen und neue aufkommende Dienstleistungen haben sich entwickelt. Biometrische Technologien, die früher mit einem erheblichen finanziellen Aufwand verbunden waren oder beträchtliche Rechenkapazität beanspruchten, sind erheblich billiger und schneller geworden. Diese Technologien sind eng mit gewissen personenbezogenen Merkmalen verbunden, und einige davon können genutzt werden, um empfindliche Daten in Erfahrung zu bringen. Außerdem ermöglichen viele von ihnen die automatisierte Verfolgung und Aufspürung von Personen sowie die Erstellung von Profilen. Insoweit können sich diese Entwicklungen erheblich auf die Privatsphäre und auf das individuelle Recht auf Datenschutz auswirken.

In dieser Stellungnahme soll ein überarbeiteter und aktualisierter Rahmen für einheitliche allgemeine Leitlinien und Empfehlungen zur Berücksichtigung von Grundsätzen des Schutzes der Privatsphäre und des Datenschutzes im Zusammenhang mit biometrischen Anwendungen beschrieben werden. Die Stellungnahme richtet sich an gesetzgebende Institutionen auf europäischer und auf nationaler Ebene, sowie an die Biometrieindustrie und an die Nutzer der entsprechenden Technologien.

Biometrische Systeme hängen von mehreren Akteuren ab: von Herstellern, integrierten Dienstleistern, Wiederverkäufern, mit der Einrichtung der Systeme befassten Fachkräften, Kunden und betroffenen Personen. Sicherheit sollte ein wesentlicher Aspekt sein, weil biometrische Daten nicht widerruflich sind. Die Datenschutzgruppe empfiehlt einen weitreichenden technischen Schutz bei der Verarbeitung biometrischer Daten. Dabei sollten die modernsten technischen Mittel zum Einsatz kommen. In diesem Zusammenhang sollten bestehende Industrienormen für den Schutz von Systemen berücksichtigt werden, in denen biometrische Informationen verarbeitet werden.

Eingebauter Datenschutz („Privacy by Design“) bedeutet, dass die Wahrung der Privatsphäre proaktiv in die Technologie selbst eingebaut wird. Das Konzept des eingebauten Datenschutzes betrifft bei biometrischen Systemen die gesamte Wertschöpfungskette. Die Datenschutzgruppe empfiehlt die Auslegung biometrischer Systeme gemäß formaler „Entwicklungslebenszyklen“, einschließlich: Spezifikation von Anforderungen gemäß einer Risikoanalyse bzw. gemäß einer speziellen Datenschutz-Folgenabschätzung; Beschreibungen und Begründungen dahingehend, wie durch die jeweilige Auslegung die bestehenden Anforderungen erfüllt werden; Validierung mithilfe von Funktions- und Sicherheitstests und Verifikation der Konformität der endgültigen Gestaltung mit dem geltenden Rechtsrahmen.

Eine Datenschutz-Folgenabschätzung (Privacy Impact Assessment, PIA) ist ein Prozess, bei dem ein Rechtssubjekt die mit der Verarbeitung personenbezogener Daten verbundenen Risiken bewertet und zusätzliche Maßnahmen zur Verringerung dieser Risiken definiert. Hierbei sollten die folgenden Aspekte berücksichtigt werden: Art der erfassten Informationen; Zweck der Informationserfassung; Zuverlässigkeit des Systems; Rechtsgrundlage und rechtliche Konformität; Zugang zum jeweiligen Gerät und interne und externe Weitergabe von Informationen durch den für die Verarbeitung Verantwortlichen, wobei personenbezogene Daten durch geeignete Sicherheitstechniken und -verfahren gegen unbefugte Zugriffe zu schützen sind; bereits getroffene, die Privatsphäre weniger beeinträchtigende Maßnahmen; Entscheidungen bezüglich der Aufbewahrungszeit und der Löschung von Daten sowie Rechte der betroffenen Personen.

Biometrische Daten erfordern insoweit besondere Aufmerksamkeit, als anhand dieser Daten einzelne Personen aufgrund ihrer individuellen verhaltensbezogenen oder physiologischen Merkmale zweifelsfrei identifiziert werden können. Daher sollte mit PIAs möglichst bewertet werden, wie Identitätsbetrug, Modifikationen des ursprünglichen Zwecks und Verletzungen des Schutzes personenbezogener Daten durch das zu analysierende System vermieden oder zumindest in erheblichem Umfang begrenzt werden können.

Wegen der Art des Datenmaterials erfordert die Verarbeitung biometrischer Daten spezielle technische und organisatorische Maßnahmen und Vorkehrungen, um Beeinträchtigungen der betroffenen Personen infolge einer Verletzung des Schutzes personenbezogener Daten zu vermeiden.

Technische Maßnahmen könnten vor allem bei großen biometrischen Datenbanken wie folgt aussehen: biometrische Templates, Speicherung auf einem persönlichen Gerät im Vergleich zu einer zentralen Speicherung, erneuerbare und widerrufbare Verknüpfungen von Identitäten, Verschlüsselung, Schutz gegen Spoofing, biometrische Ver- und Entschlüsselung sowie automatisierte Mechanismen zur Datenlöschung.

Organisatorische Maßnahmen könnten z. B. Folgendes umfassen: die Entwicklung eines klaren Verfahrens zur Bestimmung, wer auf die im System gespeicherten Informationen zugreifen kann; die Festlegung, ob die Zugriffe unbeschränkt sind oder nicht; sowie die Gewährleistung einer Rückverfolgung.

Kapitel Zwei
Die wichtigsten Entwicklungen in den Mitgliedstaaten

BELGIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

In gesetzgeberischer Hinsicht war das Jahr 2012 von vier großen Entwicklungen geprägt. Die erste ist die vom flämischen Regionalparlament angenommene Verordnung vom 13. Juli 2012 zur Schaffung und Organisation eines flämischen Dienstintegrators (ISF). Der ISF ist als Stelle definiert, die per (föderalem oder regionalem) Gesetz für die Organisation des elektronischen Datenaustauschs zwischen flämischen Regierungsbehörden sowie für den integrierten Datenzugriff verantwortlich ist. Mit Ausnahme außergewöhnlicher Umstände muss jegliche beim ISF eingehende und von ihm ausgehende Kommunikation von der 2010 gegründeten flämischen Aufsichtsbehörde (Vlaamse Toezichtcommissie) genehmigt werden. In einem föderalen Gesetz ist außerdem ein föderaler Dienstintegrator (FEDICT) vorgesehen. Für die belgische Datenschutzbehörde (CPVP) ist insbesondere Artikel 7 dieses Gesetzes von Bedeutung. Hierin wird ihr die Aufgabe übertragen, verschiedenen sektoriellen Ausschüssen die Erteilung von Genehmigungen zuzuweisen und unter Berücksichtigung der Ansichten der anderen zuständigen sektoriellen Ausschüsse zu bestimmen, welcher Ausschuss für die Erteilung der Genehmigung zuständig ist. Das Gesetz vom 3. August 2012 zur Handhabung personenbezogener Daten durch den Föderalen Öffentlichen Dienst Finanzen (FÖD Finanzen) im Rahmen seiner Tätigkeit ist das Ergebnis einer Zusammenarbeit zwischen der CPVP und diesem FÖD. Diese Zusammenarbeit geht auf den Wunsch der CPVP zurück, die wesentlichen Grundsätze des Datenschutzes bei jedem behördenübergreifenden Austausch und bei jedem Austausch mit externen Stellen zur Anwendung zu bringen. Eine vorläufige Version dieses Gesetzes wich in großem Maße und allgemein von dem gemäß Artikel 10 des Datenschutzgesetzes (LVP) gewährten Zugangsrechts im Falle einer steuerlichen Ermittlung ab. Nachdem die CPVP ihre ablehnende Meinung hinsichtlich dieser Einschränkung zum Ausdruck gebracht hatte, wurde das Gesetz abgeändert und sieht nun eine Prüfung auf Einzelfallbasis vor, um festzustellen, ob ein Zugangsrecht einer laufenden Ermittlung schaden würde oder nicht. Gegebenenfalls wird bezüglich einer Einschränkung des Zugangsrechts eine begründete, individuelle Entscheidung getroffen. Die Änderung des journalistischen Ethikkodizes, der nun eindeutig vorsieht, dass Daten aus sozialen Netzwerken wie z. B. Facebook nur dann von den Medien veröffentlicht werden dürfen, wenn die betroffenen Personen ihre ausdrückliche Einwilligung erteilt haben, ist ebenfalls das Ergebnis einer langen Zusammenarbeit mit der CPVP. Hierzu hat ganz bestimmt auch das Busunglück von Sierre im März 2012 beigetragen, infolgedessen Bilder (größtenteils von Kindern) aus sozialen Netzwerken von der Presse veröffentlicht wurden. Bei der vierten und letzten erwähnenswerten Entwicklung handelt es sich um die Änderung des Gesetzes über elektronische Kommunikation, das die Cookie-Richtlinie nach einer Empfehlung und einer Stellungnahme der CPVP in belgisches Recht umsetzte. Unter den anderen Stellungnahmen und Empfehlungen der CPVP wären die Einführung des Grundsatzes authentischer Quellen, eine zentrale Datenbank für den Austausch von Daten sowie ein „Datenschutzausschuss Wallonien-Brüssel“ für die Wallonische Region und die Französische Gemeinschaft zu nennen, die als Gegenstück zur bereits erwähnten flämischen Aufsichtsbehörde fungieren soll. In ihrer Empfehlung zur „Cyberüberwachung“, die sich auf Arbeitgeberkontrollmaßnahmen zur Überwachung der elektronischen Mitarbeiterkommunikation insbesondere per E-Mail und Internet am Arbeitsplatz bezieht, schlägt die CPVP eine faire Vereinbarung von Datenschutz für Mitarbeiter einerseits und der Achtung von Arbeitgebervorrechten und einem reibungslosen Arbeitsablauf innerhalb des Unternehmens andererseits vor (siehe auch Jahresbericht 2011).

Europäische Datenschutzreform

Zu guter Letzt wies die CPVP in der Stellungnahme zum Verordnungsentwurf der Europäischen Kommission vom Beginn des Jahres auf die vielen schwierigen Fragen und auf die starken Einwände bezüglich der Wahl des Instruments und des Inhalts dieses Vorschlags für die Reform des Datenschutzrechtsrahmens in der Europäischen Union aus Sicht der CPVP hin. Sie untermauert die wichtige Analysearbeit, die 2012 an diesem Dokument vorgenommen wurde.

Alles Weitere ist im Jahresbericht 2012 der belgischen Datenschutzbehörde einsehbar: http://www.privacycommission.be/sites/privacycommission/files/documents/rapport-annuel-2012.pdf

Organisation	Datenschutzkommission
Vorsitz und/oder Gremium	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: ein Anwalt/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	5 684 000 EUR (2012)
Personal	53 Mitarbeiter (1 Vorsitzender – 1 stellvertretender Vorsitzender) - Sekretariat des Vorsitzenden (5): juristisches Sekretariat (2), Sekretariat (2), Logistik (1) - Administrator (1) - Bereichsleiter: (3) - Personal und Organisation (16): Buchhaltung (1), Übersetzer (5), Verwaltung (3), Statistiker (1), Personalleiter (1), Empfang (2), Logistik (1), IT-Unterstützung (1), Kommunikationsleiter (1)

	- Studien und Forschung (17): Rechtsberater (15), IT-Fachkraft (1), Forschungsassistent (1) - Außenbeziehungen (Frontoffice) (11): Rechtsberater (4), Assistenten (7)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	- Stellungnahmen (auf Anfrage der Legislative oder Exekutive - siehe unten): 41 - Stellungnahmen und Initiativempfehlungen: 9 - Empfehlungen zur Weiterverarbeitung: 9
Meldungen	
Vorabprüfungen	Auch 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 Genehmigungsanträgen erteilt: - Sektorausschuss der Bundesbehörde: 46 (Einzelgenehmigungen) und 40 (allgemeine Genehmigungen) - Sektorausschuss für Statistik: 38 (Einzelgenehmigungen) - Sektorausschuss für das Nationalregister: 106 (Einzelgenehmigungen) und 229 (allgemeine Genehmigungen) - Sektorausschuss für soziale Sicherheit und Gesundheitswesen: siehe Website der Banque Carrefour de la Sécurité Sociale
Anträge betroffener Personen	Die Statistiken der belgischen Datenschutzbehörde unterscheiden nicht zwischen Auskunftsersuchen von betroffenen Personen oder von für die Datenverarbeitung Verantwortlichen: - Durch die Zentrale erteilte Auskünfte: 2012 wurden 1 892 „Fragen und Antworten“ bearbeitet (Recht an der eigenen Abbildung, Grundsätze des Datenschutzes, Konjunktur/Konsumentenkredit, Datenschutz am Arbeitsplatz und Behörden). - Die belgische Datenschutzbehörde bearbeitete außerdem 2 896 Auskunfts- oder Vermittlungsanfragen (einschließlich Überprüfungen): Darunter: 2 437 Auskunftsanfragen sowohl von öffentlichen Stellen und derzeitigen oder zukünftigen für die Verarbeitung Verantwortlichen und betroffenen Personen, 303 Vermittlungsanfragen und 156 Überprüfungen.
Beschwerden betroffener Personen	Siehe oben: 303 Vermittlungsanfragen: Vor jeder Vermittlung oder Auskunft überprüft die belgische Datenschutzbehörde stets die Zulässigkeit. Bei 149 Fällen wurde die Vermittlungsanfrage als nicht zulässig befunden, oftmals aufgrund mangelnder Informationen vonseiten der betroffenen Person (144 Fälle). 198 Anfragen (8,26 %) 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. Die häufigsten Bereiche (Auskunft, Vermittlung/Beschwerden und Prüfungen) lauten: - Aufnahmen, insbesondere Videoaufnahmen - Grundsätzliches zum Thema Datenschutz - Datenverarbeitung durch öffentliche Stellen - Kommerzielle Praktiken (vornehmlich Marketing) - Privatsphäre und Arbeit, Kredit.
Vom Parlament bzw. der Regierung angeforderte Beratung	Eine Auflistung der 2012 von der belgischen Datenschutzbehörde abgegebenen Stellungnahmen ist auf der Website der Behörde unter http://www.privacycommission.be einsehbar
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Siehe den 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	156 Prüfungen. Die Datenschutzbehörde führte im Jahr 2012 Prüfungen auf zwei Ebenen durch. Die erste Ebene betrifft die Datenverarbeitung im Zusammenhang mit Schengen-, Eurodac- und Zollinformationssystemen einerseits und Europol-Aktivitäten andererseits. Die zweite Ebene betrifft Prüfungen auf Eigeninitiative. Diese Prüfungen können wiederum in drei Arten unterteilt werden: fortlaufende Prüfungen von Child Focus und dem Sekteninformationszentrum; themenbezogene Prüfungen von Polizei- und Informationsdiensten, einschließlich Dateien in Bezug auf indirekten Zugriff (gemäß Artikel 13 des Datenschutzgesetzes zum Polizeiwesen) sowie Einzelprüfungen, die sich stets auf einen bestimmten für die Datenverarbeitung Verantwortlichen beziehen.
Sanktionsmaßnahmen	
Sanktionen	Die Datenschutzbehörde hat keine Sanktionsbefugnis. Sie kann jedoch Fälle, bei denen Verstöße ermittelt wurden, an die Staatsanwaltschaft weiterleiten.
Geldbußen	Die Datenschutzbehörde hat keine Sanktionsbefugnis. Sie kann jedoch Fälle, bei denen Verstöße ermittelt wurden, an die Staatsanwaltschaft weiterleiten.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Die Datenschutzbehörde verfügt nicht über diese Angaben.

BULGARIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	Kommission für den Schutz personenbezogener Daten (CPDP)
Vorsitz und/oder Gremium	Kommission mit Leiterin: Veneta Shopova und 4 Mitglieder: Krassimir Dimitrov, Valentin Enev, Mariya Mateva und Veselin Tselkov.
Budget	2 738 678 BGN, davon wurden 2 573 917 BGN ausgegeben.
Personal	Anzahl der Beamten: 78
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2012 wurden insgesamt 364 Beschlüsse, Stellungnahmen und Anweisungen herausgegeben, davon: - 271 Beschwerden - 77 Stellungnahmen zur Anwendung des Datenschutzgesetzes - 16 verbindliche Anweisungen
Meldungen	66 805 für die Datenverarbeitung Verantwortliche
Vorabprüfungen	1 616
Anträge betroffener Personen	247 Anträge von natürlichen und juristischen Personen sowie verschiedene Anfragen zu aktuellen Themen im Zusammenhang mit den Zuständigkeiten der CPDP.
Beschwerden betroffener Personen	531 Beschwerden, die meisten davon in den folgenden Bereichen: - Telekommunikation: 274 - Beschäftigung und Versicherungsdienstleistungen: 33 - Bankwesen: 32
Vom Parlament bzw. der Regierung angeforderte Beratung	- Anträge auf Stellungnahmen von der Nationalversammlung zur Wahrscheinlichkeit der Erstellung einer Kopie der bereitgestellten Unterschriftenliste, die gemäß dem Gesetz über die direkte Beteiligung von Staatsbürgern an der Staatsgewalt und der kommunalen Selbstverwaltung (Act for Direct Participation of Nationals in the State Authority and Local Self-government, ADPNSALS) für ein Verbot der Forschung und Förderung von Schiefergas in Bulgarien mithilfe von Hydraulic Fracturing erhoben wurde und den Mitgliedern des Initiativkomitees zugänglich gemacht und in die Nationalversammlung eingebracht werden sollte. - Antrag auf Stellungnahme durch den Ministerrat zur Schaffung eines neuen Registers für personenbezogene Daten und der diesbezüglichen Zugangsermächtigung.

Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Bezüglich der Übermittlung personenbezogener Daten sieht das Datenschutzgesetz ein Genehmigungsverfahren vor. Im Berichtszeitraum wurden acht 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 dem Verfahren zur gegenseitigen Anerkennung. 2012 wurden 14 Genehmigungsanträge eingereicht.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Die Anzahl der 2012 durchgeführten Prüfungen belief sich auf 1 718, davon: - ex-ante: 1 616 - andauernd: 71 - *ex-post*: 32, größtenteils in den folgenden Bereichen: Gesundheitswesen: 996; Handel und Dienstleistungen: 109; Aus- und Weiterbildung: 106; Tourismus: 58; Rechts- und Beratungsdienstleistungen: 54.
Sanktionsmaßnahmen	
Sanktionen	2012 verhängte die CPDP die folgenden Sanktionen: - 58 Feststellungen von Verwaltungsverstößen - 52 Bußgeldbescheide
Geldbußen	Die CPDP hat 2012 Sanktionen im Wert von 323 350 BGN (rund 161 675 Euro) verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

1. Bezüglich der erlassenen verbindlichen Anweisungen und Bußgeldbescheide:

Im Jahr 2012 wurden 16 verbindliche Anweisungen erlassen, von denen die meisten das Verwaltungs-, Finanz- und Gesundheitswesen betrafen. Zu sonstigen Sektoren gehören Justiz, Aus- und Weiterbildung, Transport, Handel und Dienstleistungen.

Die Anweisungen wurden im Zusammenhang mit den folgenden Themen erlassen:

- Fehlende organisatorische und technische Maßnahmen zur Garantie des Schutzniveaus für personenbezogene Daten: 51 % der Anweisungen;
- Unterlassung der Aktualisierung der beim Register der für die Verarbeitung personenbezogener Daten Verantwortlichen des CPDP hinterlegten Informationen: 33 %;

- Verbot der Verarbeitung bestimmter Kategorien personenbezogener Daten: 13 %;
- Versäumte Einholung einer Einwilligung in Kenntnis der Sachlage durch die Einzelperson zur Verarbeitung ihrer personenbezogenen Daten: 3 %.

Zu den häufigsten Verwaltungsverstößen, zu denen die CPDP Feststellungen herausgegeben hat, gehörten:

- Verstoß gegen die Anforderung, Einträge im Register für die Verarbeitung personenbezogener Daten der CPDP zu aktualisieren. Der Verstoß ergibt sich aus der Verarbeitung eines neuen Registers, das der für die Verarbeitung Verantwortliche nicht der CPDP gemeldet und in das System eingetragen hat;
- Fehlende Anweisungen für eine Einführung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten vor einer versehentlichen oder gesetzeswidrigen Zerstörung, einem versehentlichen Verlust oder vor einem gesetzeswidrigen Zugreifen, Berichtigen oder Verbreiten sowie vor anderen gesetzeswidrigen Verarbeitungsformen;
- Verstoß gegen die Verpflichtung, sich bei der Kommission für den Schutz personenbezogener Daten zu registrieren;
- Unterlassung einer Einführung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten vor einer versehentlichen oder gesetzeswidrigen Zerstörung, einem versehentlichen Verlust oder vor einem gesetzeswidrigen Zugreifen, Berichtigen oder Verbreiten sowie vor anderen gesetzeswidrigen Verarbeitungsformen.

2. In Bezug auf die Abgabe von Stellungnahmen zu Anfragen und Signalen, um die die CPDP — neben den in der Tabelle aufgeführten Fällen — von staatlichen Behörden gebeten wurde, sind die folgenden Stellungnahmen ebenfalls von Interesse.

2.1. Stellungnahmen der CPDP zu Anträgen auf Zugang zur Nationalen Bevölkerungsdatenbank (NBD)

Unter den häufigsten Anträgen waren solche auf Zugang zur NBD, die von der Abteilung Zivile Registrierungs- und Verwaltungsdienstleistungen (CRAS) der Generaldirektion beim Ministerium für regionale Entwicklung (MRD) gepflegt wird, oder zu den Personenstandsregistern.

In den meisten Fällen beantragten die für die Verarbeitung Verantwortlichen die Bereitstellung eines direkten Zugangs zur NBD, denen ein rechtliches Interesse zugrunde lag.

Im Zusammenhang mit einem direkten Zugang zur NBD geht die CDPD davon aus, dass zwischen der Bereitstellung von NBD-Daten aufgrund eines stichhaltigen rechtlichen Interesses und der Gewährung eines direkten Zugriffs auf die NBD unterschieden werden sollte.

Die CPDP ist der Ansicht, dass der Bereitstellung bestimmter personenbezogener Daten (ohne Direktzugang) rechtlich nichts im Wege steht, wenn die GD CRAS des MRD das gesetzlich vorgeschriebene Verfahren unter Berufung auf ein stichhaltiges rechtliches Interesse der antragstellenden Personen befolgt.

2.2. Anträge auf Zugang zu öffentlichen Informationen

Das bulgarische Datenschutzgesetz enthält keine Regelungen in Bezug auf die Informationsfreiheit und den Zugang zu Informationen, da dies in einem separaten Gesetz geregelt wird.

Die CPDP reagierte 2012 dennoch auf Anträge auf Stellungnahme der staatlichen und kommunalen Behörden im Zusammenhang mit dem Zugang zu öffentlichen Informationen.

Die zuständigen staatlichen Stellen erhielten Anträge auf die Bereitstellung von Vergütungsinformationen.

Nachdem die gestellten Fragen in Betracht gezogen wurden, gab die CPDP in einer Stellungnahme bekannt, dass Informationen zu bestimmten Stellen und deren Vergütung nur dann als personenbezogene Daten gelten, wenn die entsprechende Person eindeutig identifizierbar ist.

Die Verarbeitung solcher Daten ist nur in Fällen zulässig und rechtens, in denen eines der Zulassungskriterien erfüllt wird, wie z. B. das Bestehen öffentlichen Interesses oder die ausdrückliche Einwilligung durch die Betroffenen.

2.3. Bezüglich der Anträge in Zusammenhang mit der Vermeidung von Interessenkonflikten bei der Ernennung hochrangiger Beamter in der öffentlichen Verwaltung

Im Jahr 2012 veröffentlichte die Kommission für den Schutz personenbezogener Daten auf Anfrage der Kommission für die Vermeidung und Feststellung von Interessenkonflikten eine Stellungnahme zu der Frage, ob es gemäß dem Datenschutzgesetz erlaubt sei, infolge eines Beschlusses der Kommission (für die Vermeidung von Interessenkonflikten) Informationen im Internet zu veröffentlichen, die mit Folgendem im Zusammenhang stehen:

- Berufsbezeichnungen von Personen, die öffentliche Ämter bekleiden, in Fällen, in denen dies zur Identifizierung der Personen beitragen könnte;
- Bezeichnung des Standortes, an dem das Amt ausgeführt wird, falls der Standort ein Identifizierungsmerkmal darstellt.

Bei der Bearbeitung des Antrags auf Stellungnahme berücksichtigte die CPDP die Tatsache, dass die Kommission für die Vermeidung und Feststellung von Interessenkonflikten rechtlich dazu verpflichtet ist, ihre Beschlüsse gemäß dem Gesetz über die Vermeidung und Feststellung von Interessenkonflikten auf ihrer Website zu veröffentlichen, und demnach die allgemeine Bekanntheit und Transparenz ihrer Arbeit und ihrer Entscheidungen gegeben ist. Des Weiteren ist die Behörde dazu verpflichtet, die Identität der Person, die das Signal eingereicht hat, nicht offenzulegen.

Die CPDP kam in ihrer Stellungnahme zu dem Schluss, dass die Kommission für die Vermeidung und Feststellung von Interessenkonflikten bei der Veröffentlichung ihrer Beschlüsse auf ihrer Website dafür sorgen muss, dass die Personen, die ein Signal eingereicht haben, sowie die Personen, gegen die sich das Signal richtet, nicht persönlich identifizierbar sind. Diesbezüglich müssen neben Namen und Adresse auch Merkmale, die auf die körperliche, physiologische, genetische, psychische, psychologische, wirtschaftliche, kulturelle, gesellschaftliche oder sonstige Identität von Einzelpersonen hinweisen, gelöscht werden. Gemäß dem Zweck des Gesetzes über die Vermeidung und Feststellung von Interessenkonflikten sowie der Verpflichtung von im öffentlichen Sektor tätigen Personen, ihre Ämter im öffentlichen Interesse auf ehrliche, faire, verantwortliche und objektive Weise auszuüben und vor den Bürgern und den Behörden, die sie gewählt oder ernannt haben, Rede und Antwort zu stehen, geht die CPDP davon aus, dass die auf der Website der Kommission veröffentlichten Beschlüsse sowie Daten zu ihren Ämtern bzw. zum Standort, an denen diese ausgeübt werden, veröffentlicht werden können. Sollten die Beschlüsse personenbezogene Daten Dritter enthalten, müssen diese anonymisiert werden.

2.4. Stellungnahme der CPDP zur direkten Beteiligung von Staatsbürgern an der Staatsgewalt und der kommunalen Selbstverwaltung

Interessant war außerdem ein Antrag auf Stellungnahme von der Nationalversammlung zu der Möglichkeit, dass eine Kopie einer Unterschriftenliste, die gemäß dem Gesetz über die direkte Beteiligung von Staatsbürgern an der Staatsgewalt und der kommunalen Selbstverwaltung (Act for Direct Participation of Nationals in the State Authority and Local Self-government, ADPNSALS) für ein Verbot der Erkundung und Förderung von Schiefergas in Bulgarien mithilfe von Hydraulic Fracturing erhoben wurde, einem Mitglied des Initiativkomitees zugänglich gemacht würde, das sie in die Nationalversammlung einbringen würde.

In ihrer Stellungnahme kam die CPDP zu dem Schluss, dass die Bereitstellung der Liste für ein Mitglied des Initiativkomitees eine Verarbeitung personenbezogener Daten darstelle, und zwar in Form einer Bereitstellung von Daten gemäß § 1 Absatz 1 der zusätzlichen Bestimmungen des Datenschutzgesetzes. Die personenbezogenen Daten wurden durch die Bürgerinitiative erhoben. Die Unterschriftenliste wurde anschließend der Nationalversammlung zugeschickt. Der Liste war eine Klausel beigefügt, laut der die personenbezogenen Daten lediglich zum Zwecke der Bürgerinitiative für ein Verbot der Erkundung und

Förderung von Schiefergas in Bulgarien mithilfe von Hydraulic Fracturing verwendet würden. Die Beantragung der Bereitstellung einer Kopie der Unterschriftenliste der Bürgerinitiative für ein Verbot der Erkundung und Förderung von Schiefergas in Bulgarien mithilfe von Hydraulic Fracturing, die gemäß dem Gesetz über die direkte Beteiligung von Staatsbürgern an der Staatsgewalt und der kommunalen Selbstverwaltung erstellt wurde, durch ein Mitglied des Initiativkomitees stellt eine zusätzliche Verarbeitung personenbezogener Daten dar, die nicht dem ursprünglichen Zweck der Datenerfassung entspricht. Aus diesem Grund sollte die Unterschriftenliste nicht bereitgestellt werden.

C. Sonstige wichtige Informationen

1. Die Kommission für den Schutz personenbezogener Daten verabschiedete eine neue Verordnung über ein Minimum an technischen und organisatorischen Maßnahmen und die zugelassenen Arten des Schutzes personenbezogener Daten

Am 30. Januar 2013 verabschiedete die Kommission für den Schutz personenbezogener Daten eine neue Verordnung über ein Minimum an technischen und organisatorischen Maßnehmen und die zugelassenen Arten des Schutzes personenbezogener Daten. Der Verordnung liegt Artikel 23 Absatz 5 des Gesetzes zum Schutz personenbezogener Daten zugrunde. Sie wurde am 12. Februar 2013 im Amtsblatt veröffentlicht und trat drei Tage nach der Bekanntmachung in Kraft. Diese Verordnung ersetzt Verordnung Nr. 1 vom 7. Februar 2007.

Durch die Verordnung soll abhängig von der Beschaffenheit der Daten und der Anzahl der betroffenen Personen im Falle einer Verletzung des Datenschutzes ein angemessener Schutz personenbezogener Daten gewährleistet werden. In der Verordnung werden die wichtigsten Zwecke des Schutzes personenbezogener Daten definiert: Vertraulichkeit, Integrität und Verfügbarkeit. Sie führt fünf verschiedene Arten des Schutzes personenbezogener Daten ein: physischen Schutz, persönlichen Schutz, dokumentarischen Schutz, den Schutz vor automatischen Informationssystemen bzw. Netzwerken sowie kryptografischen Schutz. Des Weiteren führte die Verordnung den Grundsatz „Kenntnis erforderlich“ als Zugangskontrolle ein.

Um das angemessene Niveau der technischen und organisatorischen Maßnahmen und die zugelassene Art des Datenschutzes zu bestimmen, sind die für die Verarbeitung Verantwortlichen dazu verpflichtet, regelmäßig eine Folgenabschätzung der Datenverarbeitung durchzuführen. Die Folgenabschätzung dient der Bestimmung der verschiedenen Gefährdungsgrade und der entsprechenden Schutzniveaus. Jedes Schutzniveau entspricht einer präzisen Kombination technischer und organisatorischer Maßnahmen, die für die Verarbeitung Verantwortliche einzuführen haben.

Die neuen Regelungen sehen vier verschiedene Auswirkungsebenen vor, die vom Ausmaß der eventuellen negativen Effekte einer unbefugten Verarbeitung personenbezogener Daten abhängen: „sehr hoch“, „hoch“, „durchschnittlich“ und „niedrig“.

Seit Inkrafttreten der Verordnung bietet die Kommission Schulungen und Beratungsdienste an, die sich an für die Verarbeitung Verantwortliche richten, um sie für aktuelle Probleme in Bezug auf personenbezogene Daten zu sensibilisieren.

Die Verordnung ist auf der Website der CDPD in englischer Sprache verfügbar.

Im Allgemeinen legt die Kommission für den Schutz personenbezogener Daten entsprechend dem dafür vorgesehenen jährlichen Schulungsplan den Schwerpunkt auf Schulungen, die sich an für die Verarbeitung Verantwortliche richten. Des Weiteren wurden Experten der Kommission für den Schutz personenbezogener Daten vom Institut für öffentliche Verwaltung (dem nationalen Ausbildungszentrum für Beamte) dazu eingeladen, ab Oktober 2013 regelmäßig Schulungen im Bereich Datenschutz anzubieten.

2. Anwendung der Richtlinie 2006/24/EG über Vorratsdatenspeicherung

Die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetzwerke erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (Richtlinie über die Vorratsdatenspeicherung) wurde 2010 durch Änderungen des Gesetzes über elektronische Kommunikation in bulgarisches Recht umgesetzt. Nach einer Auswertung der statistischen Daten, die 2012 von Anbietern elektronischer Kommunikationsnetzwerke bzw. -dienste bereitgestellt wurden, analysierte die Kommission für den Schutz personenbezogener Daten die Probleme und Trends bei der Vorratsspeicherung von Verkehrsdaten auf nationaler Ebene. Die Kommission ermittelte die folgenden Problembereiche:

- Die Rechtsgrundlagen, aufgrund derer ein Zugang zu Verkehrsdaten beantragt werden kann, entsprechen nicht den Stellen, die zum Einreichen solcher Anträge befugt sind. Ebenso wenig entsprechen sie den Behörden, die durch das Gesetz für elektronische Kommunikation zur Einholung von Referenzen befugt sind, sondern gehen weit darüber hinaus (der bulgarische Geheimdienst gehört zu den Behörden, die den Zugang beantragen dürfen, hat jedoch nicht die Befugnis, schwere Verbrechen aufzudecken und diesbezüglich zu ermitteln).
- Eine Klassifizierung der Anträge auf Zugang und die Anordnung des Gerichts führen dazu, dass Internetserviceanbieter ohne Register für klassifizierte Daten nicht in der Lage sind, Referenzen bereitzustellen;
- Anbieter elektronischer Kommunikationsnetzwerke bzw. -dienste äußern ihre Bedenken bezüglich der fehlenden Kontrollen zu Zugangsanträgen durch die Polizei zu Ermittlungszwecken sowie bezüglich der Tatsache, dass die Personenkategorie eine äußerst leichte Methode zum Erhalt von Referenzen zu Verkehrsdaten nutzt. Die Staatsanwaltschaft der Republik Bulgarien unterstützt einen Ansatz, laut dem ein Zugangsantrag im Rahmen von Ermittlungsverfahren von einer Ermittlungsbehörde mit ausdrücklicher schriftlicher Genehmigung eines beobachtenden Staatsanwalts gestellt werden muss.
- Es gibt einen Trend zur Reduzierung der Anzahl der Unternehmen, die ihren gesetzlichen Verpflichtungen zur Bereitstellung statistischer Daten nachgekommen sind (zum Vergleich: 2011 stellten 33 Unternehmen statistische Daten bereit, 2012 waren es 22 Unternehmen). Es ist jedoch ersichtlich, dass große Unternehmen dieser Branche genaue Daten bereitstellen, von denen die Trends größtenteils abgeleitet werden können und die außerdem eine solide Grundlage für statistische Analysen bieten.
- Trotz des Standpunkts der CPDP, dass die gesetzlich erforderliche Einreichung von Daten in „Fällen, in denen Daten den zuständigen Behörden bereitgestellt wurden“, die Bereitstellung einer spezifischen und detaillierten Statistik zu allen separaten Fällen umfasst, sind die Unternehmen nicht in der Lage, derartige Informationen bereitzustellen, und reichen lediglich zusammenfassende Daten zur Gesamtzahl der Zugangsanträge ein.
- Die Anzahl der Fälle, in denen die zuständigen Behörden um die Bereitstellung von Verkehrsdaten gebeten haben, hat sich beinah verdoppelt (zum Vergleich: 2011 wurden 39 781 Anträge auf Zugang zu gespeicherten Verkehrsdaten gestellt; 2012 waren es 75 672).
- Die Anzahl der Fälle, in denen den zuständigen Behörden gemäß dem Datenschutzgesetz Daten bereitgestellt wurden, hat sich beinah verdoppelt (zum Vergleich: 2011 wurden in 38 861 Fällen Daten bereitgestellt; 2012 waren es 74 296). Die Anzahl der Fälle, in denen die Anträge nicht bearbeitet werden konnten, ist ebenfalls gestiegen (zum Vergleich: 2011 waren es 920; 2012 waren es 1 376).
- Die statistischen Daten, welche die CPDP von den Unternehmen erhalten hat, sind zusammengefasst und basieren auf verschiedenen Kriterien und Parametern. Außerdem entsprechen die Daten nicht genau den Arten von Daten, welche die Europäische Kommission erwartet.

Um den Erwartungen der Europäischen Kommission gerecht zu werden und auf nationaler Ebene Maßnahmen zur Vereinheitlichung der Praxis zu ergreifen, hat die Kommission für den Schutz

personenbezogener Daten für die unter das Datenschutzgesetz fallenden Stellen verpflichtende Anweisungen herausgegeben.

Die verpflichtenden Anweisungen regulieren alle Parameter, die bei Gesprächen mit den an der Vorratsdatenspeicherung beteiligten Institutionen vereinbart wurden.

Die Anweisungen enthalten die Anforderungen an die Inhalte der Register, die von den Behörden gemäß Artikel 250 Absatz b des Datenschutzgesetzes, den Gerichten und den Anbietern öffentlich verfügbarer elektronischer Kommunikationsnetzwerke bzw. -dienste geführt werden, da explizit darauf hingewiesen wurde, dass diese Anforderungen die minimalen erforderlichen Inhalten darstellen. Alle betroffenen Personen können auch nach eigenem Ermessen die Eintragung zusätzlicher Informationen in die Register veranlassen. Es wird darauf hingewiesen, dass die Registrierung, Speicherung und Zerstörung von Dokumenten im Zusammenhang mit den Zugangsanträgen, Genehmigungen, Ablehnungen, Zugangsanweisungen und Referenzen nach internen Regelungen der Behörde gemäß Artikel 250(b) (1) des Datenschutzgesetzes, einem Gericht oder einem Unternehmen festgelegt werden, um mit offenen und klassifizierten Dokumenten unter Berücksichtigung der geltenden Gesetze zu arbeiten. Des Weiteren werden die Anforderungen für die Zerstörung gespeicherter Daten dargelegt.

DÄNEMARK

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	Dänische Datenschutzbehörde
Vorsitz und/oder Gremium	Für das Tagesgeschäft der Datenschutzbehörde ist das Sekretariat zuständig; die Leitung obliegt der jeweiligen Direktorin/dem jeweiligen Direktor. Fälle von grundsätzlichem Interesse (ungefähr 15 Fälle pro Jahr) werden dem Rat zur Entscheidung vorgelegt. Vorsitzende/Vorsitzender des Rates ist ein Richter/eine Richterin des Obersten Gerichtshofs.
Budget	21,1 Mio. DKK
Personal	Rund 35
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A. (in den folgenden Zahlen enthalten)
Meldungen	2 031
Vorabprüfungen	2 031
Anträge betroffener Personen	2 062 (Diese Zahl umfasst alle bei der dänischen Datenschutzbehörde eingegangenen Anfragen und Beschwerden)
Beschwerden betroffener Personen	Siehe oben
Vom Parlament bzw. der Regierung angeforderte Beratung	444
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	26 Fälle im Zusammenhang mit Sicherheitsfragen
Prüfmaßnahmen	
Prüfungen, Untersuchungen	58
Sanktionsmaßnahmen	
Sanktionen	Die dänische Datenschutzbehörde kritisiert jedes Jahr eine Reihe von Verantwortlichen für die Nichteinhaltung des Gesetzes über die Verarbeitung personenbezogener Daten.

Geldbußen	Bußgelder in sechs Fällen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A. (im dänischen Recht nicht vorgesehen)

B. Rechtsprechung

Live-Übertragung von Gottesdiensten

Eine Kirche in der Stadt Ribe kontaktierte die dänische Datenschutzbehörde mit einer Anfrage bezüglich der Einhaltung des dänischen Datenschutzgesetzes bei der Live-Übertragung eines Gottesdienstes. Der Zweck der Übertragung bestand darin, Menschen, die aus verschiedenen Gründen nicht am Gottesdienst teilnehmen konnten, die Möglichkeit zu geben, sich die Zeremonie anzusehen. Ein deutlich sichtbares Schild am Kircheneingang wies darauf hin, dass der Gottesdienst aufgezeichnet wurde.

Die dänische Datenschutzbehörde ging davon aus, dass in diesem Fall die Kirchengemeinde für die Verarbeitung der personenbezogenen Daten verantwortlich ist. Es war daher die Aufgabe der Gemeinde, die berechtigten Interessen der Übertragung und die Interessen der gefilmten Personen gegeneinander abzuwägen.

Diesbezüglich sei auch anzumerken, dass der Gottesdienst der Öffentlichkeit frei zugänglich war und es sich bei den Empfängern der Übertragung um eine spezifische, begrenzte Personengruppe handelte, wie z. B. die Bewohner eines Seniorenheims.

Die ursprüngliche Einschätzung der dänischen Datenschutzbehörde lautete, dass das dänische Datenschutzgesetz nicht die Übertragung bestimmter Gottesdienste verbietet, solange die Teilnehmer eindeutig darüber informiert werden und die Übertragung nur an bestimmten Standorten stattfindet. In einigen Situationen — wie z. B. bei Taufen — ist jedoch nach wie vor die schriftliche Einwilligung der Teilnehmer erforderlich.

C. Sonstige wichtige Informationen

Videoüberwachung durch Wohnungsbaugesellschaften

Im Jahr 2012 leitete die dänische Datenschutzbehörde eine Reihe von Prüfungen ein, die die Videoüberwachung durch private Wohnungsbaugesellschaften betrafen. Der Zweck des Projekts bestand darin, praktische Erfahrung in diesem speziellen Bereich zu sammeln und in Bezug auf den Datenschutz privater Unternehmen und natürlicher Personen zu sensibilisieren. Die häufigsten Probleme traten auf, wenn eine exzessive Datenspeicherung und Videoüberwachung in die Privatsphäre einiger Wohnungen eingriffen. Im Allgemeinen wurde jedoch das Privatleben und der Datenschutz angemessen respektiert.

Die im Rahmen des Projekts gesammelten Erfahrungen wurden in einem umfassenden Leitfaden zusammengefasst, der sowohl als Druckversion als auch online veröffentlicht wurde.

Internationaler Tag des Datenschutzes

Die dänische Datenschutzbehörde feierte den Internationalen Tag des Datenschutzes in den Räumen der Behörde und versuchte, die breite Öffentlichkeit zum Thema Datenschutz aufzuklären und zu informieren. Die Mitarbeiter veranstalteten Führungen durch die Räumlichkeiten, hielten Vorträge und organisierten eine offene Fragenrunde für die Teilnehmer. Der Tag war ein Erfolg sowohl für die Mitarbeiter als auch für die Besucher, die gute Kenntnisse zum Schutz personenbezogener Daten aufwiesen und großes Interesse an dem Thema zeigten.

Verbindliche unternehmensinterne Vorschriften

Dänemark erhielt eine erhebliche Anzahl von Anträgen für verbindliche unternehmensinterne Vorschriften (BCR). Dies bedeutet, dass Dänemark bei einigen Gelegenheiten die führende Behörde stellen wird.

Eine zunehmende Anzahl dänischer Unternehmen hat die Chancen des BCR-Modells erkannt, da das Modell mehr Flexibilität in Bezug auf die Übermittlung von Daten an Drittländer bietet, sobald die Regelungen vorbereitet und implementiert wurden. Da dieser Trend sich auch weiterhin fortsetzt, geht die dänische Datenschutzbehörde auch in Zukunft von steigenden Antragszahlen aus.

2012 agierte die dänische Datenschutzbehörde außerdem als „Co-Reader" im BCR-Prozess, bei dem die britische Datenschutzbehörde die federführende Behörde war.

DEUTSCHLAND

A. Zusammenfassung der Aktivitäten und Neuerungen:

Anmerkung: In Deutschland fungiert nicht nur der Bundesbeauftragte für Datenschutz und Informationsfreiheit als Datenschutzbehörde. Auf Länderebene gibt es ebenfalls Datenschutzbeauftragte sowie in Bayern eine separate Aufsichtsbehörde für den privaten Sektor.

Die folgende Tabelle bezieht sich lediglich auf das Amt des Bundesbeauftragten für Datenschutz und Informationsfreiheit.

Organisation	Bundesbeauftragter für Datenschutz und Informationsfreiheit
Vorsitz und/oder Gremium	Peter Schaar, Bundesbeauftragter
Budget	9 125 000 EUR
Personal	86 Datenschutz: 82; Informationsfreiheit: 4
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A.
Meldungen	k. A.
Vorabprüfungen	k. A.
Anträge betroffener Personen	8 173
Beschwerden betroffener Personen	4 568
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	k. A.
Sanktionsmaßnahmen	
Sanktionen	k. A.

Geldbußen	vgl. TB 2012 – k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

1) Bundesfinanzhof sieht Steueridentifikationsnummer als mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar an

Der Bundesfinanzhof hat die Steueridentifikationsnummer, die im Jahre 2008 eingeführt worden ist, als verfassungsgemäß eingestuft, da das Interesse der Allgemeinheit an einer gleichmäßigen Besteuerung den Eingriff in das Recht auf informationelle Selbstbestimmung rechtfertige (BFH, Urteil vom 18. Januar 2012, II R 49/10), wobei aber der strikte Grundsatz der Zweckbindung und die Erforderlichkeit beachtet werden müssten. Dem Gesetzgeber steht es daher nicht frei, den Einsatz der Steueridentifikationsnummer beliebig zu erweitern, da sich aus den datenschutzrechtlichen Anforderungen, die auch in § 139b Abs. 2 bis 5 Abgabenordnung bereichsspezifisch verankert sind, strikte Grenzen ergeben. Das Bundesverfassungsgericht hatte bislang noch keine Gelegenheit über die Verfassungsmäßigkeit der Steueridentifikationsnummer zu entscheiden, sodass eine endgültige Entscheidung noch aussteht.

2) Das Urteil des Bundesverfassungsgerichts zur Antiterrordatei (1 BvR1215/07 vom 24.04.2013) ist von grundsätzlicher Bedeutung. Es enthält u. a. folgende, zentrale Aussagen:

I. Der Europäische Gerichtshof ist nicht gesetzlicher Richter i.S. des Artikel 101 Abs. 1 GG für ausschließlich deutsche Grundrechte betreffende Fragen. Eine Anwendbarkeit der Unionsgrundrechte scheidet von vorneherein aus, wenn ein nationales Gesetz innerstaatlich bestimmte Ziele verfolgt, die das Funktionieren unionsrechtlich geordneter Rechtsbeziehungen nur mittelbar beeinflussen können. In diesen Fällen bedarf es keines Vorabentscheidungsverfahrens gemäß Artikel 267 AEUV zur Klärung der Reichweite des unionsrechtlichen Grundrechtsschutzes.

II. Aus dem Grundrecht auf informationelle Selbstbestimmung folgt ein informationelles Trennungsprinzip. Danach dürfen Daten zwischen Nachrichtendiensten und Polizeibehörden grundsätzlich nicht ausgetauscht werden. Einschränkungen sind nur ausnahmsweise zulässig. Der Austausch von Daten zwischen Nachrichtendiensten und Polizeibehörden für ein mögliches operatives Tätigwerden muss grundsätzlich einem herausragenden öffentlichen Interesse dienen, das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zur Verfügung stehen, rechtfertigt.

III. Die Erhebung und Verarbeitung von Kontaktpersonendaten ist nur unter sehr restriktiven Voraussetzungen zulässig – unabhängig davon, ob die Kontaktperson vom Handeln der ihr zugeordneten Hauptperson Kenntnis hat oder nicht.

IV. Interne Entscheidungs- bzw. Zuordnungskriterien muss die Exekutive – auch zur Kontrolle durch die Datenschutzbeauftragten – extensiv dokumentieren und offen legen.

V. Die aufsichtliche Kontrolle, u. a. durch die Datenschutzbeauftragten, ist von herausragender Bedeutung und flankiert die subjektivrechtliche Kontrolle durch die Gerichte objektivrechtlich. Ein rechtlich und/oder tatsächlich nicht hinreichend effizientes aufsichtliche Kontrollregime kann einen unverhältnismäßigen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung begründen. Wesentliche Voraussetzungen für eine effiziente Aufsicht sind u. a. mit wirksamen Befugnissen ausgestattete Aufsichtsinstanzen, die vollständige Protokollierung von Zugriffen und Änderungen des Datenbestandes

sowie dessen praktikable Auswertbarkeit, die durch technische und organisatorische Maßnahmen sicherzustellen ist.

VI. Den DS-Beauftragten ist es gestattet, zusammenzuarbeiten und sich z. B. im Wege der Amtshilfe durch Delegation oder Ermächtigung bei der Wahrnehmung ihrer Befugnisse gegenseitig zu unterstützen. Zudem ist das Zusammenspiel der verschiedenen Aufsichtsinstanzen – auch praktisch wirksam – sicherzustellen.

VII. Erforderlich für eine effiziente Aufsicht sind zudem gesetzlich turnusmäßig festgelegte Pflichtkontrollen, die spätestens etwa alle zwei Jahre durchgeführt werden müssen.

VIII. Der Gesetzgeber ist aufgerufen, auch bestehende Datenübermittlungsregelungen im Hinblick auf die Wahrung dieser Grundsätze zu prüfen und ggf. anzupassen.

3) Beschluss des Bundesverfassungsgerichts zur Speicherung und Verwendung von Telekommunikationsdaten

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 Artikel 10 Grundgesetz unterliegen. Der deutsche Gesetzgeber muss hierfür eine eindeutige Regelung schaffen, die den Schutz der äußerst sensiblen Telekommunikationsverkehrsdaten gewährleistet."

