ISSN 2363-1015

Europäische Kommission

17. Bericht

der Artikel-29-Datenschutzgruppe

Berichtsjahr 2013

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).

17. Bericht der Artikel-29-Datenschutzgruppe — Berichtsjahr 2013
Europäische Kommission
Generaldirektion Justiz und Verbraucher
1049 Brüssel
BELGIEN

PDF ISBN 978-92-79-52064-8 ISSN 2363-1015 doi:10.2838/646887 DS-AA-15-002-DE-N

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

Luxemburg: Amt für Veröffentlichungen der Europäischen Union, 2016

© Europäische Union, 2016
Nachdruck mit Quellenangabe gestattet.

Titelbild: © robu_s / Fotolia.com

17. Bericht der Artikel-29-Datenschutzgruppe

Berichtsjahr 2013

Inhalt

VORWORT DES VORSITZENDEN 2
FRAGEN, ZU DENEN DIE ARTIKEL-29-DATENSCHUTZGRUPPE STELLUNG GENOMMEN HAT . 3
DIE WICHTIGSTEN ENTWICKLUNGEN IN DEN MITGLIEDSTAATEN 17
BELGIEN 18
BULGARIEN 24
DÄNEMARK 32
DEUTSCHLAND 35
ESTLAND 39
FINNLAND 44
FRANKREICH 48
GRIECHENLAND 56
IRLAND 62
ITALIEN 64
KROATIEN 70
LETTLAND 72
LITAUEN 74
LUXEMBURG 77
MALTA 80
NIEDERLANDE 83
ÖSTERREICH 87
POLEN 90
PORTUGAL 96
RUMÄNIEN 98
SCHWEDEN 101
SLOWAKEI 104
SLOWENIEN 109
SPANIEN 118
TSCHECHISCHE REPUBLIK 121
UNGARN 124
VEREINIGTES KÖNIGREICH 131
ZYPERN 136
AKTIVITÄTEN DER EUROPÄISCHEN UNION UND DER GEMEINSCHAFT 138
3.1. EUROPÄISCHES PARLAMENT 139
3.2. EUROPÄISCHE KOMMISSION 141
3.3. EUROPÄISCHER GERICHTSHOF 147

3.4. EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER 150
DIE WICHTIGSTEN ENTWICKLUNGEN IM EUROPÄISCHEN WIRTSCHAFTSRAUM 156
ISLAND 157
LIECHTENSTEIN 160
NORWEGEN 162
MITGLIEDER UND BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE 165
MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2013 166
BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2013 171

VORWORT DES VORSITZENDEN

Seit der Vorlage der Vorschläge für einen neuen Rechtsrahmen zum Datenschutz in der Europäischen Union (EU) im Januar 2012 hat die Artikel-29-Datenschutzgruppe die Reform aufmerksam verfolgt und sich 2013 zu mehreren Themen eingebracht, wie z. B. Einwilligung, berechtigtes Interesse, Zweckbindung und Profilbildung.

Während das Europäische Parlament zum Zeitpunkt des Verfassens dieses Vorwortes bereits einen Standpunkt zum Paket eingenommen hat, führt der Rat diesbezüglich nach wie vor Gespräche. Dennoch sind die Erwartungen mit Blick auf die neue Aufgabenbeschreibung der Europäischen Kommission hoch, dass die Verhandlungen zwischen den Gesetzgebern innerhalb der EU bald beginnen.

Die Reform des EU-Rechtsrahmens zum Datenschutz war natürlich eines der Hauptthemen, auf die sich die Datenschutzgruppe 2013 konzentriert hat. Es war jedoch sicherlich nicht das einzige Thema, das der Aufmerksamkeit der EU-Datenschutzbehörden bedurfte. Als Edward Snowden im Sommer 2013 enthüllte, dass die NSA willkürlich großangelegte Überwachungsaktivitäten durchführte und sich Zugriff auf alle (personenbezogenen) Daten verschaffte, die durch Firmen mit US-Sitz oder durch die USA flossen oder dort gespeichert wurden, reagierte die Welt mit Fassungslosigkeit und Wut.

Auf die Schwere der Enthüllungen und die öffentliche Empörung, die sie ausgelöst hatten, folgte ein kritischer Dialog zwischen der EU und den USA, an dem sich auch die Datenschutzgruppe und die nationalen EU-Datenschutzbehörden beteiligten. Die Menge der personenbezogenen Daten von EU-Bürgern sowie die Art und Weise, wie die Geheimdienste eines anderen Landes, eines Alliierten, darauf zugriffen, bewegte die Datenschutzgruppe dazu, die Europäische Kommission zu einer Zusammenarbeit mit den US-Behörden bezüglich der Situation aufzufordern.

Ferner gab die Datenschutzgruppe eine Stellungnahme ab, in der die wichtigsten Datenschutzrisiken mobiler Apps angesprochen und die spezifischen Verpflichtungen für App-Entwickler und alle weiteren, an der Entwicklung und der Verbreitung von Apps beteiligten Parteien nach EU-Recht genau dargelegt werden. Besonderes Augenmerk galt dabei den Apps, die an Kinder gerichtet sind.

Die Datenschutzgruppe gab 2013 außerdem eine Stellungnahme zur Zweckbindung heraus, in der sie klarstellte, dass eine Weiterverarbeitung zu einem von dem der ursprünglichen Erfassung personenbezogener Daten abweichenden Zweck nicht unbedingt bedeutet, dass der Zweck nicht damit vereinbar ist, eine Vereinbarkeit jedoch von Fall zu Fall beurteilt werden muss. In ihrer Stellungnahme bietet die Datenschutzgruppe Leitlinien zur Anwendung des Grundsatzes innerhalb des aktuellen Rechtsrahmens an, jedoch auch Empfehlungen für den zukünftigen allgemeinen Rechtsrahmen zum Datenschutz. Letzteres erfolgt als Reaktion auf die Diskussionen, die während des Überarbeitungsprozesses in Bezug auf die Zweckbindung geführt wurden.

Zu guter Letzt ist der Datenschutz kein ausschließlich EU-internes Thema, weshalb die Datenschutzgruppe mit ihren Gegenübern in allen Teilen der Welt in Kontakt geblieben ist. Der Schutz personenbezogener Daten ist ein gemeinsames Ziel und ein zunehmend globales Thema. Nur durch Zusammenarbeit untereinander sowie mit anderen weltweit werden wir in der Lage sein, global für einen angemessenen Datenschutz zu sorgen.

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 Verbindliche unternehmensinterne Vorschriften (BCR)

19.4.2013 Erläuterndes Dokument zu verbindlichen unternehmensinternen Datenschutzregelungen für Auftragsverarbeiter – WP 204

Ziel dieses Dokuments ist es, Leitlinien zur Anwendung von Artikel 26 Absatz 2 der Richtlinie 95/46/EG in Bezug auf die BCR für Auftragsverarbeiter (Auftragsverarbeiter bis Unterauftragsverarbeiter innerhalb derselben Unternehmensgruppe) bereitzustellen, der am 1. Januar 2013 zur Anwendung kam, sowie die Vereinfachung der Arbeit multinationaler Unternehmen, die im Auftrag der für die Verarbeitung Verantwortlichen personenbezogene Daten regelmäßig verarbeiten und austauschen. Dieses Arbeitsdokument soll als ein erster Schritt verstanden werden, mit dem die mögliche Verwendung von BCR für Auftragsverarbeiter auf der Grundlage eines Systems zur Selbstkontrolle und der Zusammenarbeit zwischen den Behörden beleuchtet werden soll, unbeschadet der Möglichkeit, auf andere Instrumente für die Übermittlung personenbezogener Daten ins Ausland zurückzugreifen, beispielsweise Standardvertragsklauseln oder gegebenenfalls die Grundsätze des sicheren Hafens.