C. Sonstige wichtige Informationen

FATCA

Der Foreign Account Tax Compliance Act (FATCA) ist ein im März 2010 in Kraft getretenes US-Gesetz zur Erfassung von Vermögenswerten von in den USA steuerpflichtigen Personen und Gesellschaften auf Konten im (US-)Ausland. Kern von FATCA sind erweiterte Melde- und Berichtspflichten von Banken und sonstigen Finanzinstituten im Ausland (Foreign Financial Institutions — FFIs) gegenüber der amerikanischen Steuerbehörde (Internal Revenue Service — IRS). Bei Nichtbefolgen der Melde- und Berichtspflichten drohen erhebliche Quellensteuerabzüge.

Der Umgang mit FATCA warf erhebliche datenschutzrechtliche Probleme auf. So stellte sich die Frage, ob für die Datenübermittlungen an die US-Steuerbehörde auf die gesetzliche Grundlage der §§ 4b und 4c Bundesdatenschutzgesetz (BDSG) oder allein auf die Einwilligung abzustellen ist. Zur Lösung haben sich Frankreich, Italien, Spanien, Vereinigtes Königreich und Deutschland auf ein Musterabkommen mit den USA verständigt, das als Grundlage für bilaterale Abkommen dienen soll.

Das Musterabkommen wurde am 26. Juli 2012 vorgestellt. Dabei verpflichten sich die fünf Staaten, von den in ihrem Gebiet ansässigen Finanzinstituten die Informationen über für US-Kunden geführte Konten zu erheben und der US-Behörde zur Verfügung zu stellen. Im Gegenzug verpflichten sich die USA, alle Finanzinstitute des jeweiligen Vertragspartners von der Pflicht auszunehmen, mit der US-Steuerbehörde

Vereinbarungen abzuschließen. Dieses Musterabkommen schafft einen Rahmen für die Meldung von Kontodaten durch die Finanzinstitute an ihre jeweiligen nationalen Steuerbehörden mit anschließendem Austausch der betreffenden Daten im Rahmen der bestehenden bilateralen Doppelbesteuerungsabkommen.

Das FATCA-Abkommen (Abkommen zur Förderung der Steuerehrlichkeit bei internationalen Sachverhalten und hinsichtlich der als Gesetz über die Steuerehrlichkeit bezüglich Auslandskonten bekannten US-amerikanischen Informations- und Meldebestimmungen) zwischen den USA und Deutschland ist am 31. Mai 2013 von Vertretern der Bundesrepublik Deutschland und den USA unterzeichnet worden und wurde durch Parlamentsgesetz ratifiziert. Es basiert im Wesentlichen auf dem oben genannten Musterabkommen vom 26. Juli 2012.

Während der Verhandlungen hat sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) für die datenschutzrechtlichen Kernforderungen eingesetzt. Dabei ging es insbesondere um die Schaffung einer datenschutzrechtlichen Erlaubnisnorm für die Finanzinstitute, die Festschreibung des Verwendungszwecks der übermittelten personenbezogenen Daten und die Normierung verfahrensrechtlicher und organisatorischer Schutzvorkehrungen.

Entgegen den Forderungen des BfDI werden aber die verfahrensrechtlichen Sicherungen sowie die technischen und organisatorischen Maßnahmen zur Datensicherheit in einer bloßen Durchführungsvereinbarung zum Abkommen geregelt.

Das FATCA-Abkommen sieht nunmehr einen Verwendungsvorbehalt sowie die Zusicherung der Vertraulichkeit für die zu nutzenden Daten vor. Ferner hat sich der BfDI dafür eingesetzt, dass durch die Einfügung eines geplanten § 117c Abgabenordnung (AO) eine Erlaubnisnorm für die zur Übermittlung verpflichteten Finanzinstitute geschaffen wird, die Begrenzungen der Datenverarbeitung nach Maßgabe des Zweckbindungs- und Erforderlichkeitsgrundsatzes vorsieht. Für die deutschen Finanzinstitute liegt damit eine Ermächtigungsgrundlage für die Datenübermittlung vor.

Die Pflichten der Finanzinstitute sollen durch eine Rechtsverordnung auf Grundlage des § 117c Abgabenordnung präzisiert werden.

ESTLAND

A: Zusammenfassung der Aktivitäten und Neuerungen:

Die wichtigste Aufgabe der Datenschutzbehörde besteht darin, dafür zu sorgen, dass:

- das Recht einer natürlichen Person auf Datenschutz gewahrt wird, wenn personenbezogene Daten verarbeitet werden;
- öffentliche Informationen zugänglich sind.

Die Datenschutzbehörde ist demnach die Durchführungsstelle und unabhängige Aufsichtsbehörde des Datenschutzgesetzes und des Gesetzes über die Information der Öffentlichkeit.

Darüber hinaus hat der Gesetzgeber der Datenschutzbehörde verschiedene weitere Aufgaben übertragen. Uns wurden außerdem Aufgaben im Zusammenhang mit der internationalen Gesetzgebung übertragen ([2]).

Als Schutzinstitution der informationsbezogenen Grundrechte agiert die Datenschutzbehörde als unabhängige Kommission, die Beschwerden nachgeht und aus Eigeninitiative in Gesetzesverstoßsachen ermittelt. Die Anzahl der Anfragen und Fälle von Überwachungen hat sich in den letzten Jahren stabilisiert:

	2012	2011	2010
Eingegangene Mitteilungen und Klärungs-/Auskunftsersuchen	877	940	893
Hotline-Anrufe	1202	816	1061
Eingeleitete Aufsichtsverfahren[2]	595	481	588
Ordnungswidrigkeitsverfahren (abgeschlossen)	43	34	35

Die Nutzung personenbezogener Daten ist bei Anfragen und Verfahren ein häufiges Thema:

a) bei Beschäftigungsverhältnissen (z. B. Überwachung von Mitarbeitern, Eignung einer Einwilligung oder eines Vertrags für eine Datenverarbeitung, weitere Nutzung einer E-Mail-Adresse im Namen eines ehemaligen Mitarbeiters);

b) Offenlegung des Schuldenstandes (vorwiegend die Offenlegung ohne das Filtern nach berechtigten Interessen, Offenlegung der Mitglieder von Verwaltungsstellen verschuldeter juristischer Personen);

c) in sozialen und Online-Medien (hierbei kann es sich um den Antrag einer Person handeln, ihren Namen aus Internet-Suchmaschinen löschen zu lassen, dies betrifft meist soziale Medien);

d) elektronisches Direktmarketing (unerwünschte Werbung per E-Mail oder SMS).

([2]) Der Gesetzgeber hat der Datenschutzbehörde zusätzliche Aufgaben in Bezug auf die folgenden Gesetze übertragen: das **Gesetz über elektronische Kommunikation** (Überwachung von elektronischem Direktmarketing, und zwar auch dann, wenn es sich nicht um personenbezogene Daten handelt; Bearbeitung von Verstoßmeldungen von Kommunikationsunternehmen, während erlaubt wird, dass die betroffenen Personen nicht informiert werden; einzelne Ordnungswidrigkeiten), das **Gesetz über amtliche Statistiken** (Beteiligung an der Arbeit des Statistikamtes, einzelne Ordnungswidrigkeiten), das **Gesetz zur Umsetzung der Verordnung (EU) 211/2011 des Europäischen Parlaments und des Rates über die Bürgerinitiative** (Zertifizierung der Einhaltung von Vorschriften in Bezug auf Online-Sammelsysteme für Unterstützungsbekundungen), das **Signaturgesetz** (Aussetzung der Nutzung von Zertifikaten im Verdachtsfall), das **Gesetz über die Erforschung menschlicher Gene** (Genehmigung der Methode zur Datenverschlüsselung), das **Einwohnermeldegesetz** (Abgabe einer Stellungnahme zur Ernennung des zugelassenen Verarbeiters des Registers, Genehmigung des Vertrages zur Pflege des Registers, Genehmigung von Verträgen für außergewöhnliche Datenverarbeitungen) sowie das **Gesetz über die Registrierung von Umwelteinflüssen** (Abgabe einer Stellungnahme zur Ernennung eines autorisierten Verarbeiters des Registers, Genehmigung der übergreifenden Nutzung personenbezogener Daten). Einige Aufgaben ergeben sich **direkt aus der internationalen Gesetzgebung**, vor allem, was die Teilnahme an der gemeinsamen Überwachung grenzüberschreitender Informationssysteme (wie z. B. das Schengener Informationssystem, das Europol-Informationssystem, das europäische Visa-Informationssystem, das Zollinformationssystem und das Eurodac-Fingerabdrucksregister) betrifft.

Die Nutzung von Kameras zur Überwachung von Personen und auch die Veröffentlichung von Aufzeichnungen in sozialen Medien, Unternehmen und Bildungsstätten gibt immer häufiger Anlass zu Bedenken.

Auf rechtlicher Ebene liegt der Schwerpunkt von Fragen und Streitigkeiten in der Regel auf der Rechtsgrundlage der Datenverarbeitung. Dabei stellt sich häufig die Frage, ob eine Einwilligung zur Datenverarbeitung eingeholt wurde und ob ein Vertrag oder ein Rechtsakt die Rechtsgrundlage für eine Verarbeitung ohne Einwilligung gewesen sein könnte.

Es gab weniger Fälle bezüglich der Information der Öffentlichkeit: 10 % betrafen Anfragen auf Klärung, 18 % waren Anrufe der Informations-Hotline und ein Viertel waren Beschwerden.

Im Bereich der Information der Öffentlichkeit ist die Einrichtung von Zugangsbeschränkungen nach wie vor das häufigste Thema. Solche Beschränkungen können sowohl übertrieben als auch unangemessen sein (Zugang zu Dokumenten über Online-Dokumentenregister, die gegen den Datenschutz verstoßen).

Die kompliziertesten Rechtsstreitigkeiten ergeben sich jedoch aus der Frage, ob eine Person nach dem Privatrecht öffentliche Aufgaben wahrnimmt und demnach ebenfalls ein Besitzer öffentlicher Informationen ist.

Der Missbrauch des Bevölkerungsregisters war der häufigste Grund für Ordnungswidrigkeitsverfahren (30 von 43 abgeschlossenen Verfahren). Der Missbrauch der Polizeidatenbank hat abgenommen (4 Ordnungswidrigkeitsverfahren).

Unser Hauptziel liegt darin, den Verstößen ein Ende zu bereiten, und nicht in der Bestrafung. Ein Großteil der Verstöße endet sofort mit dem Beginn der Überwachung oder mit dem Erhalt einer Empfehlung/eines Vorschlags. Im Jahr 2012 wurden in nur 48 Fällen Vorschriften erlassen ([3]). In 39 Fällen verhängten wir Geldbußen und Zwangsgelder.

Organisation	Estnische Datenschutzbehörde
Vorsitz und/oder Gremium	Generaldirektor
Budget	595 403 EUR
Personal	18
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	582
Meldungen	608 Registrierungen von Verarbeitungen sensibler personenbezogener Daten
Vorabprüfungen	23
Anträge betroffener Personen	877
Beschwerden betroffener	404

([3]) Diese Zahl enthält keine standardmäßigen Vorschriften für eine verpflichtende Registrierung der Verarbeitung personenbezogener Daten durch für die Datenverarbeitung Verantwortliche — hiervon gab es 2012 130 Fälle.

Personen	
Vom Parlament bzw. der Regierung angeforderte Beratung	21
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten: Stellungnahmen zu Informationssystemen des öffentlichen Sektors	84
Prüfmaßnahmen	
Prüfungen, Untersuchungen	457
Sanktionsmaßnahmen	
Sanktionen	40 Fälle
Geldbußen	5 918 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	137

B. Rechtsprechung

Die Anzahl der Verfahren im Zusammenhang mit dem Missbrauch von Gesundheitsdaten hat 2012 zugenommen. Die Ursache dafür ist eindeutig der Aufbau der Zusammenarbeit mit dem Gesundheitsamt und der e-Health-Stiftung. Wir tauschen Informationen bezüglich eines möglichen Missbrauchs aus. Zwei Prüfungen im Gesundheitswesen haben ergeben, dass die Maßnahmen für den Schutz personenbezogener Daten im Gesundheitsministerium und bei der Krankenkasse den Anforderungen genügen.

Im Bereich der Überwachung der Datenbankpflege wurden bei der Kommunalverwaltung des Kreises Viljandi, beim Rettungsdienst und bei der Stadtverwaltung Narva ebenfalls die Vorkehrungen zum Schutz personenbezogener Daten geprüft. Die Überwachung der letzten beiden Institutionen wird aufgrund der identifizierten Versäumnisse fortgesetzt.

Im Interesse einer rechtmäßigen Datenverarbeitung wurden die Protokolle des Registers der Eigenbeschränkung von Spielern (durch die estnische Steuer- und Zollbehörde; die Versäumnisse wurden beseitigt und die Überwachung beendet), die Gehaltsabrechnungssoftware staatlicher Behörden (durch das Finanzministerium; Folgeprüfungen werden 2013 fortgesetzt) und die Datenbank des estnischen Verkehrsrechtsschutzversicherungsfonds (Folgeprüfungen werden 2013 fortgesetzt) überprüft.

Eine Konzertierung anhand der detaillierten, in das Verwaltungssystem des staatlichen Informationssystems hochgeladenen Beschreibungen hilft ebenfalls bei der Identifizierung von Problemen im Bereich der Datenbankpflege. Die Datenschutzbehörde ist eine der Koordinierungsstellen, die die Einhaltung der Anforderungen an den Schutz personenbezogener Daten und an öffentliche Informationen überwacht. Die Anzahl der Konzertierungsverfahren belief sich 2012 auf 84 (einschließlich 16 Ablehnungen) und 2011 auf 81.

Eine im November 2012 durchgeführte vergleichende Überwachung der Offenlegung von Schuldendaten natürlicher Personen betraf die Websites von 66 Inkassounternehmen. Zwölf von ihnen hatten den Namen und oftmals auch das Geburtsdatum oder den persönlichen Identifikationscode privater Personen auf öffentlich zugänglichen Websites veröffentlicht. Sieben dieser Unternehmen beendeten die Verstöße freiwillig, fünf davon erst nach dem Erlassen von Vorschriften.

C. Sonstige wichtige Informationen

Die Überprüfung von Klärungsersuchen und Beschwerden ist eine Reaktion, die auf Einzelpersonen und individuelle Fragen abzielt. Es geht im Grunde darum, sich mit einzelnen Bäumen auseinanderzusetzen, anstatt mit dem ganzen Wald.

Wir müssen die wenigen Ressourcen nutzen, die wir noch haben, nachdem wir so effizient wie möglich auf Probleme reagiert haben, und zwar für die Prävention von Problemen, die Bereitstellung von Informationen, das Erstellen von Leitfäden, die Bereitstellung von Beratungsdiensten für wichtige Initiativen und den Aufbau von Partnerschaften.

Die Vorbereitung der Öffnung des Strommarktes ist ein Beispiel für eine Präventionsmaßnahme: Die Datenschutzbehörde war ein Jahr lang im Lenkungsausschuss der Datenbank des Strommarktes als Berater im Hinblick auf Fragen beim Schutz personenbezogener Kundendaten aktiv. In diesem Bereich kam es später nur zu einem Zwischenfall ([4]).

Beim Datenschutz war 2012 unsere oberste Priorität der Schutz personenbezogener Daten Minderjähriger. Unsere jährliche Konferenz, die am 27. Januar stattfand, stand demnach ganz im Zeichen dieses Themas. Die Leitlinien des Justizministers zur Informierung hilfsbedürftiger Kinder wurden auf der Konferenz ebenfalls vorgestellt. Wir beteiligten uns am Gemeinschaftsprojekt *Targalt Internetis* (Intelligent im Internet) unter der Leitung der estnischen Union für das Kindeswohl – alleine wären wir nicht in der Lage gewesen, ein derart großes Publikum zu erreichen. Das Online-Game *Päästa Liisa ID* (Rette Liisas ID) richteten wir auf Jugendliche aus. Wir informierten weiterhin über das Nutzerkonto des Spiels, das in sozialen Medien eröffnet wurde. Auf dem Seminar der Estonian Atlantic Treaty Association sprachen wir am 26. Oktober mit Sozialkundelehrern.

Im Rahmen der Zusammenarbeit mit der Arbeitsaufsichtsbehörde arbeiteten wir 2012 weiter an den 2011 verfassten Leitlinien zum Schutz personenbezogener Daten in Beschäftigungsverhältnissen. Wir nahmen an den vier regionalen Vorlesungsreihen der Arbeitsaufsichtsbehörde teil und erklärten Arbeitgebern, Fachkräften aus dem Personalwesen und Gewerkschaften das Thema personenbezogener Mitarbeiterdaten. Darüber hinaus veröffentlichte die Arbeitsaufsichtsbehörde unsere Leitlinien sowohl in estnischer als auch in russischer Sprache. Wir sind unseren Kollegen von der Arbeitsaufsichtsbehörde für diese großartige Zusammenarbeit sehr dankbar.

Estland ist seit 2007 Mitglied der Schengener Konvention. Der Wegfall der Grenzkontrollen an Binnengrenzen wird durch den Informationsaustausch zwischen den Strafverfolgungsbehörden der Mitgliedstaaten durch das Schengener Informationssystem und das Visa-Informationssystem kompensiert. Das Missbrauchsrisiko des Informationssystems wird durch strenge Datenschutzvorschriften verwaltet. Alle fünf Jahre beurteilen sich alle Mitgliedstaaten gegenseitig und überprüfen, ob die Aktivitäten ihrer Behörden gemäß den Anforderungen der Schengener Konvention erfolgen. Beurteilungskomitees bestehend aus Vertretern der Datenschutzbehörden prüfen die Einhaltung der Datenschutzvorschriften. Hierzu gehören die Beurteilung des Tagesgeschäfts und die Überwachung durch Polizei, Grenzschutz und Konsulate auf dem Gebiet des Datenschutzes sowie der allgemeinen Befugnisse und der Unabhängigkeit der Datenschutzbehörden.

Die Datenschutzbehörde nahm 2011 und 2012 an der Beurteilung von sechs ausländischen Behörden teil. Die baltischen Staaten wurden im Oktober 2012 beurteilt. Estland benötigte 2007 eine Folgebeurteilung

([4]) Der Stromanbieter 220 Energia OÜ ermöglichte den Zugang zu Verbraucherdaten anhand eines persönlichen Identifikationscodes. Es gab einen Missbrauchsversuch, der jedoch sofort aufgedeckt werden konnte, woraufhin der Zugang nur noch mit ID-Karten möglich war.

auf dem Gebiet des Datenschutzes, doch dieses Mal bestanden wir die Beurteilung ohne jegliche Beanstandungen.

Das Beurteilungskomitee befand unsere Online-Schengeninformationen (gründliche und harmonisierte Informationen in drei Sprache auf den Websites der Datenschutzbehörde und Partnerbehörden), die regelmäßige Zusammenarbeit zwischen estnischen Behörden und grenzüberschreitende Aktivitäten der baltischen Datenschutzbehörden für beispielhaft.

Wir möchten an dieser Stelle die Beiträge unserer Kollegen von Polizei und Grenzschutz, dem Innen- und Außenministerium sowie dem Entwicklungszentrum für Informationstechnologie des Innenministeriums würdigen, die das positive Ergebnis der Beurteilung ermöglicht haben.

Im Bereich elektronisches Direktmarketing wurden am 22. Februar 2012 detaillierte Leitlinien für Absender und Empfänger von Online-Werbung fertiggestellt. Der Entwurf dieser Leitlinien wurde im beratenden Ausschuss der Datenschutzbehörde sowie mit Unternehmen und dem Amt für Verbraucherschutz besprochen. Die Leitlinien wurden am 15. März 2012 in der Wirtschaftszeitschrift *Äripäev* veröffentlicht. Darüber hinaus beziehen wir uns bei Verfahren und in unserer Korrespondenz laufend auf diese Leitlinien.

Im Bereich Forschung und Statistik bezogen sich unsere Aktivitäten hauptsächlich auf Genehmigungen wissenschaftlicher Forschungen. Im Jahr 2012 erteilten wir 13 Genehmigungen und drei Absagen. Außerdem führten wir in Forschungsinstituten, denen wir Genehmigungen erteilt hatten, zufällige Datenschutzprüfungen durch. 2012 überprüften wir das Institut für Demographie der Universität Tallinn und stellten dabei keinerlei Versäumnisse fest.

Außerdem beaufsichtigten wir in den ersten drei Monaten des Jahres 2012 die Volks- und Wohnungszählung. Unsere Kollegen der estnischen Aufsichtsbehörde für Informationssysteme standen uns dabei beratend zur Seite. Die bei der Online-Zählung ermittelten geringfügigen Versäumnisse wurden vom estnische Statistikamt schnell ausgemerzt. Größere Probleme wurden nicht festgestellt. Nach unserem Wissen erreichte die Beteiligung an der estnischen Online-Volkszählung einen Weltrekord: 62 % aller gezählten Personen.

Im Rahmen der internationalen Zusammenarbeit war die Datenschutzbehörde in zahlreichen Arbeitsgruppen aktiv.

Die Zusammenarbeit zwischen den baltischen Datenschutzbehörden war in praktischer Hinsicht erfolgreich – unsere litauischen Kollegen traten 2012 der Partnerschaft zwischen estnischen und lettischen Behörden bei. Wir führten in allen Hotels der Marke Radisson Blue eine gemeinsame Prüfung durch. Die Prüfung betraf die Verarbeitung personenbezogener Kunden- und Mitarbeiterdaten.

Wir werden die gemeinsamen Aufsichtsaktivitäten auch 2013 fortsetzen und uns dabei auf die Glücksspielbranche konzentrieren.

Das wichtigste internationale Thema war der Reformplan für Datenschutz der Europäischen Union. Die am 23. März 2012 verabschiedete Stellungnahme der europäischen Datenschutzbehörden fiel im Großen und Ganzen positiv aus, enthielt jedoch auch eine Reihe von Beobachtungen und Kritikpunkten. Die Stellungnahme wurde nicht einstimmig verabschiedet, da viele Datenschutzbehörden sie aus verschiedenen Gründen nicht unterstützten.

Im Zusammenhang mit dem Reformplan für Datenschutz der Europäischen Union wurde außerdem die Aktualisierung übergreifender internationaler Dokumente diskutiert. Die Datenschutzbehörde gehört dem beratenden Ausschuss des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten an. Die Verhandlungen der Sachverständigen bezüglich der Änderung des Übereinkommens von 1981 wurden 2012 abgeschlossen.

Des Weiteren vertraten wir Estland in der Arbeitsgruppe für Datensicherheit und Datenschutz der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) zusammen mit dem Ministerium für Wirtschaft und Kommunikation. Die Arbeitsgruppe diskutiert die am zentralen Datenschutzdokument

der OECD, der Leitlinien für den Datenschutz und den grenzüberschreitenden Verkehr personenbezogener Daten, vorzunehmenden Änderungen. Die Diskussion dauert an.

FINNLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Vorschlag der Kommission enthält zum Beispiel einen Vorschlag für ein sogenanntes Kohärenzverfahren, also einen Rechtsakt, der – wie die gesamte Reform – auf eine bessere Harmonisierung des Datenschutzes und die Schaffung eines genuinen EU-Binnenmarktes für digitale Inhalte abzielt. Bei solchen grenzüberschreitenden Datenschutzfragen würde die Entscheidungsfindung in einer neu einzurichtenden EU-Datenschutzbehörde erfolgen. Da jedoch ein Großteil dieser grenzüberschreitenden Angelegenheiten bereits „regionale" nordische Angelegenheiten zu sein scheinen, haben wir die Anwendung des Instruments mit unseren nordischen Kollegen bereits erproben können.

Im November 2011 wurde Finnland von Hackerangriffen heimgesucht. Haben wir irgendetwas aus diesen Sicherheitsverstößen gelernt? Wir haben während des Berichtszeitraums versucht, eine Antwort auf diese Frage zu finden, indem wir mit den Parteien, die von den Hackern angegriffen wurden, eine umfangreiche Befragung durchführten. Wir wollten herausfinden, welche Probleme zu den Sicherheitsverstößen geführt haben und welche Maßnahmen die Organisationen ergriffen haben, um die Situation zu berichtigen. Das Endergebnis der Befragung war relativ düster: Ein Großteil der Befragten zog sich infolge der Sicherheitsverletzung aus dem digitalen Markt zurück. Eine sehr häufige Reaktion bestand darin, dass die für die Verarbeitung Verantwortlichen nichts taten!

Im Rahmen der Vorbereitung der besagten Studie organisierten wir zum 25. Jubiläum unseres Amtes einen umfangreichen Workshop zum Thema Datensicherheit. Während des Workshops wurden den Teilnehmern – darunter führende Köpfe der Branche – zwei Fragen gestellt: Besteht in Finnland der Bedarf an einer verbesserten Datensicherheit, und falls ja, stehen die dafür nötigen Kompetenzen zur Verfügung? Leider lautete die Antwort der Teilnehmer auf die erste Frage ja und auf die zweite Frage nein. Vielleicht unterstützt der von uns veröffentlichte Leitfaden für Kontodaten Unternehmen bei der Nutzung moderner Buchführungsanwendungen.

Neben dem bereits erwähnten Workshop wurden im Berichtszeitraum Workshops für Telefonauskunfteien, soziale Medien (zur Frage, ob es in sozialen Medien „graue Bereiche" gibt, die Behörden nicht kontrollieren können), freiwillige betriebliche Kontrolle und Datenschutz für Unternehmer organisiert. Das Jubiläumsjahr endete mit einem Seminar mit dem Titel *KnowRight2012*, das in Finnland stattfand und von uns mitorganisiert wurde.

Da der Europarat den Entwurf einer Empfehlung zum Thema Profiling erstellte, veröffentlichten wir eine Sektorstudie zu regulären Kundensystemen, die im Laufe des Jahres durchgeführt wurde ([5]). Wir fanden heraus, dass die rechtliche Qualität regulärer Kundensysteme bis zu einem gewissen Maße variiert. Einige der Befragten konnten nicht sagen, weshalb sie ein reguläres Kundensystem nutzen.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Reijo Aarnio ist seit dem 1. November 1997 der Datenschutzbeauftragte.
Budget	Das Jahresbudget liegt bei 1 737 000 EUR.
Personal	Insgesamt 20 Mitarbeiter.
Allgemeine Aktivitäten	

([5]) Sektorstudien sind ein Hilfsmittel, das wir entwickelt haben, um Prüfaktivitäten mithilfe von Technologie so effizient wie möglich durchzuführen.

Beschlüsse, Stellungnahmen, Empfehlungen	2 946
Meldungen	427
Vorabprüfungen	siehe Meldungen
Anträge betroffener Personen	986
Beschwerden betroffener Personen	(Zugang und Korrekturen) 180
Vom Parlament bzw. der Regierung angeforderte Beratung	122
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Zusammenarbeit mit für die Datenverarbeitung Verantwortlichen in den folgenden Sektoren: Bildung, Gesundheitswesen, Soziales, Telekommunikation, Beschäftigung und Wirtschaft, Marketing
Prüfmaßnahmen	
Prüfungen, Untersuchungen	102
Sanktionsmaßnahmen	97
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	> 1 000

B. Rechtsprechung

Auf Anfrage des Datenschutzbeauftragten kommentierte die Datenschutzbehörde das starke Identifikationssystem, das in einigen Buchungssystemen erforderlich ist. Die Rechtssache bezog sich auf die rechtliche Qualität des Online-Dienstes einer Optikerkette, über das Kunden mithilfe ihres Namens und ihrer Sozialversicherungsnummer Termine buchen und weitere Aufgaben erledigen konnten. Die Datenschutzbehörde stimmte der Stellungnahme des Datenschutzbeauftragten zu, laut derer das betreffende System nicht sicher genug sei und Sozialversicherungsnummern dafür verwendet würden, um Personen in Datenbanken voneinander zu unterscheiden. Der für die Datenverarbeitung Verantwortliche hat damit begonnen, das System zu reparieren.

Auf Anfrage des Datenschutzbeauftragten untersuchte die Datenschutzbehörde als wichtige Grundsatzentscheidung die Videoüberwachung in den Treppenhäusern von Wohngebäuden. Die Rechtssache bezog sich u. a. auf die Verbindung zwischen dem Gesetz zum Schutz personenbezogener Daten und dem finnischen Strafgesetzbuch. Die Datenschutzbehörde kam in ihrer Stellungnahme zu dem Schluss, dass eine Videoüberwachung gemäß dem Gesetz zum Schutz personenbezogener Daten auch in diesen Einrichtungen möglich ist.

C. Sonstige wichtige Informationen

Das Ministerium für Verkehr und Kommunikation gab zum Teil aufgrund des Mangels an umfassender rechtlicher Praxis beim Professor für Erbschaftsrecht Urpo Kangas von der Universität Helsinki eine Studie zum Rechtsstatus digitaler Nachlässe in Auftrag. Eine der Schlussfolgerungen des Berichts lautete, dass spezifischere Rechtsvorschriften erforderlich seien.

Der Datenschutzbeauftragte assistierte dem Amt für Verbraucherschutz bei der Festlegung von Strategien zur rechtlichen Beschaffung von Dienstleistungen auf Grundlage von geografischen Informationen, die durch Werbeeinnahmen finanziert werden. In diesem Fall lag die Schlüsselfrage in der Verbindung zwischen vertraglichen Vereinbarungen und einer Einwilligung.

Viele interessante Entwicklungen

Ein während des Berichtszeitraums fortlaufendes Gesetzgebungsprojekt war die Erstellung eines „Informationsgesellschaftscodes". Die Datenschutzbehörde beteiligte sich außerdem, wann immer möglich, an der Arbeit des Lenkungsausschusses und bestimmter Untergruppen. Meiner Meinung nach finden Akteure der digitalen Wirtschaft und der Dienstleistungsproduktion nur schwer eine Rechtsgrundlage zur Orientierung für ihre betrieblichen Abläufe, was hauptsächlich auf die fragmentierte Rechtslage zurückzuführen ist ([6]). Dies ist einer der Gründe für die Unsicherheiten der Akteure in diesem Sektor, was wiederum die Entwicklung beeinträchtigen kann.

Eine wichtige Reform, der nur wenig Aufmerksamkeit zukam, war die Umsetzung der Steuernummern für Beschäftigte. In Finnland erhält jede Person eine Sozialversicherungsnummer (HETU), die ins Bevölkerungsregister eingetragen wird, sowie eine elektronische Identifikationsnummer, die beim Umgang mit den Behörden verwendet wird (SATU). Außerdem hat die Steuerverwaltung nun eine Steuernummer für alle Beschäftigten eingeführt, um damit dem grauen Markt entgegenzuwirken. Zumindest in dieser Hinsicht scheint die öffentliche Verwaltung die Risiken, die mit dem Identitätsmanagement einhergehen, angemessen zu verwalten. Andererseits kommt der Ausbau der mobilen Dienstleistungen auf der Grundlage von SATU nur schwer ins Rollen.

Ein weiterer Fortschritt in der öffentlichen Verwaltung ist die Entwicklung, die durch das 2011 in Kraft getretene Gesetz zur Verwaltung öffentlicher Daten reguliert wird: Die Kontrolle der Nutzung von Informationstechnologie wurde weiter zugunsten der Entscheidungsträger staatlicher Unternehmen zentralisiert. Einer der Vorschläge, die im Laufe des Jahres unterbreitet wurden, war die Gründung eines staatlichen IT-Dienstleistungsunternehmens. Die staatliche Prüfung auf Grundlage der Datenschutzverordnung scheint gut begonnen zu haben.

Datenbilanz

Die Datenschutzbehörde hat am 24. April 2012 einen Leitfaden mit dem Titel „Erstellung einer Datenbilanz" veröffentlicht. Die Datenbilanz ist ein Wissensmanagement-Bericht, der auf einer internen Prüfung basiert und Unternehmen dabei unterstützt, ihre Datenverarbeitungsprozesse zu beurteilen. Des Weiteren kann er dazu verwendet werden, den Interessenvertretern der Organisation wichtige Punkte zur Datenverarbeitung vermitteln. Die Datenbilanz wurde als dynamisches Hilfsmittel konzipiert, das die Effizienz, den Einfluss und die Wettbewerbsfähigkeit der Organisation unterstützt.

Obwohl die Datenbilanz die gesetzlich vorgeschriebene Berichterstattung auf der Grundlage von Vermögensbilanzen und Jahresberichten ergänzen kann, ist es nicht ihr Zweck, den Verwaltungsaufwand der Organisation übermäßig zu erhöhen. Die Datenbilanz steht außerdem mit dem Grundsatz der Rechenschaftspflicht in Einklang, laut dem ein Unternehmen selbst die Einhaltung der Gesetze und bewährte Verfahrensweisen bei der Daten- und Informationsverarbeitung nachweist. Datenschutzgesetze

([6]) Ein Beispiel hierfür ist eine Regierungsvorlage für eine regulierte Nutzung biometrischer Daten im Strahlungssicherheitsgesetz, der vom Parlament behandelt wurde. Es gibt kein spezifisches finnisches Gesetz zu biometrischen Daten.

werden in Zukunft möglicherweise die Einführung von Verfahren erfordern, die dem Grundsatz der Rechenschaftspflicht genügen.

Der Leitfaden soll keine erschöpfende Formel oder Liste der Informationen darstellen, die in die Datenbilanz aufgenommen werden sollen. Ihre Inhalte können je nach Sektor, in dem die Organisation tätig ist, und nach der Art seiner Tätigkeit variieren. Daher ist es ratsam, die Datenbilanz nur in dem Maß einzuführen, in der sie der Organisation einen Mehrwert verschafft.

Die Datenschutzbehörde war an der Kontrolle der oben genannten Angelegenheiten sowie an der Kontrolle wissenschaftlicher Forschung, der Überwachung von DNS-Probenahmen, Angelegenheiten im Hinblick auf intelligente Verkehrssysteme und Straßenbenutzungsgebühren, der Kommunikation zu bedrohlichen Datenlecks von Smartphones, der Reform des Gesetzes über die Verarbeitung personenbezogener Daten durch die Polizei, der Arbeit des Ausschusses für Menschenrechte und vielen weiteren Projekten beteiligt. Neben diesem arbeitsintensiven Tagesgeschäft – von denen weitere Informationen in anderen Abschnitten dieses Jahresberichts zu finden sind – müssen wir unsere Probleme aus einer breiteren Perspektive betrachten. Ein Teil dieser breiteren Perspektive ist auf die derzeit andauernde, weitreichende europäische und nordische Zusammenarbeit zurückzuführen ([7]). Ein weiterer Teil beruht auf der Teilnahme an NETSO, einem von der finnischen Akademie finanzierten Projekt unter der Leitung von Professor Ahti Saarenpää, das die Entwicklung der Informationsgesellschaft horizontal untersucht.

([7]) Im Rahmen der nordischen Zusammenarbeit haben wir mit unseren norwegischen Kollegen eine umfassende Überprüfung von Facebook durchgeführt. Die Überprüfung begann 2011.

FRANKREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2012 war geprägt von erhöhten Aktivitäten und zahlreichen Initiativen der französischen Datenschutzbehörde CNIL zur Unterstützung von öffentlichen wie privaten Interessenvertretern bei der Einhaltung der Datenschutzvorschriften.

Der Vorschlag einer Datenschutzreform: eine große Herausforderung für Frankreich

Am 25. Januar 2012 schlug die Europäische Kommission mit einem Vorschlag einer Verordnung für einen allgemeinen Rechtsrahmen und einem Vorschlag für eine Richtlinie über die Datenverarbeitung durch Polizei und Justiz eine zweiteilige Reform der Datenschutzrichtlinie von 1995 vor.

Obwohl die CNIL den Zielen dieser Reform (verstärkte Einwilligung durch betroffene Personen, Anerkennung des Rechts auf „Datenportabilität", vereinfachte Verwaltungsverfahren für Unternehmen) zustimmt, hat sie dennoch Fragen bezüglich der Wirksamkeit des Systems und insbesondere bezüglich des Datenschutzes.

Aus diesem Grund hat die Behörde ein neues Governance-Modell vorgeschlagen, das den Bürgern eine örtliche Kontrolle ermöglichen und das Bedürfnis einer einzigen Anlaufstelle für Unternehmen, die grenzüberschreitend Daten verarbeiten, berücksichtigen soll.

Diesbezüglich müssen die Behörden auch weiterhin dazu in der Lage sein, ihre Aufgaben anhand von zwei Kriterien durchzuführen: die Bestimmung eines für die Verarbeitung Verantwortlichen/Subunternehmers oder der Zielgruppe.

Die Ernennung einer federführenden Behörde basierend auf dem Hauptkriterium für die Bestimmung sorgt für eine Zusammenarbeit der zuständigen Behörden. Diese federführende Behörde verfügt nicht über exklusive Kompetenzen, sondern vielmehr über eine anweisende und koordinierende Funktion. Entscheidungen werden im Rahmen eines gemeinsamen Verfahrens zur Entscheidungsfindung und durch Absprache mit den anderen beteiligten Behörden getroffen, deren Unabhängigkeit ebenfalls gewahrt bleibt. Der Europäische Datenschutzbeauftragte (EDSB) greift lediglich im Falle von Unstimmigkeiten zwischen den Behörden oder zur Gewährleistung einer einheitlichen Auslegung der Verordnung ein.

Die Effektivität des vorgeschlagenen Systems liegt im einschränkenden Wesen der endgültigen Entscheidung und in der Gewährleistung eines effektiven Widerspruchsrechts. Da Entscheidungen von den zuständigen Behörden genehmigt werden, können die Beteiligten bei ihrer nationalen Verwaltungsgerichtsbarkeit gegen Entscheidungen ihrer Behörden, die nicht in ihrem Interesse liegen, Einspruch einlegen. Gleichermaßen können Unternehmen bei der Gerichtsbarkeit des Landes der federführenden Behörde Einspruch einlegen.

Außerdem ist es unerlässlich, gemäß klar definierter Regeln die Kontrolle über Datenübermittlungen zu behalten und die Möglichkeit auszuschließen, zur Verwaltung dieser Übermittlungen Instrumente ohne rechtlichen Wert zu nutzen.

Die CNIL hat außerdem ihren Austausch mit der Europäischen Kommission fortgesetzt, um seinen Bedenken Ausdruck zu verleihen und den außenpolitischen Ausschuss der Nationalversammlung sowie den Europaausschuss des Senats zu sensibilisieren. Daraufhin haben die beiden Gremien in einem europäischen Beschluss ihre Bedenken bezüglich der vorgeschlagenen Verordnung im Hinblick auf die Zuständigkeitsregelungen zum Ausdruck gebracht und somit den gleichen Standpunkt wie die CNIL eingenommen. Gespräche mit der französischen Regierung wurden 2012 ebenfalls fortgesetzt.

Digitale Bildung: Die wichtigsten Maßnahmen der CNIL

Die CNIL beschloss 2012, digitale Bildung zu einer strategischen Priorität zu machen und somit seine Maßnahmen mit der Schaffung neuer Hilfsmittel und einer weiteren Verbreitung zu verstärken. In diesem Zusammenhang wurden 2012 mehrere Maßnahmen ergriffen:

- Verbesserung der dazugehörigen Website (jeunes.cnil.fr) mit pädagogischem Material
- Entwicklung eines „Serious Game" für soziale Medien
- Vergabe von Zertifikaten für „Datenschutzschulungen"
- Schulung von Schulungsleitern für Verbraucherverbände und Industrie- und Handelskammern als Schnittstellen für Unternehmen.

Beobachtung der technischen Entwicklungen

Cloud

Infolge der öffentlichen Konsultation im Jahr 2011 hat die CNIL im Juni 2012 eine Zusammenstellung von Empfehlungen veröffentlicht, die sich an Stellen und insbesondere an KMU richtet, die Cloud-Dienste nutzen möchten.

Diese Empfehlungen wurden mit Vorlagen für Vertragsklauseln kombiniert, die Cloud-Computing-Dienstleistungsvereinbarungen hinzugefügt werden können, um Datenschutzfragen zu behandeln.

Intelligente Verbrauchszähler

Die CNIL debattiert bereits seit über zwei Jahren über diese Verbrauchszähler und untersucht insbesondere ihre Auswirkungen auf die Privatsphäre. Angesichts dieser Risiken hat die Kommission 2012 eine erste Empfehlung für eine Regulierung intelligenter Verbrauchszähler angenommen.

Diese Empfehlung basiert auf dem Grundsatz, dass der Lastgang nicht systematisch, sondern nur dann erfasst werden kann, wenn Netzarbeiten durchgeführt werden oder der Nutzer dies ausdrücklich wünscht, um bestimmte Dienste in Anspruch zu nehmen.

Außerdem enthält sie eine Reihe von Sicherheitsanforderungen und verlässlichen Vorkehrungen, die vorhanden sein müssen, um eine vertrauliche Behandlung der Daten zu gewährleisten (z. B. anhand von Folgenabschätzungen vor dem Einsatz von Verbrauchszählern und Risikoanalysen zur Bestimmung angemessener technischer Maßnahmen).

Google

Nach der Bekanntgabe von Google im Januar 2012, neue Vertraulichkeitsbestimmungen und Nutzungsbedingungen für fast alle seine Dienste einzuführen, hat die CNIL im Auftrag der G29 diese neuen Regelungen überprüft.

Hierfür wurden Google zwei Fragebögen zugeschickt. Nach der Auswertung der Antworten und der Prüfung verschiedener Dokumente und technischer Mechanismen haben die G29 Google am 16. Oktober 2012 ein Schreiben mit Empfehlungen zugeschickt, der von den 27 europäischen Datenschutzbehörden unterzeichnet war.

Prüfungen

Meldungen von Verstößen gegen den Schutz personenbezogener Daten

Als 2009 die Richtlinie zum „Telekom-Paket" überarbeitet wurde, verpflichtete der europäische Gesetzgeber elektronische Kommunikationsdienste dazu, den zuständigen nationalen Behörden und in bestimmten Fällen den betroffenen Personen Verstöße gegen den Schutz personenbezogener Daten zu

melden. Diese Anforderung wurde durch die Verordnung vom 24. August 2011 und der dazugehörigen Durchführungsverordnung vom 30. März 2012 in französisches Recht umgesetzt.

Der CNIL wurde somit die neue Aufgabe übertragen, das Sicherheitsniveau von Systemen elektronischer Kommunikationsdienste zu beurteilen und sie dabei zu unterstützen, effektive Maßnahmen zum Schutz vor Verstößen gegen den Datenschutz einzurichten. Schließlich kann sie, abhängig von der Schwere des Verstoßes, von den Anbietern verlangen, die betroffenen Personen zu benachrichtigen.

Von März bis Dezember 2012 sind bei der CNIL rund 15 Meldungen eingegangen.

Zentrales Vorstrafenregister (TAJ)

Die CNIL hat eine Stellungnahme zum Verordnungsentwurf zur Einrichtung eines zentralen Vorstrafenregisters abgegeben. Der Zweck dieser Datei, die von der Polizei und der nationalen Gendarmerie gemeinsam genutzt wird, liegt in einer erleichterten Feststellung von Zuwiderhandlungen, der Beweiserhebung und der strafrechtlichen Verfolgung.

Obwohl dies für den Einzelnen neue Sicherheiten bedeutet, hat die CNIL einige Bedenken geäußert, da sie der Meinung ist, dass zur Aktualisierung der Daten in den ursprünglichen Dateien vor deren Zusammenführung ein größerer Arbeitsaufwand notwendig ist.

Des Weiteren hat die CNIL Ende 2012 eine gründliche Prüfung der Vorstrafenregister durchgeführt (20 Vor-Ort-Prüfungen und 60 Dokumentenprüfungen).

Organisation	Französische Datenschutzbehörde
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 2012 (in Mio. EUR): 17,2**
Personal	**Anzahl der Mitarbeiter: 171**
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	**2 078 Beschlüsse** (5,5 % mehr als 2011)**/113 Stellungnahmen/2 Empfehlungen**
Meldungen	Bei der CNIL gingen **88 990** Meldungen ein, darunter: **8 946** Meldungen für Videoüberwachungssysteme (49,3 % mehr als 2011) **5 483** Meldungen für Ortungssysteme (22,3 % mehr als 2010)
Vorabprüfungen	**Genehmigungen: 1 534** im Jahr 2012, darunter: **316** im Plenum angenommene Genehmigungen, **950** Genehmigungen von Datenübermittlungen an Nicht-EU-Staaten, **3**

	Rahmengenehmigungen, **795** Genehmigungen biometrischer Systeme (6,8 % mehr als 2011), **658** Genehmigungen von Datenverarbeitungen zu Zwecken medizinischer Forschungsarbeit sowie **162** Genehmigungen von Datenverarbeitungen zu Zwecken der Beurteilung oder Analyse von Pflege- und Vorbeugungspraktiken oder -aktivitäten.
Anträge betroffener Personen	**Anfragen aus der Öffentlichkeit:** Die CNIL erhielt 2012 **35 924** schriftliche und **134 231** telefonische Anfragen.
Beschwerden betroffener Personen	Bei der CNIL gingen 2012 **6 017** Beschwerden ein (4,9 % mehr als 2011). Dies ist die höchste Anzahl von Beschwerden, die jemals bei der CNIL eingegangen ist. Die Hauptanliegen der Beschwerden bezogen sich auf das Recht auf Vergessenwerden und Videoüberwachungssysteme. **Anfragen betroffener Personen: 3 682** Anträge auf indirekten Zugang in Bereichen, in denen eine Datenverarbeitung der Staatssicherheit, Verteidigung oder öffentlichen Sicherheit dient (75 % mehr als 2011).
Vom Parlament bzw. der Regierung angeforderte Beratung	Die CNIL nahm **2012 113 Stellungnahmen** an. Des Weiteren wurde die CNIL **22** Mal von Abgeordneten des französischen Parlaments **konsultiert** und nahm an Sitzungen mit Abgeordneten des französischen Parlaments zum Austausch von Ansichten zu Datenschutzfragen teil.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	**458** Untersuchungen (19 % mehr als 2011), davon **173** Untersuchungen bzgl. Videoüberwachungssystemen.
Sanktionsmaßnahmen	
Sanktionen	**13 durch die CNIL im Jahr 2012 verhängte Sanktionen.** **Rechtsstreite gegen Verantwortliche von Datenverarbeitungen: 56** (**43** Mahnungen, **4** Geldstrafen, **9** Verwarnungen), **2** Kündigungen.
Geldbußen	Die CNIL verhängte **2012** Geldbußen **im Gesamtwert von 16 001 EUR.**
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	**10 709** Institutionen ernannten einen DPO (24 % mehr als 2011).

B. Rechtsprechung

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

- Kassationsgerichtshof, Kammer für Soziales, Herr G./Société Groupe Progrès 10208450 (4. April 2012)
- Kassationsgerichtshof, 2. Zivilkammer, Herr X./Nouvelle du Journal de l'Humanité (12. April 2012)
- Kassationsgerichtshof, Zivilkammer, Aufeminin.com/Google France 1115188 (12. Juli 2012)
- Kassationsgerichtshof, Zivilkammer, Google France/Bac films (12. Juni 2012)
- Kassationsgericht, Kammer für Wirtschaft, Handel und Finanzen, eBay Inc, eBay International/LVMH et. al. (03. Mai 2012)
- Kassationsgerichtshof, Strafkammer, Damien 1180801 (06. März 2012)
- Kassationsgerichtshof, Kammer für Soziales, Boymond/Société Technique française du nettoyage 1023482 (10. Januar 2012)
- Kassationsgerichtshof, Kammer für Soziales, Herr G./Société Groupe Progrès 1020845 (4. April 2012)
- Kassationsgerichtshof, Kammer für Soziales, Herr X./Association Perce-neige (10. Mai 2012)
- Kassationsgerichtshof, Kammer für Soziales, Herr X./Nouvelle communication téléphonique (10. Mai 2012)
- Kassationsgerichtshof, Kammer für Soziales, Herr X./SAS Helpevia 1115310 (26. Juni 2012)
- Kassationsgerichtshof, Kammer für Soziales, Frau X./Société Réunion fixations 1023521 (23. Mai 2012)

GRIECHENLAND

A. Zusammenfassung der Aktivitäten und Neuerungen:

Das griechische Parlament verabschiedete das Gesetz 4070/2012, das u. a. die Richtlinie 2009/136/EG zur Verarbeitung personenbezogener Daten und zum Schutz der Privatsphäre in der elektronischen Kommunikation in griechisches Recht umsetzt.

Des Weiteren wurde im 15. Jahresbericht der Artikel-29-Datenschutzgruppe gemeldet, dass das griechische Parlament das Gesetz 4055/2012 verabschiedet hat, das bestimmte Vorkehrungen zur Regulierung von Angelegenheiten im Zusammenhang mit dem Betrieb der verfassungsrechtlich geschützten, unabhängigen Behörden im Allgemeinen und der Datenschutzbehörde (im Folgenden HDPA) im Speziellen umfasst.

Zum wiederholten Mal konnte jedoch das schwerwiegende Problem der Unterbesetzung der HDPA, das seit ihrer Gründung besteht, aufgrund der andauernden schlechten Finanzlage des Staates auch 2012 nicht gelöst werden. Darüber hinaus beeinträchtigt die fortlaufende Reduzierung des Budgets, das der HDPA für betriebliche Zwecke zugeteilt wird, die Fähigkeit der Behörde, ihren Verpflichtungen ausreichend nachzukommen.

Die HDPA veröffentlichte 2012 insgesamt 194 Beschlüsse und 5 Stellungnahmen (von denen einige kurz in Abschnitt B „Rechtsprechung“ aufgeführt werden).

Darüber hinaus äußerte sich die HDPA schriftlich zu a) der Einrichtung eines integrierten Bürgerregisters, das als Knotenpunkt der Register des Ministeriums für Finanzen, Arbeit und sozialer Sicherheit, des Ministeriums für öffentliche Ordnung und Bürgerschutz und des Innenministeriums fungiert, b) dem neuen Rahmen für E-Government-Dienste, c) dem Verordnungsentwurf zu elektronischen Signaturen und anderen Vertrauensdiensten zur Aufhebung der Richtlinie 1999/93/EG und d) dem neuen Rechtsrahmen zum Schutz personenbezogener Daten — und wurde zu einer Parlamentsanhörung geladen.

Des Weiteren fügte die HDPA anlässlich des Europäischen Datenschutztages ihrer Website neue Abschnitte hinzu, unterzog die Inhalten einer gründlichen Überarbeitung und verbesserte die gesamte Struktur. Im Hinblick auf eine verstärkte Sensibilisierung führte die Behörde außerdem einen Newsletter mit Informationen zu aktuellen Entwicklungen auf dem Gebiet des Datenschutzes auf nationaler, europäischer und internationaler Ebene ein. Schließlich führte die HDPA zur Planung neuer Sensibilisierungsmaßnahmen auf ihrer Website eine Online-Befragung zu Angelegenheiten rund um den Schutz personenbezogener Daten durch.

Organisation	Griechische Datenschutzbehörde
Vorsitz und/oder Gremium	Petros Christoforos (Vorsitzender des Gremiums).
Budget	2 213 787 EUR
Personal	Abteilung Audit: 15 Juristen und 11 IT-Fachkräfte (davon drei (3) unbezahlte Beurlaubungen und eine (1) Kündigung), Abteilung Kommunikation und PR: 5 (davon zwei (2) für einen Teil des Jahres von anderen Stellen/Behörden des öffentlichen Dienstes abgestellt, eine (1) befindet sich im Mutterschutz), Abteilung Personal und Finanzen: 16 (davon ein (1)

	Wechsel zu einer anderen Stelle des öffentlichen Dienstes).
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die HDPA veröffentlichte 194 Beschlüsse und 5 Stellungnahmen.
Meldungen	Die HDPA erhielt 540 Meldungen (335 davon betrafen die Installation und den Betrieb von Überwachungskameras, 57 betrafen die Übermittlung von Daten in Länder außerhalb der EU).
Vorabprüfungen	Die HDPA erteilte bzw. erneuerte 81 Genehmigungen zur Verarbeitung sensibler Daten, zur Verknüpfung von Dateien sowie zur Datenübermittlung an Drittländer ohne angemessenes Schutzniveau.
Anträge betroffener Personen	989
Beschwerden betroffener Personen	675 (Strafverfolgungsbehörden und Ordnungsamt: 8, Landesverteidigung: 1, öffentliche Verwaltung und lokale Behörden: 24, Besteuerung/Finanzministerium: 6, Gesundheitswesen: 13, Sozialversicherung: 4, Bildung und Forschung: 4, Bankwesen: 75, Privatwirtschaft: 64, elektronische Kommunikation: 254, Arbeitsbeziehungen: 20, Massenmedien: 23, Sonstige: 179).
Vom Parlament bzw. der Regierung angeforderte Beratung	4 – siehe Abschnitt (a) „Zusammenfassung der Aktivitäten und Neuerungen“
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Anlässlich des Europäischen Datenschutztages 2012 fügte die HDPA ihrer Website neue Abschnitte hinzu („Sicherheit von Strafverfolgungsbehörden“, „Steuerfragen“, „soziale Sicherheit“, „neue Technologien“, „Bildung/Forschung“, „Gesundheit“ und „Finanzen“), überarbeitete den gesamten Inhalt und verbesserte die Struktur. Mit dem Ziel einer verstärkten Sensibilisierung führte die Behörde einen Newsletter mit Informationen zu aktuellen Entwicklungen auf dem Gebiet des Datenschutzes auf nationaler, europäischer und internationaler Ebene ein. Die HDPA führte zur Planung neuer Sensibilisierungsmaßnahmen auf ihrer Website eine Online-Befragung zu Themen bezüglich des Schutzes personenbezogener Daten durch.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	11 Prüfungen (davon 10: von für die Datenverarbeitung Verantwortlichen im Privatsektor und insbesondere Unternehmen, die sich mit dem Kauf/Verkauf von Datenbanken mit personenbezogene Daten befassen, 1: der Nationalen SIRENE-Vertretung und des Schengener Informationssystem (SIS)). Zwei (2) Sonderprüfungen zum Betrieb von Videoüberwachungssystemen in einem Unternehmen und einer Nichtregierungsorganisation. Vier (4) weitere Prüfungen, die 2011 eingeleitet wurden, wurden 2012

	abgeschlossen (3: zum Schutz personenbezogener Daten, die von speziellen elektronischen Systemen und Diensten des Bildungsministeriums gespeichert und verarbeitet werden — siehe Rechtsprechung, 1: zum Online-Verschreibungssystem des Generalsekretariats für soziale Sicherheit des Ministeriums für Beschäftigung und sozialen Schutz.
Sanktionsmaßnahmen	
Sanktionen	Die Datenschutzbehörde verhängte 38 Sanktionen (5 Verwarnungen, 33 Geldbußen) im Zusammenhang mit den folgenden Themenbereichen: Öffentlicher Sektor (1), Gesundheitswesen (5), Europäisch/International (1), Finanzsektor (14), Verletzungen des Schutzes personenbezogener Daten (8), Massenmedien (3), Bildung und Forschung (1) und elektronische Kommunikation (4). In drei Fällen erlegte die HDPA eine Verwarnung und eine Geldbuße auf.
Geldbußen	Geldbußen: Beträge: Von der HDPA wurden Geldbußen in Höhe von 2 500–50 000 EUR (insgesamt 486 500 EUR) verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Stellungnahme 3/2012

Die HDPA veröffentlichte eine Stellungnahme bezüglich den Anforderungen zur Eingabe und Löschung von Drittstaatsangehörigen im SIS auf Grundlage des Artikels 96 des Schengener Übereinkommens sowie im nationalen Register unerwünschter Drittstaatsangehöriger. Die Behörde kam zu dem Ergebnis, dass die Eingabe eines Drittstaatsangehörigen in das nationale Register keine *ipso-jure*-Ausschreibung im SIS auslöst. Die Eingabe eines Drittstaatsangehörigen in das SIS erfolgt gemäß den Anforderungen des Artikels 96 des Schengener Übereinkommens. Die Abschiebung durch Verwaltungs- oder Justizbehörden nach nationalem Recht rechtfertigt eine Ausschreibung im nationalen Register und im SIS. Ein Drittstaatsangehöriger wird in das SIS eingegeben, wenn er infolge einer Straftat von einem nationalen Gericht zu einer Freiheitsstrafe von mindestens einem (1) Jahr verurteilt wird. Die Eingabe eines Drittstaatsangehörigen in das SIS ist dann gerechtfertigt, wenn ernsthafte Gründe bestehen, dass die betreffende Person schwere Straftaten begangen hat oder diese plant. Des Weiteren ist die Eingabe eines Drittstaatsangehörigen in das nationale Register gerechtfertigt, falls aus bestimmten Gründen eine verwaltungsrechtliche Ausweisung vorliegt und die Anwesenheit des Drittstaatsangehörigen nachweislich eine Gefahr für die öffentliche Ordnung und Sicherheit des Landes darstellt. Ein Drittstaatsangehöriger wird nach einem Zeitraum von drei Jahren nach der Ausschreibung aus dem SIS gelöscht, wenn kein gerechtfertigter Grund dafür besteht, den Eintrag weiterhin zu speichern.

Beschluss 36/2012

Die HDPA bezeichnete die Veröffentlichung des Fotos einer Mutter mit ihrer minderjährigen Tochter in einer Zeitung ohne ihre vorherige Einwilligung im Kontext eines Artikels über Endometriose als unrechtmäßige Verarbeitung, Erfassung und Aufbewahrung personenbezogener Daten. Die Behörde kam zu dem Schluss, dass das Foto ohne Bedeutung für den Inhalt des Artikels ist und bei den Lesern den Eindruck erwecken

könnte, dass die Mutter an der Erkrankung leide. Die Behörde erlegte dem für die Verarbeitung Verantwortlichen eine Geldbuße auf, ordnete die Löschung der Daten aus dem Zeitungsarchiv an und verbot eine erneute Veröffentlichung.

Beschluss 112/2012

Die HDPA untersuchte eine Reihe von Meldungen im Zusammenhang mit Ortungssystemen (mit GPS-Technologie) und ständigen Überwachungsdiensten, die von zwei Unternehmen bereitgestellt werden. Die Nutzer dieser Dienste sind in der Lage, die Funktionen des Dienstes selbst festzulegen und den geografischen Standort der Träger der Ortungsgeräte zu lokalisieren. Zu den Nutzern gehören vor allem Personen mit gesundheitlichen Problemen oder Personen, die sich um Personen mit derartigen Problemen kümmern, sowie Eltern minderjähriger Kinder, die die Geräte aus Sicherheitsgründen nutzen. Die verarbeiteten Daten der Geräteträger umfassen Standortdaten, demografische Daten sowie vertrauliche Gesundheitsdaten. Der Beschluss der HDPA sieht bestimmte Voraussetzungen und Bedingungen für den Schutz personenbezogener Daten vor, die durch derartige Ortungsdienste erhoben werden, wie z. B.: der für die Datenverarbeitung Verantwortliche muss den Geräteträger auf angemessene Weise über die Verarbeitung von, den Zugang zu und die Sicherheitsvorkehrungen in Bezug auf dessen Daten informieren; in einigen Fällen müssen die Daten durch Sicherheitsvorkehrungen verschlüsselt bzw. geschützt werden; der Geräteträger muss über die Verarbeitung in Kenntnis gesetzt werden und im Voraus seine Einwilligung erteilen; bei vertraulichen Daten muss die Einwilligung außerdem schriftlich erfolgen; falls es sich bei dem Geräteträger um eine rechtsunfähige Person handelt, muss die Einwilligung des gesetzlichen Vertreters eingeholt werden; bei Minderjährigen muss die Einwilligung der Eltern/Erziehungsberechtigten eingeholt und die Meinung der Minderjährigen berücksichtigt werden; der Geräteträger muss dazu in der Lage sein, Widerspruch einzulegen; die Nutzung dieses Systems bei Minderjährigen muss zunächst von den zuständigen staatlichen Behörden auf Risiken geprüft, kann jedoch bis dahin zu gesundheitlichen Zwecken genutzt werden.

Beschluss 117/2012

Eine politische Organisation veröffentlichte ein Plakat, das im Hintergrund – ohne deren Einwilligung – eine Gruppe demonstrierender Personen zeigte. Die HDPA kam zu dem Schluss, dass das Bild dieser Personen nicht direkt im Zusammenhang mit dem Inhalt des Plakats stand und bei Bürgern fälschlicherweise den Eindruck erwecken könnte, dass die abgebildeten Personen Anhänger der politischen Organisation seien. Demzufolge erlegte die Datenschutzbehörde der Organisation eine Sanktion auf, verbot die Veröffentlichung der Plakate und ordnete deren Vernichtung an.

Beschluss 165/2012

Die Datenschutzbehörde kam zu dem Ergebnis, dass die Veröffentlichung sensibler personenbezogener Daten (im Zusammenhang mit Strafanzeigen) auf der Website einer Zeitung gegen das Gesetz 2427/1997 zum Schutz personenbezogener Daten verstößt. Genauer gesagt stellt die rechtswidrige Veröffentlichung sensibler personenbezogener Daten per Suchmaschine im Internet nach Meinung der HDPA einen unverhältnismäßigen Verstoß gegen die Rechte betroffener Personen dar, da die betroffenen Personen durch die Verarbeitung dauerhaft mit ihrem Verhalten in der Vergangenheit in Verbindung gebracht werden und somit die einschlägigen Informationen leicht für jeden, der danach sucht, verfügbar sind – und nicht nur für Journalisten, Forscher und Gelehrte. Darüber hinaus erlegte die HDPA dem für die Verarbeitung Verantwortlichen eine Geldbuße auf, ordnete die Anonymisierung der betroffenen Person auf der Website der Zeitung an, sodass es selbst bei der Suche nach dem Veröffentlichungsdatum nicht mehr möglich ist, die betroffene Person zu identifizieren, und verwarnte den für die Verarbeitung Verantwortlichen, um das Widerspruchsrecht der betroffenen Person zu prüfen und entweder die Daten zu anonymisieren oder solche Behauptungen aus bestimmten Gründen zu widerlegen.

Beschluss 187/2012

Die HDPA mahnte das Bildungsministerium zur Einhaltung der Empfehlungen, die sie in ihrem Bericht aufgeführt hatte, nachdem die Behörde drei Prüfungen von elektronischen Systemen („elektronischer Dienst zur Ausgabe spezieller Tickets/Studierendenausweise", „E-School" und „E-Datenzentrum") auf den Schutz und die Sicherheit personenbezogener Daten durchgeführt hatte, die durch diese Systeme verarbeitet werden. Insbesondere stellte die Datenschutzbehörde bei dem für die Verarbeitung Verantwortlichen bestimmte Mängel bzw. Versäumnisse bei den Verfahren und der Organisation der Sicherheit, der nötigen Dokumentation der Sicherheitsvorkehrungen und deren systematischen Überwachung, der Nutzerauthentifizierung, der Verwaltung und Unterstützung dieser Systeme und schließlich den allgemeinen Verpflichtungen gemäß Gesetz 2472/1997 fest.

IRLAND

A. Zusammenfassung der Aktivitäten und Neuerungen:

2012 eröffnete das Amt des Datenschutzbeauftragten 1 349 Verfahren zur Untersuchung formeller Beschwerden (viele Beschwerden werden informell bearbeitet, indem Beschwerdeführer angemessen über ihre Rechte informiert werden). 2012 wurden 864 Beschwerdeverfahren abgeschlossen. Wie in den Jahren zuvor konnte ein Großteil der Beschwerden gütlich beigelegt werden; nur 36 Beschwerden gaben Anlass zu formellen Beschlüssen. Die ersten Verfahren richteten sich gegen Telekommunikationsunternehmen, die sich nicht an die neuen Regelungen zur Meldung von Verstößen gegen den Datenschutz gemäß der Rechtsverordnung 336 von 2011 (zur Umsetzung der Richtlinie 2002/58/EG, geändert durch Richtlinien 2006/24/EG und 2009/136/EG, in irländisches Recht) hielten. Informationen bezüglich strafrechtlicher Verfolgungen im Jahr 2012 sind in Abschnitt B dieses Berichts enthalten. Das Amt verzeichnete weiterhin einen Anstieg der Meldungen von Verstößen gegen den Schutz personenbezogener Daten (1 592 im Jahr 2012). Somit setzt sich die Entwicklung infolge der Einführung des Verhaltenskodex für Verstöße gegen den Schutz personenbezogener Daten im Jahr 2010 fort.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Billy Hawkes
Budget	1 458 000 EUR. Ausgegeben: 1 552 468 EUR.
Personal	28 zum 31. Dezember 2012.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	36 formelle Beschlüsse.
Meldungen	5 338
Vorabprüfungen	k. A.
Anträge betroffener Personen	9 500 Anträge per E-Mail. Außerdem schriftliche Anträge.
Beschwerden betroffener Personen	1 349
Vom Parlament bzw. der Regierung angeforderte Beratung	Regelmäßige informelle Konsultationen zu Gesetzesvorschlägen/Vorschlägen von Rechtsvorschriften.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	1 592 Meldungen über Verletzungen des Schutzes personenbezogener Daten.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	40 Audits (Prüfungen)

Sanktionsmaßnahmen	
Sanktionen	195 Verfahren gegen 11 Rechtssubjekte.
Geldbußen	7 500 EUR zuzüglich Kosten. 99 500 EUR vom Gericht angeordnete Spenden zu wohltätigen Zwecken gemäß dem Probation Act, zuzüglich Kosten.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

In den meisten Fällen konnten Beschwerden an den Datenschutzbeauftragten unter Berufung auf Abschnitt 10 der irischen Datenschutzgesetze von 1988 und 2003 gütlich beigelegt werden, ohne auf formelle Beschlüsse oder Durchsetzungsmaßnahmen zurückgreifen zu müssen. Solche gütlichen Einigungen können zum Beispiel eine finanzielle Zuwendung durch den für die Verarbeitung Verantwortlichen an die betroffene Person oder an eine geeignete Wohltätigkeitsorganisation umfassen. Gegebenenfalls kommt es zu Durchsetzungsmaßnahmen, zum Beispiel dann, wenn für die Verarbeitung Verantwortliche die Zugriffsrechte betroffener Personen missachten. In einigen Fällen werden für die Verarbeitung Verantwortliche in Fallstudien erwähnt, die im Jahresbericht des Datenschutzbeauftragten enthalten sind. Im Laufe des Jahres 2012 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 336 aus dem Jahr 2011 (Umsetzung der Richtlinie 2002/58/EG, geändert durch 2006/24/EG und 2009/136/EG, in irländisches Recht). Im Jahr 2012 wurden 195 Verfahren gegen 11 Rechtssubjekte eingeleitet. Hierzu gehörten erste Verfahren gegen Telekommunikationsunternehmen, die sich nicht an die neuen Regelungen zur Meldung von Verstößen gegen den Datenschutz gemäß der Rechtsverordnung 336 von 2011 hielten, mehrere Verfahren im Zusammenhang mit unerwünschten Marketing-SMS und -E-Mails sowie Straftaten im Zusammenhang mit den Datenschutzgesetzen unterliegenden Registrierungen.

Der High Court entschied in der Berufungsinstanz im Zusammenhang mit einer Rechtsfrage bezüglich Datenzugriff in einer Rechtssache, bei der zwischen den Parteien ein Gerichtsverfahren andauerte. Der High Court entschied wie folgt: „Die Existenz eines Gerichtsverfahrens zwischen einem Antragsteller auf Datenzugriff und einem für die Verarbeitung Verantwortlichen schließt weder aus, dass der Antragsteller auf Datenzugriff einen Antrag auf Zugriff gemäß dem Datenschutzgesetz stellt, noch berechtigt es den für die Verarbeitung Verantwortlichen dazu, den Antrag abzulehnen“. In einer weiteren Anfechtung vor dem High Court bestätigte dieser den Beschluss des Datenschutzbeauftragten, einer Beschwerde nicht nachzugehen, die er als „leichtfertig oder lästig“ erachtete, sowie die Tatsache, dass die höheren Gerichte nicht für einen Rechtsbehelf zuständig seien, da keine Ermittlung stattgefunden habe.

C. Sonstige wichtige Informationen

Der Datenschutzbeauftragte tauschte sich auch weiterhin mit großen öffentlichen Organisationen über das Ausmaß des Datenaustauschs im öffentlichen Sektor aus. Dem Jahresbericht 2012 der Datenschutzbehörde war im Anhang ein Bericht der Ermittlungen der Behörde in Sachen INFOSYS, einem Datenaustauschsystem des irischen öffentlichen Sektors, beigefügt. Bei den Ermittlungen wurde eine gescheiterte Unternehmensführung in einigen der geprüften öffentlichen Organisationen aufgedeckt und Empfehlungen für eine verbesserte Unternehmensführung ausgesprochen, wie z. B. im Zusammenhang mit einer höheren Transparenz und verbesserten Zugangs- und Sicherheitskontrollen.

In Anerkennung der erhöhten Zuständigkeiten, die der Datenschutzbehörde aller Wahrscheinlichkeit nach zukommen werden, wenn die Gesetzgebungsvorschläge zum Datenschutz, die derzeit im Ministerrat der Europäischen Union und im Europäischen Parlament besprochen werden, in irisches Recht umgesetzt werden, wurden der Datenschutzbehörde Ende 2012 zusätzliche Mitarbeiter zugeteilt. Diese Ressourcen umfassten einen leitenden Technologieberater und einen Rechtsberater sowie zusätzliches Verwaltungspersonal. Die nicht gehaltsbezogene Budgetzuteilung der Datenschutzbehörde wurde 2013 ebenfalls erhöht.

ITALIEN

A. Zusammenfassung der Aktivitäten und Neuerungen:

Das neue Kollegium der italienischen Datenschutzbehörde trat am 19. Juni 2012 ihr Amt an und löste das Kollegium unter der Leitung von Prof. Francesco Pizzetti (2005–12) ab. Zur neuen Kommission gehören Antonello Soro, Vorsitzender, Augusta Iannini, stellvertretende Vorsitzende, Giovanna Bianchi Clerici und Prof. Licia Califano, Mitglieder. Giuseppe Busia ist der neue Generalsekretär der Datenschutzbehörde.

Gesetzesänderungen

Elektronische Kommunikation – Meldung von Verstößen gegen den Datenschutz

Im Laufe des Jahres 2012 wurde die Richtlinie 2009/136/EG in italienisches Recht umgesetzt. Insbesondere die Gesetzesverordnung Nr. 69/2012 setzte das Konzept der Verstöße gegen den Schutz personenbezogener Daten in italienisches Recht um und führte Verpflichtungen ein, denen Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste im Falle eines solchen Verstoßes nachzukommen haben (siehe Abschnitt 32 des italienischen Datenschutzgesetzes).

Weitere Gesetzesänderungen betreffen in diesem Zusammenhang die Änderungen einiger im Datenschutzgesetz enthaltener Definitionen (die Bezeichnung „Vertragspartei“ wurde durch „Teilnehmer“ ersetzt); die Regelungen zur Speicherung von und zum Zugriff auf Daten in der Endeinrichtung der Vertragspartei mit speziellem Augenmerk auf „Cookies“ (Abschnitt 122 des Datenschutzgesetzes); die von Anbietern öffentlicher elektronischer Kommunikationsdienste umzusetzenden Sicherheitsvorkehrungen (gemäß den Abschnitten 32 und 132 a des Datenschutzgesetzes) sowie die entsprechenden Änderungen der entsprechenden Sanktionen (im Abschnitt 162 b bezüglich „Verstöße gegen den Schutz personenbezogener Daten“).

Maßnahmen zur „Vereinfachung“

Die Änderungen des Datenschutzgesetzes wurden außerdem durch Maßnahmen zur „Vereinfachung“ herbeigeführt, die dringend von der italienischen Regierung per Verordnung am 9. Februar 2012 angenommen wurden und daraufhin mit zusätzlichen Änderungen mit Gesetz Nr. 35 am 4. April 2012 in Kraft traten. Vor allem im Hinblick auf Sicherheitsvorkehrungen wurde bei der Verordnung auf die Anforderung an für die Verarbeitung Verantwortlichen, ein „Sicherheitsstrategiedokument“ zu erstellen, durch eine Selbstzertifizierungserklärung ersetzt. Mit der Verordnung wurde der italienischen Datenschutzbehörde außerdem die Befugnis entzogen, vereinfachte Vorkehrungen für die Umsetzung minimaler Sicherheitsvorkehrungen anhand eigener Maßnahmen zu treffen.

Selbige Verordnung erlaubt die Verarbeitung von Strafverfolgungsdaten im Sinne von Absichtserklärungen, die Unternehmen mit dem Innenministerium (oder dessen Dienststellen) zur Prävention und Bekämpfung organisierter Kriminalität abgeschlossen haben – vorausgesetzt, dass die Kategorien der verarbeiteten Daten sowie die anzuwendenden Verarbeitungsverfahren detailliert werden (siehe Abschnitte 21 (1 a) und 27 des Datenschutzgesetzes).

„Meldung von Missständen“

Gemäß des neuen Abschnittes 54 a der Rechtsverordnung Nr. 165/2001 („Schutz öffentlicher Bediensteter nach Meldungen rechtswidrigen Verhaltens“) werden öffentliche Bedienstete, die beim Nachgehen ihrer Tätigkeit rechtswidriges Verhalten bemerken und dieses den Justizbehörden, dem Rechnungshof und/oder ihren Vorgesetzten melden, diesbezüglich unter keinen Umständen bestraft, entlassen oder diskriminierenden Maßnahmen ausgesetzt, die ihre beruflichen Bedingungen beeinträchtigen.

Wichtige Themen

Die wichtigsten Themen, mit denen sich die Datenschutzbehörde 2012 auseinandergesetzt hat, sind der Behörde im Laufe der Jahre wiederholt begegnet. Zu den häufigsten Fällen des Jahres 2012 gehörten

Schutzmechanismen für betroffene Personen im Zusammenhang mit Telemarketing, datenschutzfreundlicher Nutzung von (intelligenter) Videoüberwachungsausrüstung und beruflichen Angelegenheiten, einschließlich der Nutzung von Biometrie für Zugangskontrollen (die im Vergleich zu ihrem Zweck meist als übertrieben und unverhältnismäßig betrachtet wurden). Es folgt eine Zusammenfassung weiterer Angelegenheiten, die Neuerungen beinhalten.

Verstöße gegen den Schutz personenbezogener Daten

Die italienische Datenschutzbehörde veröffentlichte spezifische Leitlinien zur Erläuterung des obligatorischen Meldeverfahrens für Telekommunikations- und Internetdienstanbieter im Falle von Verstößen gegen den Schutz personenbezogener Daten. In den Leitlinien wird erläutert, wer unter welchen Umständen einen Verstoß melden muss, ob und wie Nutzer und Vertragsparteien benachrichtigt werden und welche technischen und organisatorischen Sicherheitsvorkehrungen getroffen werden müssen (siehe Beschluss vom 26. Juli 2012 im italienischen Amtsblatt Nr. 183 vom 7. August 2012 – Web-Dok. Nr. 1915485).

Foren, Blogs, Online-Archive von Tageszeitungen

Im Februar 2012 wurden Leitlinien für die angemessene Verarbeitung personenbezogener Daten durch Blogs, Foren, soziale Netzwerke und Websites im Gesundheitsbereich veröffentlicht. Die Leitlinien richten sich nicht an Online-Gesundheits- oder Telemedizindienste. Die wichtigste Empfehlung lautet, dass Website-Betreiber Nutzer über die Risiken informieren sollten, die sich potenziell aus dem Einstellen und der Verbreitung ihrer gesundheitsbezogenen Informationen im Internet ergeben, indem auf der Startseite eine „Ad-hoc-Risikomeldung“ angezeigt wird.

Auf einen Beschluss des italienischen Kassationsgerichts (Nr. 5525/2012) zum sogenannten „Recht auf Vergessenwerden“ hin gab die italienische Datenschutzbehörde einer Beschwerde statt, welche die Änderung eines Artikels auf der Website einer führenden Tageszeitung – und diesbezüglich eine Berücksichtigung der Entwicklungen – forderte. Es sei anzumerken, dass der betreffende Artikel bereits nicht mehr indexiert war. Insbesondere wurde dem Verlag angeordnet, z. B. durch eine Meldung neben einzelnen Artikeln, darauf hinzuweisen, dass weitere Entwicklungen stattgefunden haben. Auf diese Weise wäre dafür gesorgt, dass die Identität der betroffenen Person geachtet und Leser dennoch auf zuverlässige, genaue Weise informiert werden.

Genehmigungen: Genetische Daten, medizinische, biomedizinische oder epidemiologische Forschung

Die allgemeine, von der Datenschutzbehörde erteilte Genehmigung der Verarbeitung genetischer Daten wurde infolge einer Stellungnahme an das italienische Gesundheitsministerium im Dezember 2012 erneut erteilt. Dies erfolgte unter Berücksichtigung gesammelter Erfahrungen und der Beiträge angesehener Sachverständiger. Die Genehmigung wurde außerdem gemäß der geltenden Rechtsvorschriften öffentlichen und privaten Vermittlungsorganisationen erteilt.

Die allgemeine Genehmigung, die vorläufig im März 2012 erteilt wurde, um unter bestimmten Umständen die Verarbeitung personenbezogener Daten zu medizinischen, biomedizinischen und epidemiologischen Forschungszwecken ohne eine Inkenntnissetzung der betroffenen Personen zu ermöglichen, wurde im Dezember 2012 überarbeitet und erweitert. Die Genehmigung sieht nun vor, dass neben medizinischen Daten auch Informationen zu Sexualleben, Rasse oder ethnischer Herkunft ohne die Einwilligung der Patienten verarbeitet werden dürfen, falls es nachweislich entweder aus „ethischen Gründen“ oder aufgrund von „organisatorischen Hindernissen“ unmöglich ist, Patienten darüber in Kenntnis zu setzen. Zu weiteren Bedingungen, die in solchen Fällen erfüllt werden müssen, zählen eine begründete positive Stellungnahme zum jeweiligen Forschungsprojekt durch die zuständige Ethikkommission. In allen anderen Fällen bleibt die Einwilligung durch den Patienten eine notwendige Bedingung und muss unmittelbar bei der Kontaktaufnahme des Patienten mit der jeweiligen medizinischen Institution eingeholt werden – vor allem, wenn es sich um eine ambulante Behandlung handelt.

Internationale Aktivitäten

Die italienische Datenschutzbehörde setzte ihre aktive Teilnahme an der Artikel-29-Datenschutzgruppe fort. Die Datenschutzbehörde konnte auch die laufende Debatte zur Reform des EU-Datenschutzrechtsrahmens verfolgen, indem seine Sachverständigen in der italienischen Delegation sich an der DAPIX-Arbeitsgruppe des Rates beteiligten.

Die Datenschutzbehörde beteiligte sich aktiv an der Arbeit der OECD und des Europarats, insbesondere über die Arbeitsgruppe zu Informationssicherheit und Datenschutz (WPISP) und den Beratenden Ausschuss und Amt T-PD. Letzterer arbeitet seit geraumer Zeit an der Überarbeitung der Konvention Nr. 108/1981. Die Datenschutzbehörde ist Mitglied gemeinsamer Kontrollinstanzen auf EU-Ebene (gemeinsame Kontrollinstanzen von Europol und Schengen, CIS, Eurodac-Koordinierungsgruppe) und beteiligt sich außerdem regelmäßig an der sogenannten Berlin Group (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation).

Die Datenschutzbehörde setzte ihre Arbeit im Rahmen der Programme IPA, TAIEX und Twinning der Europäischen Kommission für neue Beitrittsländer, Beitrittskandidaten (Türkei, Kroatien, ehemalige jugoslawische Republik Mazedonien), Balkanländer, Russland und die ENP-Länder fort, um die Annäherung der Gesetzgebung dieser Länder an den Datenschutzrechtsrahmen der EU zu fördern.

Organisation	Italienische Datenschutzbehörde
Vorsitz und/oder Gremium	Vorsitzender des Gremiums: Dr. Antonello SORO Gremium: Augusta IANNINI Giovanna BIANCHI CLERICI Licia CALIFANO
Budget	Ungefähr 8,8 Mio. EUR (von der Regierung bereitgestellt)
Personal	122
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Beschlüsse des Gremiums: 440
Meldungen	1 053
Vorabprüfungen	13
Anträge betroffener Personen	Anfragen insgesamt: etwa 4 900 Auskunftsersuchen („questiti“): 320 2012 von betroffenen Personen eingereichte Berichte und Forderungen („segnalazioni“ und „reclami“): 4 592
Beschwerden betroffener Personen	(durch das Datenschutzgesetz speziell geregelte formelle Beschwerden betreffend den Zugang zu personenbezogenen Daten einer Person): 233

Vom Parlament bzw. der Regierung angeforderte Beratung	Stellungnahmen zu parlamentarischen Untersuchungen: 6 Stellungnahmen für Ministerien und das Amt des Premierministers: 23 Themen: Polizei, öffentliche Sicherheit: 3 Rechtsprechung: 2 E-Government und Datenbanken: 6 Aus- und Weiterbildung: 1 Gesundheitswesen: 1 Unternehmen: 1 Ausübung von Rechten: 2 Sozialhilfe: 3 Elektronische Dokumente: 2
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Im Frontoffice der Datenschutzbehörde gingen 2012 rund 34 000 Anrufe und E-Mails ein Nationale Genehmigungen für internationale Übermittlungen: 3
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen bzw. Untersuchungen (vor Ort): 395 (in 56 Fällen wurden Verstöße krimineller Art bei den Justizbehörden zur Anzeige gebracht)
Sanktionsmaßnahmen	
Sanktionen	Etwa 600
Geldbußen	Betrag: etwa 3,8 Mio. EUR, im Namen der Datenschutzbehörde von der für Kontrollen zuständigen Finanzpolizei verhängt
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Kassationsgericht — Recht auf Vergessenwerden und Aktualisierung von Zeitungsartikeln

Aus einer Entscheidung des Kassationsgerichts (Nr. 5525/2012) zu einem Artikel, der im Online-Archiv einer bekannten Tageszeitung verfügbar war, ging hervor, dass der Verlag dafür Sorge zu tragen hat, dass die Information sowohl vor dem einschlägigen Hintergrund bereitgestellt und aktualisiert werden muss, um die betroffene Person zu schützen und die Öffentlichkeit angemessen und korrekt zu informieren. Entsprechend wies das Gericht den Verlag an, die nötigen Vorkehrungen zu treffen, um die Entwicklungen in diesem Fall – d. h. die Tatsache, dass zu diesem Fall eine endgültige gerichtliche Entscheidung vorliegt –

neben dem ursprünglichen Artikel anzuzeigen und den Nutzern solche zusätzlichen Informationen schnell und unkompliziert zugänglich zu machen.

Gericht von Mailand – Geografischer Anwendungsbereich des Datenschutzgesetzes

In seinem Urteil über die gegen einen Beschluss der Datenschutzbehörde vom 7. April 2011 eingelegte Berufung befasste sich das Gericht von Mailand mit dem Begriff „Ausrüstung", wie er in Abschnitt 5(2) des Datenschutzgesetzes verwendet wird. Das Gericht kam insbesondere zu dem Schluss, dass der Begriff „bloße Kommunikationsvermittlung" nicht auf den Dienst eines Marketingunternehmens zutrifft, das seine Werbeaktivitäten über US-Server abwickelt, doch seine für Italien bestimmten Faxe teilweise über einen Knotenpunkt in Italien versendet. Dieser Knotenpunkt wurde von einer Telefongesellschaft mit Sitz in Italien verwaltet. Der betreffende Knotenpunkt war eine komplexe IT-Einrichtung, die den Absender über die (nicht) erfolgreiche Zustellung der einzelnen Faxe benachrichtigte. Diese Benachrichtigungen enthielten die IP-Adresse und Faxnummer des Absenders, die Faxnummer des Empfängers, das Sendeergebnis, die Anzahl der abgeschickten Faxe und den Inhalt der Nachricht(en). Somit verband das betreffende System auf italienischem Boden das Internet mithilfe eines speziellen Gerätes namens „Fax-Gateway", das personenbezogene Daten verarbeitete, mit dem Telefonnetz. In Anbetracht dessen bestätigte das Gericht von Mailand den Beschluss der Datenschutzbehörde und kam zu dem Schluss, dass die Datenverarbeitung in den Anwendungsbereich des italienischen Datenschutzgesetzes fällt.

Kassationsgericht – Öffentliche Bekanntmachungen einer Gemeinde

Das Kassationsgericht bestätigte einen Beschluss der Datenschutzbehörde vom 9. Dezember 2003 betreffend eines Mitarbeiternamens, der in einer öffentlichen Bekanntmachung einer Gemeinderatssitzung aufgeführt wurde (Beschluss Nr. 12726/2012). Die öffentliche Bekanntmachung – die von einem Durchsetzungsverfahren gegen einen Mitarbeiter handelte – wurde im Hinblick auf die geltenden Rechtsvorschriften zu Kommunalbehörden (Rechtsverordnung Nr. 267/2000) als gesetzeskonform eingestuft. Die Menge der offengelegten personenbezogenen Daten wurde jedoch im Vergleich zu den Transparenz- und Informationsbestrebungen der Gemeinde als übertrieben und unverhältnismäßig erachtet.

C. Sonstige wichtige Informationen

Interessenbekundung für eine Anhörung des italienischen Staates bei Verfahren des Europäischen Gerichtshofs

Die Datenschutzbehörde brachte ihr Interesse zum Ausdruck, den italienischen Staat bei den folgenden Verfahren des Europäischen Gerichtshofs anzuhören:

- Rechtssache C-119/12 (Ersuchen um Vorabentscheidung gemäß Artikel 267 AEUV) zur Auslegung von Artikel 6 der Richtlinie 2002/58/EG, um eine Auslegung des besagten Artikels zu unterstützen, die mit der Art und Weise, wie er in italienisches Recht umgesetzt wurde, in Einklang stehen sollte (siehe Abschnitt 123 des Datenschutzgesetzes). Die betreffende Vorkehrung legt fest, unter welchen Bedingungen personenbezogene Verkehrsdaten zu kommerziellen Zwecken (hier: zu Zwecken der Rechnungslegung) verarbeitet werden dürfen, um mit den Grundsätzen der Datenminimierung und der Verhältnismäßigkeit in Einklang zu stehen und die Interessen auf angemessene Weise abzuwägen.
- Rechtssache C-131/12 (Ersuchen um Vorabentscheidung gemäß Artikel 267 AEUV) zur Auslegung der Artikel 2, 4, 12 und 14 der Richtlinie 95/46/EG mit Hauptaugenmerk auf den Begriffen einer Niederlassung auf dem Gebiet eines Mitgliedstaates und der „Nutzung von Ausrüstung auf dem Gebiet des besagten Mitgliedstaates" sowie zur Speicherung von Daten, die von Suchmaschinen indexiert wurden, und zum Recht auf Löschung von Daten. Es wurde vorgebracht, dass Rechtssachen ähnlich dem Fall, bei dem die spanische Audiencia Nacional beim Europäischen Gerichtshof Berufung

eingelegt hat, von der Datenschutzbehörde bearbeitet wurden, indem die Quellwebsites (d. h. diejenigen, die für die geposteten und anschließend von Suchmaschinen erfassten Daten verantwortlich waren) dazu aufgefordert wurden, Maßnahmen zu ergreifen, um einen Abruf der personenbezogenen Daten der betroffenen Personen durch externe Suchmaschinen zu vermeiden. Solche Maßnahmen haben insbesondere eine Kompilierung der robots-txt-Datei gemäß „Robots Exclusion Protocol“ sowie die Nutzung von „Robots Meta Tags“ zur Folge.

LETTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen:

Im Jahr 2012 wurde der Änderungsentwurf des Datenschutzgesetzes ausgearbeitet. Die Änderungen bezogen sich hauptsächlich auf die folgenden Themen:

- Klärung der Begriffsbestimmung des für die Verarbeitung Verantwortlichen, einschließlich der Begriffsbestimmung der gemeinsamen für die Verarbeitung Verantwortlichen, durch die Festlegung der Rechte und Pflichten sowie der geteilten Verantwortung;
- Bestimmung mehrerer weiterer Ausnahmen von der Meldepflicht;
- Spezifische Anforderungen bezüglich der Datenübermittlung an Drittländer, die nicht ebenso hohe Datenschutzniveaus wie Lettland gewährleisten;
- Anforderung an staatliche und kommunale Regierungsbehörden, eine Beurteilung der Effektivität des Schutzes personenbezogener Daten umzusetzen;
- Bestimmung der Rechte der Datenschutzbehörde zur Festlegung eines bestimmten Zeitrahmens, innerhalb dessen die Informationen bei der Datenschutzbehörde eingereicht werden sollten, damit sie ihr Amt ausüben kann.

Des Weiteren wurden Änderungen bezüglich des Schengener Informationssystems vorgenommen. Die lettische Datenschutzbehörde hat in Zusammenarbeit mit dem Justizministerium eine Stellungnahme abgegeben, laut der überprüft werden soll, ob alle Institutionen Zugang zum SIS benötigen und zu welchen Zwecken.

Auf nationaler Ebene gab die lettische Datenschutzbehörde Stellungnahmen zu verschiedenen Rechtsakten und politischen Initiativen ab. Die Wichtigsten darunter lauten:

1) Gesetzentwurf zur Kreditauskunftei;
2) Gesetzentwurf zur Schuldenbeitreibung;
3) Gesetzentwurf zur elektronischen Identifikation.

Im Oktober 2012 wurde Lettland hinsichtlich Datenschutz der Schengen-Evaluierung unterzogen. Dies war demzufolge auch der Schwerpunkt der Behörde (was sich in zahlreichen Kontrollaktivitäten und einer Beurteilung des Informationsmaterials niederschlug).

In Anbetracht der Beschwerden, die 2011 und 2012 bei der lettischen Datenschutzbehörde eingingen, konnten die folgenden Schwerpunkte ermittelt werden:

1) Die Verarbeitung personenbezogener Daten im Rahmen von Inkassoverfahren;
2) Der für die Verarbeitung Verantwortliche hat der betroffenen Person nicht die nötigen Informationen bereitgestellt;
3) Die Veröffentlichung personenbezogener Daten im Internet.

Es wurden 10 Seminare organsiert sowie drei Prüfungen für Datenschutzbeauftragte abgehalten. 12 Personen haben den Rang eines Datenschutzbeauftragten erreicht.

Kernthemen bei Beratungsanträgen von öffentlichen Stellen

Die Datenschutzbehörde verfügt über keine Statistik zu den Anträgen auf Beratungsdienste von öffentlichen Stellen. Es gehen jedoch täglich Anrufe von verschiedenen öffentlichen Stellen zu verschiedenen Angelegenheiten im Zusammenhang mit der Verarbeitung personenbezogener Daten ein – angefangen bei der Notwendigkeit, die Verarbeitung personenbezogener Daten zu melden, bis hin zu den

Zugangsrechten der betroffenen Personen sowie kompliziertere Fragen, die eine gründliche Analyse erfordern, um die beste Lösung zum Schutz personenbezogener Daten zu finden. (Es gab z. B. viele Fragen aus dem öffentlichen und privaten Sektor bezüglich der Verarbeitung von Daten am Arbeitsplatz und Datensicherheitsangelegenheiten. Daher wird die lettische Datenschutzbehörde diesbezüglich 2013 Empfehlungen ausarbeiten.)

Informationen über Sensibilisierungsmaßnahmen

Die Datenschutzbehörde organisierte mehrere Seminare zu Themen rund um den Schutz personenbezogener Daten, die sich an unterschiedliche Zielgruppen richteten, wie z. B. Bildungseinrichtungen, kommunale Regierungsinstitutionen, Vertreter aus dem Bank- und Finanzwesen, medizinische Fachkräfte usw. Die Datenschutzbehörde bietet Seminare an, die allen Interessierten offenstehen.

Pro Woche gehen mindestens vier Medienanfragen zu verschiedenen Datenschutzthemen ein. Die Aufmerksamkeit der Medien galt außerdem den Angelegenheiten, mit denen sich die Artikel-29-Datenschutzgruppe befasst, sowie dem Ergebnis der gemeinsamen Ermittlungen der baltischen Staaten im Zusammenhang mit der Verarbeitung personenbezogener Daten.

Da zahlreiche Kontrollaktivitäten im Zusammenhang mit Treuekarten durchgeführt wurden, erhielten wir diesbezüglich Unterstützung vonseiten der Medien, indem die Öffentlichkeit dazu ermutigt wurden, ihre personenbezogenen Daten als Wertsachen anzusehen und sorgfältiger zu beurteilen, in welchen Fällen personenbezogene Daten nicht an Personen/Unternehmen weitergegeben werden sollten, wenn diese sie anfragen.

Organisation	Lettische Datenschutzbehörde (Datu valsts inspekcija)
Vorsitz und/oder Gremium	Vorsitzende: Signe Plūmiņa
Budget 2012	266 907 LVL (rund 370 457 EUR)
Personal	19 (einschließlich des Verwaltungs- und Instandhaltungspersonals)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Bzgl. Statistiken zu Beschlüssen und Stellungnahmen: k. A. Bzgl. Empfehlungen: 2012 wurden keine Empfehlungen abgegeben; für 2013 sind zwei Empfehlungen geplant
Meldungen	352 (einschließlich der Meldungen von Änderungen der Verarbeitung personenbezogener Daten)
Vorabprüfungen	234; mit Schwerpunkt auf den (für jedes Jahr festgelegten) Risikobereichen, wie z. B. die Verarbeitung sensibler Daten, die Verarbeitung biometrischer Daten (einschließlich Videoüberwachung) und die Übermittlung personenbezogener Daten an Drittländer.

Anträge betroffener Personen	k. A.
Beschwerden betroffener Personen	Gesamtzahl der Prüfungen: 496 (80 % der Prüfungen wurden aufgrund erhaltener Beschwerden durchgeführt). 4 Beschwerden betroffener Personen aus Drittländern bezüglich der Verarbeitung ihrer personenbezogenen Daten im Rahmen des SIS. 11 Beschwerden im Zusammenhang mit SPAM (diesbezüglich wurden 11 Prüfungen durchgeführt).
Vom Parlament bzw. der Regierung angeforderte Beratung	Bezüglich zahlreicher Rechtsakte, wie z. B. des Gesetzentwurfs zur Kreditauskunftei, des Gesetzentwurfs zur Schuldenbeitreibung und der Änderung des Gesetzes über das Schengener Informationssystem.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Im Rahmen der telefonischen Konsultation lauteten die häufigsten Fragen der Anrufer wie folgt: 1. Gelten bestimmte Informationen als personenbezogene Daten? 2. Wer kann wo zu welchem Zeitpunkt Videoüberwachung durchführen? 3. Wie kann man gegen die rechtswidrige Verarbeitung personenbezogener Daten im Internet vorgehen? 4. Die Verarbeitung personenbezogener Daten im Rahmen von Inkassoverfahren. 5. Wie können betroffene Personen ihr Recht auf Datenschutz besser wahrnehmen?
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Ein Großteil der Personen, die sich an die lettische Datenschutzbehörde wandten, meldete einen potenziellen Verstoß gegen das Datenschutzgesetz in den folgenden Bereichen (ähnlich dem Vorjahr): 1) die Verarbeitung personenbezogener Daten im Internet (auch in Fällen, in denen der für die Verarbeitung Verantwortliche keine angemessenen technischen Maßnahmen zum Schutz der Daten vorgesehen hat); 2) die Verarbeitung personenbezogener Daten im Zusammenhang mit Schuldenbeitreibung und Bonitätsprüfungen; 3) Identitätsdiebstahl: Rechtswidrige Verarbeitung personenbezogener Daten nach der Bereitstellung ebendieser (zahlreiche Fälle, bei denen der staatlichen oder kommunalen Polizei bei mehreren Ordnungswidrigkeiten die falschen Daten gegeben wurden); 4) Datenverarbeitung durch interne Wartungsfirmen; 5) Videoüberwachung.

Sanktionsmaßnahmen	
Sanktionen	Die von der Datenschutzbehörde verhängten Sanktionen werden gemäß dem Lettischen Ordnungswidrigkeitsgesetzbuch verhängt.
Geldbußen	Es wurden Geldbußen in Höhe von bis zu 18 910 LVL (ca. 26 119 EUR) verhängt. Der höchste Betrag belief sich auf 2 000 LVL (ca. 2 762 EUR) und wurde einem Inkassounternehmen wegen der rechtswidrigen Verarbeitung personenbezogener Daten und der unterlassenen Inkenntnissetzung einer betroffenen Person auferlegt. Zwei Bußgelder wurden im Zusammenhang mit der Verarbeitung personenbezogener Daten im Rahmen des SIS erhoben.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	12 registrierte Datenschutzbeauftragte.

B. Rechtsprechung

Im Jahr 2012 nahm die Anzahl der Fälle von Verletzungen des Datenschutzgesetzes zu, die dem Strafrecht unterliegen. Daher wurden diese Fälle der Staatsanwaltschaft übergeben. Des Weiteren erhöhte sich die Anzahl der Fälle, bei deren Ermittlungen die Notwendigkeit bestand, mit Datenschutzbehörden anderer EU-Länder zusammenzuarbeiten.

LITAUEN

A: Zusammenfassung der Aktivitäten und Neuerungen

Am 30. Januar 2012 wurde der Europäische Datenschutztag gefeiert. Im Seimas der Republik Litauen fanden an diesem Tag eine Pressekonferenz und Aktivitäten zum Thema „Datenschutz und moderne Technologien" statt. Am 7. Februar 2012 wurde der Datenschutztag im Lyzeum Vilnius begangen. Ziel des Tages war es, auf die Bedrohungen für personenbezogene Daten bei der Nutzung moderner Technologien aufmerksam zu machen. Die Hauptzielgruppe waren Schüler des Lyzeums sowie die Allgemeinheit.

Im März 2012 kamen die Datenschutzbehörden Estlands, Lettlands und Litauens in Estland zusammen, um die Zusammenarbeit der baltischen Staaten zu beginnen. Während der Sitzung wurde beschlossen, gemeinsam gegen internationale Unternehmen zu ermitteln, die in allen drei Ländern tätig sind. Es wurden Informationen zu wichtigen geplanten Aktivitäten und die Prioritäten der Institutionen für das Jahr 2012 ausgetauscht. Außerdem wurden wichtige Fragen zur bevorstehenden Schengen-Evaluierung und zur Reform des EU-Datenschutzes besprochen. Des Weiteren wurde beschlossen, derartige Sitzungen jährlich zu wiederholen.

Infolge der Sitzung von 2012 wurden in allen drei Ländern in Hotels der internationalen Kette Radisson Blue Untersuchungen durchgeführt. Dabei wurde überprüft, ob die Verarbeitung der personenbezogenen Daten von Hotelgästen zu Unterbringungszwecken rechtmäßig erfolgt. Bei den Ermittlungen wurden zahlreiche Unvereinbarkeiten mit den Datenschutzanforderungen aufgedeckt und den Hotels entsprechend Anordnungen erteilt.

Die SDPI organisierte gemeinsam mit der Aktiengesellschaft Expozona die Konferenz „Die Verarbeitung personenbezogener Mitarbeiterdaten und die Offenlegung von Daten an Dritte", die am 19. Mai 2012 stattfand. Die Veranstaltung war dem 15. Jubiläum der SDPI gewidmet und richtete sich an Unternehmen, Institutionen, Organisationen, Manager, Juristen und Fachkräfte, die für die Verarbeitung personenbezogener Mitarbeiterdaten verantwortlich sind.

Am 14. Juni 2012 unterzeichneten der Litauische Unternehmensverband und die SDPI ein Kooperationsabkommen, dessen Ziel es ist, eine effektivere und konstruktivere Zusammenarbeit zwischen Unternehmen und öffentlichen Einrichtungen beim Schutz personenbezogener Daten zu erzielen. Eine stärkere Zusammenarbeit trägt zur Prävention von Verstößen gegen das Gesetz zum Schutz personenbezogener Daten der Republik Litauen (nachfolgend „Datenschutzgesetz") bei und ermutigt Unternehmen, sich an die Datenschutzvorschriften zu halten.

Organisation	Litauische Datenschutzbehörde
Vorsitz und/oder Gremium	Dr. Algirdas Kunčinas
Budget	Zugewiesen und ausgegeben: 2 001 Mio. LTL (579 530 EUR)
Personal	30
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	k. A.
Meldungen	1 258
Vorabprüfungen	308

Anfragen von Bürgern	15
Beschwerden von Bürgern	324
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	4 008 Konsultationen; 103 öffentliche Mitteilungen; 3 Zusammenfassungen der Ergebnisse der Untersuchungen von Beschwerden und der Rechtsprechung; 99 Schlussfolgerungen zu Dokumenten der EU und des Europarates; 108 Antworten auf Anfragen von Parteien im Zusammenhang mit dem Übereinkommen (ETS Nr. 108); 277 koordinierte Rechtsakte und Dokumente von für die Datenverarbeitung Verantwortlichen; 6 vorbereitete Rechtsakte; 4 öffentliche Konsultationen.
Prüfmaßnahmen	
Prüfungen	45 (Zulässigkeit der Verarbeitung von Daten, Umfang von Internet-Shops und die Rechte von betroffenen Personen, öffentliche Versorgungseinrichtungen).
Sanktionsmaßnahmen	
Sanktionen	Die SDPI erstellte 37 Protokolle zu Verwaltungsverstößen.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Verarbeitung personenbezogener Daten im Zusammenhang mit Leitern von juristischen Personen

Die SDPI erhielt eine Beschwerde mit der Frage, ob es für Verbände eine Rechtsgrundlage gebe, nach der sie Journalisten Informationen über die Höhe der Schulden, die der Beschwerdeführer bei den Verbänden hatte, weiterleiten dürften, die anschließend in der Zeitung veröffentlicht wurden. Die SDPI stellte fest, dass die in der Zeitung veröffentlichten Informationen sich lediglich auf den Beschwerdeführer als Geschäftsführer des Unternehmens bezogen und dies demnach nicht dem Datenschutzgesetz unterliege. Dieser Beschluss wurde vom Beschwerdeführer vor dem Bezirksverwaltungsgericht Vilnius angefochten. Das Gericht lehnte dies als unbegründet ab und kam zu dem Schluss, dass die Daten zum Unternehmen, wie z. B. der Name des Geschäftsführers, als Daten einer juristischen Person erachtet werden müssen. Der Beschwerdeführer legte gegen diese Entscheidung beim obersten Verwaltungsgericht Berufung ein, doch auch dieses Gericht urteilte, dass die Daten als Daten einer juristischen Person erachtet werden müssen, die der Öffentlichkeit frei zugänglich sind, und demnach nicht gegen das Datenschutzgesetz verstoßen wurde, das die Verarbeitung von Daten natürlicher Personen regelt.

Veröffentlichung personenbezogener Daten im Internet zu präventiven Zwecken

Die SDPI hat ein Protokoll mit Ordnungswidrigkeiten des Försters eines Forstunternehmens (im Folgenden „Unternehmen“) ausgearbeitet, das auf seiner Website die personenbezogenen Daten von Einzelpersonen (Vorname, Nachname, vollständige Adresse und Informationen über das an die Einzelperson ausgestellte Ordnungswidrigkeitsprotokoll, das jedoch zu der Zeit nicht wirksam war) veröffentlichte, ohne dass es dafür eine Rechtsgrundlage gemäß Artikel 5 des Datenschutzgesetzes oder sonstiger Kriterien einer rechtmäßigen Veröffentlichung der erwähnten Daten gegeben hätte. Das Bezirksgericht schloss den Fall, ohne das Unternehmen für schuldig befunden zu haben. Das Gericht kam zu dem Schluss, dass die oben erwähnten Daten im berechtigten Interesse einer Prävention veröffentlicht worden seien, da Artikel 254 des Verwaltungsgesetzes der Republik Litauen es vorsehe, Ordnungswidrigkeiten öffentlich zu machen. Um die aufklärenden und präventiven Aspekte solcher Fälle hervorzuheben, können diese direkt bei Arbeitskollektiven, der Lernstätte der verwaltungsrechtlich haftbaren Person oder dem Wohnsitz in Erfahrung gebracht werden.

Das Oberste Verwaltungsgericht öffnete auf Antrag der SDPI erneut das Verfahren und schloss aus, dass in diesem Fall eine Offenlegung personenbezogener Daten gegen das Datenschutzgesetz verstoße. Das Gericht nahm zur Kenntnis, dass eine Prävention von Ordnungswidrigkeiten eine mögliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstelle. Eine Jury kam jedoch zu dem Schluss, dass bei einer Abwägung zwischen dem Ziel der Offenlegung und der Art der veröffentlichten personenbezogenen Daten und der Vollständigkeit der Daten sowie aufgrund der Tatsache, dass Daten von Protokollen veröffentlicht wurden, die noch nicht wirksam waren, und trotz der Tatsache, dass die Person gegen das betreffende Gerichtsprotokoll Berufung eingelegt hatte, diese weiterhin veröffentlicht wurden, das öffentliche Interesse an der Prävention von Ordnungswidrigkeiten in diesem Fall nicht über dem Recht auf Datenschutz des Einzelnen steht. Das Oberste Verwaltungsgericht entschied, dass unter diesen Umständen die präventive und aufklärende Funktion auch ohne derart detaillierten personenbezogenen Daten (Vorname, Nachname und Anschrift des Wohnsitzes) erfüllt werden könne. Insbesondere der Wohnsitz stehe im Allgemeinen nicht mit der Ordnungswidrigkeit im Zusammenhang und habe keinerlei aufklärende Wirkung, wodurch die Veröffentlichung der Anschrift als übertrieben einzustufen sei. Die Veröffentlichung des Vor- und Nachnamens einer Person betreffe lediglich die betroffene Person selbst. Für die Öffentlichkeit haben Informationen, die auf die Unvermeidbarkeit der Verantwortung und die Tatsache hinweisen, dass das Vergehen strafbar ist und welche Strafen die Person erhält, eine präventive und aufklärende Auswirkungen

LUXEMBURG

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetzesänderungen

Im Jahr 2012 gab es keine Gesetzesänderungen auf dem Gebiet des Datenschutzes.

Wichtige Themen

Die CNPD beriet die luxemburgische Regierung durch Stellungnahmen zu vielen verschiedenen Gesetzen und Regulierungen, zu denen sie konsultiert wurde. Die wichtigsten Themen des Jahres 2012 waren:

- die Einrichtung einer nationalen Schülerdatenbank durch das Bildungsministerium;
- das nationale Register natürlicher Personen, das Bevölkerungsregister der Gemeinden und die elektronische ID-Karte;
- das nationale Krebsregister;
- die Reform des Gesetzes über das Strafregister;
- das Gesetz zur Überschuldung;
- die Einführung eines elektronischen Petitionssystems für das luxemburgische Parlament.

Neuerungen

Die luxemburgische Datenschutzbehörde musste 2012 mehrere Male die Einhaltung des Datenschutzgesetzes überprüfen. Bei einem Fall kam es zu einem unbefugten Zugriff auf eine Datenbank des Sportministeriums, in der die personenbezogenen Daten von über 48 000 Menschen erfasst sind. In einem weiteren Fall prüfte die CNPD, ob die Aufbewahrungsfristen für bereits gespeicherte Fotos von Bürgern beim Ersatz ihrer defekten ID-Karten eingehalten wurden. Im Dezember 2012 wurden die CNPD und CNIL (Frankreich) von der Artikel-29-Datenschutzgruppe dazu eingeladen, die Analyse der Servicevereinbarung und der Online-Datenschutzrichtlinie von Microsoft zu leiten.

Wichtige Veranstaltungen und Sensibilisierung

Die CNPD organisierte die Frühjahrskonferenz der europäischen Datenschutzbehörden, die vom 2. bis 4. Mai 2012 in Luxemburg stattfand. An der Konferenz nahmen 138 Datenschutzbeauftragte aus 38 Ländern sowie Vertreter der Europäischen Kommission, des Europarats und der OECD teil. Das Thema lautete: *„Die Reform des EU-Datenschutzes: Wird sie den Erwartungen gerecht?"*. Die Veranstaltung bot die Gelegenheit, darüber zu diskutieren, wie die Modernisierung des EU-Rechtsrahmens den Datenschutz der Bürger im digitalen Zeitalter und in einer globalisierten Welt verbessern soll und welche Maßnahmen zur Vorbereitung dieser Änderungen ergriffen werden müssen.

Neben dieser großen Veranstaltung nahm die luxemburgische Datenschutzbehörde an zahlreichen Sensibilisierungsveranstaltungen teil, die an die breite Öffentlichkeit gerichtet waren, wie z. B. der Europäischer Datenschutztag mit dem Motto *Votre vie privée n'est pas privée de droits (*Ihre Privatsphäre ist kein gesetzloser Raum*).* Die CNPD nahm außerdem an zahlreichen Seminaren und Schulungen teil, um auch das Fachpublikum stärker für das Thema Datenschutz zu sensibilisieren.

Organisation	Nationale Datenschutzbehörde (Commission nationale pour la protection des données, CNPD)
Vorsitz und/oder Gremium	Gérard LOMMEL, Vorsitzender Thierry LALLEMANG, Beauftragter Pierre WEIMERSKIRCH, Beauftragter
Budget	1 636 000 EUR
Personal	Gremium: 3 Rechtsabteilung: 5 Meldungen und Vorabprüfungen: 2 Allgemeine Verwaltung: 3 Kommunikation und Dokumentation: 1 IT und Logistik: 1 Gesamt: 15
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	438
Meldungen	586
Vorabprüfungen	423
Anträge betroffener Personen	228
Beschwerden betroffener Personen	133
Vom Parlament bzw. der Regierung angeforderte Beratung	6
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Treffen und Konsultationen (öffentlicher/privater Sektor) 132 Informationssitzungen und Konferenzen: 10 Verbindliche unternehmensinterne Vorschriften als leitende Datenschutzbehörde: 2
Prüfmaßnahmen	
Prüfungen, Untersuchungen	18
Sanktionsmaßnahmen	

Sanktionen	0
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Im Laufe des Jahres 2012 ernannte DPO: 11 (Zum Zeitpunkt der Erstellung des Berichts) insgesamt ernannte DPO: 47

B. Rechtsprechung

Bezirksgericht Luxemburg, 13. Strafgerichtskammer (1. Februar 2012, Nr. 534/2012) zur Gültigkeit von Videoüberwachungsbildern, die ohne eine vorherige Genehmigung durch die CNPD aufgezeichnet wurden.

Diese Rechtssache bezog sich auf einen Unfall mit Fahrerflucht in einem Tunnel, der von Überwachungskameras aufgezeichnet wurde, für die zuvor keine Genehmigung eingeholt worden war. Der Strafverteidiger des Beklagten plädierte vor der Streitsache dafür, dass die Videoaufnahmen des Unfalls nicht als Beweismittel zugelassen werden dürften, da für die Überwachung zuvor bei der CNPD keine Genehmigung eingeholt worden war.

Das Gericht urteilte, dass die Bilder dennoch als Beweismittel zugelassen werden. Abschließend zu dieser Angelegenheit führte das Gericht eine Analyse der Bedingungen für Rechtmäßigkeit besagter Überwachung durch und bezog sich eindeutig auf den im luxemburgischen Datenschutzgesetz vorgesehenen Zwecktest.

Im Gegensatz zu dem Fall, über den 2009 berichtet wurde (Bezirksgericht Luxemburg, 9. Strafkammer, Nr. 387/2009) und den die CNPD als höchst abträglich einstufte, da er auf vage juristische Konzepte der eigenen Überzeugung des Richters beruhte, führt dieser neue Fall eine transparentere und korrektere Methode zur Analyse der Gültigkeit von Beweismitteln ohne vorherige Genehmigung durch die CNPD ein.

MALTA

A: Zusammenfassung der Aktivitäten und Neuerungen:

Während des Berichtszeitraums wurden am Datenschutzgesetz keinerlei Änderungen vorgenommen. Es wurde jedoch ein Rechtsverordnungsentwurf erstellt, in dem der 1. Januar 2013 als Datum genannt wurde, zu dem alle Vorkehrungen der Rechtsverordnung 239 von 2011 in Kraft treten. Mit dieser Verordnung wird die Datenschutzrichtlinie für elektronische Kommunikation 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 in maltesisches Recht umgesetzt. Die Datenschutzbehörde stieß die Erstellung von Ad-hoc-Leitlinien an, um für die Datenerarbeitung Verantwortlichen bezüglich der Umsetzung der Anforderung zur Zustimmung zu Cookies die notwendige Orientierung bereitzustellen.

Das Gesetz zur Informationsfreiheit (Kapitel 496 der Gesetze von Malta) wurde 2008 vom Parlament verabschiedet. Der Zweck dieses Gesetzes ist die Einführung des Rechts auf Informationen, die von öffentlichen Stellen gespeichert werden, mit dem Ziel, die Transparenz und die Verantwortlichkeit der Regierung zu fördern. Das Gesetz trat am 1. September 2012 vollständig in Kraft und stattete den Datenschutzbeauftragten mit zusätzlichen Verantwortlichkeiten aus, wie z. B. die Befugnis, Anträge auf eine Überarbeitung von Entscheidungen öffentlicher Stellen entgegenzunehmen und über diese zu entscheiden; öffentlichen Stellen Vollzugsmitteilungen auszustellen, damit diese seinen Beschlüssen Folge leisten; sowie die Einhaltung des Datenschutzgesetzes zu fördern. Im Berichtszeitraum gingen beim Datenschutzbeauftragten drei Beschwerden ein, von denen sich zwei gegen die Polizei von Malta und eine gegen das ständige Sekretariat des Innenministeriums richtete.

Die Datenschutzbehörde setzte ihre Bemühungen fort, mit Vertretern verschiedener Sektoren zusammenzukommen, um Datenschutzfragen zu besprechen und nötige Leitlinien bereitzustellen. Mit zwei großen Kreditauskunfteien der Insel kam es zu einer Reihe von Besprechungen, infolge derer Leitlinien formuliert und angenommen wurden, um bewährte Methoden der Verarbeitung personenbezogener Daten durch Kreditinstitute zu fördern.

Im Jahr 2012 fühlten sich vier Personen durch den Beschluss des Datenschutzbeauftragten benachteiligt und legten vor dem Berufungsgericht für Datenschutz Berufung ein. Während eine Berufung nach der ersten Sitzung des Gerichts vom Berufungskläger zurückgezogen wurde, war das Verfahren der zweiten Berufung zum Jahresende nach wie vor anhängig. In den beiden anderen Fällen entschied das Gericht zugunsten des Datenschutzbeauftragten und lehnte die Berufungsklagen ab. Diese Entscheidungen wurden als endgültig und rechtskräftig erachtet, da keine Partei die Beschlüsse innerhalb des gesetzlich vorgeschriebenen Zeitraums von 30 Tagen vor dem Berufungsgericht angefochten hat.

Infolge der ersten Evaluierung durch den Datenschutzausschuss der Schengen-Evaluierung, die 2006 im Rahmen der Vorbereitungen Maltas auf den Beitritt zum Schengen-Raum erfolgte, wurde die Datenschutzbehörde im Juli von selbigem Ausschuss einer zweiten Evaluierung unterzogen. Sachverständige wurden bei der Datenschutzbehörde vorstellig, um die internen Abläufe und insbesondere die Ausübung der Aufsichtsfunktion des Datenschutzbeauftragten zu evaluieren. Es folgten Vorträge des Datenschutzbeauftragten, technischer Mitarbeiter und des Datenschutzbeauftragten des Außenministeriums. Das Ergebnis der Evaluierung wurde auf der Tagung des Rates der Arbeitsgruppe „Schengen-Evaluierung“ vorgelegt. Diese kam zu dem Schluss, dass die Datenschutzbehörde hinreichend auf die Ausübung der Rolle der Datenschutzaufsichtsbehörde für alle für die Verarbeitung Verantwortlichen, einschließlich der Polizei, ausgerichtet ist. Außerdem wurde eine minimale Anzahl von Empfehlungen abgegeben, denen die Datenschutzbehörde unverzüglich Folge leistete.

Am 28. Januar feierte die maltesische Datenschutzbehörde gemeinsam mit anderen Datenschutzbehörden in ganz Europa 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 jeher fest davon überzeugt, dass fortlaufend in Bildung und die Sensibilisierung der jungen Generation investiert werden muss, um eine effektive kulturelle Veränderung zu ermöglichen.

Zu weiteren Sensibilisierungsmaßnahmen der Datenschutzbehörde im Berichtszeitraum gehörten Vorträge vor verschiedenen Verantwortlichen aus einer Reihe von Sektoren der maltesischen Gesellschaft, die Teilnahme an regionalen Fernseh- und Radioprogrammen mit Zuschauer-/Hörerbeteiligung 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	Amt des Informations- und Datenschutzbeauftragten
Vorsitz und/oder Gremium	Informations- und Datenschutzbeauftragter
Budget	rund 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 48 Beschlüsse veröffentlicht. Darüber hinaus wurden 23 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	228 neue Meldungen
Vorabprüfungen	5 Anträge auf Vorabprüfung
Anträge betroffener Personen	Anfragen per Telefon – durchschnittlich 10 Anrufe pro Tag Anfragen per E-Mail: 156
Beschwerden betroffener Personen	72 Beschwerden

Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	8 Prüfungen wurden in Bezug auf Untersuchungen von Beschwerden betroffener Personen und Routineprüfungen der Polizeisysteme, insbesondere SIS und Europol, durchgeführt.
Sanktionsmaßnahmen	
Sanktionen	Es wurden offizielle Verwarnungen an für die Datenverarbeitung Verantwortliche ausgesprochen. Es wurden keine Gerichtsverfahren eingeleitet.
Geldbußen	Es wurden keine Geldbußen auferlegt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Es wurden 12 Datenschutzbeauftragte ernannt.

B. 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 insgesamt 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, verwendet 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 2012 u. a. auf folgenden Bereichen: Profiling, angemessener Schutz medizinischer Daten und Datensicherheit.

Eine der wichtigsten Ermittlungen des Jahres 2012 betraf das Profiling durch eine große Supermarktkette in den Niederlanden. Aus öffentlichen Äußerungen des Einzelhändlers wurden Pläne ersichtlich, Kunden personalisierte Angebote auf Grundlage einer Analyse ihrer Kaufhistorie zu unterbreiten. Diesbezüglich wollte die Kette die Daten nutzen, die für alle Käufe mit der Treuekarte des Kunden erfasst wurden. Nach den Ermittlungen kam die niederländische Datenschutzbehörde zu dem Schluss, dass die Einwilligung, die der Einzelhändler von seinen Kunden eingeholt hatte, ungültig sei, u. a. aufgrund eines Mangels an Informationen zur Datenerfassung und der darauffolgenden Analysen. Infolge der Ermittlungen beschloss der Einzelhändler, die Einführung der personalisierten Angebote aufzuschieben. In der Zwischenzeit hat der Einzelhändler die Datenschutzrichtlinie und die allgemeinen Geschäftsbedingungen aktualisiert und wird die Einwilligung seiner Kunden erneut einholen.

Im Jahr 2012 wurde infolge eines Aufruhrs unter der Bevölkerung bezüglich einer Fernsehsendung, die den Alltag der Notaufnahme eines großen Amsterdamer Krankenhauses zeigen sollte, eine weitere Ermittlung durchgeführt. Für die Sendung wurden sowohl Patienten als auch Mitarbeiter während ihres Aufenthalts in der Notaufnahme gefilmt. Sobald das Fernsehteam die „Fälle“ der Patienten als für eine Ausstrahlung interessant genug befunden hatte, wurden sie um ihre Einwilligung gebeten, das Videomaterial für die Übertragung zu nutzen und weitere Aufnahmen zu machen. In Anbetracht des Drehortes – ein Krankenhaus – wurden während der Dreharbeiten hauptsächlich medizinische Daten besprochen, die besondere Aufmerksamkeit erforderten. Die niederländische Datenschutzbehörde kam zu dem Schluss, dass die erforderliche Einwilligung vom Fernsehteam aus verschiedenen Gründen nicht rechtmäßig eingeholt worden war. Erstens wurde die Einwilligung nicht vor dem Beginn der Datenverarbeitung eingeholt, da die Aufnahmen vom Augenblick des Betretens der Notaufnahme durch die Patienten und das Team begannen. Zweitens waren die Informationen, die den Patienten zur Entscheidung in voller Kenntnis der Sachlage bereitgestellt wurden, unzureichend. Schließlich würden die Patienten angesichts der Tatsache, dass im Allgemeinen in einer Notlage in die Notaufnahme kommen, derart von den Diensten des Krankenhauses abhängen, dass sie nach Ansicht der niederländischen Datenschutzbehörde auch in voller Kenntnis der Sachlage niemals eine selbstbestimmte Einwilligung erteilen könnten.

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. Im Jahr 2012 beriet die Datenschutzbehörde im Hinblick auf den Vorschlag einer zusätzlichen Mieterhöhung für Haushalte mit mittlerem Einkommen (zwischen 33 000 EUR und 43 000 EUR pro Jahr). Für diese Mieter würde dies eine jährliche Mietpreiserhöhung in Höhe der Inflation plus einem Prozent bedeuten. Um zu beurteilen, bei welchen Mietern ein solcher

Mietpreisanstieg wirksam werden würde, würde die Steuerbehörde Daten zur Einkommenshöhe der Mieter an die Vermieter übermitteln. Die niederländische Datenschutzbehörde teilte mit, dass der Vorschlag in ihren Augen nicht ausreichend motiviert ist und nicht den Grundsätzen der Verhältnismäßigkeit und Subsidiarität entspricht. Die Regierung konnte nicht zeigen, in welchem Ausmaß dieser Verstoß gegen das Grundrecht auf Datenschutz zu einer höheren Verfügbarkeit von Mietwohnungen beitragen würde (der festgestellte Zweck des Gesetzentwurfs) und weshalb nicht andere, weniger in die Privatsphäre eingreifende Maßnahmen ähnliche Ergebnisse liefern würden.

Organisation	Niederländische Datenschutzbehörde
Vorsitz und/oder Gremium	Jacob Kohnstamm, Vorsitzender Wilbert Tomesen, Datenschutzbeauftragter und Vizevorsitzender Madeleine McLaggan-Van Roon, Datenschutzbeauftragte* Madeleine McLaggan wurde für den Zeitraum, in dem sie auf Anfrage des Staatssekretärs für Sicherheit und Justiz einen wissenschaftlichen Bericht zu den Beziehungen zwischen Wettbewerbsrecht und Datenschutz erstellt, von ihren Aufgaben als Datenschutzbeauftragte der niederländischen Datenschutzbehörde befreit.
Budget	Zugewiesen: 7 679 000 EUR Ausgegeben: 7 746 000 EUR
Personal	75,8 Vollzeitmitarbeiter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	213 (Untersuchungen, Leitlinien, Verhaltensregeln, Vorabprüfungen, Sanktionen und Beratung zu Gesetzgebungsverfahren)
Meldungen	5 966
Vorabprüfungen	93
Signale ([8]) betroffener Personen	6 042
Vom Parlament bzw. der Regierung angeforderte Beratung	42
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	58

([8]) Seit April 2011 werden alle Bürgerkontakte als Signale registriert. Diese Signale dienen der Priorisierung unserer Aufgaben. Daher werden Signale nicht anhand der Art und Weise, wie sie bei der Datenschutzbehörde eingehen, sondern anhand der betroffenen Sektoren registriert.

Sanktionsmaßnahmen	
Sanktionen	12
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	345 ([9])

B. Rechtsprechung

Während des Berichtszeitraums befassten sich die niederländischen Gerichte mit mehreren Rechtssachen im Zusammenhang mit dem Datenschutz. In einer der Rechtssachen befand das Amsterdamer Gericht, dass ein Buch als Datei im Sinne des Datenschutzgesetzes erachtet werden kann, wenn es ein Personenregister umfasst. In einer Rechtssache im Zusammenhang mit der Höhe der fälligen Miete für bestimmte Arten von Unterkünften urteilte das Gericht in Den Haag, dass das niederländische Datenschutzgesetz vollständig unter Berücksichtigung des Artikels 8 EMRK (Recht auf Schutz der Privatsphäre) gelesen werden müsse. Verhältnismäßigkeit und Subsidiarität müssten zu jeder Zeit berücksichtigt werden, auch bezüglich des Zwecks der vorgeschlagenen Maßnahme, und dürften bei einem ministeriellen Beschluss nicht ignoriert werden.

In einer Rechtssache von 2012 war ein Beschluss der niederländischen Datenschutzbehörde Gegenstand eines Verfahrens vor dem Rotterdamer Gericht. Der zu Rotterdam gehörende Bezirk Charlois hatte eine verpflichtende Registrierung des Geburtslandes eingeführt, um eine sogenannte Präferenzbehandlung umzusetzen und Kinder mit Problemen zu unterstützen (schlechte Leistungen in der Schule, frühe kriminelle Tendenzen, Misshandlung usw.).[10] Angesichts der Tatsache, dass die meisten Kinder mit Problemen einen Migrationshintergrund haben, erachtete es der Bezirk als hilfreich, potenzielle problematische Situationen unter Berücksichtigung des Geburtslandes abzuschätzen. Die niederländische Datenschutzbehörde befand jedoch, dass dies einem „Racial-Profiling“ gleichkomme und demnach eine Verarbeitung sensibler Daten darstelle. Da es für solch eine Verarbeitung keine Rechtsgrundlage gab, wies die niederländische Datenschutzbehörde den Bezirk an, die Registrierung des Geburtslandes einzustellen, und drohte eine bedingte Geldbuße in Höhe von 2 000 EUR pro Tag an, falls die Verarbeitung fortgesetzt werde. Der Bezirk legte Berufung ein, verlor das Verfahren jedoch. Die umstrittene Verarbeitung ist inzwischen eingestellt worden.

([9]) Stand: September 2013.

([10]) Siehe auch 15. Jahresbericht 2011.

ÖSTERREICH

A. Neue Entwicklungen und Aktivitäten

Im Berichtszeitraum wurde im Parlament die **Verwaltungsgerichtsbarkeits-Novelle 2012** beschlossen. ([11]) Diese Novelle zum Bundes-Verfassungsgesetz (B-VG) 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. Im Fall der Datenschutzkommission war dies in dieser Form nicht möglich, da schon aufgrund des Artikel 28 der Richtlinie 95/46/EG nach Auflösung der Datenschutzkommission eine neue Datenschutzbehörde gegründet werden muss, der die Aufgaben der Datenschutzkommission übertragen werden. Eine entsprechende Novelle zum Datenschutzgesetz 2000 (so genannte „DSG-Novelle 2014') ([12]) sieht auch dementsprechend die Neueinrichtung einer **monokratischen Datenschutzbehörde** vor, die an die Stelle der Datenschutzkommission tritt. Weiter ist ein Rechtszug von der Datenschutzbehörde an das (ebenfalls ab 2014 neu gegründete) Bundesverwaltungsgericht vorgesehen.

Im Berichtzeitraum wurde das **„Elektronische Gesundheitsakte-Gesetz' (ELGA-G)** beschlossen. Eine wesentliche Rolle bei der Entstehung des Gesetzes spielte dabei das Arbeitspapier der Artikel 29 Gruppe WP 131 zur Verarbeitung von Patientendaten in elektronischen Patientenakten (EPA) aus dem Jahr 2007, dem in weiten Teilen entsprochen wird. Allerdings sieht das Gesetz — teilweise abweichend von dem in WP 131 beschriebenen nach Sensibilität der Daten abgestuften System — ein durchgängiges Opt-out-System vor.

Zum **Europäischen Datenschutztag 2012** wurde - inzwischen schon einer Tradition folgend - gemeinsam mit dem Datenschutzrat und dem Bundeskanzleramt eine Veranstaltung abgehalten, die dem neuen **Datenschutz-Paket der EU** gewidmet war. Die Veranstaltung fand knapp nach der Präsentation der Entwürfe einer Datenschutz-Grundverordnung und einer Richtlinie für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen durch die Europäische Kommission statt und gewann dadurch an besonderer Aktualität.

In den Berichtszeitraum fiel auch das **Urteil des EuGH zur Unabhängigkeit der Kontrollstelle** in Österreich ([13]), mit dem der EuGH die Republik Österreich wegen mangelnder Unabhängigkeit der Datenschutzkommission verurteilte. Im Wesentlichen wurde eine zu große Verflechtung der Geschäftsstelle der Datenschutzkommission mit dem Bundeskanzleramt, die Stellung des geschäftsführenden Mitglieds (es bestehe zumindest der Anschein der Abhängigkeit vom Bundeskanzleramt) und die zu weit gehende Berichtsverpflichtung der Datenschutzkommission gegenüber dem Bundeskanzler gerügt. ([14])

Organisation	Österreichische Datenschutzkommission
Vorsitz und/oder Gremium	Vorsitz: Dr. Anton SPENLING Geschäftsführendes Mitglied: Dr. Eva SOUHRADA-KIRCHMAYER Gremiumsmitglieder: Dr. Anton SPENLING, Dr. Eva SOUHRADA-KIRCHMAYER, Mag. Helmut HUTTERER, Dr. Claudia ROSENMAYR-KLEMENZ, Dr. Klaus HEISSENBERGER, Mag. Daniela ZIMMER

([11]) BGBl I 51/2012 .

([12]) BGBl. I Nr. 83/2013.

([13]) EuGH 16.10.2012, Rs C-614/10, Kommission/Österreich.

([14]) Der Gesetzgeber hat als Reaktion auf dieses Urteil die „DSG-Novelle 2013", BGBl. I Nr. 57/2013, erlassen, wodurch die Datenschutzkommission als eigene Dienstbehörde und Personalstelle eingerichtet wurde.

Budget	Kein eigenes Budget im Jahr 2012. Die Ausgaben werden aus dem Budget des Bundeskanzleramts gedeckt.
Personal	Bis November 2012 20,65 Vollzeitstellen (16 Vollzeit- und 8 Teilzeitbeschäftigte), ab Mitte November 2012 21,65 Stellen.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	149 formale Beschlüsse (Beschwerden), 246 Fälle für den Bürgerbeauftragten, 2 Empfehlungen und 61 Genehmigungen (Datenübermittlung in Drittländer, Forschung und Gutachten).
Meldungen	6 197
Vorabprüfungen	3 393
Anträge betroffener Personen	Schriftlich: 940 Telefonisch: nicht schriftlich dokumentiert
Beschwerden betroffener Personen	Beschwerden, denen eine formale Entscheidung folgte: 149 Beschwerden, denen eine Klärung oder Empfehlung folgte: 246
Vom Parlament bzw. der Regierung angeforderte Beratung	Diese Aufgabe fällt in die Zuständigkeit zweier anderer Institutionen: des Datenschutzrats und der Rechtsabteilung der Regierung im Bundeskanzleramt.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Es wurden 125 Millionen bereichsspezifische Personenkennzeichen herausgegeben. Des Weiteren wurden von der zur Datenschutzbehörde gehörenden E-Government-Registerbehörde über 5 000 neue Personen sowie rund 1,1 Mio. neue juristische Personen im Register für elektronische Identitäten registriert. Diese Behörde ist für das bereichsspezifische Identitätsmanagement des österreichischen E-Government zuständig.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	22, die meisten Fälle stehen im Zusammenhang mit Videoüberwachung.
Sanktionsmaßnahmen	
Sanktionen	Keine. Die österreichische Datenschutzbehörde kann keine Sanktionen verhängen.
Geldbußen	Keine. Die österreichische Datenschutzbehörde kann keine Geldbußen auferlegen.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Keine. Das österreichische Recht sieht keine Datenschutzbeauftragten vor.

B. Fallrecht

1. Videokamera auf PKW

Im Berichtsjahr wurde die Meldung einer Datenanwendung *„Videoüberwachung zum Zwecke des Schutzes des überwachten Objekts (Umgebung der Situation im unmittelbaren Bereich des eigenen, privat genutzten PKWs) bzw. der Erfüllung rechtlicher Sorgfaltspflichten, jeweils einschließlich der Beweissicherung, mit ausschließlicher Auswertung in dem durch die Zweckbezeichnung definierten Anlassfall, sofern bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt könnte das Ziel oder der Ort eines gefährlichen Angriffs werden"* von der Datenschutzkommission abgelehnt.

Der Antragsteller hatte diese Datenanwendung an das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister als Videoüberwachung (§§ 50a ff DSG 2000) zur Registrierung gemeldet. Als geplante Übermittlungsempfänger nannte der Meldungsleger „Zuständige Behörden bzw. zuständiges Gericht (zur Beweismittellieferung in Strafrechtsangelegenheiten)', „Sicherheitsbehörden (zu sicherheitspolizeilichen Zwecken)', „Gerichte (zur Beweismittellieferung in Zivilrechtsangelegenheiten)' und „Versicherungen (zur Abwicklung von Versicherungsfällen)'. Entsprechend zur Stellungnahme aufgefordert, gab der Antragsteller an, die Anwendung diene ausschließlich privaten (wie Videokameras auf der Kärntner Straße oder Sportler mit Helmkameras), also weder kommerziellen noch nicht-privaten Zwecken. Eine Videoüberwachung im Sinne einer systematischen, insbesondere fortlaufenden Feststellung von Ereignissen, die ein bestimmtes Objekt oder eine bestimmte Person betreffen, sei nicht gegeben. Im Anlassfall könnten die Aufnahmen aber zur Verfolgung von Straftaten verwendet werden. Es gebe kein konkretes Objekt, das erfasst werden solle. Private Aufnahmen könnten beliebig lang aufbewahrt werden, die Daten würden zyklisch überschrieben.

Die Datenschutzkommission hat in der Begründung ihres ablehnenden Bescheides ausgeführt, dass die gegenständliche Datenanwendung als Videoüberwachung anzusehen sei. Es handle sich um eine systematische (Aufzeichnung jeder Fahrt bzw. zumindest bestimmter Arten von Fahrten), insbesondere fortlaufende (Aufzeichnung der gesamten Fahrtstrecke) Feststellung von Ereignissen (Straßenverkehr um sein Fahrzeug), die ein bestimmtes Objekt (sein Fahrzeug) bzw. eine bestimmte Person (jedenfalls den Fahrzeuglenker) betreffe. Es handle sich auch nicht um eine ausschließliche Datenverwendung für persönliche oder familiäre Zwecke. Im gegenständlichen Fall sei die Überwachung des Verkehrs bzw. der Umgebung des eigenen Fahrzeugs von der erkennbaren Intention geprägt, Beweismaterial für die allfällige Übermittlung an Strafverfolgungsbehörden, Gerichte usw. zu generieren. Dies schließe die „ausschließliche' Verwendung für private Zwecke jedenfalls aus. Im Übrigen mangle es dem Antragsteller an der „gesetzlichen Zuständigkeit' oder „rechtlichen Befugnis', eine Videoüberwachung im öffentlichen Raum durchzuführen. Aufgrund des staatlichen Gewaltmonopols seien grundsätzlich nur die Sicherheitsbehörden zur Durchführung von Videoüberwachungen im öffentlichen Raum berechtigt und richtet sich deren Zulässigkeit nach den Anforderungen des Sicherheitspolizeigesetzes.

2. Die Datenschutzkommission hat in einer Empfehlung ein Unternehmen aufgefordert, es möge die Annahme der Allgemeinen Geschäftsbedingungen (und damit den Abschluss eines entsprechenden Vertrags) nicht von einer in den Allgemeinen Geschäftsbedingungen enthaltenen Zustimmungsklausel abhängig machen.

Der Einschreiter hatte ausgeführt, dass das Unternehmen in seinen allgemeinen Geschäftsbedingungen (AGB) in einer Klausel Zustimmungen von den Kunden für die Verwendung ihrer Daten u. a. für Gewinnspiele und Spendenaktionen einholt. Der Einschreiter sah sich im Ergebnis dadurch in seinem Recht auf Geheimhaltung verletzt, dass er durch die Einbindung dieser Zustimmungserklärung in die AGB den dort genannten Datenanwendungen zustimmen müsse.

Die Datenschutzkommission nahm dies zum Anlass, ein Verfahren nach § 30 DSG 2000 (Kontroll- und Ombudsmannverfahren) einzuleiten. Das Unternehmen vertrat die Meinung, dass die gegenständliche

Zustimmungserklärung trotz ihrer Einbettung in die AGB als „freiwillig' zu qualifizieren sei, da das der Zustimmungserklärung zugrunde liegende Angebot einen freiwilligen Produktbezug darstelle, für welchen sich der Betroffene frei entscheiden könne. Folglich sei die mit dem Produktbezug einhergehende Zustimmungserklärung frei von Zwang.

Die Datenschutzkommission hat (unter Zitierung verschiedener Kommentare und auch der Stellungnahme 15/2011 zur Definition der „Einwilligung' (iSd Datenschutz-Richtlinie 95/46/EG der Artikel 29 Datenschutzgruppe, WP 187) ausgeführt, dass es im hier zu beurteilenden Fall für den Kunden nicht möglich sei, den angestrebten Vertrag mit dem Unternehmen abzuschließen, ohne gleichzeitig die in einem Punkt der AGB enthaltene Zustimmungserklärung abzugeben. Dieser Umstand sei auch nach Ansicht der Datenschutzkommission mit dem Erfordernis der Freiwilligkeit iSd § 4 Z 14 DSG 2000 und § 8 Abs. 1 Z 2 DSG 2000 nicht vereinbar. Vielmehr müsse dem Kunden die Möglichkeit gegeben werden, den angestrebten Vertrag auch ohne die Abgabe der datenschutzrechtlichen Zustimmungserklärung abzugeben („Opt-in'-Lösung), etwa durch eine Gestaltung der AGB, bei der die Zustimmungserklärung gesondert anzuklicken sei.

POLEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Am 1. Januar 2012 trat das Gesetz über den Informationsaustausch zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union in Kraft (Gesetzblatt der Republik Polen von 2011 Nr. 230 Position 1371). Mit diesen Gesetz wurde der Rahmenbeschluss des Rates 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, teilweise in polnisches Recht umgesetzt. Des Weiteren wurden dadurch einige Bestimmungen des Gesetzes zum Schutz personenbezogener Daten geändert.

Infolge einer ab dem 1. Januar 2012 geltenden Änderung des Artikels 7a (2) des Gesetzes vom 19. November 1999 über die geschäftliche Tätigkeit (Gesetzblatt der Republik Polen von 1999 Nr. 1178), welches die im Handelsregister enthaltenen personenbezogenen Daten von der Anwendung des Gesetzes vom 29. August 1997 über den Schutz personenbezogener Daten (Gesetzblatt der Republik Polen von 2002 Nr. 101/926 mit Änderungen), im Folgenden „Datenschutzgesetz", ausschließt, unterliegen derzeit die personenbezogenen Daten natürlicher Personen dem in diesem Gesetz vorgesehenen Schutz, unabhängig davon, ob sie Geschäftstätigkeiten ausführen oder nicht.

Im Jahr 2012 nahm die Verwaltungsvollstreckung ihre Arbeit auf. Diese neue Organisationseinheit der polnischen Datenschutzbehörde wurde im Zuge der Änderung des Gesetzes zum Schutz personenbezogener Daten ins Leben gerufen, das am 7. März 2011 in Kraft trat und dem Generalinspektor für den Schutz personenbezogener Daten (GIODO) die Befugnis einer Durchsetzungsbehörde mit der Aufgabe der Verwaltungsvollstreckung immaterieller Verpflichtungen erteilte (Artikel 12 (3)).

Vom 15. bis 17. April 2012 wurde in Polen die zweite Evaluierungsmission zur Beurteilung der Umsetzung des Schengen-Besitzstandes durchgeführt. In ihrem Missionsbericht wies die EK nachdrücklich auf die bedeutenden Erfolge des GIODO in den Bereichen Bildung und Information hin und stufte die rechtlichen Instrumente für den Datenschutz in Polen und die Kompetenz des GIODO bei der Aufsicht und Überwachung der Verarbeitung personenbezogener Daten in Polen hoch ein.

Der GIODO beteiligte sich weiterhin an der Reform des EU-Datenschutzrechtsrahmens. Zu den wichtigsten Veranstaltungen und Aktivitäten gehörten diesbezüglich Folgende:

1. Der Datenschutzbeauftragte nahm an einer Sitzung der Kommission für Justiz und Menschenrechte im Seym (16. Februar 2012) und im Senat (Unter- und Oberhaus des polnischen Parlaments) teil, in deren Rahmen er den Parlamentsabgeordneten die grundlegenden Ziele der EU-Datenschutzreform präsentierte.
2. Am 7. März 2012 organisierten der Generalinspektor für den Schutz personenbezogener Daten, die nationale Hochschule für öffentliche Verwaltung (KSAP) und die Vertretung der Europäischen Kommission in Polen in den Räumlichkeiten der KSAP in Warschau eine Konferenz zum Thema „Die Reform der Vorschriften zum Schutz personenbezogener Daten in der Europäischen Union. Erste Beurteilung ihres Umfangs und ihrer Konsequenzen". Die Konferenz stieß eine umfassende Debatte zu den Plänen eines neuen Datenschutzmodells in der Europäischen Union an.
3. Im Hinblick auf die EU-Datenschutzreform ist der Generalinspektor an Konsultationen mit verschiedenen Sektoren beteiligt. Bislang hat er an Konsultationsgesprächen mit den folgenden Sektoren und Institutionen teilgenommen:
   - Bankwesen;
   - Polnischer Versicherungsverband;
   - Polnische Handels- und Vertriebsorganisation;

- Vertreter des Telekommunikations- und IT-Sektors unter dem Dach der polnischen Kammer für Informatik und Telekommunikation;
- Landesrat für Gerichtswesen;
- usw.

4. Der GIODO nahm an der interparlamentarischen Ausschusssitzung zum Thema „Die Reform des EU-Datenschutzrechtsrahmens – Mehr Vertrauen in einer digitalen und globalisierten Welt“ teil, die am 9. und 10. Oktober 2012 im Europäischen Parlament in Brüssel stattfand. Die interparlamentarische Ausschusssitzung wurde gemeinsam vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (LIBE) und dem Referat Legislativer Dialog (LDU) organisiert. Sie sollte die wichtigsten Themen widerspiegeln und die Abgeordneten des Europäischen Parlaments und der nationalen Parlamente in einen Meinungsaustausch und konstruktiven Dialog einbinden.
5. Die Besprechung zwischen dem GIODO und dem stellvertretenden Europäischen Datenschutzbeauftragten fand am 12. Dezember 2012 statt. Bei dieser Gelegenheit sprach der GIODO gemeinsam mit Vertretern der Regierungsverwaltung über Fragen der EU-Datenschutzreform und deren Auswirkungen auf das nationale Recht.

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	15 060 000 PLN
Personal	126
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	1 297 Beschlüsse (427 im Zusammenhang mit Anmeldeverfahren, 53 im Zusammenhang mit Prüfungen, 762 zu Verfahren infolge von Beschwerden und 51 zu Genehmigungen von Datenübermittlungen in Drittländer). In 126 Fällen wurde an staatliche Behörden, territoriale Selbstverwaltungsbehörden sowie staatliche und kommunale Organisationseinheiten, öffentliche Aufgaben ausführende private Stellen, natürliche und rechtliche Personen, Organisationseinheiten ohne Rechtspersönlichkeit und weitere Rechtsträger im Hinblick auf einen effizienten Schutz personenbezogener Daten herangetreten.
Meldungen	Es wurden 16 267 Datenspeichersysteme gemeldet.
Vorabprüfungen	Infolge der Anmeldeverfahren (Vorabprüfungen) wurden 3 359 Datenspeichersysteme mit sensiblen Daten in das Register der Datenspeichersysteme mit personenbezogenen Daten aufgenommen. Die Verarbeitung von Datenspeichersystemen mit sensiblen Daten darf erst nach Abschluss des Anmeldeverfahrens aufgenommen werden.

	Im Zusammenhang mit der Umsetzung nationaler Komponenten des VIS-Systems wurden bezüglich des nationalen Informationssystems (KSI) im Polizeipräsidium gemäß dem Gesetz vom 24. August 2007 über die Beteiligung der Republik Polen am Schengener Informationssystem und am Visa-Informationssystem Prüfungen durchgeführt.
Anträge betroffener Personen	Der polnischen Datenschutzbehörde wurde 4 208 rechtliche Fragen zugeschickt. Über die Informations-Hotline der GIODO wurden außerdem 11 001 Erklärungen bereitgestellt.
Beschwerden betroffener Personen	Beschwerden über Verletzungen des Schutzes personenbezogener Daten, unter anderem in folgenden Bereichen: Öffentliche Verwaltung (88 Beschwerden); Gerichte, Staatsanwaltschaft, Polizei, Gerichtsvollzieher (44 Beschwerden); Banken und andere Finanzinstitute (129 Beschwerden); Internet (84 Beschwerden); Marketing (28 Beschwerden); Wohnungswesen (56 Beschwerden); Sozial-, Sach- und Personenversicherungen (12 Beschwerden); Schengener Informationssystem (12 Beschwerden); Telekommunikation (40 Beschwerden); Beschäftigung (11 Beschwerden); sonstige (386 Beschwerden).
Vom Parlament bzw. der Regierung angeforderte Beratung	Dem GIODO wurden 598 Gesetzentwürfe zur Prüfung vorgelegt.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	66 – Anzahl der durch den GIODO durchgeführten Schulungen zu den Bestimmungen zum Schutz personenbezogener Daten, insbesondere für öffentliche Einrichtungen. 207 Bildungseinrichtungen, darunter Grund-, Mittel- und weiterführende Schulen sowie Berufsausbildungszentren für Lehrer, nahmen im Schuljahr 2012/2013 an der dritten Ausgabe des landesweiten Programms „Deine Daten, deine Verantwortung. Bildungsinitiative für Schüler und Lehrer“ teil.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	165 Prüfungen: - 17 Prüfungen im Zusammenhang mit der Verarbeitung personenbezogener Daten durch das nationale Informationssystem, das es öffentlichen Verwaltungs- und Justizbehörden ermöglicht, die per SIS und VIS erfassten Daten

	zu nutzen; - 9 Prüfungen in Genossenschaftsbanken und 2 in Banken, die mit Genossenschaftsbanken in Verbindung stehen; - 5 Prüfungen von Betreibern öffentlicher Telekommunikationsnetzwerke und Anbietern von öffentlich verfügbaren Telekommunikationsdiensten; - 8 Prüfungen in Knochenmarkspenderdateien; - 10 Prüfungen des Hochschulinformationssystems; - 11 Prüfungen bei Hotelbetreibern.
Sanktionsmaßnahmen	
Sanktionen	Der GIODO führt keine allgemeine Statistik über Sanktionen. Im Zusammenhang mit der Befugnis des GIODO als Durchsetzungsbehörde wurden jedoch 99 Verwaltungsverfahren eingeleitet. In Verbindung mit Prüfungen leitete der GIODO 2012 46 Verwaltungsverfahren gegen für die Datenverarbeitung Verantwortliche ein und veröffentlichte 23 Beschlüsse, die eine Anordnung zur Wiederherstellung eines rechtmäßigen Zustandes umfassten. Des Weiteren veröffentlichte der GIODO 64 Beschlüsse zu unterlassenen Meldungen von Datenspeichersystemen. Im Berichtszeitraum wurden keine Sanktionen verhängt.
Geldbußen	2012 wurden keine Geldbußen verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Im Jahr 2012 wurden in Rechtssachen, an denen der GIODO beteiligt war, vom Obersten Verwaltungsgericht und vom Verwaltungsgericht der Woiwodschaft Warschau 73 Urteile gefällt. Davon sind die folgenden Urteile besonders bemerkenswert.

I. Urteil (Ref. Nr. II SA/WA 2333/11) durch das Verwaltungsgericht der Woiwodschaft Warschau

Das Gericht bestätigte den negativen Standpunkt des GIODO zu einer Rechtssache, in der ein Unternehmen von einer Gewerkschaft, die in diesem Unternehmen tätig war, die Offenlegung einer Liste mit Namen ihrer Mitglieder zum Zweck der Verifizierung bestimmter Rechte der Vorstandsmitglieder dieser Gewerkschaft verlangte. Das Gericht wies nachdrücklich darauf hin, dass die Angabe der Anzahl der Gewerkschaftsmitglieder für eine solche Verifizierung ausreichen würde und dass die zu derartigen Zwecken erfolgende Erfassung sensibler Daten, also Daten zur Gewerkschaftsmitgliedschaft, durch den Arbeitgeber gemäß Artikel 27 (1) des Gesetzes zum Schutz personenbezogener Daten keine

Rechtsgrundlage habe. Spezifische Regulierungen, wie z. B. das Gewerkschaftsgesetz oder das Arbeitsgesetzbuch, würden ebenfalls nicht als Rechtsgrundlage dienen. Des Weiteren würde die Offenlegung einer solchen Liste mit den Namen aller Mitglieder nach Ansicht des Gerichts gegen die Grundsätze der Zweckbindung, der Notwendigkeit und der Verhältnismäßigkeit verstoßen.

II. Urteil (Ref. Nr. II SA/WA 2367/11) durch das Verwaltungsgericht der Woiwodschaft Warschau

Das Gericht bestätigte die Einschätzung des GIODO in einer Rechtssache betreffend die Verarbeitung personenbezogener Daten im Zusammenhang mit der Abtretung von Forderungen, die zu einer Zeit erfolgte, zu der der Kläger geschäftlich tätig war und direkt mit dieser Tätigkeit in Zusammenhang stand. In der Stellungnahme des Gerichts heißt es, dass die Datenschutzbehörde nicht dafür zuständig ist, die Richtigkeit zivilrechtlicher Verträge und daraus entstandener Rechtsstreitigkeiten zu beurteilen, insbesondere im Hinblick auf die Beurteilung, ob eine Forderungsabtretung zulässig, wirksam oder gültig ist, da in diesem Zusammenhang lediglich die ordentlichen Gerichte über eine Zuständigkeit verfügen. Die Offenlegung personenbezogener Daten in Verbindung mit der Abtretung von Forderungen aus Sicht der Grundsätze des Schutzes personenbezogener Daten verstößt jedoch nicht gegen die Bestimmungen des Gesetzes zum Schutz personenbezogener Daten.

III. Urteil (Ref. Nr. II SA/WA 2848/11) durch das Verwaltungsgericht der Woiwodschaft Warschau

Das Gericht bestätigte eine Stellungnahme der Datenschutzbehörde, laut der die Offenlegung von Rechnungen mit den personenbezogenen Daten des Klägers vor einem Bezirksgericht zum Zwecke eines zivilrechtlichen Verfahrens und vor dem Polizeipräsidium zum Zwecke eines Strafverfahrens durch ein Unternehmen in Art. 23 (1) Sätze 2 und 5 des Gesetzes zum Schutz personenbezogener Daten eine Rechtsgrundlage habe, d. h. falls es zur Ausübung von Rechten und Pflichten aufgrund von gesetzlichen Vorschriften notwendig sei und falls eine Verarbeitung im berechtigten Interesse des für die Verarbeitung Verantwortlichen nötig sei. Des Weiteren bestätigte das Gericht unter Berufung auf die ständige Rechtsprechung, dass der GIODO nicht für die Kontrolle straf- oder zivilrechtlicher Verfahren durch die zuständige Behörde zuständig ist, einschließlich Beweisverfahren unter Verwendung personenbezogener Daten.

C. Sonstige wichtige Informationen

Im Berichtszeitraum setzte sich der Trend einer zunehmenden Anzahl registrierter Dateien mit personenbezogenen Daten im Vergleich zu den Vorjahren (2010: 9 921; 2011: 11 845; 2012: 16 267) weiter fort. Des Weiteren wurde bei der Anzahl der für eine Registrierung gemeldeten Dateien ein Anstieg beobachtet (um 40 % im Vergleich zu 2011, um 164 % im Vergleich zu 2010 und um ganze 184 % im Vergleich zu 2009). Im Jahr 2012 bearbeitete der GIODO 4 090 von für die Verarbeitung Verantwortlichen erstatteten Aktualisierungsmeldungen. Außerdem beschloss der GIODO in 287 Fällen eine Löschung von Datenspeichersystemen aus dem landesweiten offenen Register für Systeme zur Speicherung personenbezogener Daten.

Anlässlich des Europäischen Datenschutztages am 30. Januar 2012 organisierte der Generalinspektor in der Hauptgeschäftsstelle für alle Bürger einen Tag der offenen Tür sowie eine Konferenz mit dem Titel „Was weiß der Staat über seine Bürger? Die Grundsätze der Datenverarbeitung in öffentlichen Registern“. Außerdem wurde der Europäische Datenschutztag wie üblich auch in Brüssel gefeiert.

Als Reaktion auf das große Interesse der Öffentlichkeit an den Tagen der offenen Tür anlässlich des Datenschutztages im Januar im Amtssitz in Warschau hat der GIODO eine neue Initiative zur Organisation solcher Veranstaltungen auch an anderen Tagen und in anderen Städten in ganz Polen ins

Leben gerufen. Im Jahr 2012 wurden auch in anderen polnischen Städten Tage der offenen Tür organisiert, wie z. B. am 22. November in Dąbrowa Górnicza und am 23. November in Krakau.

Am 23. und 24. April 2012 organisierte der GIODO im polnischen Sopot die 51. Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation (der sogenannten Berlin Group). Der Schwerpunkt lag hierbei auf der Datenverarbeitung durch Cloud-Computing-Lösungen, der Ausübung des Rechts auf Vergessenwerden und das Profiling von Internetnutzern durch Marketingunternehmen mithilfe spezieller Analysetools. Ein großer Erfolg der Sitzung war die Verabschiedung eines Arbeitsdokuments namens Sopot-Erklärung, das den gemeinsamen Standpunkt der Gruppe zu den Grundsätzen des Datenschutzes im Falle einer Datenverarbeitung durch Cloud-Computing enthält.

Im Jahr 2012 wurde das Projekt „Raising awareness of data protection issues among employees working in the EU" (Verbessern des Bewusstseins zu Datenschutzthemen unter den in der EU tätigen Arbeitnehmern) im Rahmen des Leonardo-da-Vinci-Partnerschaftsprogramms auf den Weg gebracht. Das Ziel des Projekts liegt in der Bereitstellung von Bildungsmaterial für natürliche Personen, die in einem der Teilnehmerländer erwerbstätig sind. Die Projektpartner, also Datenschutzbehörden aus Polen, der Tschechischen Republik, Kroatien und Bulgarien, arbeiten an einer Publikation, die sich auf die Bereitstellung von Leitlinien und Ratschlägen zum Schutz personenbezogener Daten für Personen konzentriert, die in einem der Teilnehmerländer erwerbstätig sind oder eine derartige Erwerbstätigkeit planen.

Darüber hinaus sei anzumerken, dass der polnische Verband der Automobilindustrie in Zusammenarbeit mit dem GIODO den „Verhaltenskodex zum Schutz der personenbezogenen Daten von Kunden und potenziellen Kunden" entwickelt hat. Das Dokument ist ein wesentlicher Bestandteil des Kooperationsabkommens zwischen den beiden Institutionen und wurde am 16. November 2012 abgeschlossen.

PORTUGAL

A. Zusammenfassung der Aktivitäten und Neuerungen

Die Datenschutzbehörde konsolidierte im Laufe des Jahres 2012 seine internen Dematerialisierungsverfahren. Sie erhöhte somit die Möglichkeiten einer elektronischen Meldung von Datenverarbeitungen und verkürzte die Reaktionszeit auf Anfragen der für die Verarbeitung Verantwortlichen.

Des Weiteren erhöhte die Datenschutzbehörde seine Prüftätigkeit, entweder infolge von Beschwerden betroffener Personen oder auf Eigeninitiative. Die eingegangenen Beschwerden betrafen am häufigsten die Themen Videoüberwachung, unerwünschte elektronische Kommunikation zu Marketingzwecken und Überwachung von Mitarbeitern am Arbeitsplatz (z. B. durch GPS-Geräte in Fahrzeugen).

Die Datenschutzbehörde setzte seine genaue Beobachtung von E-Government-Projekten durch öffentliche Stellen fort, insbesondere im Gesundheits- und Polizeiwesen, und griff fortlaufend durch die Abgabe von knapp 100 Stellungnahmen zu Gesetzentwürfen im Zusammenhang mit Datenschutz in den Gesetzgebungsprozess ein.

Außerdem förderte die Datenschutzbehörde das Zustandekommen von Gesprächen mit Interessenvertretern bezüglich der Umsetzung der neuen Regelungen der Datenschutzrichtlinie für elektronische Kommunikation und der Nutzung von GPS am Arbeitsplatz.

Hinsichtlich Sensibilisierungsmaßnahmen sei darauf hingewiesen, dass die seit 2007 andauernden Bemühungen der Datenschutzbehörde, ein spezielles, strukturiertes Projekt für Kinder in Schulen – das DADUS-Projekt – zu entwickeln, zu Unterstützung durch die Regierung auf hohem Niveau geführt hat. Das Bildungsministerium führte 2012 offiziell Datenschutzthemen in Form von Lernzielen in den Lehrplan für Informations- und Kommunikationstechnologien ein. Dieses Fach ist für alle Schülerinnen und Schüler der 7. und 8. Jahrgangsstufen (12 bis 14 Jahre) verpflichtend. Daher wird das DADUS-Projekt entsprechend überarbeitet, um es besser an diese neuen Gegebenheiten anzupassen, bei denen die Datenschutzbehörde anstelle einer Führungsrolle vermehrt eine unterstützende Rolle einnehmen wird.

Organisation	Nationale Datenschutzkommission
Vorsitz und/oder Gremium	Gremium bestehend aus 7 Mitgliedern: Filipa Calvão (Vorsitzender), Luís Barroso, Ana Roque, Carlos Campos Lobo, Helena Delgado António, Vasco Almeida, Luís Paiva de Andrade
Budget	Zugewiesenes Budget: 2 324 352 EUR Staatliches Budget: 1 193 885 EUR Aus den eigenen Einnahmen der Datenschutzbehörde: 1 130 467 EUR (tatsächlich erhalten: 1 556 838 EUR) Ausgegebene Haushaltsmittel: 1 445 188,45 EUR
Personal	25
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen,	12 006 verbindliche Beschlüsse (darunter 10 083 Genehmigungen

Empfehlungen	von Datenverarbeitungen, Beschlüsse zu Verstoßverfahren sowie Beschlüsse in Bezug auf Zugangsanträge durch Dritte, Schengen-Zugriffs- und Löschungsrechte usw.)
Meldungen	11 306
Vorabprüfungen	10 325
Anträge betroffener Personen	Keine Zahlen vorhanden (die Zentrale bearbeitet Anträge betroffener Personen und für die Verarbeitung Verantwortlicher)
Beschwerden betroffener Personen	588 (offiziell eingeleitete Verfahren)
Vom Parlament bzw. der Regierung angeforderte Beratung	90 Stellungnahmen zu Gesetzentwürfen mit Anordnungen zum Thema Datenschutz
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	13 504 neue Verfahren (Meldungen, Beschwerden, Stellungnahmen, Verstöße, Zugang durch Dritte, und andere); 130 Anträge auf Zugang zu und Löschung von Daten im Schengener Informationssystem (indirekter Zugang über die Datenschutzbehörde); 684 Anträge auf Stellungnahme durch Telekommunikationsanbieter bezüglich einer Aufhebung der Anrufergeheimhaltung bei störenden Anrufen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	1 005 begonnene Prüfungen (Verstoßverfahren), darunter 359 Prüfungen vor Ort
Sanktionsmaßnahmen	
Sanktionen	169 von der Datenschutzbehörde verhängte Geldbußen
Geldbußen	rund 283 000 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

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

C. Sonstige wichtige Informationen

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 (ca. 751 131 EUR)
Personal	42 sowie Präsidentin und Vizepräsident der Datenschutzbehörde
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	834 (davon 2 normative Beschlüsse)
Meldungen	10 014
Vorabprüfungen	k. A.
Anträge betroffener Personen	59
Beschwerden betroffener Personen	667
Vom Parlament bzw. der Regierung angeforderte Beratung	51
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	131 vor Ort und 41 schriftlich
Sanktionsmaßnahmen	
Sanktionen	24 Geldbußen in Höhe von insgesamt 36 000 RON (ca. 8 115 EUR)
Geldbußen	84 Verwarnungen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Rechtsprechung 1

Auf der Grundlage zahlreicher Hinweise eines Petenten führte die Datenschutzbehörde bei einem Telefon- und Internetdienstanbieter eine Reihe von Prüfungen durch.

Geprüft wurde dabei die Art und Weise, wie die Verarbeitung der Verkehrsdaten der Nutzer der Internetdienste des für die Verarbeitung Verantwortlichen, insbesondere im Zusammenhang mit der Aktivierung, Abmeldung und Funktionsweise des MyClicknet-Dienstes, durchgeführt wurde.

Mehrere Prüfungen ergaben, dass der für die Datenverarbeitung Verantwortliche den MyClicknet-Dienst nutzte, um die Internet-Navigation seiner Nutzer individuell anzupassen und verhaltensorientierte Werbung bereitzustellen sowie die Verkehrsdaten anhand von Cookies zu analysieren und zu verarbeiten, die auf den Computern der Nutzer installiert wurden, bevor diese dem Dienst zustimmten.

Dies musste gemäß den Artikeln 4 und 5 des Gesetzes Nr. 506/2004 erfolgen.

Die Datenschutzbehörde verlangte einen Nachweis der Einholung einer vorherigen schriftlichen Einwilligung in Kenntnis der Sachlage gemäß Gesetz Nr. 506/2004.

Der für die Verarbeitung Verantwortliche war diesbezüglich nicht in der Lage, einen solchen Nachweis zu erbringen. Die allgemeinen Geschäftsbedingungen für die Bereitstellung der Dienste des für die Verarbeitung Verantwortlichen enthielten keinerlei Klauseln, die als eine ausdrückliche Einwilligung in Kenntnis der Sachlage zu einer derartigen Verarbeitung verstanden werden könnten.

Des Weiteren war der für die Datenverarbeitung Verantwortliche nicht in der Lage, die Einwilligung in Kenntnis der Sachlage durch die Nutzer zur Abwahl der installierten Cookies vor oder nach der Bereitstellung der Einladungsseite nachzuweisen.

Infolge der Prüfungen wurde dem für die Verarbeitung Verantwortlichen aus folgenden Gründen eine Sanktion auferlegt:

1. Verstoß gegen Artikel 4 Absatz 2 des Gesetzes Nr. 506/2004, da der für die Verarbeitung Verantwortliche die Kommunikations- und dazugehörigen Verkehrsdaten seiner Nutzer erfasst hat, ohne die in Artikel 4 Absatz 2 Buchstaben a bis c des Gesetzes Nr. 506/2004 enthaltenen Bedingungen zu erfüllen;
2. Verstoß gegen Artikel 4 Absatz 5 und Artikel 5 des Gesetzes Nr. 506/2004, da der für die Verarbeitung Verantwortliche die Verkehrsdaten seiner Nutzer verarbeitet hat, um den MyClicknet-Dienst bereitzustellen, wofür die Nutzung des elektronischen Kommunikationsnetzes nötig war, um Informationen in den Endgeräten zu speichern, um sich (durch die Installation von Cookies) Zugang zu diesen Informationen zu verschaffen, ohne zuerst die ausdrückliche Einwilligung in Kenntnis der Sachlage einzuholen, vorher die Einladungsseite bereitzustellen, auf der es möglich ist, der Aktivierung der MyClicknet-Dienste zuzustimmen oder diese abzulehnen, und nachher das Rücktritts-Cookie bei denjenigen zu installieren, die ihre Einwilligung nicht erteilt hatten.

Rechtsprechung 2

Zahlreiche Petenten beschwerten sich über die (auf portal-just.ro zugänglichen) Webseiten zahlreicher Gerichte, die mehr personenbezogene Daten enthielten als nötig. Nach mehreren Prüfungen stellte die Datenschutzbehörde einen Verstoß gegen das Gesetz Nr. 677/2001 fest und gab dem Justizministerium und dem Obersten Rat der Magistratur Empfehlungen in Bezug auf die Art und Weise, wie der ECRIS-Antrag von den Gerichtshöfen genutzt wird:

a) die genaue Bestimmung der personenbezogenen Daten, die zwingend nötig sind, um den Zweck der gerichtlichen Websites unter Einhaltung der Datenschutzgrundsätze zu erfüllen, laut derer die

Daten angemessen, sachdienlich und in einem vernünftigen Umfang vorhanden sein müssen (also lediglich den Vor- und Nachnamen der Urteilsparteien enthalten);

b) das Erstellen einheitlicher Anweisungen zur Verarbeitung personenbezogener Daten auf zentraler Ebene, die für alle ECRIS-Antragsteller unter der Aufsicht des für die Datenverarbeitung Verantwortlichen gelten;

c) die Schulung von Mitarbeitern, die gemäß Gesetz Nr. 677/2001 und insbesondere in Bezug auf die Verarbeitung personenbezogener Daten im Rahmen des ECRIS-Antrags und des Portals der Gerichtshöfe auf Weisung des für die Datenverarbeitung Verantwortlichen handeln;

d) die Überprüfung der bislang im Rahmen des ECRIS-Antrags vorgenommenen Registrierungen gemäß den oben genannten Empfehlungen sowie die Löschung von personenbezogenen Daten, die nicht den rechtmäßigen Bedingungen einer Verarbeitung der personenbezogenen Daten entsprechen;

e) eine begrenzte, verhältnismäßige Aufbewahrungsfrist für personenbezogene Daten im Rahmen des ECRIS-Antrags und des Portals der Gerichtshöfe gemäß der Zivilprozessordnung, der Strafprozessordnung und des nationalen Archivierungsgesetzes;

f) der angemessene Schutz personenbezogener Daten vor versehentlichem oder rechtswidrigem Löschen, Verlieren, Ändern, Offenlegen oder unberechtigtem Zugang.

Die Beschwerden konnten geregelt werden, indem die überflüssigen personenbezogenen Daten von den Gerichtshöfen gelöscht wurden.

Rechtsprechung 3

Die infolge von Beschwerden durchgeführten Prüfungen mehrerer für die Datenverarbeitung Verantwortlicher ergab, dass die Aufzeichnung der Arbeitsstunden von Mitarbeitern anstatt durch die Erfassung biometrischer Daten auch durch weniger gegen die Privatsphäre verstoßende Methoden erfolgen könne. Vor der Einführung des biometrischen Systems wurde die Arbeitszeit mithilfe eines Anwesenheitsverzeichnisses und mithilfe von Zugangskarten aufgezeichnet. Selbst nach der Einführung des biometrischen Systems mussten sich bestimmte Mitarbeiter nach wie vor in das Anwesenheitsverzeichnis eintragen.

Den für die Datenverarbeitung Verantwortlichen wurde aufgrund von Verstößen gegen die Artikel 31 und 32 des Gesetzes Nr. 677/2001 eine Geldbuße auferlegt. Außerdem wies der Vorsitzende der Datenschutzbehörde den für die Datenverarbeitung Verantwortlichen an, die Verarbeitung der biometrischen Mitarbeiterdaten einzustellen und die bereits erfassten biometrischen Daten zu löschen.

Bei einer Folgeuntersuchung bei den für die Datenverarbeitung Verantwortlichen, die aufgrund einer Beschwerde erfolgte, laut der die Anordnung nicht eingehalten werde, erwies sich die Beschwerde als unbegründet.

C. Sonstige wichtige Informationen

Zu einer Reihe von der Datenschutzbehörde vorgelegten Gesetzesvorschlägen wurden negative Stellungnahmen abgegeben, da die Vorschläge nicht den Verfassungsgrundsätzen und gesetzlichen Vorschriften, den Rechtsakten der Europäischen Union, den Verträgen, dessen Vertragspartei Rumänien ist, bzw. der Rahmengesetzgebung entsprachen.

All diese Aspekte machten eine positive Stellungnahme unmöglich, woraufhin die Datenschutzbehörde die erneute Prüfung und Umformulierung der Entwürfe der normativen Rechtsakte vorschlug.

Die Datenschutzbehörde hat u. a. zu den folgenden Gesetzentwürfen eine negative Stellungnahme abgegeben:

- ein Gesetzentwurf zur Aufbewahrung von Daten, die von Anbietern öffentlich zugänglicher elektronischer Kommunikation oder öffentlicher Kommunikationsnetzwerke erfasst oder verarbeitet werden;
- ein Gesetzesvorschlag zur Erfassung und Speicherung der personenbezogenen Daten von Kunden elektronischer Kommunikationsdienste, die durch Prepaid-Karten bereitgestellt werden.

Verarbeitung der personenbezogenen Daten von Prepaid-Kartennutzern

Die Datenschutzbehörde gab zu einem Gesetzesvorschlag über die Erfassung und Speicherung von Daten, die für die Identifizierung der Kunden von Anbietern elektronischer Kommunikationsdienste durch Prepaid-Karten benötigt werden, eine negative Stellungnahme ab. Der Gesetzesvorschlag widersprach den Grundsätzen der Konvention Nr. 108 des Europarates sowie den Vorkehrungen der Richtlinien 95/46/EG, 2006/24/EG und 2009/136/EG über die allgemeinen Service- und Nutzerrechte bei elektronischen Kommunikationsdiensten und -netzen.

Des Weiteren verstieß der Gesetzesvorschlag gegen das Recht auf Achtung der Privatsphäre des Einzelnen (gemäß Artikel 26 der geänderten rumänischen Verfassung). Die Verarbeitung der persönlichen Identifikationsnummer (CNP) könnte gemäß den Bedingungen von Artikel 8 des Gesetzes Nr. 677/2001 und denjenigen von Beschluss 132/2011 erfolgen. In der Art und Weise, wie der Gesetzesvorschlag verfasst war, verstieß dieser jedoch gegen die Grundsätze der Verhältnismäßigkeit und der Datenaufbewahrung gemäß Richtlinie 95/46/EG und Gesetz Nr. 677/2001.

Die Datenschutzbehörde kam zu dem Schluss, dass der Gesetzesvorschlag gegen das Verbot der Rückwirkung von Gesetzen gemäß Artikel 15 Absatz 2 der rumänischen Verfassung verstoße, da er die Verpflichtung enthält, auch die personenbezogenen Daten von natürlichen Personen zu kommunizieren, die bereits vor dem Inkrafttreten des vorgeschlagenen Gesetzes elektronische Kommunikationsdienste genutzt haben.

Der Gesetzesvorschlag verstieß außerdem gegen das Recht der Verbraucher auf das Treffen von Entscheidungen im Hinblick auf die Nutzung von Prepaid-Kommunikationsdiensten, da die Verpflichtung zur Identifizierung Einfluss auf die Entscheidung der Verbraucher nehmen könnte, solche Dienste in Anspruch zu nehmen oder nicht.

SCHWEDEN

A. Zusammenfassung der Aktivitäten und Neuerungen:

Aufsicht

Im Rahmen ihrer Aufsichtsbefugnis befasste sich die Datenschutzbehörde 2012 mit der Verarbeitung personenbezogener Daten in den Bereichen E-Government, Gesundheitswesen, Forschung, Sozialfürsorge, Strafverfolgung, vertrauliche Informationen über Schülerinnen und Schüler in Schulen, Kompetenzdatenbanken, Mitgliedsdaten politischer Parteien, Smartphone-Apps im Bankwesen usw.

Sensibilisierung

Die Medienberichterstattung über unsere Aktivitäten erreichte 2012 einen neuen Höchststand. Des Weiteren verzeichneten wir eine beträchtliche Erhöhung der telefonischen und per E-Mail eingesandten Fragen der Öffentlichkeit sowie der Besucherzahlen auf unserer Website. Ähnlich wie in den Vorjahren veröffentlichten wir im Laufe des Datenschutzjahres 2012 eine Broschüre mit den wichtigsten Datenschutzfragen.

Organisation	Schwedische Datenschutzbehörde
Vorsitz und/oder Gremium	Generaldirektor Göran Gräslund (ab 1. Juni 2013 übernimmt Kristina Svahn Starrsjö den Posten der Generaldirektorin)
Budget	36 931 000 SEK = 3 987 841 EUR
Personal	Rund 45
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	115 Stellungnahmen zu Gesetzgebungsvorschlägen auf Anfrage von Regierungsstellen 68 Stellungnahmen in Absprache mit Datenschutzbeauftragten 6 Leitlinien, Empfehlungen und Berichte
Meldungen	
Vorabprüfungen	247 (vorwiegend in Bezug auf Forschung und die Verarbeitung von DNS-Daten)
Anträge betroffener Personen	Unser Helpdesk: 8 000 Anrufe, 5 600 E-Mails Formelle Anträge: 219
Beschwerden betroffener Personen	323
Vom Parlament bzw. der Regierung angeforderte Beratung	Siehe bereits erwähnte Beschlüsse, Stellungnahmen usw.

Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Pressemitteilungen: 69, Vorträge und Seminare: 52
Prüfmaßnahmen	
Prüfungen, Untersuchungen	267 (abgeschlossene Prüfungen) (43 Vor-Ort-Prüfungen, 143 Dokumentenprüfungen und 81 Umfragen) Die wichtigsten Themen: Polizei, Kameraüberwachung, Veröffentlichung im Internet, Bank-Apps, Kompetenzdatenbanken, vertrauliche Daten in der Schule, politische Parteien und deren Mitglieder
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	6 825

B. Rechtsprechung

Das Oberste Verwaltungsgericht wies in einem Beschluss vom März 2012 die Berufungsklage zweier weiterführender Schulen ab, die in ihren Innenräumen Überwachungskameras installiert hatten. Die Datenschutzbehörde hatte die Schulen angewiesen, die Überwachung untertags einzustellen. Die Videoüberwachung könne nur dann erlaubt werden, wenn ein wesentlicher Bedarf für eine derartige Überwachung bestehe, der das Recht der Schülerinnen und Schüler, nicht überwacht zu werden, überwiege. Die Schule legte beim Berufungsgericht Berufung ein, dies wurde jedoch zurückgewiesen. Das Oberste Verwaltungsgericht bestätigte diese Entscheidung und urteilte, dass eine Kameraüberwachung in Klassenzimmern, Korridoren, der Schulbibliothek, in Pausenbereichen usw. generell als Verstoß gegen das Recht auf Datenschutz der betroffenen Personen erachtet werden müsse. Die Datenschutzbehörde hat inzwischen eine Checkliste erstellt, mit der Schulen besser einschätzen können, ob eine Kameraüberwachung gemäß dem Datenschutzgesetz zulässig ist oder nicht.

In einem weiteren Fall bestätigte das Oberste Verwaltungsgericht den Beschluss der Datenschutzbehörde, laut dem eine Sozialversicherungsgesellschaft eine Risiko- und Schwachstellenbewertung ihres SMS-Dienstes zur Meldung von Krankheitsfällen für den Erhalt von Sozialleistungen durchzuführen hatte. Das Oberste Verfassungsgericht bestätigte in seinem Urteil die Ansicht der Datenschutzbehörde, dass die Versicherungsgesellschaft den Zweck und die Mittel der Verarbeitung beschlossen habe und sie demnach für die Verarbeitung personenbezogener Daten im Zusammenhang mit dem SMS-Dienst verantwortlich sei.

SLOWAKEI

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2012 kann als Jahr voller Veränderungen und erfolgreicher Gesetzesvorlagen bezeichnet werden. Basierend auf dem Gesetzgebungsplan der slowakischen Regierung für das zweite Halbjahr 2012 hat die Datenschutzbehörde der Slowakischen Republik (im Folgenden Datenschutzbehörde) einen völlig neuen Entwurf des Gesetzes zum Schutz personenbezogener Daten ausgearbeitet.

Das Ziel der Gesetzesänderung war die vollständige Umsetzung der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates sowie der Beschlüsse und Empfehlungen der slowakischen Schengen-Evaluierung im Bereich des Schutzes personenbezogener Daten und der Gesetzesanalyse aus Anwendungssicht.

Ab Januar 2012 führte die Datenschutzbehörde sogenannte wöchentliche Überwachungs- und Beurteilungsdienste für Material ein, das im Gesetzgebungsprozess im Rahmen des interministeriellen Überprüfungsverfahrens enthalten ist. Das Ziel dieses Verfahrens ist die kontinuierliche Erfassung jeglichen Materials des interministeriellen Überprüfungsverfahrens und demzufolge eine effektive Beurteilung und Kommentierung dieses Materials. Die Datenschutzbehörde beurteilte sämtliches Material im Hinblick auf die Einhaltung des Datenschutzgesetzes, um die gesetzlich geschützten, grundlegenden Anforderungen des gesellschaftlichen Lebens festzustellen und dabei die Verstöße gegen das Recht auf Datenschutz und die Privatsphäre des Einzelnen zu minimieren. Zu diesem Zweck muss jeder Gesetzentwurf, dessen Inhalt die Verarbeitung personenbezogener Daten betrifft, den grundlegenden Anforderungen des Datenschutzgesetzes genügen.

Landesweite Prüfungen durch die Datenschutzbehörde

Im Laufe des Jahres 2012 führte die Datenschutzbehörde gemäß des jährlichen Prüfplans mehrere landesweite Prüfungen durch. Bei der Erstellung des jährlichen Prüfplans konzentrierte sich die Datenschutzbehörde gemäß den Entwicklungen der sozialen Beziehungen und der Gesetzgebung zum Schutz personenbezogener Daten auf die Prüfung der Datenverarbeitung durch für die dafür Verantwortlichen und Auftragsverarbeiter im Zusammenhang mit Datenspeichersystemen.

Kopieren amtlicher Dokumente für den Antrag auf steuerliche Vergünstigungen

Die Datenschutzbehörde untersuchte 2012 die Rechtmäßigkeit der Verarbeitung personenbezogener Daten zur Überprüfung des Rechtes auf steuerliche Vergünstigungen gemäß dem Einkommensteuergesetz in vier ausgewählten Steuerbehörden der Slowakischen Republik. Bei der Prüfung kam die Datenschutzbehörde zu dem Schluss, dass die Steuerbehörden amtliche Dokumente natürlicher Personen kopierten und aufbewahrten, um steuerliche Vergünstigungen festzustellen. Das Einkommensteuergesetz untersagte jedoch zum Zeitpunkt der Prüfung das Kopieren und Aufbewahren amtlicher Dokumente zu diesem Zweck. Demnach verstieß das Verfahren der Steuerbehörden gegen Abschnitt 10 Absatz 6 des Gesetzes zum Schutz personenbezogener Daten Nr. 428/2002 Coll.

Verarbeitung personenbezogener Daten durch Immobilienvermittlungen

Die Datenschutzbehörde führte 2012 Prüfungen bei vier Immobilienvermittlungen durch. Dabei wurden die Aktivitäten der Immobilienvermittlungen als Verantwortliche für die Verarbeitung personenbezogener Daten zum Abschluss von Leasingverträgen oder Kaufverträgen für die Immobilie und den dazugehörigen Grundbuch- und Eigentumsregistereintragungen überprüft. Die Datenschutzbehörde stellte bei der Prüfung fest, dass sich die für die Verarbeitung Verantwortlichen einige personenbezogenen Daten durch Kopieren amtlicher Dokumente verschafften. Eine derartige Erfassung personenbezogener Daten war gemäß Abschnitt 6 Absatz 1 Punkt (d) in Zusammenhang mit Abschnitt 10 Absatz 6 des Gesetzes Nr. 428/2002 Coll. für den Zweck der Verarbeitung nicht nötig.

Verarbeitung personenbezogener Daten durch Waisenhäuser

Die Datenschutzbehörde überprüfte 2012 in fünf ausgewählten Waisenhäusern das Schutzniveau bei der Verarbeitung personenbezogener Daten gemäß dem geänderten Gesetz Nr. 305/2005 Coll. über den sozialrechtlichen Schutz von Kindern und soziale Kinderbetreuung sowie über die Änderung anderer Gesetze. Bei der Prüfung wurden vor allem fehlerhafte Datenspeichersysteme und eine unzureichende Anweisung der befugten Personen festgestellt.

Verarbeitung personenbezogener Daten durch Unterbringungseinrichtungen

Die Datenschutzbehörde prüfte im Jahr 2012 außerdem die Verarbeitung personenbezogener Daten durch Unterbringungseinrichtungen gemäß dem geänderten Gesetz Nr. 253/1998 Coll. zur Einwohnermeldepflicht von Bürgern der Slowakischen Republik und dem Bevölkerungsregister der Slowakischen Republik sowie dem geänderten Gesetz Nr. 404/2001 Coll. zur Meldepflicht für Ausländer. Die Prüfungen wurden bei fünf ausgewählten für die Verarbeitung Verantwortlichen durchgeführt.

Verarbeitung personenbezogener Daten durch Reiseagenturen

Die Datenschutzbehörde konzentrierte sich 2012 im Rahmen ihrer Kompetenz als Aufsichtsbehörde für den Datenschutz auf die Verarbeitung personenbezogener Daten durch Reiseagenturen als Verantwortliche für Datenspeichersysteme. Dabei wurde der Status des Schutzes personenbezogener Daten und die Einhaltung der Bedingungen der Verarbeitung vor allem zu Zwecken des Reisevertragsabschlusses überprüft. Die Datenschutzbehörde verifizierte die Verwaltungsvorgänge von fünf für die Verarbeitung Verantwortlichen. Bei der Prüfung konnten zwei Rechtsgrundlagen für die Verarbeitung personenbezogener Daten festgestellt werden: die Einwilligung der betroffenen Person sowie die Notwendigkeit personenbezogener Daten zur Erfüllung von Verträgen, bei denen die betroffene Person eine Vertragspartei ist, gemäß Abschnitt 7 Absatz 4 Punkt (b) des Gesetzes Nr. 428/2002 Coll.

Grenzüberschreitende Übermittlung personenbezogener Daten

Im Jahr 2012 genehmigte die Datenschutzbehörde 25 grenzüberschreitende Übermittlungen personenbezogener Daten in Länder, die nicht über ein angemessenes Datenschutzniveau verfügen. Die Genehmigungen wurden hauptsächlich von für die Verarbeitung Verantwortlichen mit Sitz in der Slowakischen Republik beantragt, die größtenteils zu multinationalen Holdinggesellschaften gehörten. Die personenbezogenen Daten bezogen sich hauptsächlich auf Mitarbeiter, Kunden und Geschäftspartner der für die Verarbeitung Verantwortlichen.

Internationale Zusammenarbeit

Internationale Aktivitäten resultierten größtenteils aus der EU-Mitgliedschaft und erfolgten in Arbeitsgruppen unter der Schirmherrschaft und gemäß den Rechtsakten der Europäischen Gemeinschaften.

Im Frühjahr 2012 richtete die Datenschutzbehörde auf Anfrage des serbischen Amtes des Regierungsbevollmächtigten eine Sitzung zum Schutz personenbezogener Daten und Informationen von öffentlicher Bedeutung aus. Die Sitzung wurde in Zusammenarbeit mit dem Zentrum zum Austausch von Integrations- und Reformerfahrung der slowakischen Agentur für internationale Entwicklungszusammenarbeit des slowakischen Außenministeriums organisiert.

Das Thema der Sitzung war die Bereitstellung sachkundiger Konsultationen zu ausgewählten Themen auf dem Gebiet der Verarbeitung personenbezogener Daten in der Slowakischen Republik für Direktmarketing, die Verarbeitung personenbezogener Daten in elektronischen Medien, die Veröffentlichung personenbezogener Daten durch für die Verarbeitung Verantwortliche im Justizwesen, in Kommunalbehörden und in den Medien, die Verarbeitung spezieller Kategorien personenbezogener Daten und die außenpolitische Agenda. Die Konsultationen wurden durch Beispiele aus der Praxis der Datenschutzbehörde ergänzt.

Organisation	Behörde für den Schutz personenbezogener Daten der Slowakischen Republik
Vorsitz und/oder Gremium	Dr. Eleonóra Kročianová
Budget	876 324 EUR
Personal	34 Mitarbeiter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	200
Vorabprüfungen	0
Anträge betroffener Personen	Im Berichtszeitraum ging die Datenschutzbehörde 5 Anträgen betroffener Personen nach, die gemäß Abschnitt 20 des Gesetzes Nr. 428/2002 Coll. von ihrem Recht auf Auskunft bezüglich der Verarbeitung ihrer personenbezogenen Daten und bezüglich der Quelle, von der der Verarbeiter ihre personenbezogenen Daten bezieht, Gebrauch gemacht haben. Der Verarbeiter ist dazu verpflichtet, die betroffenen Personen schriftlich über den Status der Verarbeitung ihrer personenbezogenen Daten zu informieren. In allen Fällen ergab die Prüfung durch die Datenschutzbehörde, dass die Meldungen durch die betroffenen Personen gerechtfertigt waren und die Verarbeiter demnach ihren gesetzlichen Verpflichtungen nicht nachgekommen sind.
Beschwerden betroffener Personen	Im Berichtszeitraum erhielt die Datenschutzbehörde 200 Meldungen von natürlichen Personen, die den Schutz ihrer Rechte und per Gesetz geschützten Interessen beansprucht haben. Die Datenschutzbehörde erhielt außerdem 52 Meldungen mutmaßlicher Verstöße gegen das Datenschutzgesetz. Im Berichtszeitraum prüfte die Datenschutzbehörde 321 Meldungen und Vorschläge und leitete auf Eigeninitiative 69 Verfahren ein. Diese Verfahren richteten sich gegen Stellen sowohl im privaten als auch im öffentlichen Sektor. Zur Berichtigung der Missstände veranlasste die Datenschutzbehörde insgesamt 131 Maßnahmen. Von insgesamt 252 geprüften Meldungen und Vorschlägen in Bezug auf Verstöße gegen das Gesetz Nr. 428/2002 Coll. haben 4 Beschwerdeführer von ihrem Recht Gebrauch gemacht und innerhalb der gesetzlichen Frist von 30 Tagen Beschwerde eingelegt. In 3 Fällen schob die Datenschutzbehörde eine wiederholte Beschwerde gemäß dem entsprechenden Gesetz aufgrund eines Mangels an neuen Fakten auf.

Vom Parlament bzw. der Regierung angeforderte Beratung	
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Das Jahr 2012 stand hauptsächlich im Zeichen des Führungswechsels innerhalb der Datenschutzbehörde und der damit einhergegangenen Zusammenführung der Belegschaft. Ein weiterer Schwerpunkt war die Umsetzung des Schengen-Besitzstandes. Zu guter Letzt arbeitete die Datenschutzbehörde am neuen Gesetz zum Schutz personenbezogener Daten.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Die Datenschutzbehörde führte im Berichtszeitraum insgesamt 112 Prüfungen durch. Diese erfolgten auf Grundlage des jährlichen Prüfplans der Datenschutzbehörde. Bei der Erstellung des Prüfplans konzentrierte sich die Datenschutzbehörde auf den Status der Verarbeitung personenbezogener Daten durch die für die Verarbeitung Verantwortlichen und Verarbeiter und deren befugte Mitarbeiter sowie auf die Einhaltung gesetzlicher Vorschriften und internationaler Dokumente. Die Datenschutzbehörde richtete ihr Augenmerk auf die praktische Anwendung des Datenschutzes und auf potenzielle Probleme bei der Anwendung des Gesetzes Nr. 428/2002 Coll. und weiterer Gesetze. Die Datenschutzbehörde beobachtete im Berichtszeitraum vermehrt Probleme bei der Verarbeitung personenbezogener Daten. Diese Probleme bezogen sich auf den Betrieb von Kamerasystemen größtenteils durch natürliche Personen. Im Rahmen der Prüfungen beteiligte sich die Datenschutzbehörde außerdem an der Koordinierung der Zusammenarbeit mit ausländischen Datenschutzbehörden. Auf Anfrage der ungarischen Datenschutzbehörde verifizierte die Datenschutzbehörde den Status des Datenschutzes bei Unternehmen, die Call-Center-Dienste anbieten.
Sanktionsmaßnahmen	
Sanktionen	
Geldbußen	Die Datenschutzbehörde zielte bei ihrer Arbeit größtenteils auf Prävention ab. Dies führte zu einer minimalen Sanktionierung von für die Verarbeitung Verantwortlichen und Verarbeitern. Im Berichtszeitraum verhängte die Datenschutzbehörde insgesamt 5 Geldbußen mit einem Gesamtwert von 8 050 EUR.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	42 411

B. Rechtsprechung

Im Jahr 2012 endete ein langer Rechtsstreit zwischen der Datenschutzbehörde und einem Unternehmen, das personenbezogene Daten verarbeitete und außerdem im Bereich der außergerichtliche Beitreibung von Forderungen und dazugehöriger Aufgaben für einen Verarbeiter aktiv war, der als bankfremde Einrichtung ungebundene Kredite vergab. Dieser für die Verarbeitung Verantwortliche beantragte eine gerichtliche Prüfung und eine anschließende Nichtigerklärung eines Beschlusses der Datenschutzbehörde, die ihm für die unbefugte Offenlegung personenbezogener Daten eine Geldbuße auferlegte, als der für die Verarbeitung Verantwortliche auf den Briefumschlägen vermerkte, dass der Adressat Zahlungen umgangen habe, und er demnach die personenbezogenen Daten über die wirtschaftliche Identität betroffener Personen unrechtmäßig preisgegeben hatte. Das Gericht kam zu dem Ergebnis, dass die Entscheidung des Datenschutzbeauftragten rechtmäßig und sachgerecht ist.

C. Sonstige wichtige Informationen

Der Schutz personenbezogener Daten ist ein wesentlicher Bestandteil des Rechts auf Datenschutz des Einzelnen und eines der Grund- und Freiheitsrechte, die durch die Verfassung der Slowakischen Republik garantiert sind. Das Recht auf den Schutz personenbezogener Daten ist ein neuer, jedoch sich schnell entwickelnder Bereich. Seit der Gründung der Slowakischen Republik sind 20 Jahre vergangen. In diesen Jahren hat das Thema des Schutzes personenbezogener Daten in der Praxis an Bedeutung gewonnen, insbesondere aufgrund der Entwicklungen von sozialen Plattformen und der Informationstechnologien. Diese Faktoren hatten großen Einfluss auf die Sensibilisierung und die Gesetzgebung auf dem Gebiet des Schutzes personenbezogener Daten. Neue Herausforderungen und Anforderungen haben die Maßnahmen im Zusammenhang mit der Verarbeitung und Übermittlung einer zunehmenden Menge an personenbezogenen Daten sowie den Zugang auf selbige beeinflusst.

Die Aufsicht der Verarbeitung personenbezogener Daten auf dem Gebiet der Slowakischen Republik wurde der Datenschutzbehörde zum 1. September 2002 durch das Gesetz Nr. 428/2002 Coll. übertragen, welche nun im Rahmen ihrer Befugnisse den Schutz personenbezogener Daten überwacht. Dies kann als langfristiger Prozess erachtet werden, der sich mit jeder einzelnen Aufgabe der Datenschutzbehörde, jedoch vor allen Dingen mit der Bereitstellung von Konsultationen von Öffentlichkeit und Fachleuten sowie durch die Prüfaktivitäten der Datenschutzbehörde weiterentwickelt. Im Berichtszeitraum war die angemessene Ausführung ihrer Aufgaben das Hauptanliegen der Datenschutzbehörde, die mit mangelnder Finanzierung und Personalbesetzung zu kämpfen hatte.

Aufgrund ihrer Erfahrungen in der Vergangenheit kommt die Datenschutzbehörde zu dem Schluss, dass der Schutz personenbezogener Daten kein leichtverständliches Thema ist. Die Ergebnisse der Prüfungen durch die Datenschutzbehörde und die enorme Menge der von der Öffentlichkeit gestellten Fragen zur Anwendung des Datenschutzgesetzes weisen auf das mangelnde Wissen und die schlechte Anwendung der Bestimmungen zum Schutz personenbezogener Daten hin, vor allem aufseiten kleiner und mittlerer Unternehmen und Kommunalbehörden, die ebenfalls mit der schlechten wirtschaftlichen Lage und Sparmaßnahmen zu kämpfen hatten.

Andererseits zeigen dank der gesellschaftlichen und technologischen Entwicklungen in jüngster Zeit die Statistiken zur Leistung der Datenschutzbehörde, dass die Existenz eines Rechts auf den Schutz personenbezogener Daten und ein Interesse an einer rechtmäßigen und sicheren Datenverarbeitung zunehmend ins Bewusstsein der Bevölkerung rückt. Diese besonderen Umstände hatten ungeachtet der Aktivitäten der Datenschutzbehörde eine wachsende und verbesserte Vorsicht und Prävention aufseiten natürlicher Personen zur Folge. Demzufolge kann die Sensibilisierung der Öffentlichkeit als erster Schritt in Richtung auf eine Erfüllung der Verpflichtungen auf dem Gebiet des Datenschutzes und auf die Ausübung der Rechte im Alltag erachtet werden.

Im Allgemeinen war das Niveau des Schutzes personenbezogener Daten in der Slowakischen Republik im Berichtszeitraum zufriedenstellend. Es liegt jedoch im Interesse aller betroffenen Personen, dass das

Niveau und die Qualität des Schutzes der personenbezogenen Daten natürlicher Personen im Zuge weiterer Entwicklungen das erforderliche Datenschutzniveau erreicht.

SLOWENIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2012 kann als Jahr ehrgeiziger Regierungspläne für die zusätzliche, zügige Informatisierung großer öffentlicher Datenbanken sowie als ein Jahr des zunehmenden Bedarfs einer vermehrten Verarbeitung personenbezogener Daten durch den öffentlichen Sektor erachtet werden. Alarmierend ist dabei, dass der Staat, der gemäß der slowenischen Verfassung für Datenschutz sorgen sollte, versucht, das Fundament des Datenschutzgesetzes zu untergraben.

Die Datenschutzbeauftragte bearbeitete mehr als 80 Vorschläge für Gesetzesänderungen, die eine Erfassung und Verarbeitung personenbezogener Daten vorsehen. Dies entspricht einer Steigerung von mehr als einem Drittel im Vergleich zu 2011. Viele der Vorschläge sind unserer Ansicht nach ein Versuch, eine unverhältnismäßige Erfassung und Verarbeitung personenbezogener Daten zu legalisieren, was weder zu einer Vereinfachung von Verwaltungsverfahren noch zu Sparmaßnahmen beiträgt, jedoch für Bürger ein geringeres Datenschutzniveau zur Folge hat. Zu den Gesetzen, die geändert werden sollen, gehören das Gesetz über den Schutz der Privatsphäre in der elektronischen Kommunikation, das Gesetz über polizeiliche Aufgaben und Behörden, das Gesetz über die Regulierung des Arbeitsmarktes, das Erbschaftsgesetz, das Gesetz über die Vergabe von öffentlichen Aufträgen und das Gesetz über die öffentliche Verwaltung. Bei den meisten Änderungsvorschlägen fehlt eine Datenschutz-Folgenabschätzung, die im Zusammenhang mit den geplanten Datenverarbeitungsaktivitäten hätte durchgeführt werden sollen. Wie es scheint, hat die Finanzkrise den Informatisierungsbereich nicht so sehr getroffen wie andere Bereiche des öffentlichen Sektors. Viele der geplanten Informatisierungen werden hingegen mit erheblichen Kosten einhergehen.

Die Datenschutzbeauftragte bearbeitete in ihren beiden Tätigkeitsbereichen eine äußerst hohe Anzahl von Fällen, die eine Stellungnahme, Beschwerde oder Berufung umfassten. Derartige Umstände sind zum einen positiv zu werten, da sie zeigen, dass die Menschen immer besser informiert und zunehmend im Hinblick auf den Zweck und die Bedeutung der beiden Menschenrechte sensibilisiert sind, deren Umsetzung und Schutz in den Zuständigkeitsbereich des Datenschutzbeauftragten fallen. Gleichzeitig kann ein solcher Anstieg von Beschwerden und Fällen im Zusammenhang mit Prüfungen auch auf besorgniserregende Maßnahmen verantwortlicher Behörden auf dem Gebiet des Zugriffs auf öffentliche Informationen einerseits und auf den hohen (und vielleicht sogar zu hohen) Bedarf verschiedener für die Datenverarbeitung Verantwortlicher aus dem privaten und öffentlichen Sektor an der Verarbeitung personenbezogener Daten andererseits zurückzuführen sein.

Ungeachtet der steigenden Zahl von Fällen strebt die Datenschutzbeauftragte nach einer höheren Reaktionsfähigkeit und Professionalität, was aufgrund der hohen Anzahl der zu bearbeitenden Fälle jedoch nur schwer möglich ist. Dennoch freue ich mich, dass wir es 2012 trotz alledem wieder geschafft haben und die Öffentlichkeit unsere Bemühungen anerkennt, die beiden Grundrechte (das Recht auf den Zugang zu öffentlichen Informationen und das Recht des Schutzes personenbezogener Daten) zu schützen. Aus diesem Grund hat die Öffentlichkeit der Datenschutzbeauftragten im vergangenen Jahr erneut ein hohes Maß an Vertrauen entgegengebracht.

Forschungen des Zentrums für Meinungs- und Massenkommunikationsforschung zufolge war das Vertrauen in die Datenschutzbeauftragte im Januar 2013 bezeichnenderweise wieder hoch (52 %) und erreichte unter den vier untersuchten Aufsichtsbehörden den höchsten Wert. Da bei früheren Messungen ebenfalls ein hohes Vertrauen festgestellt werden konnte und der Prozentsatz schon immer in der oberen Hälfte gelegen hat, ist dies der klare Ausdruck eines fortlaufenden Vertrauens, was sehr zufriedenstellend ist und uns gleichzeitig dazu ermutigt, unsere Arbeit fortzusetzen und nach Verbesserungsmöglichkeiten zu suchen.

Im Hinblick auf den Datenschutz wurden 2012 von der Datenschutzbeauftragten 725 Prüfungen (6 % mehr als 2011) und 158 Strafverfahren (16 % mehr als 2011) bearbeitet. Bezüglich Trends möchte ich

eindringlich auf Cloud-Computing hinweisen, das hinsichtlich Datenschutz und technologischen Entwicklungen einen immer größeren Stellenwert einnimmt. Das Potenzial von Cloud-Computing ist enorm, doch sollte dies nicht zu einer Reduzierung des Datenschutzniveaus – eines der Grundrechte – führen. Die Datenschutzbeauftragte veröffentlichte 2012 gemeinsam mit Cloud Security Alliance (CSA) – Slovenia Chapter, ISACA Slovenia Chapter und Eurocloud Slovenia als eine der ersten EU-Behörden Leitlinien für den Datenschutz im Cloud-Computing, um zur Schaffung angemessener Standards auf diesem Gebiet beizutragen ([15]). Zweck des Dokuments ist die Einrichtung von Kontrollpunkten, die Nutzer und Aufsichtsbehörden in die Lage versetzen, bezüglich der Nutzung und der Überwachung von Cloud-Computing-Diensten informierte Entscheidungen zu treffen, was die Verarbeitung personenbezogener Daten betrifft. Andererseits haben Initiativen für eine sicherere Nutzung und Zertifizierung von Cloud-Diensten damit die Möglichkeit, auf Leitlinien für zukünftige Entwicklungen zurückzugreifen, deren Ziel in der Einhaltung der Datenschutzgesetze liegt. Die Datenschutzbeauftragte ist der Ansicht, dass zahlreiche Anbieter von Cloud-Diensten ihren Kunden noch nicht alle Informationen bereitstellen, die sie benötigen, um eine informierte Entscheidung zu treffen. Es fehlen nach wie vor Mechanismen, die eine Unterscheidung von vertrauenswürdigen und nicht vertrauenswürdigen Anbietern ermöglichen.

Organisation	Informationsbeauftragte der Republik Slowenien
Vorsitz und/oder Gremium	Nataša Pirc Musar
Budget	1 610 000 EUR
Personal	33 Angestellte: Kabinett (2 bis 6 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	143 umfassende und 2 048 kurze Stellungnahmen und Empfehlungen auf der Grundlage von Anfragen betroffener Personen und für die Datenverarbeitung Verantwortlicher
Meldungen	153 Meldungen zu Datenspeichersystemen mit personenbezogenen Daten.
Vorabprüfungen	23 Vorabprüfungen: 7 zu Biometrik, 5 zur Übermittlung von Daten an Drittländer, 12 zur Verknüpfung von Speichersystemen.
Anträge betroffener Personen	2 048 Anträge auf Stellungnahmen/Klärungen von betroffenen Personen.
Beschwerden betroffener Personen	Insgesamt 747 Beschwerden betroffener Personen, davon 497 berechtigt. Bereiche: 226 zur unrechtmäßigen Übermittlung oder Offenlegung von Daten, 144 zur unrechtmäßigen Datenerfassung, 118 zu Direktmarketing, 72 zu Videoüberwachung, 44 zu Datensicherheit, 153 sonstige. Darüber hinaus 63 Beschwerden zum Umgang mit Rechten betroffener Personen.

([15]) https://www.ip-rs.si/index.php?id=308

Vom Parlament bzw. der Regierung angeforderte Beratung	Der Gesetzgeber und die für die Erarbeitung von Gesetzentwürfen zuständigen Behörden konsultierten die Datenschutzbeauftragte zu 80 Gesetzen und sonstigen Rechtstexten, unter anderem zum Gesetz über den Schutz der Privatsphäre in der elektronischen Kommunikation, das Gesetz über polizeiliche Aufgaben und Behörden, das Gesetz über die Regulierung des Arbeitsmarktes, das Erbschaftsgesetz, das Gesetz über die Vergabe von öffentlichen Aufträgen, das Gesetz über die öffentliche Verwaltung usw.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Weitere Tätigkeiten der Datenschutzbeauftragten im Jahr 2011: - Fortsetzung der Präventivarbeit (Vorträge, Konferenzen) gemeinsam mit dem slowenischen Zentrum für ein sichereres Internet; - Beteiligung an einer Reihe von ressortübergreifenden Arbeitsgruppen im Bereich E-Government, u. a. auch im Bereich elektronische Identität; - Veröffentlichung von Leitlinien zu Hilfsmitteln für den Online-Datenschutz sowie ein Sonderbericht zum Thema Treuekarten; - Konsultationen bzgl. einer Reihe von Gesetzen; - Fortsetzung der starken internationalen Beteiligung.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	725 Prüfungen: 245 im öffentlichen Sektor, 480 im privaten Sektor.
Sanktionsmaßnahmen	
Sanktionen	Es wurden 158 Verfahren eingeleitet (29 im öffentlichen Sektor, 78 im privaten Sektor, 51 zu Privatpersonen), davon wurden 17 Verwarnungen und 61 Ermahnungen ausgesprochen sowie 58 Geldbußen und 7 Zahlungsanordnungen verhängt.
Geldbußen	Die Datenschutzbehörde verhängte Geldbußen in Höhe von 50 037 EUR (zuzüglich Verwaltungssteuern).
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Daten zu Druckvorgängen von Mitarbeitern

Bei der Datenschutzbeauftragten ging eine Beschwerde gegen die Leitung einer staatlichen Behörde ein, die eine Liste aller Mitarbeiter und deren Nutzung von Druckern am Arbeitsplatz (Vor- und Nachname, Anzahl der Druckvorgänge, Bezeichnungen der Dokumente) angefordert hatte. Eine dementsprechende Prüfung ergab, dass die Behörde durch eine Überwachung der Druckkosten festgestellt hatte, dass Mitarbeiter die Drucker exzessiv und auch für das Ausdrucken persönlicher Dokumente nutzten. Die

Datenschutzbeauftragte kam zu dem Schluss, dass die Behörde keine Daten zur Bezeichnung der Dokumente oder der ausgedruckten Websites hätte erfassen müssen, da es sich dabei um personenbezogene Daten handele, die für eine effektive Verwaltung der Abläufe und Druckkosten durch die Behörde nicht nötig seien. Die Datenschutzbeauftragte ordnete an, dass besagte Daten nicht mehr erfasst werden dürfen und das Verfahren geändert werden muss. Die Behörde beschloss jedoch, das Verfahren nicht mehr anzuwenden.

Datenerfassung zu Online-Direktmarketingzwecken

Die Datenschutzbeauftragte erhielt eine Reihe von Beschwerden gegen einen für die Datenverarbeitung Verantwortlichen, der angeblich ohne die Einwilligung in eine Verarbeitung personenbezogener Daten durch die betroffenen Personen E-Mail-Direktmarketing betrieb. Bei einer Prüfung stellte sich heraus, dass der für die Verarbeitung Verantwortliche in seinen Datenbanken die Daten von über 100 000 Personen, registrierten Nutzern seiner Website und Nutzern bestimmter Facebook-Anwendungen gespeichert hatte. Die Datenschutzbeauftragte kam zu dem Schluss, dass der für die Datenverarbeitung Verantwortliche ausreichend Nachweise für die Einholung einer Einwilligung der auf seiner Website registrierten Nutzer erbracht habe, jedoch nicht genügende Nachweise für die Nutzer der Facebook-Anwendungen präsentiert habe, die angeblich bei der Installation verschiedener Anwendungen ihre Einwilligung gegeben hätten. Die Server des für die Verarbeitung Verantwortlichen hätten bei der Installation einer Facebook-Anwendung durch einen Nutzer von vornherein einige Hintergrunddaten aufzeichnen sollen, wie z. B. den Zeitpunkt der Installation, die IP-Adresse oder Ähnliches. Da der für die Verarbeitung Verantwortliche nichts dergleichen vorzuweisen hatte und stattdessen behauptete, dass die bloße Existenz dieser Daten in seiner Datenbank beweise, dass die Nutzer eine Einwilligung erteilt haben, ordnete die Datenschutzbeauftragte eine Löschung der Daten an. Der für die Datenverarbeitung Verantwortliche leistete dem Folge.

Erfassung biometrischer Daten in einem Fitnessstudio

Bei der Datenschutzbeauftragten ging eine Beschwerde ein, dass ein Fitnessstudio beim Betreten des Gebäudes die biometrischen Daten seiner Kunden kontrolliert und in den Umkleideräumen Überwachungskameras installiert hat. Bei einer Prüfung stellte sich heraus, dass das Fitnessstudio tatsächlich die biometrischen Daten seiner Kunden beim Betreten des Gebäudes kontrollierte, die Kunden sich jedoch zwischen einer Schlüsselkarte mit Chip und ohne biometrische Daten und einer biometrischen Kontrolle entscheiden konnten. Letztere umfasste ein Template des Fingerabdrucks des Kunden. Der für die Verarbeitung Verantwortliche speicherte nicht die Fingerabdrücke der Kunden, sondern lediglich ein Template davon, und war davon überzeugt, dass ein derartiger Vorgang nicht als Verarbeitung biometrischer Daten gelte. Die Datenschutzbeauftragte stellte klar, dass eine Speicherung von Templates eine Verarbeitung biometrischer Daten darstellt. Sie wies das Fitnessstudio an, die Verarbeitung der biometrischen Daten einzustellen, da es für eine solche Verarbeitung keine Rechtsgrundlage gibt. Das Datenschutzgesetz lässt unter bestimmten Bedingungen lediglich eine Verarbeitung von biometrischen Mitarbeiterdaten zu, jedoch nicht von Kundendaten. Außerdem stellte sich heraus, dass das Fitnessstudio in den Umkleideräumen Überwachungskameras installiert hatte, was gesetzlich verboten ist. Die Datenschutzbeauftragte wies das Fitnessstudio an, entweder die Videoüberwachung in den Umkleideräumen einzustellen oder dafür zu sorgen, dass den Kunden andere Räume zur Verfügung stehen, in denen sie sich unbeobachtet umziehen können.

Umleitung der Besucher einer Glücksspiel-Website an eine andere Website

Die Datenschutzbeauftragte leitete ein Verfahren gegen die Aufsichtsbehörde von Glücksspielen ein, das eine Domain registriert hatte, an die alle Besucher von Glücksspiel-Websites, die ohne eine Konzession der Regierung betrieben werden, umgeleitet wurden. Bei einer Prüfung stellte sich heraus, dass es für die

Erfassung und Verarbeitung dieser Besucherdaten keine Rechtsgrundlage gibt. Das Glücksspielgesetz ([16]) sieht zwar vor, dass der Zugang zu solchen Websites eingeschränkt werden kann. Die Verarbeitung der Besucherdaten in Form einer Weiterleitung an die Website des für die Verarbeitung Verantwortlichen sowie eine Verarbeitung der Daten (wie z. B. die IP-Adresse, den Zeitpunkt des Besuchs, Browserdaten usw.) sei jedoch nicht vorgesehen. Die Datenschutzbeauftragte kam zu dem Schluss, dass es sich bei den IP-Adressen sowie bei den Browserdaten um personenbezogene Daten handelt, die einen einzigartigen Fingerabdruck der Besucher darstellen. Die Datenschutzbeauftragte wies den für die Datenverarbeitung Verantwortlichen an, diejenigen Daten aus seiner Datenbank zu löschen, durch die Besucher eindeutig identifizierbar sind, und eine Erfassung solcher Daten in Zukunft zu unterlassen. Der für die Verarbeitung Verantwortliche leistete dieser Anordnung Folge und legte beim Verwaltungsgericht gegen den Beschluss der Datenschutzbeauftragten Berufung ein. Das Gericht hat in dem Fall noch nicht entschieden.

Verarbeitung personenbezogener Daten durch den Fahrradverleih BicikeLJ

Bei der Datenschutzbeauftragten ging eine Reihe von Beschwerden gegen den neuen Fahrradverleih BicikeLJ ein, da der für die Datenverarbeitung Verantwortliche von Nutzern, die sich für den Dienst anmelden wollten, einige personenbezogene Daten verlangte, die im Zusammenhang mit dem Dienst nicht erforderlich waren. Bei einer Prüfung stellte sich heraus, dass der für die Datenverarbeitung Verantwortliche verschiedene personenbezogene Daten zum gewünschten Dienst und zur Zahlungsmethode (Kredit- oder Bankkartendaten) erfasst und verarbeitet. Die Rechtsgrundlage ist der Vertrag zwischen dem Nutzer und dem Dienstleistungserbringer. Es stellte sich heraus, dass der für die Datenverarbeitung Verantwortliche in keinem der Fälle zeigen konnte, dass er für die Vertragserfüllung Daten bezüglich des Geschlechts und der Mobiltelefonnummer der Nutzer benötigte. Außerdem ist es für den für die Datenverarbeitung Verantwortlichen nicht erforderlich, für eine Kreditkartenzahlung die Anschrift des Nutzers zu verlangen. Die Datenschutzbeauftragte kam zu dem Schluss, dass die besagten Daten zwar erfasst und verarbeitet werden dürfen, hierfür jedoch eine freiwillige Einwilligung durch den Nutzer erforderlich ist und der Nutzer die Wahl haben muss, ob er dem Dienstleistungserbringer die Daten bereitstellt oder nicht, da diese Daten für die Erfüllung des Fahrradverleihvertrages nicht zwingend notwendig sind. Der für die Datenverarbeitung Verantwortliche leistete dieser Anordnung Folge und legte beim Verwaltungsgericht gegen den Beschluss der Datenschutzbeauftragten Berufung ein.

C. Sonstige wichtige Informationen

Mitarbeiter der Datenschutzbeauftragten nehmen regelmäßig an internationalen Seminaren und Konferenzen teil, auf denen sie häufig selbst Vorträge halten.

Als nationale Aufsichtsbehörde für den Schutz personenbezogener Daten arbeitet die Datenschutzbeauftragte mit den zuständigen Behörden der Europäischen Union (EU) und dem Rat der Europäischen Union in Datenschutzfragen zusammen.

Im Jahr 2012 beteiligte sich die Datenschutzbeauftragte aktiv an sechs EU-Arbeitsgruppen, die mit der Aufsicht der Umsetzung des Datenschutzes in verschiedenen Bereichen der EU betraut sind, und zwar an Folgenden:

- Artikel-29-Datenschutzgruppe für den Schutz personenbezogener Daten sowie vier ihrer Untergruppen (Technologie, Zukunft des Datenschutzes, verbindliche unternehmensinterne Vorschriften (BCR) sowie Grenzschutz, Reisen und Strafverfolgung (BTLE));
- gemeinsame Kontrollinstanz für Europol;
- gemeinsame Kontrollinstanz für Schengen;

([16]) Offizielles Amtsblatt der slowenischen Republik, Nr. 27/1995 47/2006, s spremembami, v nadaljevanju ZEN.8427/15527 mit Änderungen.

- gemeinsame Kontrollinstanz für Zölle;
- Koordinationssitzungen des Europäischen Datenschutzbeauftragten (EDSB) mit nationalen Behörden für den Schutz personenbezogener Daten zur Überwachung des CIS;
- Koordinationssitzungen des Europäischen Datenschutzbeauftragten (EDSB) mit nationalen Behörden für den Schutz personenbezogener Daten (Eurodac).

Die Datenschutzbeauftragte war auch 2012 die Vizevorsitzende der gemeinsamen Kontrollinstanz für Europol. Im Februar 2012 beteiligte sich ein stellvertretender Datenschutzbeauftragter an der internationalen Arbeitsgruppe, die bei Eurojust in Den Haag eine Datenschutzprüfung durchführte. Des Weiteren beteiligte sich die Datenschutzbeauftragte regelmäßig an der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation (IWGDPT). Ein Vertreter der Datenschutzbeauftragten beteiligte sich 2012 erneut am Beratenden Ausschuss des Europarates (T-PD) zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108).

Die Datenschutzbeauftragte empfing 2012 Vertreter ähnlicher Institutionen verschiedener Länder, darunter Serbien, Georgien, Mazedonien und Albanien, und präsentierte ihnen ihre Aktivitäten und bewährten Verfahren innerhalb ihrer Zuständigkeitsbereiche. Als Juniorpartnerin schloss sie erfolgreich das Partnerschaftsprojekt IPA 2009 Nr. MN/09/IB/JH/03 – Umsetzung einer Strategie zum Schutz personenbezogener Daten in Montenegro – ab und begann mit der Umsetzung des Partnerschaftsprojekts SR/2009/IB/JH/01 – Erhöhung des Schutzes personenbezogener Daten –, das sich auf eine Erhöhung des Datenschutzniveaus in Serbien konzentriert.

Die Datenschutzbeauftragte schloss im September 2012 ihre Arbeit am europäischen LAPSI-Projekt (Legal Aspects of Public Sector Information, rechtliche Aspekte von Informationen im öffentlichen Sektor) ab, dessen Ziel es war, ein thematisches Netzwerk aus Sachverständigen auf dem Gebiet der Wiederverwendung öffentlicher Informationen zur Beseitigung von Hindernissen bei seiner praktischen Umsetzung zu bilden.

SPANIEN

A. Zusammenfassung der Aktivitäten und Neuerungen:

Das Jahr 2012 war im Vergleich zu den Vorjahren noch stärker von einem bemerkenswerten Anstieg der Aktivitäten der Datenschutzbehörde geprägt. Dies betraf vor allen Dingen die Meldungen von Datenverarbeitungen und Prüfungen, die um 15 bzw. 40 % zunahmen. Das ganze Jahr über arbeiteten wir an Maßnahmen zur Vereinfachung und Förderung der Bürgerrechtsausübung und der Einhaltung der Vorschriften. An dieser Stelle sei insbesondere auf unsere neue E-Services-Plattform – https://sedeagpd.gob.es/sede-electronica-web/ – sowie auf die Verbesserungen der Informationsdienste auf unserer Website verwiesen.

Bezüglich der Prüfungen und der Ausübung unserer Sanktionsbefugnis sei darauf hingewiesen, dass ein beträchtlicher Anstieg schriftlicher Verwarnungen (um 34,2 % im Vergleich zu 2011) verzeichnet wurde, wenngleich die Zahlen der Geldbußen unverändert geblieben ist. Diese Möglichkeit hat zusammen mit einer Reihe von Kriterien, die eine Abstufung der Geldbußen ermöglichen, dazu geführt, dass die Schwere der Sanktion besser auf die Schwere und die realen Konsequenzen des Verstoßes abgestimmt werden kann.

Die Datenschutzbehörde setzte außerdem ihre Bemühungen für einen höheren Schutz von Kindern fort. In dieser Hinsicht arbeiteten wir das ganze Jahr über intensiv an einer pädagogischen Website, die sowohl Kindern als auch Pädagogen einschlägige Informationen und Hilfsmittel bereitstellt und höchstwahrscheinlich im letzten Quartal 2013 online gestellt wird.

Ein weiterer Schwerpunkt lag auf der Umsetzung der Reform der Datenschutzrichtlinie für elektronische Kommunikation, die per Königlicher Verordnung im April 2012 in spanisches Recht umgesetzt wurde. Seitdem arbeitet die Datenschutzbehörde mit allen nationalen und internationalen Interessenvertretern zusammen. Als Ergebnis dieser Arbeit werden 2013 Leitlinien und Hilfsmittel im Zusammenhang mit der richtigen Anwendung von Cookies mithilfe von Vorkehrungen und Meldungen von Datenschutzverstößen veröffentlicht.

Organisation	Spanische Datenschutzbehörde
Vorsitz und/oder Gremium	José Luis Rodríguez Álvarez
Budget	13 929 550 EUR
Personal	159
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	11 907
Meldungen	630 251
Vorabprüfungen	k. A.
Anträge betroffener Personen	111 933
Beschwerden betroffener	10 787

Personen	
Vom Parlament bzw. der Regierung angeforderte Beratung	292
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2 266
Sanktionsmaßnahmen	
Sanktionen	896
Geldbußen	21 054 656,02 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Zunächst sei das Urteil des Obersten Gerichtshofs vom Februar 2012 zur Beilegung von Rechtsmitteln im Zusammenhang mit der Königlichen Verordnung 1720/2007 vom 21. Dezember zu nennen, mit der die Regulierung zur Umsetzung des Gesetzes 15/1999 vom 13. Dezember zum Schutz personenbezogener Daten angenommen wurde. Der Beschluss erklärte Artikel 10.2.(b) der Regulierung im Hinblick auf eine Vorabentscheidung des EuGH (Urteil vom 24.11.2011 in den Rechtssachen C-468/10 und C-469/10 – ASNEF/FECEMD) für ungültig.

Weitere nennenswerte Beschlüsse des Obersten Gerichtshofs lauten wie folgt:

Informationen im Zusammenhang mit dem Urteil zu einem Fall sexuellen Missbrauchs gelten nicht als Daten zum Sexualleben im Sinne von Artikel 8 der Richtlinie 95/46.

Eine Zustimmungsklausel, die eine Zusendung von Werbeangeboten von einer Unternehmensgruppe erlaubt, könnte als ausreichend erachtet werden, um von selbigen Unternehmen Stellenangebote zu senden.

Die Beweislast im Zusammenhang mit der Einhaltung der Informationspflicht liegt beim für die Verarbeitung Verantwortlichen.

Videoüberwachungsgeräte dürfen nur dann dazu verwendet werden, die Einhaltung von Arbeitszeiten zu überwachen, wenn die Mitarbeiter ausdrücklich im Voraus darüber informiert wurden, dass diese Möglichkeit besteht.

Es liegt ein Verstoß gegen die Geheimhaltungspflicht vor, wenn Gesundheitsdaten – in diesem Fall eine Liste mit den Patienten, die mit Methadon behandelt werden – an der Anschlagtafel eines Gesundheitszentrums veröffentlicht werden. Gleiches gilt, wenn Daten über ein Peer-to-peer-Dateiaustauschsystem zugänglich gemacht werden.

Ebenfalls im Zusammenhang mit der Geheimhaltungspflicht gilt die Veröffentlichung der Verurteilung eines Angestellten des öffentlichen Diensts für eine Straftat in einem Amtsblatt als Verstoß gegen die Geheimhaltungspflicht.

Die bloße Existenz einer Beschwerde verpflichtet die Aufsichtsbehörde nicht zur Einleitung eines Verstoßverfahrens.

Der Nationale Gerichtshof (Audiencia Nacional) war 2012 ebenfalls mit Datenschutzangelegenheiten befasst. Einige relevante Urteile lauten wie folgt:

- Bilder von Kindern dürfen nur dann in sozialen Netzwerken veröffentlicht werden, wenn zuvor die Einwilligung der Eltern oder Erziehungsberechtigten eingeholt wurde. Ebenso ist die Einführung von Mechanismen zur Altersverifizierung sowie die Einholung der elterlichen Einwilligung verpflichtend, wenn ein für die Verarbeitung Verantwortlicher im Rahmen von Marketingkampagnen im Internet die Daten von Kindern verarbeiten möchte.
- Bezüglich der Entscheidung des Obersten Gerichtshofs zur Ausübung berechtigter Interessen als Rechtsgrundlage für eine Datenverarbeitung hat der Nationale Gerichtshof mehrere Urteile gefällt, von denen die folgenden besonders erwähnenswert sind:
    - Das berechtigte Interesse einer Zeitung wurde als stärker vorhanden erachtet, wenn die Angaben zu Sanktionsbescheiden im Zusammenhang mit Inhabern öffentlicher Ämter veröffentlicht wurden. Gleiches gilt für die Veröffentlichung von Identifikationsdaten der Bewerber für Stellen in der öffentlichen Verwaltung.
    - Das berechtigte Interesse einer Gewerkschaft wurde für die interne Verarbeitung von Mitarbeiterdaten und zu direkt mit Arbeitnehmervertretungsaufgaben verbundenen Zwecken als stärker vorhanden erachtet.
    - Gleiches gilt für die Nutzung der Kontaktdaten von Mitgliedern einer beruflichen Kammer durch andere Mitglieder im Rahmen eines internen Wahlverfahrens.
    - Andererseits wurde das Interesse am Erstellen einer Datenbank mit den Daten von 37 Millionen Menschen nicht vermehrt als vorhanden erachtet, wenn das angebliche Interesse der bloßen Absicht der Vermarktung der Datenbank galt.
- Das Hinzufügen von Bildern als Beweismittel, die ein Privatdetektiv im Rahmen eines Prozesses aufgenommen hatte, wurde als rechtmäßig erachtet, als die Bilder im Laufe des Verfahrens vom Richter akzeptiert wurden. Im Gegensatz dazu wurde es als rechtswidrig erachtet, Bilder einer Einzelperson im Schaufenster eines Fotografen auszustellen, ohne deren Einwilligung eingeholt zu haben.
- Der Aufdruck des Begriffs „celiac patient“ (Zöliakiepatient) auf den Briefumschlag wurde im Rahmen einer Produktwerbung als Verarbeitung von Gesundheitsdaten erachtet. Ebenfalls auf dem Gebiet der sensiblen Daten wurde das Einrichten eines falschen Profils, mit dem vorgegeben wurde, ein Dritter zu sein, in einem sozialen Netzwerk, das sich in erster Linie an Homosexuelle richtet, als Verarbeitung von Daten zum Sexualleben erachtet.

C. Sonstige wichtige Informationen

Der sogenannte Google-Fall spielte im Berichtszeitraum aufgrund der themenbezogenen Fragen und der Beteiligung des Europäischen Gerichtshofs auf Antrag des spanischen Gerichtshofs ebenfalls eine wichtige Rolle. Der Fall selbst begann mit dem Antrag eines Bürgers auf Ausübung des Widerspruchsrechts bezüglich der Datenverarbeitung durch eine Zeitung – eine öffentliche Bekanntmachung vor mehreren Jahren – im Zusammenhang mit Daten, die er trotz der Tatsache, dass sie ihn bis in die Gegenwart betreffen könnten und problemlos per Suchmaschine im Internet gefunden werden können, nicht nur als veraltet, sondern als irrelevant erachtete.

Die Zeitung verweigerte die Löschung der Daten mit der Begründung, dass sie aufgrund einer gesetzlichen Verpflichtung veröffentlicht wurden, die sich aus einer Anordnung durch eine zuständige Behörde ergab.

In einem zweiten Schritt übte der Bürger sein Widerspruchsrecht gegen Google aus und beantragte die Löschung von Links, die auf den Artikel auf der Website der Zeitung verwiesen. Dies richtete sich gegen Google Spain, SL. Auch dieser Antrag wurde von dem Unternehmen abgelehnt.

Schließlich beschwerte sich der Bürger bei der spanischen Datenschutzbehörde, um von seinem Recht Gebrauch zu machen. Er bezog sich dabei auf die beiden Unternehmen Google Inc. und Google Spain, SL.

Als Reaktion auf die Beschwerde forderte die spanische Datenschutzbehörde Google Inc. und Google Spain in einem Beschluss dazu auf, ihren Verpflichtungen nachzukommen. Bezüglich der Zeitung wurde nichts unternommen.

Beide Unternehmen legten vor dem nationalen Gerichtshof Berufung ein. Das Gericht befasste sich neben mehreren früheren Beschlüssen zu ähnlichen Fällen mit der Rechtssache. Aufgrund der zunehmenden Zahl von Anträgen und der Beschaffenheit der betreffenden Angelegenheiten beschloss das Gericht, eine öffentliche Anhörung anzuberaumen, bei der beide Parteien ihre Ansichten darlegen. Das Gericht beschloss außerdem, den Europäischen Gerichtshof um eine Vorabentscheidung zu bitten.

Es ging dabei um zwei wichtige Fragen:

a) Einerseits um den Anwendungsbereich der Richtlinie 95/46 bezüglich der den EU-Bürgern von Google Inc. bereitgestellten Diensten. Vor diesem Hintergrund legte das Gericht einen Fragenkatalog bezüglich des Anwendungsbereichs von Artikel 4.1 der Richtlinie vor, da Google Spain, SL als Tochtergesellschaft von Google Inc. mit der Suchmaschine geschäftlich tätig war. Des Weiteren wurde berücksichtigt, dass Google Spain, SL von Google Inc. ausdrücklich als Vertreterin ernannt wurde, um Letzterer Forderungen und Anträge von spanischen Bürgerinnen und Bürger zu übermitteln. Außerdem bat das Gericht in Bezug auf die Wendung „Ausrüstung auf dem Gebiet eines Mitgliedstaates“ um Klärung. In diesem Sinne erwähnte das Gericht unmittelbar den Artikel 8 des EMRK und ließ verlauten, dass es gerechtfertigt sei, das Gesetz des Landes anzuwenden, in dem der Konflikt ausgetragen wird, um einen wirkungsvollen Schutz der Bürger zu gewährleisten.

b) b. Andererseits wurde ein Fragenkatalog zur Beschaffenheit der Suchmaschinen vorgelegt. Zunächst fragte das Gericht unter Berücksichtigung der in der Richtlinie enthaltenen Bestimmung des Begriffs Datenverarbeitung nach der Möglichkeit, eine Indexierung im Sinne der Richtlinie 95/46 als Verarbeitung personenbezogener Daten zu erachten. Unter der Annahme einer positiven Antwort richtete sich die zweite Frage an die wahre Beschaffenheit der rechtlichen Verantwortlichkeiten des Unternehmens, das die Dienste anbietet … direkt, voll oder einfach als Tochtergesellschaft des für die Datenverarbeitung Verantwortlichen, der für das Internet verantwortlich ist, in dem die Informationen ursprünglich verarbeitet wurden. Unter diesen Voraussetzungen und gemäß den Kriterien des EuGH wäre eine Auslegung im Sinne einer direkten Ansprache des für die Suchmaschine Verantwortlichen möglich, um die Indexierung der betroffenen Informationen zu vermeiden.

Eine endgültige Entscheidung wird im letzten Quartal 2013 erwartet.

TSCHECHISCHE REPUBLIK

A. Zusammenfassung der Aktivitäten und Neuerungen

Das internationale Projekt „Raising awareness of data protection issues among employees working in the EU" (Verbessern des Bewusstseins zu Datenschutzthemen unter den in der EU tätigen Arbeitnehmern) wurde vom Leonardo-da-Vinci-Partnerschaftsprogramm **gefördert**. Im Rahmen des Projekts wurde ein umfassendes Handbuch für ein breites Publikum europäischer Arbeitnehmer erstellt, das durch Sensibilisierungsveranstaltungen ergänzt wurde. Am Projekt beteiligt sind Datenschutzbeauftragte aus Polen (Projektkoordinator), der Tschechischen Republik, Bulgarien und Kroatien. Das Projekt läuft bis Juli 2014.

Vom 12. bis 14. März 2012 veranstaltete unser Amt für drei Mitarbeiter der albanischen Datenschutzbehörde einen **dreitägigen Studienbesuch**. Die Veranstaltung wurde von TAIEX finanziert und konzentrierte sich auf die Bearbeitung von Beschwerden, Überprüfungsverfahren, Registrierung und Aktivitäten der Presseabteilungen.

Vom 11. bis 12. Juni 2012 hielt eine unserer Fachkräfte einen Vortrag auf dem **TAIEX-Seminar**, das sich mit den Themen Überprüfungen und Einhaltung der Datenschutzvorschriften befasste und vom mazedonischen Datenschutzbeauftragten in Skopje ausgerichtet wurde.

Am Datenschutztag veranstalteten wir zum sechsten Mal den **Kinder- und Jugendwettbewerb** „My privacy! Don't look, don't poke about!" (Meine Privatsphäre! Nicht kucken, nicht rumstöbern!), der das Bewusstsein zu Datenschutz unter der jungen Generation fördern soll. Diesmal konzentrierten wir uns auf die Nutzung des Internets und ermutigten die Teilnehmer dazu, sich in Form eines Aufsatzes, einer Erzählung, eines Videoclips oder eines Comics mit den Folgen für den Datenschutz auseinanderzusetzen. Von den insgesamt 67 Einsendungen wurden die drei besten ausgezeichnet.

Organisation	Amt für Datenschutz – Tschechische Republik
Vorsitz und/oder Gremium	Dr. Igor Němec, Präsident
Budget	146 219 000 CZK = 5 665 207 EUR (Wechselkurs August 2013: 25,81 CZK/EUR)
Personal	97 Festanstellungen (von denen 10 in den Bereichen Gebäudemanagement und Buchhaltung tätig und demnach nicht direkt mit Datenschutz befasst sind).
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	12 Stellungnahmen (vorwiegend zu den Themen Videoüberwachung, Internet und Marketing). Veröffentlichung einer umfassenden Methodik für Betreiber von Videoüberwachungssystemen (auch in englischer Sprache erhältlich).
Meldungen	5 169 Meldungen (davon 4 618 registriert). Die Anzahl der gemeldeten für die Verarbeitung Verantwortlichen liegt bei 3 397, da einige von ihnen mehr als nur eine Verarbeitung registriert haben.

Vorabprüfungen	105
Anträge betroffener Personen	2 503 (davon 47 von ausländischen betroffenen Personen). Konsultationen wurden nicht nur von natürlichen Personen, sondern auch von juristischen Personen und öffentlichen Stellen in Anspruch genommen.
Beschwerden betroffener Personen	Beschwerden: 1 319 (davon 197 zur weiteren Prüfung, 69 bzgl. Verwaltungsverfahren, 13 zur Weiterleitung an andere öffentliche Verwaltungsstellen, 1 040 als ungerechtfertigt abgelehnt). Darüber hinaus betrafen 7 933 Meldungen (davon 3 772 abgeschlossen) das Thema Spam.
Vom Parlament bzw. der Regierung angeforderte Beratung	Das Parlament nahm zweimal Beratungsdienste in Anspruch: zum Thema PNR und zum Entwurf des Datenschutzgesetzes.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Im Rahmen des **interministeriellen Stellungnahmeverfahrens** beurteilten und kommentierten wir 85 Gesetzentwürfe und 94 Entwürfe von Durchführungsverordnungen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	129 eingeleitete Prüfungen (Untersuchungen), 9 abgeschlossen (wurden im Vorjahr eingeleitet). Diese Zahl umfasst keine Maßnahmen im Zusammenhang mit Spam. Auf diesem Gebiet wurden 87 Prüfungen eingeleitet und auch abgeschlossen (sowie eine weitere, die im Vorjahr eingeleitet wurde).
Sanktionsmaßnahmen	
Sanktionen	49 Sanktionen. Darüber hinaus wurden im Zusammenhang mit Spam drei Sanktionen verhängt. Anmerkung: Unter Sanktionen wird eine nichtfinanzielle Abhilfemaßnahme verstanden, die einem für die Datenverarbeitung Verantwortlichen auferlegt wird. Im Rahmen einer Untersuchung wurde oft eine Reihe unterschiedlicher Sanktionen (Abhilfemaßnahmen) verhängt, doch zum Zweck dieser Informationen gilt eine Reihe von Sanktionen im Rahmen einer bestimmten Untersuchung als eine Sanktion. Der Durchschnitt pro Aktion liegt bei etwa 2,7.
Geldbußen	125 Geldbußen, davon 23 Geldbußen im Zusammenhang mit Spam.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	K. A. Das tschechische Recht sieht keine Datenschutzbeauftragten vor.

B. Rechtsprechung

Auf der Grundlage eines Antrags wurde **bei der Tschechischen Post eine Überprüfung** eingeleitet. Die Zusteller trugen ein GPS-Gerät bei sich, mit dem ihre Aufenthaltsorte überwacht wurden. Nach eigenen Angaben habe die Tschechische Post das System eingeführt, um Kundenbeschwerden nachzugehen, laut derer die Mitarbeiter ein Paket/Einschreiben nicht zugestellt hätten. Die Datenschutzbehörde kam zu dem Schluss, dass für die Verarbeitung personenbezogener Daten (Überwachung der Außendienstmitarbeiter) eine Rechtsgrundlage fehlt und die Tschechische Post gegen das Datenschutzgesetz verstößt. Die Tschechische Post legte 2012 gegen dieses Ergebnis Widerspruch ein. Der Fall wurde daher an ein Verwaltungsverfahren übergeben.

Infolge einer Kundenbeschwerde bezüglich die Nutzung der auf der Kundenkarte gespeicherten personenbezogenen Daten führten wir **bei einer Apothekenkette eine Überprüfung** durch. Der Prüfer vermutete einen Verstoß gegen das Datenschutzgesetz, insbesondere gegen zwei Artikel im Zusammenhang mit der Löschung von Daten und den Rechten der betroffenen Personen. Außerdem verarbeitete das Unternehmen sensible Kundendaten. Als offizieller Zweck der Verarbeitung wurde die Pflege der Krankenakten der Kunden angegeben, um Kontraindikationen, Wechselwirkungen mit verschriebenen Arzneimitteln oder Allergien zu erkennen. Alle Daten wurden mit der schriftlichen Genehmigung der betroffenen Personen erfasst. Die Prüfung ergab, dass das Unternehmen ausreichende technische und organisatorische Maßnahmen eingeführt hatte. Es wurde jedoch versäumt, die Daten auf Kundenwunsch oder nach einer Kündigung der Kundenkarte sofort zu löschen. Der Grund dafür war eine unzureichende Schulung der Mitarbeiter. Das Versäumnis wurde noch während der Prüfung behoben. Daher wurden keine Sanktionen oder Geldbußen verhängt.

In einem Prager Krankenhaus wurde eine Doppelprüfung durchgeführt. Der erste Teil der Prüfung wurde aufgrund des jährlichen Prüfplans durchgeführt und konzentrierte sich auf Identifikationsarmbänder für Patienten. Der zweite Teil erfolgte nach einer Beschwerde aufgrund eines Videos einer Operation, das zusammen mit den personenbezogenen Daten des Patienten (Name, Teil des Nachnamens, Geburtsdatum) ins Internet gestellt wurde und eine Identifizierung des Patienten erlaubte. Die Armbänder werden jedem Patienten bei der Aufnahme ausgehändigt. Standardpatienten erhalten ein blaues, Patienten mit ernsthaften Diagnosen ein gelbes. Die Armbänder enthalten unterschiedliche Daten bezüglich Identifikation, Diagnose, Behandlung usw. Der Strichcode auf diesen Armbändern ist lediglich aus 10 bis 20 cm Entfernung lesbar und schließt eine Standortüberwachung der Patienten im Krankenhausbereich aus. Im Fall des Online-Videos legte die Krankenhausleitung ein Formular vor, das die Einwilligung des betroffenen Patienten in Kenntnis der Sachlage enthielt. Man wies außerdem darauf hin, dass die Offenlegung des Geburtsdatums des Patienten nicht dem primären Zweck des Vorgangs diente. Daraufhin entfernte man das gesamte Material aus dem Internet. Der Prüfer kam demnach zu dem Schluss, dass in keinem der Fälle ein Verstoß gegen das Datenschutzgesetz vorliegt.

Eine weitere Stichprobenprüfung wurde bei einer **Wohnungsbaugesellschaft** durchgeführt, die im Internet eine (öffentlich zugängliche) Liste ihrer Schuldnermitglieder einschließlich Name, Nachname und Schuldenhöhe veröffentlicht hatte. Die Gesellschaft ist dazu befugt, Daten über die Höhe der Schulden ohne die Einwilligung der Schuldner zu speichern, wie es das Datenschutzgesetz vorsieht: Personenbezogene Daten dürfen verarbeitet werden, wenn dies erforderlich ist, um die Rechte und rechtlichen Interessen des für die Verarbeitung Verantwortlichen zu wahren. Andererseits darf eine derartige Verarbeitung nicht die Rechte der betroffenen Personen auf Datenschutz und Privatsphäre beeinträchtigen. Die betreffende Verarbeitung würde nicht im Widerspruch zu den Rechten dieser betroffenen Personen stehen, wenn lediglich die Mitglieder der Gesellschaft, die gleichzeitig die Gläubiger sind, darauf zugreifen könnten. Für eine uneingeschränkte Offenlegung im Internet wäre die Einwilligung der Schuldner erforderlich. Demzufolge hat die Wohnungsbaugesellschaft mit der Veröffentlichung der Schuldnerliste zusammen mit der Höhe ihrer Schulden auf der öffentlich zugänglichen Website der Gesellschaft gegen das Datenschutzgesetz verstoßen. Die Datenschutzbehörde verhängte eine Geldbuße gegen die Gesellschaft. Der für die Verarbeitung Verantwortliche hat als Abhilfemaßnahme die entsprechende Webseite mit Passwortschutz versehen.

Weitere interessante Fälle werden im Jahresbericht der tschechischen Datenschutzbehörde ausführlich dargelegt. Die englischsprachige Version ist verfügbar auf: http://www.uoou.cz/uoou.aspx?menu=159&lang=en .

C. Sonstige wichtige Informationen

Wir begannen das Jahr 2012 mit einer neuen Kompetenz im Zusammenhang mit **Meldungen von Verstößen gegen den Datenschutz** im Bereich der elektronischen Kommunikation. Diesbezüglich haben wir einen speziellen Abschnitt auf der Website der Behörde eingerichtet, der eine Liste der einschlägigen Regulierungen sowie eine Erläuterung der Verpflichtungen und Meldeformulare (eines für die Verstoßmeldungen durch die Behörde und eines für Meldungen durch Betroffene) enthält. Insgesamt erhielten wir im Berichtszeitraum nur eine Meldung (2013 erhielten wir bislang ebenfalls eine Meldung).

Es wurden Prüfungen in drei **Botschaften und Konsulaten** der Tschechischen Republik (Russland, Türkei und Kasachstan) durchgeführt. Diese konzentrierten sich jeweils auf die Verarbeitung personenbezogener Daten im Rahmen des Visaverfahrens und des Schengener Informationssystems. Außerdem wurde die physische Sicherheit der Datenbanken überprüft.

Wir erhielten 18 Anträge für **internationale Datenübermittlungen**, von denen keine abgelehnt, 13 genehmigt und fünf aus verfahrenstechnischen Gründen ausgesetzt wurden.

UNGARN

A. Zusammenfassung der Aktivitäten und Neuerungen:

Organisation	Nationale Behörde für Datenschutz und Informationsfreiheit
Vorsitz und/oder Gremium	Dr. Attila Péterfalvi
Budget	390 211 000 HUF
Personal	59
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2 152 (Datenschutz: 1 825, Informationsfreiheit: 327)
Meldungen	12 166
Vorabprüfungen	Datenschutzprüfungen sind per Gesetz ab dem 1. Januar 2013 erlaubt.
Anträge betroffener Personen	1 388 (Datenschutz: 1 212, Informationsfreiheit: 176)
Beschwerden betroffener Personen	764
Vom Parlament bzw. der Regierung angeforderte Beratung	207 + 46 (Anreize für Gesetzesänderungen)
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2 152
Sanktionsmaßnahmen	
Sanktionen	
Geldbußen	11
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Ausrichtung der DPO-Konferenz (Juni 2012)

B. Rechtsprechung

B1) rechtswidrige Datenverarbeitung – Anbieter von Websites (www.ingatlandepo.com und www.ingatlanbazar.com)

Die ungarische Datenschutzbehörde erlegte einem Website-Anbieter (im Folgenden „Beklagter") eine Geldbuße in Höhe von 10 000 000 HUF auf. Dies entspricht dem gesetzlichen Höchstbetrag. Für die Inserate von Immobilien im Namen der betroffenen ungarischen Personen (im Folgenden „Kläger") auf der Website des Beklagten wurden zwischen den beiden Parteien Verträge abgeschlossen.

Wenn die Immobilien verkauft waren, die Inserate verfielen oder die Kläger ihre Inserate einfach löschen oder sie vom Beklagten löschen lassen wollten, geschah dies jedoch nicht. Trotz der nachdrücklichen und wiederholten Anfragen wurden die Inserate vom Beklagten nicht gelöscht. Außerdem gab der Beklagte die personenbezogenen Daten der Kläger u. a. an Forderungsmanagementunternehmen weiter.

Diesbezüglich gingen beim ungarischen DBA zahlreiche Beschwerden ein. Daher eröffnete die Datenschutzbehörde ein Ermittlungsverfahren und rief den Beklagten dazu auf, innerhalb einer festgelegten Frist zu seinem Verhalten Stellung zu nehmen. Da der Beklagte es versäumte, innerhalb der von der Datenschutzbehörde vorgegebenen Frist Stellung zu nehmen und während des Verfahrens die Zusammenarbeit verweigerte, leitete die Datenschutzbehörde ein Datenschutzverfahren ein.

Infolge des Datenschutzverfahrens kam die Datenschutzbehörde zu dem Schluss, dass der Beklagte mehrfach gegen das Recht auf Datenschutz der Kläger verstoßen hat. Der Beklagte 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 Beklagte die zahlreichen Einwände der Kläger im Hinblick auf die Datenverarbeitung durch den Beklagten. Daher fehlte dem Beklagten die rechtliche Grundlage für verschiedene Datenverarbeitungsaktivitäten.

Demzufolge beschloss die Datenschutzbehörde, in Bezug auf die hohe Anzahl der Personen, die von dem Verstoß betroffen sind, sowie dessen Schwere und Wiederholung zusammen mit der mangelnden Bereitschaft des Beklagten zu einer Zusammenarbeit mit den relevanten staatlichen Behörden und Interessenvertretern eine Geldbuße zu verhängen, und veröffentlichte ihren Beschluss, die Rechte einer größeren Anzahl betroffener Personen zu schützen.

Die Rechtssache ist noch anhängig.

B2) Google Street View (GSV)

Nach zahlreichen Konsultationen mit Vertretern von Google Inc. (Anbieter von GSV), mehreren Prüfungen durch den ehemaligen Datenschutzbeauftragten im Jahr 2009 und der Berücksichtigung neuer Urteile (C-468/10 und C-469/10) des EuGH gab die ungarische Datenschutzbehörde eine Stellungnahme heraus, in der sie die Einführung von GSV in Ungarn unter der Voraussetzung genehmigte, dass Google die von der Datenschutzbehörde in ihrer Stellungnahme aufgeführten geltenden Grundsätze und Bedingungen des Datenschutzes (u. a. eine vorherige Benachrichtigung der Bevölkerung, das Ermöglichen einer Löschung auf Antrag der betroffenen Personen; eine schnellstmögliche Unkenntlichmachung personenbezogener Daten usw.) einhält.

B3) Nutzung von Videoüberwachungsgeräten an Arbeitsplätzen

Bei der Datenschutzbehörde sowie beim ehemaligen Datenschutzbeauftragten (im Folgenden DS-Beauftragter) sind in den letzten Jahren zahlreiche Petitionen eingegangen, mit denen sich die Antragsteller über die weit verbreitete Nutzung von Videoüberwachungsgeräten an Arbeitsplätzen beklagen.

Ab 2012 wurden sowohl das ehemalige Arbeitsgesetzbuch als auch das Datenschutzgesetz von 1992 durch neue Rechtsinstrumente ersetzt. Das neue Arbeitsgesetzbuch, das zum 1. Juli 2012 in Kraft trat, enthält bereits geltende Vorkehrungen (§§ 9 und 11), die hinsichtlich Videoüberwachungsgeräten an Arbeitsplätzen berücksichtigt werden müssen. Diese allgemeinen Vorkehrungen können jedoch zu einer unterschiedlichen Umsetzung des Rechts auf informationelle Selbstbestimmung führen.

Infolge einer gründlichen Prüfung hat die Datenschutzbehörde eine Empfehlung abgegeben, in der Leitlinien vorgeschlagen werden, die es Arbeitgebern ermöglichen sollen, die gesetzlichen Anforderungen an den Datenschutz am Arbeitsplatz einzuhalten.

B4) Biometrische Identifizierung

Eine Frau stellte einen Antrag auf eine offizielle Erklärung der Datenschutzbehörde zu der Frage, ob die Datenverarbeitung einer Schule rechtmäßig sein könne, falls diese an den Eingängen ein biometrisches Identifikationssystem einführen würde.

Im Hinblick auf die einschlägigen nationalen und EU-Vorschriften wurde der Frau Folgendes mitgeteilt:

Die Fingerabdrücke einer natürlichen Person stellen personenbezogene Daten und deren Erfassung eine Verarbeitung ebendieser dar. Sowohl die einschlägige nationale Gesetzgebung als auch die EU-Datenschutzrichtlinie sehen wesentliche rechtliche Grundsätze vor, die auch bei einer Datenverarbeitung berücksichtigt werden müssen. Hierzu gehört z. B. der Grundsatz der Verhältnismäßigkeit (et al.).

Die Datenschutzbehörde kam zu dem Schluss, dass ein biometrisches System – zur Erfassung der Fingerabdrücke von Schülern beim Betreten der Schule – zum Zwecke der Sicherheit und dem Schutz des Eigentums nicht dem Verhältnismäßigkeitsgrundsatz entspreche. Eine bessere Identifikation könne auch durch andere – harmlosere und weniger auf Kosten der Privatsphäre gehende – Methoden erzielt werden.

Demzufolge würde die Einführung eines solchen Zugangssystems das Recht auf Datenschutz der betroffenen Personen gefährden.

B5) Cloud-Computing

Eine politische Vereinigung hat bei der Datenschutzbehörde eine Petition eingereicht und eine Stellungnahme zur Rechtmäßigkeit der Datenverarbeitung durch die politische Vereinigung beantragt. Die Vereinigung (im Folgenden „der für die Datenverarbeitung Verantwortliche“) möchte die personenbezogenen Daten ihrer Anhänger mithilfe von Cloud-Computing-Technologie verarbeiten. Außerdem plane man, einen Cloud-Computing-Anbieter zu wählen, dessen Muttergesellschaft zwar in den USA registriert ist, jedoch eine Tochtergesellschaft in Irland unterhält. Der betreffende Dienstleistungsanbieter sei auf der Safe-Harbour-Liste des US-Handelsministeriums aufgeführt.

Die Datenschutzbehörde kam zu dem Ergebnis, dass die Sicherheitsbedenken aufgrund der Vertraulichkeit der personenbezogenen Daten von Anhängern einer politisch aktiven Vereinigung erheblich verstärkt werden. Demnach sprach sich die Datenschutzbehörde gegen die Übermittlung solcher personenbezogenen Daten zur „Cloud“ aus.

B6) Hackerangriff auf die Website von Capital Mineral Water and Beverage Co. Ltd.

Im Oktober 2012 soll eine türkische Hackergruppe einen Angriff auf die Website der besagten Firma getätigt haben. Dabei wurden mehr als 50 000 personenbezogene Datenelemente (Name, E-Mail-Adresse, Geburtsdatum usw.) entwendet. Daraufhin gab die Datenschutzbehörde eine Stellungnahme ab, in der hinterfragt wurde, weshalb die personenbezogenen Daten von Verbrauchern online zugänglich und unverschlüsselt waren. Gleichzeitig rief die Behörde zu einer verstärkten Ergreifung und Anwendung von Maßnahmen zur Datensicherheit auf, um ähnliche Verstöße gegen den Datenschutz zu vermeiden.

Diesbezüglich wird weiterhin ein Verwaltungsverfahren aufgrund eines Verstoßes gegen den Datenschutz durchgeführt.

B7) Finanzielle Sanktion gegen einen Website-Anbieter

Die Datenschutzbehörde erhielt eine Beschwerde, in der eine Einzelperson angab, von einem Unternehmen unerwünschte Marketing-E-Mails zu erhalten, ohne dem zugestimmt zu haben. Außerdem habe das Unternehmen trotz wiederholter Aufforderungen den Dienst nicht eingestellt und die Kontaktdaten der betroffenen Person nicht gelöscht.

Nach einer Prüfung und einem anschließenden Verwaltungsverfahren aufgrund eines Verstoßes gegen den Datenschutz erhob die Datenschutzbehörde eine Geldbuße in Höhe von 3 Mio. HUF. Die hohe Summe wurde aufgrund der folgenden erschwerenden Umstände beschlossen: die hohe Anzahl der von einer rechtswidrigen Datenverarbeitung betroffenen Personen, die hohe Anzahl betroffener Minderjähriger, die Schwere des Verstoßes sowie die außergewöhnlich lange Dauer der rechtswidrigen Situation. Mildernde Umstände wurden ebenfalls wie folgt berücksichtigt: das Erstellen einer neuen Datenschutzrichtlinie und deren Veröffentlichung auf der Website sowie die Meldung der Änderungen beim Datenschutzregister. Die Bereitschaft des für die Verarbeitung Verantwortlichen, mit der Datenschutzbehörde zu kooperieren, wurde durch die schnelle Durchführung der notwendigen Modifikationen deutlich, die sofort nach der Einleitung des Verwaltungsverfahrens vorgenommen wurden.

B8) Datenverarbeitung durch Dating-Websites

Die Datenschutzbehörde untersuchte einen Fall, bei dem einem ungarischen Betreiber von rund 40 Websites (im Folgenden „Unternehmen“) aufgrund eines Verstoßes gegen die Datenschutzrechte Minderjähriger und der damit verbundenen rechtswidrigen Datenverarbeitungsaktivitäten u. a. im Zusammenhang mit bereitgestellten E-Mail-Marketingdiensten eine Geldbuße in Höhe von 3 Mio. HUF auferlegt wurde. Der Fall wurde aufgrund einer Beschwerde eines Bürgers gegen das Unternehmen eingeleitet, in der er behauptete, dass er laufend ohne seine Einwilligung Werbe-E-Mails erhalte, das Unternehmen trotz seiner entsprechenden Aufforderung seine Daten nicht gelöscht habe und ihm sogar weiterhin die Newsletter des Unternehmens zugeschickt habe.

Bei ihren Ermittlungen stellte die Datenschutzbehörde fest, dass die Angaben zur Datenverarbeitung auf den vom Unternehmen betriebenen Websites, einschließlich der Übermittlung von Daten an Dritte bei der Registrierung, nicht eindeutig genug waren. Die Nutzer hatten nicht die Möglichkeit, ihre Einwilligung in den Erhalt von Marketing-E-Mails zu erteilen, da die Einwilligung als automatisch mit der Registrierung erteilt betrachtet wurde. Des Weiteren stellte sich heraus, dass die Informationen zum Zweck der Datenverarbeitung unzureichend waren und Nutzer nicht die Möglichkeit hatten, sich vom Newsletter des Unternehmens abzumelden. Bei ihren Ermittlungen fiel der Datenschutzbehörde außerdem ein weiteres, äußerst bedenkliches Problem auf, nämlich die schlecht verwaltete Registrierung Minderjähriger insbesondere auf Dating-Websites.

Die Rechtsgrundlagen, auf die die Datenschutzbehörde ihren Beschluss gründete, waren Gesetz CXII von 2011 über die informationelle Selbstbestimmung und Informationsfreiheit, Gesetz XLVII von 2008 zum Verbot unlauterer Geschäftspraktiken gegenüber Verbrauchern, Gesetz CVIII von 2001 über elektronischen Geschäftsverkehr und Gesetz IV von 1959 über das Bürgerliche Gesetzbuch. Die Datenschutzbehörde berücksichtigte außerdem die Stellungnahmen 5/2004, 5/2009 und 15/2011 der Artikel-29-Datenschutzgruppe zu sozialen Online-Netzwerken, die Empfehlung 2006/952/EG des Europäischen Parlaments und des Rates vom 20. Dezember 2006 über den Schutz Minderjähriger und den Schutz der Menschenwürde und über das Recht auf Gegendarstellung im Zusammenhang mit der Wettbewerbsfähigkeit des europäischen Industriezweiges der audiovisuellen Dienste und Online-Informationsdienste sowie den Bericht KOM(2011) 556 der Europäischen Kommission zum Schutz von Kindern in einer digitalen Welt.

Die Datenschutzbehörde schloss ihr Verwaltungsverfahren (neben anderen, kleineren Einwänden) mit der Aussage ab, dass die Datenverarbeitung des Unternehmens mit den erwähnten Rechtsakten mit und ohne Rechtscharakter nicht im Einklang stehen. Die Verarbeitung stellte eine ernsthafte Gefährdung der Rechte Minderjähriger auf Datenschutz dar, da gänzlich darauf verzichtet wurde, die nötige Einwilligung der gesetzlichen Vertreter (Eltern) der Minderjährigen einzuholen. Des Weiteren wurden die Datenschutzrechte der betroffenen Personen verletzt, indem es keine angemessene Möglichkeit gab, bei der Registrierung eine ausdrückliche Einwilligung zu erteilen, dass die E-Mail-Adressen der betroffenen Personen zu Marketingzwecken weitergegeben und für den Versand von Marketing-E-Mails verwendet werden dürfen. Außerdem fehlten eindeutige Informationen zu Datenschutzvorschriften und -verfahren sowie die Möglichkeit, sich vom Newsletter des Unternehmens abzumelden. Was die E-Mail-Marketingpraktiken des Unternehmens betrifft, schlug die Datenschutzbehörde die sogenannte Opt-in-Lösung vor, die bei der Registrierung ein separates und eigens zu diesem Zweck vorhandenes Ankreuzfeld vorsieht.

B9) Datenverarbeitung eines Rabatt-Beschaffungssystems

Bei der Datenschutzbehörde ging die Beschwerde einer natürlichen Person in Bezug auf die angeblich unrechtmäßige Datenverarbeitung eines Absatzmittlers (im Folgenden „Unternehmen“) ein. Das Unternehmen unterhielt ein Rabattkartensystem, das registrierte Mitglieder dazu berechtigte, Produkte bestimmter Unternehmer zu niedrigeren Preisen zu erwerben. Die Registrierung beim System war ausschließlich auf Einladung eines bereits registrierten Mitglieds möglich. Beim Anwerben neuer Mitglieder erhielten die aktiven Mitglieder für die Rekrutierung Preisnachlässe. Später beschwerten sich Mitglieder bei der Datenschutzbehörde, dass das System nicht gemäß den geltenden Datenschutzvorschriften arbeite. Die Datenschutzbehörde leitete zunächst ein Ermittlungsverfahren ein, um sich einen Überblick über die Fakten zu verschaffen. Da der für die Verarbeitung Verantwortliche nach mehrmaliger Kontaktaufnahme nicht reagierte, beschloss die Datenschutzbehörde, ein Verwaltungsverfahren aufgrund eines Verstoßes gegen den Datenschutz einzuleiten. Dabei kam die Datenschutzbehörde zu dem Schluss, dass der für die Datenverarbeitung Verantwortliche über keine umfassende, leicht verständliche Datenschutzrichtlinie verfügt und Kunden demnach nicht über ihre Rechte informiert werden und einer Verarbeitung ihrer personenbezogenen Daten nicht frei zustimmen können.

C. Sonstige wichtige Informationen

Wichtige Gesetzesänderungen

Aufgrund grundlegender Änderungen der ungarischen Verfassungsstruktur infolge einer Entscheidung der ungarischen Nationalversammlung aus dem Jahr 2011 wurde die Arbeit des ehemaligen Datenschutzbeauftragten beendet. Die neu gegründete nationale Behörde für Datenschutz und Informationsfreiheit, die mit den zuvor genannten Aufgaben betraut wurde, 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 angenommen und trat zum 1. Januar 2012 in Kraft.

Einige Vorkehrungen des neuen ungarischen Datenschutzgesetzes (Gesetz CXII von 2011 über das Recht auf informationelle Selbstbestimmung und Informationsfreiheit, das am 1. Januar 2012 in Kraft getreten ist), welches das Mandat des Vorsitzenden der ungarischen Datenschutzbehörde (im Folgenden „Vorsitzender“) regelt, wurden – auch unter Berücksichtigung der kritischen Anmerkungen der Europäischen Kommission – in erheblichem Maße modifiziert, um die Unabhängigkeit des Vorsitzenden zu stärken (Änderungsrechtsakt: Gesetz XXV von 2012). Im Folgenden werden die entsprechenden Änderungen erläutert.

- In Fällen, in denen der Beschluss zur Beendigung des Mandats des Vorsitzenden auf schriftlichen Antrag des Premierministers durch den ungarischen Präsidenten getroffen werden soll, hat der

Vorsitzende das Recht, diesen Antrag vor Gericht anzufechten. Der Einspruch wird gegen den Premierminister erhoben. Der Grund für diese Änderung war die Tatsache, dass das Mandat des Vorsitzenden nur beendet werden sollte, wenn der Antrag des Premierministers zweifelsohne rechtmäßig und sachgerecht ist.

- Die Änderung berechtigt den Vorsitzenden zur Teilnahme an und zur Mitsprache bei der Sitzung des parlamentarischen Ausschusses und ermächtigt ihn demnach dazu, die Abgeordneten über seine Tätigkeit zu informieren und Vorschläge in Bezug auf den Rechtsetzungsprozess und Gesetzentwürfe zu unterbreiten.
- Eine weitere Änderung sieht vor, dass der Vorsitzende – gemäß weiteren Bedingungen – mindestens zehn Jahre Erfahrung in der Beaufsichtigung von Verfahren im Zusammenhang mit Datenschutz bzw. Informationsfreiheit aufzuweisen hat. Zuvor waren fünf Jahre Berufserfahrung ausreichend gewesen.

VEREINIGTES KÖNIGREICH

A. Zusammenfassung der Aktivitäten und Neuerungen:

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Christopher Graham, Datenschutzbeauftragter
Budget	Jährlich 20 Mio. GBP
Personal	330 Vollzeitmitarbeiter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Aufklärung und Anweisung Das ICO veröffentlichte einen Verhaltenskodex zur Verwaltung der Datenschutzrisiken durch Anonymisierung und war damit die erste europäische Datenschutzbehörde, die zu diesem Thema einen Verhaltenskodex herausgab. Das ICO veröffentlichte außerdem Leitlinien zu den Themen Cloud-Computing, das Löschen personenbezogener Daten und Vermögensvernichtung. Des Weiteren führten wir eine öffentliche Konsultation bezüglich eines neuen Verhaltenskodex zum Zugang zu gespeicherten Daten durch. Medienaktivitäten Das ICO nahm 1 673 Anrufe von Journalisten entgegen und gab 113 Medieninterviews. Außerdem veröffentlichten wir 50 Pressemitteilungen, die für eine umfassende und weitgehend positive Berichterstattung sorgten. Auf der Website des ICO wurden 900 Aktualisierungen und Verbesserungen vorgenommen. Des Weiteren wurden 45 Leitlinien veröffentlicht oder umfassend überarbeitet.
Meldungen	372 369
Vorabprüfungen	k. A.
Anträge betroffener Personen	213 813 Helpline-Anrufe 29 042 schriftliche Beratungsanfragen
Beschwerden betroffener Personen	20 515 (bezüglich des Datenschutzgesetzes von 1998 und des Gesetzes über Datenschutz und elektronische Kommunikation von 2003/11)
Vom Parlament bzw. der	Das ICO arbeitet laufend mit der Regierung an der datenschutzbezogenen Gesetzgebung, indem es vom Parlament

Regierung angeforderte Beratung	angehört wird und auf Konsultationen reagiert. Es folgt eine Zusammenfassung der diesjährigen Aktivitäten: Anhörung durch das Parlament Sonderausschuss Justiz: Stellungnahme zu den Vorschlägen zum Datenschutzrechtsrahmen der Europäischen Union; Ausschuss für schottische Angelegenheiten: Blacklisting am Arbeitsplatz. Reaktionen auf Konsultationen Cabinet Office: Einführung eines gesetzlich vorgeschriebenen Lobbyistenregisters Bürgerberatungsstelle: Konsultation zu Consumer Futures Consumer Focus: Vorschläge für eine regulierte Brancheneinheit Ministerium für kommunale Angelegenheiten und örtliche Selbstverwaltung: Betrug im sozialen Wohnungswesen Bildungsministerium: Änderungsvorschlag zur Nutzung von Schülerdaten Ministerium für Umwelt und Klimawandel: Intelligenter Datenzugriff und Datenschutz Gesundheitsministerium: Konsultation zur Stärkung der NHS-Konstitution Justizministerium (NI): Spürbare Neuerungen: Ein verbesserter Zugang zur Justiz für Opfer und Zeugen von Verbrechen: eine Fünfjahresstrategie Generalstaatsanwalt: Interim-Leitlinien für Staatsanwälte zur Beurteilung des öffentlichen Interesses in Medienfällen Finanzministerium: Umsetzung des FATCA-Abkommens zwischen dem Vereinigten Königreich und den USA Innenministerium: Protection of Freedoms Act 2012: Konsultation zum Verhaltenskodex für Überwachungskameras Kommission für Recht: Ordnungsmittelkonsultation Law Society: Reform des Gesetzes zu Taxi- und privaten Transportdiensten Justizministerium: Wie wir Opfern und Zeugen gerecht werden - eine Leitlinie Justizministerium: Umbau der Rehabilitierung – eine Reform des Umgangs mit Straftätern Justizministerium: Schnelle und sichere Justiz: Die Regierungspläne für eine Reform des Strafrechtssystems Nominet: Konsultation zur neuen .uk-Domäne Nationales Statistikamt: Zukünftige Strategie zur Veröffentlichung

	nationaler Statistiken zu Straftaten in England und Wales Leveson-Inquiry: Reaktion auf den Bericht über Kultur, Praxis und Ethik der Presse Regierung von Wales: Registrierung und Überwachung von Heimunterricht Regierung von Wales: Der Gesetzentwurf für Transplantationen beim Menschen (Wales) und Begründung Regierung von Wales: Unterstützung der Gemeindesteuer in Wales
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Jährliche ICO-Konferenz der Datenschutzbeauftragten Der Datenschutzbeauftragte hieß in Manchester anlässlich der fünften jährlichen Konferenz der Datenschutzbeauftragten mehrere Hundert Datenschutzbeauftragte aus dem gesamten Vereinigten Königreich willkommen. David Smith, stellvertretendes Kommissionsmitglied und Leiter für Datenschutz, informierte die Teilnehmer in seiner Grundsatzrede über die neuesten Reformentwicklungen in der EU. EU-Entwicklungen Das ICO veröffentlichte im Februar 2012 seine Erstanalyse der EU-Datenschutzreform. Das ICO veranstaltete im Frühjahr 2012 eine Sitzung der Interessenvertreter und arbeitete mit anderen politischen Interessenvertretern des Vereinigten Königreichs sowie mit dem Justizministerium zusammen, um die Auswirkungen der neuen EU-Vorschläge zu untersuchen und über diese aufzuklären. Durchsetzung Die Höhe der vom ICO gemäß dem Datenschutzgesetz und dem Gesetz über Datenschutz und elektronische Kommunikation verhängten Geldbußen belief sich im vergangenen Jahr auf etwas über 2,6 Mio. GBP (vor der Bereinigung um Nachlässe aufgrund von frühzeitiger Zahlung). Mit einer Ausnahme: Die gemäß dem Datenschutzgesetz verhängten Geldbußen erfolgten aufgrund eines unterlassenen Schutzes personenbezogener Daten. Der Bereich der Durchsetzungsarbeit des ICO, der am meisten Aufmerksamkeit erregte, waren die Maßnahmen gegen unerwünschte Werbeanrufe und Spam-SMS. Im März richteten wir ein Online-Meldeinstrument ein, mit dem betroffene Personen die von ihnen erhaltenen Nachrichten melden können. Über 155 000 Personen haben mittlerweile von diesem Instrument Gebrauch gemacht, um uns Informationen zukommen zu lassen, die wir wiederum für unsere Ermittlungen nutzen.

	Prüfungen und bewährte Verfahren Das ICO hat Ergebnisberichte eingeführt, welche die häufigsten Themen der Prüfungen zusammenfassen und auf bewährte Verfahren und Verbesserungspotenzial in den Bereichen öffentlicher Sektor, Gesundheitswesen, Kommunalbehörden, Zentralregierung, Polizei und Bewährung hinweisen. In ausgewählten Foren konnte wir durch Vorträge über unsere Prüfungen und deren Ergebnisse über bewährte Verfahren aufklären. Des Weiteren haben wir ein Beratungsseminar organisiert, das es uns ermöglicht, noch mehr Organisationen zu erreichen. Das ICO hat über 400 Schulen darum gebeten, an einer Datenschutzbefragung teilzunehmen. Mit den Ergebnissen haben wir einen Bericht mit bewährten Praktiken und Verbesserungsmöglichkeiten erstellt und praktische Ratschläge zur Anwendung des Datenschutzgesetzes erteilt. Gewährleistung einer effizienten Öffentlichkeitsarbeit in allen Regionen Im Februar führte das ICO in Wales eine Reihe von äußerst erfolgreichen Workshops mit Praxisbezug durch, die sich mit bewährten Verfahren im Umgang mit personenbezogenen Daten befassten. Die Workshops richteten sich an Fachkräfte des öffentlichen und dritten Sektors, die direkt an der Bereitstellung von Dienstleistungen beteiligt sind und möglicherweise nur wenig Erfahrung mit Datenschutz haben. Dabei wurde verstärkt auf Beispiele bewährter und schlechter Verfahren aus den Prüf- und Durchsetzungsabteilungen des ICO zurückgegriffen. Datenschutz im Gesundheitswesen Das ICO beteiligte sich am *Information Governance Review Panel* des Gesundheitsministeriums. Das ICO hofft, dass diese Arbeit dazu beitragen wird, die Information-Governance in einem Bereich, in dem einige unserer sensibelsten Daten aufbewahrt werden, zu verwandeln. Anonymisierung Das ICO hat neben dem neuen Verhaltenskodex zur Anonymisierung das *UK Anonymisation Network* eingeführt. Ziel dieses Netzes ist der Austausch von Problemlösungen und bewährten Verfahren auf dem Gebiet der Anonymisierung. Dies soll mithilfe einer Website, sozialen Medien, Veranstaltungen und Fallstudien erreicht werden. Den Zuschlag für die Finanzierung des Netzes erhielt im Rahmen einer Ausschreibung eine Arbeitsgemeinschaft der University of Manchester, der University of Southampton, des britischen Statistikamts und des Open Data Institute.

	Leveson-Inquiry: Datenschutz und die Presse Der Verstoß gegen den Datenschutz durch die Presse ist derzeit ein wichtiges Thema auf der Agenda der britischen Regierung und unabhängiger Aufsichtsbehörden. Das ICO gab eine vorläufige Stellungnahme zum Leveson-Bericht infolge der (unter der Leitung des High-Court-Richters Lord Justice Leveson stehenden) Leveson-Inquiry zur Kultur, Praxis und Ethik der Presse im Vereinigten Königreich heraus. Wir beteiligten uns an den Ermittlungen, indem wir unsere bisherigen Untersuchungen zur Rolle der Medien beim illegalen Handel mit personenbezogenen Daten schilderten. Unsere zukünftige Arbeit wird sich vor dem Hintergrund der Regierungspläne für eine zukünftige Regulierung der Medien abspielen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	58 Prüfungen und 35 Folgeprüfungen. 78 Beratungen
Sanktionsmaßnahmen	
Sanktionen	23
Geldbußen	17 Vereinbarungen, 2 Vollzugsmitteilungen, 6 Strafverfolgungen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Laut Datenschutzgesetz von 1998 sind alle für die Datenverarbeitung Verantwortlichen (z. B. Unternehmen, Einzelunternehmer) dazu verpflichtet, jegliche Form der Verarbeitung personenbezogener Daten beim ICO zu registrieren, es sei denn, sie sind davon ausgenommen. Derzeit sind mehr als 370 000 Organisationen registriert.

B. Rechtsprechung

—

C. Sonstige wichtige Informationen

Der Protection of Freedoms Act 2012 des Vereinigten Königreichs enthält die folgenden Vorkehrungen, die sich auf die Aktivitäten des ICO beziehen:

Teil 1; Regulierung biometrischer Daten. Dies umfasst Bestimmungen im Zusammenhang mit der Löschung, Speicherung und Nutzung von Fingerabdrücken, Schuhsohlenprofilen und DNS-Proben und -Profilen. Außerdem gehören hierzu Bestimmungen zum Schutz biometrischer Daten von Kindern in Schulen.

Teil 2; Regulierung von CCTV und sonstiger Videoüberwachungstechnologie. Dies wird zur Einführung eines neuen Videoüberwachungsbeauftragten führen.

Teil 3; Schutz des Eigentums vor unverhältnismäßigen Vollstreckungsmaßnahmen. Diese Regulierungen beziehen sich auf Zugangsbefugnisse, Befugnisse zur Parkplatzüberwachung und eine potenziell verstärkte Nutzung von Technologie zur automatischen Nummernschilderkennung.

Teil 5; Schutz gefährdeter Gruppen und Strafregister. In diesem Teil wird darüber hinaus der Offenlegungs- und Sperrdienst eingeführt (der die Verantwortlichkeiten des Criminal Records Bureau und der Independent Safeguarding Authority übernimmt und zusammenführt). Dieser Teil sieht außerdem vor, dass bestimmte sexuelle Straftaten unberücksichtigt bleiben.

Teil 6; Änderungen des Datenschutzgesetzes von 1998. Die Änderungen beziehen sich auf Folgendes:

- Ernennung und Amtszeit des Datenschutzbeauftragten von fünf auf sieben Jahre;
- Änderung der Zuständigkeiten der Minister in Bezug auf Führungsbefugnisse;
- Wegfall der Zustimmung von Gebührenbefugnissen durch den Minister;
- Wegfall der Genehmigung von Mitarbeiterzahlen und Bedingungen durch Minister.

ZYPERN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Amt des Datenschutzbeauftragten beteiligte sich aktiv an den Gesprächen zum Vorschlagspaket für den Datenschutz, das die Kommission im Januar 2012 vorgestellt hat. Im Februar 2012 wurde eine Absichtserklärung zwischen dem Datenschutzbeauftragten und dem Minister für Justiz und öffentliche Ordnung geschlossen, das ein Verfahren für die Annahme allgemeingültiger Standpunkte und die Ernennung eines Datenschutzbeauftragten (DPA) als Vorsitzender von DAPIX, der Arbeitsgruppe des Rates, in der das Vorschlagspaket besprochen wurde, vorsieht. Im März 2012 beraumte das Amt des Datenschutzbeauftragten in Zusammenarbeit mit dem Ministerium eine öffentliche Konsultation für diese Vorschläge an und nahm vor und während der zypriotischen Ratspräsidentschaft an zahlreichen Gesprächen mit wichtigen Interessenvertretern teil. Der zypriotische Vorsitz von DAPIX brachte die Gespräche zu den Vorschlägen voran und identifizierte eine Reihe von horizontalen Problemen, zu denen die Delegationen gemeinsame Bedenken äußersten, nämlich die große Anzahl der in den Vorschlägen enthaltenen delegierten und Durchführungsrechtsakte, der hohe Verwaltungsaufwand für kleine und mittlere Unternehmen sowie unklare Regelungen/Ausnahmen für den öffentlichen Sektor, die im Rahmen der informellen Gespräche der Gruppe „Freunde des Vorsitzes“ besprochen wurden. Die Arbeit der zypriotischen Ratspräsidentschaft wird im einschlägigen Fortschrittsbericht dargelegt, der von dem Rat der JI-Minister im Dezember 2012 angenommen wurde.

Im Rahmen der Aktivitäten zur Feier des Europäischen Datenschutztages nutzte das Amt des Datenschutzbeauftragten ein Budget in Höhe von EUR 4,300 für gedrucktes Informationsmaterial und Geschenke (Wecker und Taschenlampen) mit dem Logo und der E-Mail-Adresse des Amtes, die am 28. Januar verteilt wurden. Der Tag stand unter dem Motto „Time for awakening, time for enlightenment“ (Zeit zum Aufwachen, Zeit zur Aufklärung). Der Datenschutzbeauftragte und seine Mitarbeiter erschienen in einer Reihe von Fernseh- und Radiosendungen.

Im Jahr 2012 wurde das Grundgesetz (Gesetz 138(I)/2001) geändert, um die Vorkehrungen der Richtlinie 95/46/EG besser in zypriotisches Recht umzusetzen. Dies geschah im Einklang mit den Stellungnahmen der Kommission im Rahmen eines strukturierten Dialogs und zur Verbesserung der effektiven Funktionsweise des Amts des Datenschutzbeauftragten.

2012 ging das Amt des Datenschutzbeauftragten einer Beschwerde gegen ein Versicherungsunternehmen nach, das von der Beschwerdeführerin angeblich eine unverhältnismäßig hohe Anzahl medizinischer Dokumente angefordert hatte, um ihren Entschädigungsanspruch aufgrund von Arbeitsunfähigkeit angesichts ihrer gesundheitlichen Verfassung geltend zu machen. Nach der Überprüfung der Bedingungen der Versicherungspolice und der Anzahl der (zusätzlichen) Dokumente, die die Beschwerdeführerin teilweise einreichen musste, bat der Datenschutzbeauftragte das Unternehmen um eine Stellungnahme, weshalb es die Forderung nicht einfach irgendwann unter Berücksichtigung einer angemessenen Anzahl von Dokumenten akzeptiert bzw. abgelehnt, sondern stattdessen um zusätzliche Tests und Dokumente gebeten und dadurch die Untersuchung des Anspruchs verlängert habe – eine Praxis, die auf den ersten Blick nach einem Verstoß gegen den Grundsatz der Verhältnismäßigkeit aussieht. Der Fall wird zur Zeit noch geprüft. Die Entscheidung des Datenschutzbeauftragten steht noch aus.

Infolge der Überprüfung einer Beschwerde, die Mitarbeiter durch ihre Gewerkschaften gegen zwei private Krankenhäuser vorgebracht hatten, die kürzlich Systeme zur Überwachung der Anwesenheit installiert hatten und biometrische Daten (Fingerabdrücke) nutzten, die lediglich auf an Mitarbeiter ausgegebene Smartcards und nicht in einer zentralen Datenbank gespeichert wurden, kam man im Rahmen eines Beschlusses zu dem Ergebnis, dass die Nutzung dieser Systeme einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit darstellt. Die Krankenhäuser wurden aufgefordert, die Verarbeitung einzustellen und

die Systeme zu deinstallieren. Eines der Krankenhäuser leistete dem Beschluss Folge, das andere focht den Beschluss vor Gericht an. Das Urteil steht noch aus.

Organisation	Kommission für den Schutz personenbezogener Daten
Vorsitz und/oder Gremium	Yiannos Danielides
Budget	Zugewiesenes Budget: 307 570 EUR Ausgegebene Haushaltsmittel: 265 609 EUR
Personal	Verwaltungsbedienstete: 7 Fachkräfte für Informationstechnologie: 2 Bürofachkräfte: 6 Hilfskräfte: 2
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Stellungnahmen: 47 Beschlüsse: 5 Empfehlungen: 1
Meldungen	260
Vorabprüfungen	k. A.
Anträge betroffener Personen	Schriftlich oder telefonisch: k. A.
Beschwerden betroffener Personen	Genehmigungen für die Verknüpfung von Speichersystemen: 43 Genehmigungen für Übermittlungen an Drittländer: 46
Vom Parlament bzw. der Regierung angeforderte Beratung	In 28 Fällen wurde unser Amt von parlamentarischen Ausschüssen des zypriotischen Parlaments um Beratungsdienste/Konsultationen gebeten.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen: 1. Anzahl der bearbeiteten Beschwerden: 233 von 325
Sanktionsmaßnahmen	
Sanktionen	In einem Beschluss erließ der Datenschutzbeauftragte eine Verwaltungssanktion, in deren Rahmen die Verarbeitung personenbezogener Daten eingestellt und die Daten gelöscht werden sollten. In einem weiteren Beschluss gab der Datenschutzbeauftragte Empfehlungen an den für die Verarbeitung Verantwortlichen ab.

Geldbußen	Im Rahmen von drei Beschlüssen wurden für die Verarbeitungen Verantwortlichen Geldbußen in Höhe von insgesamt 3 500 EUR auferlegt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Im Jahr 2011 meldete der Datenschutzbeauftragte gemäß Abschnitt 23(a) des Datenschutzgesetzes dem Polizeipräsidenten ein mutmaßliches Vergehen einer journalistische Website, die sich weigerte, dem Beschluss des Datenschutzbeauftragten Folge zu leisten, laut dem die Verarbeitung der personenbezogenen Daten von Asylsuchenden eingestellt und die Daten zerstört werden sollten, da diese Verarbeitung einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit darstelle. Der Artikel mit den besagten Daten war wochenlang auf der Website einsehbar gewesen. Außerdem weigerte sich die Website, die Geldbuße in Höhe von 3 000 EUR zu zahlen. Der Fall kam vor Gericht. Da der Beklagte das Gericht über die nachträgliche Befolgung des Beschlusses und demzufolge die Zerstörung der Daten und das Einstellen der Verarbeitung informierte, entschied das Gericht zugunsten des Beschlusses des Datenschutzbeauftragten und ordnete der Website die Zahlung der Gebühr als Zivilschuld an

Kapitel Drei

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. EUROPÄISCHE KOMMISSION

3.1.1. **Vorschlag der Kommission für eine Verordnung des Europäischen Parlaments und des Rates** KOM(2012) 11 vom 25. Januar 2012 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr **(Datenschutz-Grundverordnung).**

3.1.2. **Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates** KOM(2012) 10 vom 25. Januar 2012 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr.

3.1.3. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen KOM(2012) 09 Schutz der Privatsphäre in einer vernetzten Welt Ein europäischer Datenschutzrahmen für das 21. Jahrhundert.

3.1.4. **Arbeitsdokument der Kommissionsdienststellen** SEC(2012) 75 vom 25. Januar 2012 Bericht der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen auf der Grundlage von Artikel 29 Absatz 2 des Rahmenbeschlusses des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Die Europäische Kommission hat eine umfassende Reform der EU-Datenschutzvorschriften von 1995 vorgeschlagen, um die Rechte des Einzelnen auf Wahrung der Privatsphäre im Internet zu stärken und die digitale Wirtschaft Europas anzukurbeln. Der technische Fortschritt und die Globalisierung haben die Art und Weise, wie Daten erhoben, abgerufen und verwendet werden, grundlegend verändert. Außerdem haben die 27 Mitgliedstaaten der EU die Vorschriften von 1995 unterschiedlich umgesetzt, was zu Unterschieden bei ihrer Durchsetzung geführt hat. Eine einheitliche Regelung soll daher jetzt der bestehenden Fragmentierung und dem hohen Verwaltungsaufwand ein Ende bereiten und den Unternehmen dadurch Einsparungen von etwa 2,3 Mrd. EUR jährlich ermöglichen. Zudem sollen das Vertrauen der Verbraucher in Onlinedienste gestärkt und so dringend benötigte Impulse für mehr Wachstum, Arbeitsplätze und Innovationen in Europa gegeben werden. Die Grundsätze der Datenschutzrichtlinie von 1995 sollen durch die Vorschläge der Kommission aktualisiert und modernisiert werden, damit der Schutz personenbezogener Daten auch in Zukunft garantiert ist. Die Vorschläge der Kommission legen die politischen Ziele der Kommission dar und umfassen zwei Legislativvorschlägen. Dabei handelt es sich um eine **Verordnung** zur Festlegung eines allgemeinen Datenschutz-Rechtsrahmens der EU und eine **Richtlinie** zum Schutz personenbezogener Daten, die zum Zweck der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und für damit verbundene justizielle Tätigkeiten verarbeitet werden.

Zu den wichtigsten Zielen der Reform gehört ein EU-weit geltendes **Gesamtregelwerk** für den Datenschutz. Unnötige **administrative Anforderungen**, wie bestimmte Meldepflichten für Unternehmen, werden beseitigt. Dadurch werden Unternehmen Kosten in Höhe von etwa 2,3 Mrd. EUR jährlich einsparen. Anstelle der bisher den Unternehmen obliegenden Pflicht, den Datenschutzbeauftragten sämtliche datenschutzrelevanten Tätigkeiten zu melden (was den Unternehmen unnötigen Verwaltungsaufwand sowie Kosten in Höhe von schätzungsweise 130 Mio. EUR jährlich verursacht hat), sieht die Verordnung künftig mehr **Verantwortung und Rechenschaftspflicht** der Verarbeiter personenbezogener Daten vor.

Unternehmen und Organisationen sollen bei einer schweren **Verletzung des Schutzes personenbezogener Daten** künftig die nationale Aufsichtsbehörde unverzüglich (d. h. nach Möglichkeit binnen 24 Stunden) benachrichtigen. Alleiniger Ansprechpartner für Organisationen wird künftig die **nationale Datenschutzbehörde** des EU-Landes sein, in dem sie ihre Hauptniederlassung haben. Ebenso sollen sich Bürger künftig auch dann an die **Datenschutzbehörde** ihres Landes wenden können, wenn ihre Daten von einem außerhalb der EU niedergelassenen Unternehmen verarbeitet werden.

In Bezug auf Datenverarbeitungen, die der vorherigen **Genehmigung** bedürfen, wird nunmehr klargestellt, dass die Genehmigung ausdrücklich erteilt werden muss und nicht stillschweigend vorausgesetzt werden darf. Die Bürger sollen leichter **auf ihre eigenen Daten zugreifen** und diese bei einem Wechsel zwischen Dienstleistern leichter **„mitnehmen“** können (Recht auf Datenportabilität). Dadurch wird der Wettbewerb

unter den Anbietern derartiger Dienste zunehmen. Das **„Recht auf Vergessenwerden"** soll eine bessere Beherrschung der bei Onlinediensten bestehenden Datenschutzrisiken ermöglichen. Alle Bürger sollen das Recht erhalten, ihre eigenen Daten zu löschen, wenn keine legitimen Gründe für deren Vorhaltung bestehen. Jedwede **außerhalb der EU erfolgende Bearbeitung von personenbezogenen Daten** durch auf dem EU-Markt aktive Unternehmen, die EU-Bürgern ihre Dienste anbieten, soll künftig den EU-Vorschriften unterliegen.

Die **Unabhängigkeit der nationalen Datenschutzbehörden** soll gestärkt werden, damit diese die EU-Vorschriften in ihren Ländern besser durchsetzen können. Sie sollen künftig Geldbußen gegen Unternehmen verhängen können, die gegen die Datenschutzbestimmungen der EU verstoßen. Die Höhe der Geldbuße soll bis zu 1 Mio. EUR oder 2 % des Jahresumsatzes eines Unternehmens betragen können.

Durch die neue **Richtlinie** sollen allgemeine Datenschutzgrundsätze und -regeln für die **polizeiliche und justizielle Zusammenarbeit** in Strafsachen eingeführt werden. Die Bestimmungen sollen sowohl für inländische als auch für grenzüberschreitende Datenübermittlungen gelten.

3.1.5. Konferenz am 19. März 2012 zur Privatsphäre und zum Schutz personenbezogener Daten, Washington, D.C./Brüssel.

Die Konferenz, die zeitgleich in Washington und Brüssel stattfand, bot Interessenvertretern der öffentlichen und privaten Sektoren der USA und der EU ein Forum, um sich umfassende, genaue und aktuelle Informationen zu den Datenschutzgrundsätzen der EU und der laufenden Reform zu verschaffen und den kommerziellen Datenschutz aus US- und EU-Perspektive zu diskutieren.

3.1.6. Abkommen vom 1. Juni 2012 zwischen **der Europäischen Union und Australien** über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records, PNR) und deren Übermittlung durch die Fluggesellschaften an den Australian Customs and Border Protection Service — L 186, 14/07/2012, S. 4.

Der Zweck einer Übermittlung von Daten an den Australian Customs and Border Protection Service, den das Abkommen vorsieht, ist die Verhütung, Aufdeckung, Aufklärung und strafrechtliche Verfolgung von terroristischen Straftaten und schwerer grenzüberschreitender Kriminalität. Für ein besseres Verständnis des Anwendungsbereichs enthält das Abkommen Begriffsbestimmungen dieser Straftaten. Im Anhang des Abkommens werden die PNR-Daten aufgelistet, die australische Behörden nutzen dürfen.

Der Australian Customs and Border Protection Service darf lediglich auf Grundlage der Datenübermittlungen durch Fluggesellschaften per „Push"-System auf EU-PNR-Daten zugreifen.

Der Schutz personenbezogener Daten und das Recht natürlicher Personen auf Zugriff und Berichtigung ihrer personenbezogenen Daten greift unabhängig von der Nationalität oder dem Wohnsitz.

Nach Inkrafttreten wird die Durchführung des Abkommens, einschließlich seiner operativen Effektivität, alle vier Jahre überprüft.

Wenngleich PNR in der Regel keine sensiblen Daten (wie z. B. personenbezogenen Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, Religion oder Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben) enthalten, müssen diese ggf. vom Australian Customs and Border Protection Service herausgefiltert und gelöscht werden.

Das Abkommen sieht eine Speicherfrist von fünfeinhalb Jahren vor. Bereits nach drei Jahren werden personenbezogene Daten jedoch unkenntlich gemacht.

Der Australian Customs and Border Protection Service wird den Austausch analytischer Informationen, die von EU-PNR-Daten stammen, mit den zuständigen Behörden von EU-Staaten und in entsprechenden Fällen mit Europol und Eurojust austauschen, um die polizeiliche und justizielle Zusammenarbeit zwischen Australien und der EU sowie die Gegenseitigkeit zu stärken.

Zur Gewährleistung der Rechtssicherheit über längere Zeit läuft das Abkommen zunächst über einen Zeitraum von sieben Jahren, kann jedoch anschließend auf weitere sieben Jahre verlängert werden.

Es enthält Standards bezüglich der Überwachung einer korrekten Implementierung, Überprüfung und effektiven Streitbeilegung sowie die Modalitäten einer Übermittlung von PNR-Daten, um Fluggesellschaften Rechtssicherheit zu bieten und die Kosten auf einem annehmbaren Niveau zu halten. PNR-Daten müssen mithilfe des „Push„-Systems übermittelt werden. Dies darf pro Flug höchstens fünf Mal geschehen.

3.1.7. **Abkommen** vom 1. Juli 2012 zwischen **der Europäischen Union und den Vereinigten Staaten von Amerika** über die Verarbeitung von **Fluggastdatensätzen** und deren Übermittlung durch Fluggesellschaften an das United States Department of Homeland Security, Bureau of Customs and Border Protection — L 215, 11. August 2012, S. 5.

Laut diesem Abkommen liegt der Zweck einer Bereitstellung von PNR-Daten an das US Department of Homeland Security in der Verhütung, Aufdeckung, Untersuchung und strafrechtlichen Verfolgung terroristischer und damit verbundener Straftaten sowie anderer grenzüberschreitender Straftaten, die mit einer Freiheitsstrafe von drei oder mehr Jahren geahndet werden können. Für ein besseres Verständnis des Anwendungsbereichs enthält das Abkommen Begriffsbestimmungen dieser Straftaten. Im Anhang des Abkommens werden die PNR-Daten aufgelistet, die US-Behörden nutzen dürfen.

Fluggesellschaften übermitteln PNR-Daten nach dem „Push"-Verfahren an das Department of Homeland Security.

Allen Passagieren stehen unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitzland Rechtsbehelfe in Bezug auf die verwaltungsrechtlichen Entscheidungen des DHS zur Verfügung. Die Durchführung des Abkommens wird regelmäßig überprüft. Außerdem wird das Abkommen vier Jahre nach Inkrafttreten gemeinsam evaluiert.

Sensible Daten (wie z. B. personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, Religion oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben) müssen herausgefiltert und unkenntlich gemacht und dürfen nicht weiter verarbeitet oder genutzt werden, es sei denn, es handelt sich um außergewöhnliche Umstände, in denen eine Gefahr für Leib und Leben von Personen besteht. PNR-Daten enthalten jedoch in der Regel keine sensiblen Daten.

Die Daten dürfen fünf Jahre in einer aktiven Datenbank und bis zu zehn Jahre in einer ruhenden Datenbank gespeichert werden. Während dieser Zeit werden die Daten allmählich anonymisiert und unkenntlich gemacht und der Zugang zu diesen Daten wird weiter eingeschränkt.

Das Department of Homeland Security wird den Austausch analytischer Informationen, die aus den EU-PNR-Daten gewonnen wurden, mit den zuständigen Behörden von EU-Staaten und in entsprechenden Fällen mit Europol und Eurojust austauschen, um die polizeiliche und justizielle Zusammenarbeit zwischen den USA und der EU sowie die Gegenseitigkeit zu stärken.

Zur Gewährleistung der Rechtssicherheit über längere Zeit läuft das Abkommen zunächst über einen Zeitraum von sieben Jahren, kann jedoch anschließend auf weitere sieben Jahre verlängert werden.

3.1.8. **Durchführungsbeschluss der Kommission** vom 21. August 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in der Republik Östlich des Uruguay im Hinblick auf die automatisierte Verarbeitung personenbezogener Daten (bekanntgegeben unter Aktenzeichen C(2012) 5704) Text von Bedeutung für den EWR — AB L 227, 23. September 2012.

Für die Zwecke von Artikel 25 Absatz 2 der Richtlinie 95/46/EG wird die Republik Östlich des Uruguay als Land angesehen, das ein angemessenes Schutzniveau bei der Übermittlung personenbezogener Daten aus der Europäischen Union bietet.

3.1.9. **Arbeitsunterlage der Kommissionsdienststellen** SWD (2012) 454 vom 14. Dezember 2012 Bericht zur zweiten gemeinsamen Überprüfung der Durchführung des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und

deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten von Amerika für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP) vom Oktober 2012

Die zweite gemeinsame Überprüfung wurde gemeinsam von einem US-Überprüfungsteam und einem EU-Team durchgeführt. Gemäß Artikel 13 Absatz 3 wird die EU bei gemeinsamen Überprüfungen durch die Kommission vertreten. Das EU-Überprüfungsteam stand demnach unter der Leitung eines führenden Kommissionsbeamten und bestand aus drei Kommissionsmitarbeitern und drei externen Fachkräften (zwei Datenschutzfachleuten und einer juristischen Fachkraft, die die Kommission bei der Überprüfung des Abkommens unterstützt haben).

Die Überprüfung erfolgte in zwei Hauptphasen: am 4. Oktober 2012 in den Diensträumen von Europol in Den Haag sowie am 30. und 31. Oktober 2012 in den Diensträumen des US Treasury Department (im Folgenden „US-Finanzministerium") in Washington.

Beide Überprüfungsteams kamen zunächst im Hauptsitz von Europol in Den Haag zusammen und wurden von Europol-Führungskräften und -Fachleuten über die Durchführung und praktische Anwendung des Abkommens durch Europol informiert. Die Teams besuchten den abgesicherten Ort, an dem Europol die US-Anfragen abwickelt, und lernten die Personen kennen, die Zugriff auf die betreffenden Daten haben.

Zur Vorbereitung des Besuchs in Washington hatte das EU-Team im Vorfeld wie im Abkommen vereinbart einen Fragebogen mit spezifischen Fragen zu allen Aspekten der Überprüfung an das US-Finanzministerium geschickt. Das US-Finanzministerium beantwortete die Fragen schriftlich. Das EU-Überprüfungsteam stellte Beamten des US-Finanzministeriums außerdem weitere Fragen, um alle Parameter des Abkommens abzudecken.

Die Überprüfungsteams erhielten Zugang zu den einschlägigen Diensträumen des US-Finanzministeriums, darunter der Ort, an dem das TFTP durchgeführt wird. Aus Sicherheitsgründen mussten Mitglieder des Überprüfungsteams sich im Vorfeld einer Sicherheitsüberprüfung unterziehen, um Zugang zur TFTP-Einrichtung zu erhalten. Den Überprüfungsteams wurden unter Einhaltung der geltenden US-Vertraulichkeitsanforderungen Suchvorgänge in den bereitgestellten Daten vorgeführt. Die Ergebnisse wurden anschließend von den Analysten auf einem Bildschirm gezeigt und erläutert.

Die Überprüfungsteams tauschten sich mit den für das TFTP-Programm verantwortlichen Mitarbeitern des US-Finanzministeriums sowie mit den die Suchvorgänge gemäß dem TFTP-Abkommen überprüfenden Aufsehern und dem vom bezeichneten Anbieter beschäftigten Vollzeitprüfer des TFTP aus. Die Überprüfungsteams führten keine Systemprüfungen oder Kontrollen auf Grundlage der Protokolldateien durch.

Das EU-Überprüfungsteam ist der Ansicht, dass die im Bericht vom März 2011 zur ersten gemeinsamen Überprüfung dargelegten Empfehlungen größtenteils berücksichtigt wurden und somit die Durchführung des Abkommens verbessern. Die Bereitstellung besser nachprüfbarer Erkenntnisse zum tatsächlichen Mehrwert des TFTP, die bevorzugt anhand von öffentlichen Informationen ohne die Gefährdung der Effektivität dieses Instruments und unter Achtung der Vertraulichkeit der genutzten Verfahren und Abläufe gewonnen werden, bleibt auch weiterhin eine Herausforderung.

Das EU-Überprüfungsteam stellte weitere Verbesserungen insbesondere der Verifizierungs- und Aufsichtsmechanismen fest, von denen einige über die im Abkommen genannten Anforderungen hinausgehen. Im Großen und Ganzen hat die Durchführung des Abkommens über zwei Jahre nach dem Inkrafttreten ein zufriedenstellendes Niveau erreicht, von dem auch die EU im Rahmen der spezifischen Reziprozitätsanforderungen zunehmend profitiert.

3.1.10. Durchführungsbeschluss der Kommission vom 19. Dezember 2012 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Datenschutzniveaus in Neuseeland (bekanntgegeben unter Aktenzeichen C(2012) 9557) Text von Bedeutung für den EWR — AB L 28/12, 30. Januar 2013.

Für die Zwecke von Artikel 25 Absatz 2 der Richtlinie 95/46/EG wird Neuseeland als Land angesehen, das ein angemessenes Schutzniveau bei der Übermittlung personenbezogener Daten aus der Europäischen Union bietet.

3.2. EUROPÄISCHER GERICHTSHOF

3.2.1. Urteil des Gerichtshofs (Dritte Kammer) vom 22. November 2012 — Josef Probst/mr.nexnet GmbH **(Rechtssache C-119/12):** Mit seiner Frage wollte das vorlegende Gericht wissen, ob und unter welchen Bedingungen Art. 6 Abs. 2 und 5 der Richtlinie 2002/58 dem Dienstanbieter die Übermittlung von Verkehrsdaten an einen Zessionar seiner Forderungen und diesem die Verarbeitung dieser Daten erlaubt.

Gemäß Art. 6 Abs. 2 der Richtlinie 2002/58 dürfen Verkehrsdaten, die zum Zwecke der Gebührenabrechnung erforderlich sind, verarbeitet werden, da sie die Verarbeitung von Verkehrsdaten nicht nur für die Gebührenabrechnung, sondern auch die Einziehung von Forderungen erlaubt. Indem diese Bestimmung die Verarbeitung von Verkehrsdaten „bis zum Ablauf der Frist [zulässt], innerhalb der die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann", bezieht sie sich nämlich nicht nur auf die Verarbeitung der Daten zum Zeitpunkt der Gebührenabrechnung, sondern auch auf die Verarbeitung, die erforderlich ist, um die Zahlung der Gebühren zu erreichen.

Art. 6 Abs. 5 der Richtlinie 2002/58 sieht vor, dass die nach Art. 6 Abs. 2 dieser Richtlinie erlaubte Verarbeitung von Verkehrsdaten „nur durch Personen erfolgen [darf], die auf Weisung der [Dienst]Anbieter öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen zuständig sind", und „auf das [für diese Tätigkeit] erforderliche Maß zu beschränken" ist.

Es ergibt sich, dass ein Dienstanbieter im Hinblick auf die Einziehung seiner Forderungen Verkehrsdaten an einen Zessionar dieser Forderungen übermitteln darf und dass Letzterer diese Daten verarbeiten darf, sofern er erstens hinsichtlich der Verarbeitung dieser Daten „auf Weisung" des Dienstanbieters handelt und sich zweitens auf die Verarbeitung derjenigen Verkehrsdaten beschränkt, die für die Einziehung dieser Forderungen erforderlich sind.

Da die genaue Bedeutung des Ausdrucks „auf Weisung" unklar ist, ist daher zur Bestimmung der Bedeutung dieses Ausdrucks sein Sinn nach dem gewöhnlichen Sprachgebrauch zu erwägen, wobei auch zu berücksichtigen ist, in welchem Zusammenhang er verwendet wird und welche Ziele mit der Regelung verfolgt werden, zu der er gehört. Nach dem gewöhnlichen Sprachgebrauch ist davon auszugehen, dass eine Person auf Weisung einer anderen Person handelt, wobei Erstere auf Anweisung und unter der Kontrolle Letzterer handelt.

Art. 5 Abs. 1 der Richtlinie 2002/58 sieht vor, dass die Mitgliedstaaten die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten sicherstellen müssen. Art. 6 Abs. 2 und 5 der Richtlinie 2002/58 sehen eine Ausnahme von der in Art. 5 Abs. 1 dieser Richtlinie festgelegten Vertraulichkeit der übertragenen Nachrichten vor, indem er die Verarbeitung von Verkehrsdaten im Hinblick auf die Erfordernisse im Zusammenhang mit der Gebührenabrechnung erlaubt. Als Ausnahme ist diese Bestimmung der genannten Richtlinie und damit auch der Ausdruck „auf Weisung" eng auszulegen. Eine solche Auslegung impliziert, dass der Dienstanbieter eine tatsächliche Kontrollbefugnis besitzt, die es ihm ermöglicht zu überprüfen, ob der Zessionar der Forderungen die ihm für die Bearbeitung von Verkehrsdaten vorgeschriebenen Bedingungen beachtet.

Art. 6 Abs. 5 der Richtlinie 2002/58 ist daher im Licht der ähnlichen Bestimmungen der Richtlinie 95/46 auszulegen. Aus den Art. 16 und 17 dieser Richtlinie, die das Maß der Kontrolle festlegen, das ein für die Verarbeitung Verantwortlicher über den von ihm bestimmten Auftragsverarbeiter ausüben muss, ergibt sich, dass Letzterer nur auf Weisung des für die Verarbeitung Verantwortlichen handelt und dass dieser Verantwortliche sich von der Einhaltung der Maßnahmen überzeugt, die zum Schutz personenbezogener Daten gegen jede Form der unrechtmäßigen Verarbeitung vereinbart wurden. Während Art. 6 Abs. 5 der Richtlinie 2002/58 zwar die Verarbeitung von Verkehrsdaten durch Dritte zum Zweck der Einziehung von Forderungen erlaubt, wodurch es dem Dienstanbieter ermöglicht wird, sich auf die Erbringung von elektronischen Kommunikationsdienstleistungen zu konzentrieren, soll die Richtlinie, indem sie vorsieht, dass die Verarbeitung von Verkehrsdaten nur durch Personen erfolgen darf, die „auf Weisung" des

Dienstanbieters handeln, jedoch gewährleisten, dass eine solche Auslagerung nicht das für persönliche Daten der Nutzer bestehende Schutzniveau beeinträchtigt.

Aus dem Vorstehenden ergibt sich, dass der Zessionar nur auf Anweisung dieses Dienstanbieters und unter dessen Kontrolle handelt. Der zwischen dem Dienstanbieter und dem Zessionar der Forderungen geschlossene Vertrag muss insbesondere Bestimmungen enthalten, die die rechtmäßige Verarbeitung der Verkehrsdaten durch den Letzteren gewährleisten, und es dem Dienstanbieter ermöglichen, sich jederzeit von der Einhaltung dieser Bestimmungen durch den Zessionar zu überzeugen. Es ist Sache des nationalen Gerichts zu prüfen, ob diese Voraussetzungen vorliegen.

Der Gerichtshof hat für Recht erkannt, dass Art. 6 Abs. 2 und 5 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in dem Sinne auszulegen ist, dass danach ein Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher elektronischer Kommunikationsdienste im Hinblick auf die Einziehung seiner Telekommunikationsleistungen betreffenden Forderungen Verkehrsdaten an einen Zessionar dieser Forderungen übermitteln und dieser Zessionar diese Daten verarbeiten darf, sofern er erstens in Bezug auf die Verarbeitung dieser Daten auf Weisung des Dienstanbieters handelt und sich zweitens auf die Verarbeitung derjenigen Verkehrsdaten beschränkt, die für die Einziehung der abgetretenen Forderungen erforderlich sind. Unabhängig von der Einstufung des Abtretungsvertrags wird der Zessionar im Sinne von Art. 6 Abs. 5 der Richtlinie 2002/58 als auf Weisung des Dienstanbieters handelnd erachtet, wenn er für die Verarbeitung von Verkehrsdaten nur auf Anweisung dieses Dienstanbieters und unter dessen Kontrolle handelt. Der zwischen Zessionar und Dienstanbieter geschlossene Vertrag muss insbesondere Bestimmungen enthalten, die die rechtmäßige Verarbeitung der Verkehrsdaten durch den Zessionar gewährleisten und es dem Dienstanbieter ermöglichen, sich jederzeit von der Einhaltung dieser Bestimmungen durch den Zessionar zu überzeugen.

3.2.2. **Urteil des Gerichtshofs** (Große Kammer) vom 16. Oktober 2012 — Europäische Kommission gegen Österreich **(Rechtssache C-614/10):** Die Kommission leitete wegen der fehlerhaften Umsetzung von Art. 28 Abs. 1 der Richtlinie 95/46 durch die Republik Österreich ein Verfahren gegen Österreich ein, da nach der bestehenden nationalen Regelung die Datenschutzkommission (DSK) nicht die Möglichkeit habe, ihre Aufgaben „in völliger Unabhängigkeit“ im Sinne der genannten Bestimmung wahrzunehmen. Die Kommission machte geltend, dass, da das geschäftsführende Mitglied der DSK stets ein Beamter des Bundeskanzleramts sein müsse, alle laufenden Geschäfte der DSK faktisch durch einen Bundesbeamten betrieben würden, der weiterhin an die Weisungen der Bundesregierung gebunden sei und der Dienstaufsicht unterliege. Des Weiteren machte die Kommission geltend, dass die DSK aufgrund der organisatorischen Verflechtungen mit den anderen Ämtern der Bundesregierung weder institutionell noch materiell unabhängig sei. Alle Mitarbeiter der Geschäftsstelle der DSK seien nämlich dienstrechtlich dem Bundeskanzleramt zugeordnet und unterlägen somit dessen Dienstaufsicht. Drittens verweist die Kommission auf das Unterrichtungsrecht des Bundeskanzlers nach österreichischem Recht.

Der Gerichtshof merkte an, dass Art. 28 Abs. 1 der Richtlinie 95/46 den Mitgliedstaaten vorschreibt, eine oder mehrere Kontrollstellen für den Schutz personenbezogener Daten einzurichten, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Dieses Erfordernis ergibt sich auch aus dem Primärrecht der Union, insbesondere aus der Charta der Grundrechte.

Der Gerichtshof wies das Argument zurück, dass die DSK in dem nach der Richtlinie erforderlichen Maße unabhängig sei, weil sie das Unabhängigkeitskriterium erfülle, das der Einstufung als Gericht eines Mitgliedstaats innewohne, und kam zu dem Schluss, dass der Ausdruck „in völliger Unabhängigkeit“ in der Richtlinie autonom auszulegen sei. Vor allem aber müssten die für den Schutz personenbezogener Daten zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein, die es ihnen ermöglicht, ohne jegliche äußere Einflussnahme, sei sie unmittelbar oder mittelbar, die ihre Entscheidungen zu beeinflussen imstande ist, ihre Aufgaben wahrzunehmen.

Der Gerichtshof befand, dass unabhängig davon, welcher Bundesbehörde das geschäftsführende Mitglied der DSK angehört, feststeht, dass zwischen ihm und dieser Bundesbehörde ein Dienstverhältnis besteht, das es dem Vorgesetzten des geschäftsführenden Mitglieds ermöglicht, dessen Tätigkeiten zu überwachen. Nach dieser weitreichenden Befugnis ist der Vorgesetzte nämlich nicht nur befugt, darauf zu achten, dass seine Mitarbeiter ihre dienstlichen Aufgaben gesetzmäßig und in zweckmäßiger und wirtschaftlicher Weise erfüllen, sondern er kann seine Mitarbeiter auch bei der Ausführung Ihrer Aufgaben anleiten, Fehler und Missstände abstellen, für die Einhaltung der Dienstzeit sorgen, das dienstliche Fortkommen seiner Mitarbeiter nach Maßgabe ihrer Leistungen fördern und ihren Einsatz so zu lenken, dass er ihren Fähigkeiten bestmöglich entspricht.

Zwar zielt das österreichische Recht darauf ab, den Vorgesetzten des geschäftsführenden Mitglieds der DSK daran zu hindern, diesem Weisungen zu erteilen, doch weist es dem Vorgesetzten eine Überwachungsbefugnis zu, die geeignet ist, die Unabhängigkeit der DSK bei der Wahrnehmung ihrer Aufgaben zu beeinträchtigen.

Zum Zweiten stellte das Gericht fest, dass die DSK zwar nicht über eine eigene Haushaltslinie verfügen muss, um das Unabhängigkeitskriterium erfüllen zu können. Allerdings darf die Zuweisung der von einer solchen Stelle benötigten personellen und sachlichen Mittel diese Stelle nicht daran hindern, ihre Aufgaben „in völliger Unabhängigkeit“ wahrzunehmen. Die Personalbesetzung der DSK mit Beamten des Bundeskanzleramts, die der Dienstaufsicht des Bundeskanzleramts unterliegen, ist nicht mit dem Unabhängigkeitserfordernis vereinbar.

Dass die Geschäftsstelle aus Beamten des Bundeskanzleramts besteht, das selbst der Kontrolle der DSK unterliegt, birgt die Gefahr einer Beeinflussung der Entscheidungen der DSK. Eine solche organisatorische Verzahnung der DSK mit dem Bundeskanzleramt verhindert, dass die DSK über jeden Verdacht der Parteilichkeit erhaben ist, und ist damit nicht mit dem Erfordernis der „Unabhängigkeit“ vereinbar.

Abschließend kam der Gerichtshof zu dem Ergebnis, dass das Recht des Bundeskanzlers, sich beim Vorsitzenden und beim geschäftsführenden Mitglied der DSK jederzeit über alle Gegenstände ihrer Geschäftsführung zu unterrichten, dazu angetan ist, die DSK einem mittelbaren Einfluss seitens des Bundeskanzlers auszusetzen, der nicht mit dem Unabhängigkeitskriterium vereinbar ist. Dies steht einer Einstufung der DSK als Stelle entgegen, deren Handlungen unter allen Umständen über jeden Verdacht der Parteilichkeit erhaben sind.

Der Gerichtshof hat für Recht erkannt, dass die Republik Österreich dadurch gegen ihre Verpflichtungen aus Art. 28 Abs. 1 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 verstoßen hat und nicht alle Vorschriften erlassen hat, die erforderlich sind, damit die in Österreich bestehende Rechtslage in Bezug auf die Datenschutzkommission dem Kriterium der Unabhängigkeit genügt, und zwar im Einzelnen dadurch, dass sie eine Regelung eingeführt hat, wonach das geschäftsführende Mitglied der Datenschutzkommission ein der Dienstaufsicht unterliegender Bundesbediensteter ist, die Geschäftsstelle der Datenschutzkommission mit den Ämtern des Bundeskanzleramts verflochten ist und der Bundeskanzler über ein unbedingtes Recht verfügt, sich über alle Gegenstände der Arbeit der Datenschutzkommission zu unterrichten.

3.3. EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

A: Zusammenfassung der Aktivitäten und Neuerungen:

Im Laufe des Jahres 2012 hat der EDSB erneut in verschiedenen Tätigkeitsbereichen neue Maßstäbe gesetzt. 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 wurden die Auswirkungen seiner neuen Strategie für die Durchsetzung der Datenschutzbestimmungen sichtbar: Wenngleich einige Organe und Einrichtungen der EU ihre Anstrengungen zur Einhaltung der Datenschutzverordnung noch verstärken sollten, verzeichnen die meisten, darunter auch zahlreiche Agenturen, diesbezüglich gute Fortschritte.

Bei der Beratung zu neuen Rechtsetzungsmaßnahmen gab der EDSB eine Rekordzahl von Stellungnahmen zu einem breiten Themenspektrum ab. Die Überprüfung des EU-Rechtsrahmens für den Datenschutz stand im Mittelpunkt des Interesses des EDSB. Darüber hinaus wirkten sich die Umsetzung des Stockholmer Programms für den Raum der Freiheit, der Sicherheit und des Rechts sowie die Digitale Agenda im Datenschutzbereich aus. Gleiches gilt für einige Themen im Bereich des Binnenmarkts, wie beispielsweise die Reform des Finanzsektors, sowie im Gesundheitswesen und im Verbraucherschutz. Ferner hat der EDSB seine Zusammenarbeit mit anderen Kontrollbehörden verstärkt.

Es wurden besondere Anstrengungen unternommen, um die Effizienz und Wirksamkeit der Einrichtung des EDSB vor dem Hintergrund der derzeit verfolgten Sparpolitik zu verbessern. In diesem Zusammenhang hat der EDSB eine umfassende strategische Überprüfung abgeschlossen, welche die Festlegung klarer Ziele für den Zeitraum 2013 bis 2014, die Verabschiedung einer Geschäftsordnung für alle Tätigkeiten des EDSB und die Einführung eines jährlichen Managementplans zum Ergebnis hatte.

Organisation	Europäischer Datenschutzbeauftragter (EDSB)
Vorsitz und/oder Gremium	Herr Peter Hustinx, Europäischer Datenschutzbeauftragter Giovanni Buttarelli, Stellvertretender Europäischer Datenschutzbeauftragter
Budget	7 624 090 EUR
Personal	58 (alle Kategorien zusammengefasst)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden 33 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 15 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. 37 informelle Kommentare

Meldungen	Die Datenschutzbeauftragten der Institutionen und Organe der EU reichten 119 Meldungen von Datenverarbeitungsvorgängen zur Vorabprüfung ein.
Vorabprüfungen	Es wurden 71 Stellungnahmen im Rahmen einer Vorabprüfung durchgeführt, insbesondere zu Gesundheitsdaten, zu Beurteilungen und zur Einstellung von Personal, zum Verdacht auf Verstöße und zu elektronischer Überwachung. 11 Stellungnahmen zu Verarbeitungen, die nicht einer Vorabprüfung unterliegen.
Anträge betroffener Personen	116 Informations- und Beratungsanfragen von Bürgern oder Interessengruppen, darunter Anfragen zu Themen wie die EU-Rechtsvorschriften zum Datenschutz und ihre Überprüfung, Cloud-Computing, ACTA, elektronische Gesundheitsdienste, Cookies und Schutz der Privatsphäre in der elektronischen Kommunikation, biometrische Technologien, Einwilligung, IT-Großsysteme wie SIS und Eurodac sowie die datenschutzrelevanten Themen in der EU-Verwaltung, wie z. B. Verarbeitungsvorgänge von Organen, Einrichtungen und Agenturen der EU.
Beschwerden betroffener Personen	86 eingegangene Beschwerden, 40 davon zulässig Vorrangige Arten mutmaßlicher Verstöße: Zugang zu bzw. Berichtigung von Daten, Widerspruch bzw. Löschung, übermäßige Datenerhebung, Übermittlung von Daten, Datenqualität und Unterrichtung der betroffenen Personen, Datensicherheit sowie Offenlegung von Daten.
Vom Parlament bzw. der Regierung angeforderte Beratung	Der Großteil der 33 oben genannten legislativen Stellungnahmen wurde auf Anfrage der Europäischen Kommission abgegeben (Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001).
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	27 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	15 Prüfungen vor Ort und 6 Besuche
Sanktionsmaßnahmen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	58 DPO in Einrichtungen, Organen und Agenturen der EU

B. Rechtsprechung

Beteiligungen des EDSB an Gerichtsverhandlungen

2012 trat der EDSB vier Verfahren vor dem Gerichtshof der Europäischen Union und dem Gericht für den öffentlichen Dienst als Streithelfer bei.

In der ersten Rechtssache ging es um die vermeintlich mangelnde Unabhängigkeit der österreichischen Datenschutzkommission (DSK). Der EDSB unterstützte den Standpunkt der Kommission, demzufolge die nach österreichischem Recht vorgesehene funktionelle Unabhängigkeit der DSK unzureichend war. Das Gericht folgte dieser Argumentation und befand, dass die DSK aufgrund ihrer engen Beziehungen zum österreichischen Bundeskanzleramt nicht über jeden Verdacht der Parteilichkeit erhaben sein könne.

Das zweite Verfahren, dem der EDSB als Streithelfer des Klägers beitrat, betraf die Rechtssache *Egan und Hackett/Europäisches Parlament* (Rechtssache T-190/10). Dies war seit dem wegweisenden Urteil des Gerichts vom 29. Juni 2010 in der Rechtssache *Bavarian Lager/Kommission* (C-28/08 P) die letzte von drei Rechtssachen, in denen das Gericht über das Verhältnis zwischen der Verordnung über den Zugang der Öffentlichkeit zu Dokumenten und der Datenschutzverordnung befinden musste. Wie in den beiden anderen Rechtssachen sprach sich der EDSB auch in diesem Fall für eine größere Transparenz aus.

Der EDSB trat zwei weiteren Verfahren als Streithelfer bei, die bei Redaktionsschluss noch anhängig waren. Der erste Fall betraf ein Vertragsverletzungsverfahren gegen Ungarn, das die Unabhängigkeit der Datenschutzbehörde zum Gegenstand hatte. Die zweite Rechtssache wurde vor dem Gericht für den öffentlichen Dienst verhandelt und betraf einen mutmaßlichen Verstoß gegen die EU-Datenschutzverordnung (EG) Nr. 45/2001 während eines internen Untersuchungsverfahrens der EIB wegen Mobbings.

Mehrere weitere Rechtssachen verfolgte der EDSB mit großer Aufmerksamkeit, ohne den Verfahren als Streithelfer beizutreten, darunter den spanischen Google-Fall, in dessen Zentrum die Frage der Anwendbarkeit der spanischen Rechtsvorschriften zur Umsetzung der europäischen Datenschutzrichtlinie im Hinblick auf die Tätigkeiten von Google steht, sowie zwei weitere Rechtssachen im Zusammenhang mit der Gültigkeit der europäischen Richtlinie über die Vorratsdatenspeicherung.

C. Sonstige wichtige Informationen

Überprüfung des Rechtsrahmens der EU für den Datenschutz

Das wichtigste Rechtsetzungsvorhaben des Jahres 2012 war für den EDSB zweifelsohne das Datenschutzreformpaket. Er unterstrich wiederholt die Notwendigkeit auf den neuesten Stand gebrachter und strengerer EU-Datenschutzvorschriften, und am 25. Januar verabschiedete die Kommission ihr Reformpaket, das zwei Rechtsetzungsvorschläge umfasst: einen Vorschlag für eine allgemeine Verordnung zum Datenschutz und einen Vorschlag für eine spezielle Richtlinie zum Datenschutz im Bereich Polizei und Justiz.

In einer ersten Reaktion begrüßte der EDSB die allgemeine Verordnung als einen riesigen Schritt vorwärts für den Datenschutz in Europa und einen ausgezeichneten Ausgangspunkt für die Annahme europäischer Regeln zum Datenschutz, die robust genug sind, um den Herausforderungen, vor die uns die Informationstechnologie stellt, gerecht zu werden.

Andererseits äußerte er sich jedoch äußerst kritisch über den unzureichenden Inhalt der Richtlinie. Er betonte, dass die Kommission ihrem Versprechen, ein robustes System für den Datenschutz im Bereich Polizei und Justiz zu schaffen, nicht gerecht geworden sei, und hinterfrage, warum die Kommission diesen Bereich von ihrer ursprünglichen Absicht, einen umfassenden Rechtsrahmen vorzulegen, ausgeschlossen habe.

Am 7. März nahm der EDSB eine Stellungnahme an, in der er seinen Standpunkt zu den beiden Vorschlägen ausführlicher darlegte. In einer öffentlichen Erklärung kam er zu dem Schluss, dass mit den beiden Rechtsetzungsvorschlägen Europa nach wie vor weit von einem umfassenden Paket von Datenschutzregeln auf nationaler und EU-Ebene in allen Politikbereichen der EU entfernt sei. Dies sei insbesondere darauf zurückzuführen, dass die Vorschläge zahlreiche existierende EU-Datenschutzregeln unangetastet ließen, so zum Beispiel die Datenschutzregeln für die EU-Organe und -Einrichtungen sowie alle spezifischen Instrumente im Bereich der Strafverfolgung.

Was die vorgeschlagene Richtlinie betrifft, so begrüßte der EDSB die Tatsache, dass der Vorschlag auch die innerstaatliche Verarbeitung personenbezogener Daten abdeckt, als besondere Verbesserung. Zugleich betonte er jedoch, dass dies nur dann einen Mehrwert habe, wenn die Richtlinie das Datenschutzniveau in dem Bereich deutlich anhebe, was aber nicht der Fall sei.

Er unterstrich, dass die vorgeschlagenen Regeln für den Datenschutz im Strafverfolgungsbereich unannehmbar schwach seien. Er stellte fest, dass es in vielen Fällen keine Rechtfertigung dafür gebe, von den in der Verordnung vorgeschlagenen Regeln abzuweichen. Des Weiteren betonte er, der Strafverfolgungsbereich brauche spezifische Regeln, jedoch keine generelle Senkung des Datenschutzniveaus.

Der EDSB äußerte sich insbesondere besorgt über die folgenden Aspekte:

- Mangel an Rechtssicherheit bezüglich der Weiterverwendung personenbezogener Daten durch Strafverfolgungsbehörden;
- Fehlen einer allgemeinen Verpflichtung für Strafverfolgungsbehörden, die Einhaltung der Datenschutzbestimmungen zu belegen;
- unzureichende Bedingungen für Datenübermittlungen in Drittländer;
- unangemessen eingeschränkte Befugnisse der Aufsichtsbehörden.

Im Laufe des Jahres hielt der EDSB mehrere Vorträge, in denen er seinen Standpunkt zum Reformpaket erläuterte, und beteiligte sich an den einschlägigen Diskussionen. Er stand dem EU-Gesetzgeber weiterhin mit Empfehlungen oder Erläuterungen zu seiner Position zur Verfügung. Ferner leistete er im Rahmen seiner Mitwirkung in der Artikel-29-Datenschutzgruppe Beiträge zu mehreren konkreteren Fragestellungen.

Darüber hinaus unternahm der EDSB Anstrengungen, um die Diskussion voranzutreiben. Im September und November organisierte er in enger Zusammenarbeit mit der Europäischen Rechtsakademie (ERA) zwei Seminare zu den Vorschlägen. Bei diesen Seminaren kamen zahlreiche Sachverständige aus nationalen Verwaltungen, Datenschutzbehörden, Organen der EU, wissenschaftlichen Einrichtungen, Drittländern und dem privaten Sektor zusammen. Ferner wurde eine Website zum Reformprozess eingerichtet, auf der alle einschlägigen Dokumente bereitgestellt werden und die über einen Link auf der Website des EDSB zugänglich ist.

Kapitel Vier

Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

ISLAND

A. Zusammenfassung der Aktivitäten und Neuerungen:

Anfang 2012 forderte das Gesundheitsministerium von plastischen Chirurgen die Daten aller Frauen an, denen seit 2000 Brustimplantate eingesetzt worden waren. Der Grund dafür war das Bekanntwerden von Gesetzesverstößen bei der Herstellung von Brustimplantaten der Marke PIP. Der isländische Ärzteverband, der sich gegen die Datenanforderung aussprach, bat die Datenschutzbehörde bezüglich der Frage um Rat, ob es gegen das Gesetz verstoße, dem Gesundheitsministerium personenbezogene Daten der betroffenen Personen, darunter Diagnosen und Identitäten, zukommen zu lassen. Die geplante Datenerfassung durch das Gesundheitsministerium hatte u. a. zum Zweck, Frauen mit PIP-Brustimplantaten zu kontaktieren und zu überprüfen, ob sie regelmäßig zur Brustkrebsvorsorge gehen, sowie statistische gesundheitliche Abweichungen von Frauen mit PIP-Brustimplantaten und Frauen mit anderen Brustimplantaten zu ermitteln. Dem isländischen Ärzteverband zufolge brachten viele Frauen bezüglich der Freigabe ihrer Daten jedoch Bedenken zum Ausdruck. Des Weiteren ließ der Verband verlauten, dass Frauen mit PIP-Brustimplantaten bereits von ihren plastischen Chirurgen ein Schreiben erhalten hätten, um sie über das Problem zu informieren. Die Datenschutzbehörde gab diesbezüglich zwei Stellungnahmen ab, eine davon im April bezüglich der Daten von Frauen mit PIP-Brustimplantaten und eine im März in Bezug auf Frauen mit anderen Implantaten. Bei beiden Stellungnahmen kam man zu dem Schluss, dass das Gesundheitsministerium nicht über die rechtliche Befugnis verfüge, um die betreffenden Daten einzuholen, und dass es den plastischen Chirurgen demnach nicht erlaubt sei, die Daten ohne Einwilligung der betroffenen Personen offenzulegen.

Ein weiterer erwähnenswerter Fall des Jahres 2012 betraf die Verbreitung personenbezogener Daten natürlicher Personen mit finanziellen Schwierigkeiten durch den Bürgerbeauftragten für Schuldner. Der Bürgerbeauftragte vertritt die Interessen von Schuldnern teilweise durch eine Vermittlung zwischen Gläubigern und Schuldnern in Sachen Schuldenminderung. Im Rahmen dieser Aufgabe schickte der Bürgerbeauftragte eine E-Mail an vier Pensionsfonds, die allesamt Gläubiger von Immobilienkrediten sind, sowie – versehentlich – eine E-Mail an das nationale Krankenhaus. Der E-Mail war eine Liste mit rund 3 000 Mandanten des Bürgerbeauftragten beigefügt. Der Grund der Übermittlung dieser Liste bestand darin, bei den Pensionsfonds nachzufragen, ob die Personen auf der Liste eine bestimmte schuldenmindernde Maßnahme in Anspruch genommen haben. Einer der Pensionsfonds brachte Bedenken in Bezug auf die Übermittlung der Daten zum Ausdruck und informierte die Datenschutzbehörde, welche der Sache nachging. Die Datenschutzbehörde kam zu dem Ergebnis, dass das Amt des Bürgerbeauftragten per Gesetz dazu befugt sei, sich darüber zu informieren, ob Mandanten die betreffende Maßnahme in Anspruch genommen haben. Die Datenschutzbehörde betonte jedoch, dass das Amt des Bürgerbeauftragten beim Erfassen von Daten nicht dazu befugt sei, umfassende Mandantenlisten zu übermitteln, nur weil die Empfänger möglicherweise über einschlägige Daten zu einigen dieser Personen verfügen könnten. Folglich kam die Datenschutzbehörde zu dem Schluss, dass die Übermittlung der Liste einen Verstoß gegen das Datenschutzgesetz darstellt. Des Weiteren wies die Datenschutzbehörde das Amt des Bürgerbeauftragten an, das Sicherheitsverwaltungssystem seiner Verarbeitung personenbezogener Daten schriftlich darzulegen.

Organisation	Isländische Datenschutzbehörde
Vorsitz und/oder Gremium	Frau Sigrún Jóhannesdóttir, Kommissionsmitglied; Frau Björg Thorarensen, Vorsitzende.
Budget	60 176 567 ISK (rund 353 418 EUR zum 31. Dezember 2012)

Personal	5 Juristen, 1 Sekretärin.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Etwa 150
Meldungen	551
Vorabprüfungen	133 Genehmigungen zur Verarbeitung von Daten.
Anträge betroffener Personen	Etwa 500
Beschwerden betroffener Personen	111
Vom Parlament bzw. der Regierung angeforderte Beratung	Etwa 50
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	2012 wurden insgesamt 1 489 neue Fälle registriert.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	3
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. 2012 wurden keine Geldbußen in Form von Tagessätzen verhängt.
Geldbußen	Mit Ausnahme der verhängten Geldbußen in Form von Tagessätzen für jeden Tag, an dem die Forderungen der Datenschutzbehörde nicht erfüllt werden, hat die Datenschutzbehörde keine Sanktionsbefugnisse. 2012 wurden keine Geldbußen in Form von Tagessätzen verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Am 27. August 2012 hob der Oberste Gerichtshof in der Rechtssache 562/2012 die Anordnung der Vorinstanz auf, laut der alle Mobilfunkanbieter, die ihre Dienste auf den Westmännerinseln anbieten, dazu verpflichtet wären, der Polizei die Daten aller Telefonanrufe mitzuteilen, die am Morgen des 6. August 2012 während eines zehnminütigen Zeitraums über bestimmte Mobilfunkmasten ein- bzw.

abgingen. Die gerichtliche Anordnung wurde im Zusammenhang mit den polizeilichen Ermittlungen bezüglich einer Sexualstraftat erteilt, die angeblich während dieses Zeitraums in der Nähe der betreffenden Mobilfunkmasten begangen wurde. Zu der Zeit wurde ein Verdächtiger anhand von Videoüberwachungsmaterial dabei beobachtet, wie er vom Tatort wegrannte und dabei mit seinem Mobiltelefon telefonierte. Laut Artikel 80 der Strafprozessordnung ist die Polizei dazu befugt, Telekommunikationsanbieter um die Herausgabe von Daten „bezüglich Telefonaten oder sonstiger Telekommunikationsaktivitäten mit einem bestimmten Telefon, Computer oder sonstigen Telekommunikationsgerät“ zu bitten. Der Oberste Gerichtshof kam zu dem Ergebnis, dass Artikel 71 der isländischen Verfassung, laut dem eine derartige Bereitstellung von Daten gegen das Recht auf Datenschutz verstößt, nicht weiter ausgelegt werden kann, als die wortwörtliche Formulierung dies zulässt. Demnach muss der Antrag auf eine gerichtliche Anordnung abgelehnt werden, da diese keine Informationen zu einem bestimmten Telefon enthält.

LIECHTENSTEIN

A. Zusammenfassung der Aktivitäten und Neuerungen

2012 war das Datenschutzgesetz (DSG) zehn Jahre in Kraft. Aus diesem Anlass wurde eine repräsentative Umfrage bei der Bevölkerung in Auftrag gegeben. Diese Umfrage stützte sich auf den Eurobarometer 225 aus dem Jahre 2008. Zusammenfassend kann Folgendes festgehalten werden: Die Bevölkerung hat ein großes Vertrauen vor allem gegenüber öffentlichen Institutionen und der Gesetzgebung. Dies wird allerdings dadurch relativiert, dass 70 % der Bevölkerung angeben, nur wenig über den Datenschutz zu wissen. Aus Sicht der Datenschutzstelle zeigt die Umfrage, dass die Bevölkerung besser sensibilisiert werden sollte. Die Umfrage zeigt zudem — nicht überraschend — dass Jugendliche nur wenig sensibilisiert sind und dass sich die Bevölkerung zwar ihrer Rechte bewusst ist. Die Anzahl Personen, die über das Auskunftsrecht Bescheid wussten, war jedoch im Vergleich zum Lösch- oder Berichtigungsrecht geringer. Dies ist eigentlich paradox, kann doch ein Löschanspruch erst dann wahrgenommen werden, wenn man weiß, was für Daten bearbeitet werden. Und eben dies erfährt man über das Auskunftsrecht. Am auffälligsten war aus unserer Sicht, dass nur 40 % wussten, dass es einen grundsätzlichen Schadenersatzanspruch gibt; 42 % verneinten dies. Die allgemeine Datenschutzrichtlinie 95/46/EG sieht einen solchen Anspruch vor, der in Liechtenstein nicht ins DSG übernommen wurde, aber dennoch gilt. Schließlich gaben rund 28 % an, von einer unabhängigen Datenschutzbehörde zu wissen. Von diesen 28 % gaben nur 15 % an, je mit ihr Kontakt gehabt zu haben. Dies kann darin begründet sein, dass aufgrund des erwähnten hohen Vertrauens kein Grund zu einer Kontaktaufnahme bestand; ein anderer Grund kann darin bestehen, dass die Sensibilisierung eben zu niedrig ist und ein mögliches Problem nicht erkannt wurde; ein dritter möglicher Grund kann im Nichtwissen über eine Schadenersatzmöglichkeit gegeben sein. Einzelheiten sind dem Tätigkeitsbericht 2012 zu entnehmen.

Eine Änderung des DSG trat auf Anfang Oktober in Kraft. Hauptgegenstand der Änderung war die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Damit wurde der Vorbehalt zur Geltung des DSG auf hängige Strafverfahren aufgehoben und Datenschutzbestimmungen in die Strafprozessordnung eingeführt. Zudem wurde die Bestimmung zur vorgängigen Information ausgeweitet und der Richtlinie 95/46/EG angepasst. Auf Verlangen der EFTA Surveillance Authority wurde die Bestimmung zur Meldepflicht von Datensammlungen durch Unternehmen ausgedehnt.

Am Europäischen Datenschutztag wurde wiederum eine öffentliche Veranstaltung mit der Universität Liechtenstein durchgeführt. Das Thema der Veranstaltung lautete: „Was weiß das Internet über mich?" Meine Daten als Handelsware. Dabei wurde auf die Problematik von Online Targeting eingegangen.

In der heutigen Gesellschaft ist die Anonymisierung eine wichtige Maßnahme zum Schutz von Personendaten. Auch die Pseudonymisierung ist wichtig. Zu diesen beiden Themen wurde eine Richtlinie ausgearbeitet und veröffentlicht.

Organisation	Datenschutzstelle
Vorsitz und/oder Gremium	Herr Philipp Mittelberger
Budget	596 000 EUR
Personal	2,3 Recht, 1,0 Technik, 0,8 Administration
Allgemeine Aktivitäten	

Beschlüsse, Stellungnahmen, Empfehlungen	9 Stellungnahmen zu Gesetzesvorhaben ([17]) 4 Bewilligungen von Videoüberwachungsanlagen
Meldungen	Insgesamt per Jahresende 384 Datensammlungen im Register aufgeführt (Reduktion zum Vorjahr insbesondere aufgrund der Bezeichnung von Datenschutzverantwortlichen durch Behörden und Private, wodurch diese von der Meldepflicht enthoben wurden).
Vorabprüfungen	k. A.
Anträge betroffener Personen	89 Anfragen von Privatpersonen
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	Keine
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	640 Anfragen ([18]) (inkl. Privatpersonen, siehe oben)
Prüfmaßnahmen	
Prüfungen, Untersuchungen	3 Kontrollverfahren abgeschlossen
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	50 Datenschutzverantwortliche

B. Rechtsprechung

Nichts Nennenswertes.

([17]) Vgl. Tätigkeitsbericht 2012 der Datenschutzstelle, unter Punkt 3, http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

([18]) Siehe Anfragenstatistik der Datenschutzstelle, unter Punkt 8.1., http://www.llv.li/pdf-llv-dss-taetigkeitsbericht_2012.pdf.

NORWEGEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Neue Strategien

Im Anschluss an die Strategie im Gesundheitswesen entwickelten wir weitere Strategien für Polizei und Justiz sowie im Hinblick auf unsere internationalen Verpflichtungen. Des Weiteren haben wir der Art und Weise, wie wir unsere Aufsichts- und Verwaltungsverfahren durchführen, mehr Aufmerksamkeit zukommen lassen.

2012 erhöhten wir die Anzahl der Prüfungen um 20 Prozent, verbesserten den Umgang mit individuellen Fällen und professionalisierten unseren Beratungsdienst.

Folgen des Anschlags vom 22. Juli 2011

Prüfungen mehrerer Vorschläge des Justizministeriums haben ergeben, dass die Gesetzesentwürfe hart und gerechtfertigt sind. Außerdem kamen wir zu dem Schluss, dass wir auch nach den tragischen Ereignissen vom 22. Juli 2011 einen kühlen Kopf bewahren müssen. Des Weiteren hat es sich als wichtig erwiesen, nach außen zu kommunizieren, dass die Datenschutzbehörde beim Lösen zukünftiger Probleme durch Fachkompetenzen im Feld der neuen Technologien und Kommunalentwicklung kooperativ arbeiten möchte.

Neue Website

Eine strategische Priorität besteht darin, allen Bürgern einen angemessenen Datenschutz zu gewährleisten. Eine der wichtigsten Maßnahmen war dabei der Launch unserer neuen Website. Beim Design wurde auf eine benutzerfreundliche Handhabung und das Angebot nützlicher Informationen Wert gelegt.

Organisation	Norwegische Datenschutzbehörde
Vorsitz und/oder Gremium	Herr Bjørn Erik Thon, Direktor
Budget	36 Mio. NOK
Personal	41
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	2 954 neue Meldungen, insgesamt 10 909 aktive Meldungen. (Zum Ende des Jahres lagen über 2 000 neue Meldungen vor, die noch nicht bearbeitet waren. Die tatsächliche Anzahl der neuen Meldungen sollte demnach höher sein.)
Vorabprüfungen	132
Anträge betroffener Personen	Insgesamt erhielt der Beratungsdienst der norwegischen

	Datenschutzbehörde 4 675 telefonische Anträge und 2 175 Anträge per E-Mail.
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	Wir erhielten 105 Aufforderungen zur Kommentierung neuer Gesetzesentwürfe und reichten 58 Kommentare ein.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Telekommunikation, Internet und DLD: 7 Arbeitsplatz: 10 Finanzsektor: 6 Gesundheitswesen: 5 Justiz und Polizei - 2 Öffentlicher Sektor: 13 Videoüberwachung: 4 Informationssicherheit: 4 Wiederholungsprüfungen: 4 Insgesamt: 55
Sanktionsmaßnahmen	
Sanktionen	7 Geldbußen und 2 Zwangsgelder, alle von der Datenschutzbehörde verhängt
Geldbußen	Geldbußen von insgesamt 1 300 000 NOK, Zwangsgelder 49 000 NOK
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	203 DPO, die insgesamt 390 Unternehmen und öffentliche Stellen repräsentieren.

B. Rechtsprechung

Im Folgenden werden die wichtigsten Regelungen aus dem Jahr 2012 dargelegt.

Rechtssache GE – unbefugte Weitergabe von Gesundheitsinformationen

Im März 2012 wurde die Datenschutzbehörde über die unbefugte Weitergabe von Gesundheitsinformationen durch mehrere Unternehmen (für die Verarbeitung Verantwortliche) an den Anbieter GE Healthcare Systems (GE) aus den USA in Kenntnis gesetzt. Wir gehen davon aus, dass die Daten einer nicht unerheblichen Anzahl von Patienten erfasst und an GE übermittelt wurden, einschließlich Namen, Identifikationsnummern, Geburtsdatum und Gesundheitsinformationen. Die Unstimmigkeiten stammen von elf norwegischen Unternehmen. Anfangs hieß es, dass es sich um die Daten von 126 344 Patienten handele, doch diese Zahl gilt als ungenau.

Die betreffenden Krankenhäuser hatten mit dem Anbieter GE eine Vereinbarung über den Betrieb, die Wartung und die Beobachtung von Geräten abgeschlossen. Die Verbindung ermöglichte GE den ungehinderten Abruf von Gesundheitsinformationen.

Unsere Regelung besagt, dass solche für die Verarbeitung Verantwortliche angemessene Schutzmechanismen einzurichten haben, um eine vertrauliche Handhabung der Daten zu gewährleisten, und dass die betroffenen Patienten über den Zwischenfall informiert werden müssen.

Die Rechtssache Nettby

Die Datenschutzbehörde beschloss 2011 die Löschung personenbezogener Daten der mittlerweile geschlossenen Social-Networking-Website Nettby (die sich im Besitz von VG, einer der größten norwegischen Boulevardzeitungen, befindet). VG focht den Beschluss an, woraufhin die Rechtssache vom Beschwerdeausschuss für Datenschutz geprüft wurde. Man kam zu dem Schluss, dass die Verpflichtung bestünde, einige der in den Dokumenten enthaltenen Informationen, die VG in der Nationalbibliothek aufbewahren wollte, zu hinterlegen, darunter die Inhalte der offenen Foren sowie die Teile, die für eine Indexierung durch Suchmaschinen herangezogen werden konnten. Der Beschluss gilt außerdem für Informationen, die nicht für eine Indexierung verwendet werden konnten, jedoch allen Mitgliedern von Nettby zugänglich waren. Vor der Löschung der Informationen musste VG dieser Verpflichtung nachkommen.

Der Beschluss ist in Anbetracht der Tatsache, dass Social-Networking-Websites von vielen Menschen genutzt werden, von Relevanz. Die Öffentlichkeit denkt vermutlich, dass sie zu einem geringen Teil selbst entscheiden könne, wie lange Informationen gespeichert werden und wer darauf Zugriff hat, sowohl gegenwärtig als auch in Zukunft.

Der Beschwerdeausschuss ist der Ansicht, dass jeder, der eine Plattform wie Nettby anbietet, dazu verpflichtet ist, „Dokumente“ in der Nationalbibliothek zu hinterlegen.

C. Sonstige wichtige Informationen

Bericht zur elektronischen Überwachung am Arbeitsplatz

Die Datenschutzbehörde veröffentlichte 2012 den Bericht „Ein normaler Arbeitstag – elektronische Überwachung am Arbeitsplatz“. Der Zweck dieses Berichts bestand darin aufzuzeigen, wie personenbezogene Daten im Arbeitsalltag erfasst und genutzt werden, und diesbezüglich zu informieren und zu sensibilisieren. Im Rahmen des Berichts untersuchten wir einen Arbeitstag in drei verschiedenen Berufsgruppen: Busfahrer, häusliche Krankenpfleger und Sachbearbeiter. Wir führten Gespräche mit Vertretern der Geschäftsleitung und Angestellten an zwei Arbeitsstellen in jeder dieser drei Berufsgruppen.

Kapitel Fünf

Mitglieder und Beobachter der Artikel-29-Datenschutzgruppe

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2012

Belgien	Bulgarien
Herr Willem Debeuckelaere Datenschutzkommission (Commission de la protection de la vie privée/ Commissie voor de bescherming van de persoonlijke levenssfeer) Rue de la Presse 35 - 1000 Brüssel Tel.: +32 (0)2/274 48 00 Fax: +32 (0)2/274 48 35 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. BG - 1431 Sofia Tel.+359 2 915 3501 Fax: +359 2 915 3525 E-Mail: kzld@government.bg, kzld@cpdp.bg Website: http://www.cpdp.bg/
Dänemark	**Deutschland**
Frau Janni Christoffersen Dänische Datenschutzbehörde (Datatilsynet) Borgergade 28, 5. Stock - DK - 1300 Kopenhagen 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) Ratapihantie 9, 6. Stock - FI - 00251 Helsinki (P.O. Box 800) Tel.: +358 295 666 700 Fax: +358 295 666 735 E-Mail: tietosuoja@om.fi Website: http://www.tietosuoja.fi
Frankreich	**Griechenland**
Frau Isabelle Falque Pierrotin Vorsitzende Präsidentin 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 E-Mail: Ifalquepierrotin@cnil.fr Website: http://www.cnil.fr	Herr Petros Christoforos Griechische Datenschutzbehörde (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) Kifisias Av. 1-3, PC 115 23 Athen Tel.: +30 210 6475608 Fax: +30 210 6475789 E-Mail: p.christoforos@dpa.gr Website: http://www.dpa.gr
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 Antonello Soro 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, a.soro@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 Tel.: + 371 67223131 Fax + 371 67223556 E-Mail: info@dvi.gov.lv Website: www.dvi.gov.lv	Herr Algirdas Kunčinas Litauische 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) 1, avenue du Rock'n'Roll, L - 4361 Esch-sur-Alzette 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 Amt des Informations- und Datenschutzbeauftragten 2, Airways House High Street Sliema SLM 1549 Malta Tel.: +356 2328 7100 Fax: +356 2328 7198 E-Mail: joseph.ebejer@gov.mt Website: http://www.idpc.gov.mt
Niederlande	**Österreich**
Herr Jacob Kohnstamm Niederländische Datenschutzbehörde (College Bescherming Persoonsgegevens - CBP) Juliana van Stolberglaan 4-10, P.O Box 93374 2509 AJ Den Haag Tel.: +31 70 8888500 Fax: +31 70 8888501 E-Mail: info@cbpweb.nl / international@cbpweb.nl Website: http://www.cbpweb.nl http://www.mijnprivacy.nl	Frau Eva Souhrada-Kirchmayer Österreichische Datenschutzkommission (Datenschutzkommission) Hohenstaufengasse 3 - AT - 1014 Wien Tel.: +43 1 531 15 / 202525 Fax: +43 1 531 15 /202690 E-Mail: dsk@dsk.gv.at Website: http://www.dsb.gv.at/

Polen	Portugal
Herr Wojciech Rafał Wiewiórowski Generalinspektor für den Schutz personenbezogener Daten (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 - PL - 00193 Warschau 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	Frau Filipa Calvão 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) Bd. Gral. Ghe. Magheru 28-30, 5. Stock, Zimmer 5, 1. Bezirk, PLZ 010336, RO - Bukarest Tel.: +40 31 805 9211 Fax: +40 31 805 9602 E-Mail: international@dataprotection.ro; anspdcp@dataprotection.ro Website: www.dataprotection.ro	Frau Kristina Svahn Starrsjö Schwedische Datenschutzbehörde (Datainspektionen) Drottninggatan 29, 5. Stock (Box 8114) - SE - 104 20 Stockholm Tel.: +46 8 657 61 57 Fax: +46 8 652 86 52 E-Mail: datainspektionen@datainspektionen.se, Website: http://www.datainspektionen.se
Slowakei	**Slowenien**
Frau Eleonóra Kročianová Behörde für den Schutz personenbezogener Daten der Slowakischen Republik (Úrad na ochranu osobných údajov Slovenskej republiky) Hraničná 12 - SK - 82007 Bratislava 27 Tel.: +421 2 323 132 11 Fax: +421 2 323 132 34 E-Mail: statny.dozor@pdp.gov.sk Website: http://www.dataprotection.gov.sk	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: gp.ip@ip-rs.si Website: http://www.ip-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 Praha 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 Dr. Attila Péterfalvi Präsident Nationale Behörde für Datenschutz und Informationsfreiheit (Nemzeti Adatvédelmi és Információszabadság Hatóság) Szilágyi Erzsébet fasor 22/c - HU - 1125 Budapest Tel.: +36 1 391 1400 Fax: +36 1 391 1410 E-Mail: ugyfelszolgalat@naih.hu Website: www.naih.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: www.ico.org.uk
Zypern	**Europäischer Datenschutzbeauftragter**
Herr Yiannos Danielides Kommissionsmitglied für den Schutz personenbezogener Daten (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα) 1, Iasonos str. Athanasia Court, 2. Stock - 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	Herr Peter Hustinx Europäischer Datenschutzbeauftragter — EDSB Anschrift: 60, rue Wiertz, BE - 1047 Brüssel Amt: 30, rue Montoyer, BE - 1000 Brüssel Tel.: +32 2 283 1915 Fax: +32 2 283 1950 E-Mail: edps@edps.europa.eu Website: www.edps.europa.eu

BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2012

Ehemalige jugoslawische Republik Mazedonien	Island
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	Frau Sigrún Jóhannesdóttir Isländische Datenschutzbehörde (Persónuvernd) Rauðararstígur 10 - IS - 105 Reykjavík Tel.: +354 510 9600 Fax: +354 510 9606 E-Mail: postur@personuvernd.is Website: http://www.personuvernd.is
Kroatien	**Liechtenstein**
Herr Dubravko Bilić Direktor Frau Sanja Vuk Leiterin der Abteilung für EU- und Rechtsfragen Kroatische Datenschutzbehörde (Agencija za zaštitu osobnih podataka - AZOP) Martićeva 14. 10000 Zagreb Tel.: +385 1 4609 000 Fax +385 1 4609 099 E-Mail: azop@azop.hr oder info@azop.hr Website: http://www.azop.hr/default.asp	Herr Philipp Mittelberger Kommissionsmitglied für Datenschutz Datenschutzstelle, DSS Kirchstrasse 8, Postfach 684 — FL-9490 Vaduz Tel.: +423 236 6090 Fax: +423 236 6099 E-Mail: info.dss@llv.li Website http://www.dss.llv.li
Norwegen	
Herr Kim Ellertsen Norwegische 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

DS-AA-15-001-DE-N

Publications Office

doi: 10.2838/607091