1.1.2 Übermittlungen ins Ausland zu bestimmten Zwecken

4.4.2013 Schreiben der Artikel-29-Datenschutzgruppe an Herrn López Aguilar, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, bezüglich des Vorschlags für eine neue Richtlinie zur Verhinderung von Geldwäsche und Terrorismusfinanzierung

In diesem Schreiben informiert die Datenschutzgruppe den zuständigen Ausschuss des Europäischen Parlaments über ihre Bedenken bezüglich der Gesetzgebung zur Verhinderung von Geldwäsche und Terrorismusfinanzierung. Die Datenschutzgruppe kommt unter anderem zu dem Schluss, dass die sogenannten "Tipping-off"-Bestimmungen eine unbegründete Beschränkung der Rechte auf Zugang und Berichtigung darstellen, und empfiehlt, genau anzugeben, welche Verarbeitungen nicht unter diese Bestimmungen fallen. Des Weiteren weist sie nationale Aufsichtsbehörden und die Industrie an, die nötigen Anpassungen vorzunehmen.

Die Datenschutzgruppe spricht sich außerdem für die Klärung der Umstände aus, die eine Übermittlung personenbezogener Daten zu Zwecken der Verhinderung von Geldwäsche und Terrorismusfinanzierung an Drittländer legitimieren, die kein angemessenes Datenschutzniveau garantieren. Mitgliedsstaaten sollten festlegen, welche wichtigen öffentlichen Interessen für die Übermittlung der jeweiligen Daten an das jeweilige Land gelten und welche Garantien für einen wirkungsvollen Datenschutz vorliegen.

Die Datenschutzgruppe rät, bei jeder Profiling-Maßnahme genauere Modalitäten bzw. angemessene Schutzmechanismen hinzuzufügen, wie z. B. CDD, und ermutigt beteiligte Akteure zu einer besseren Zusammenarbeit im Bereich Datenschutz entweder durch einen Verweis auf das Erfordernis von Vorabprüfungen gemäß Artikel 20 der Richtlinie 95/46/EG oder durch einen Verweis auf das Erfordernis einer Datenschutz-Folgenabschätzung gemäß Artikel 33 des Verordnungsentwurfs.

13.6.2013 Endgültiges einheitliches Anmeldeverfahren und Standardvorlagen für Bürgerinnen und Bürger

Die Datenschutzgruppe hat in Zusammenarbeit mit US-Behörden einen Standardantrag für den Zugang zu bzw. die Berichtigung, Löschung oder Sperrung von personenbezogenen Daten entwickelt, die im Zusammenhang mit dem Programm des US-Finanzministeriums zum Aufspüren der Finanzierung des Terrorismus (TFTP) zur Nutzung durch Datenschutzbehörden gespeichert werden. Dies umfasst auch ein

detailliertes einheitliches Verfahren, nachdem eine betroffene Person einen Antrag auf Zugang zu bzw. Berichtigung, Löschung oder Sperrung von personenbezogenen Daten gestellt hat.

11.7.2013 Schreiben an Frau Cecilia Malmström, Kommissarin für innere Angelegenheiten, bezüglich vorab übermittelter Fluggastdaten (Advance Passenger Information, API)

Diese Anfrage der Datenschutzgruppe an die Kommission ist eine Reaktion auf die Anforderung, dass Luftfahrtunternehmen in der EU Fluggastdaten vorab an die Behörden in Drittländern, welche die Zielorte der einschlägigen Flüge sind, übermitteln. Die Datenschutzgruppe ist sich nicht sicher, dass es derzeit eine Rechtsgrundlage für solche Übermittlungen gibt, selbst dann, wenn die gesuchten Daten denen entsprechen, die Fluggäste ohnehin bei der Einreise in das Zielland bereitstellen würden. Demnach bittet die Datenschutzgruppe die Europäische Kommission darum, Schritte zur Einführung einer spezifischen Rechtsgrundlage einzuleiten, um die Rechtsunsicherheit zu beseitigen und für Kohärenz zu sorgen.

Diese Rechtsgrundlage sollte enthalten, dass Daten nur dann erfasst und übermittelt werden, wenn das Recht des Ziellandes dies vorsieht. Die Daten sollten von Luftfahrtunternehmen nur für den Zweck der Erfüllung der Grenzschutzverpflichtungen des Drittlandes beim Check-in erfasst und übermittelt und ohne Verzögerungen gelöscht werden, sobald das Flugzeug seinen endgültigen Bestimmungsort erreicht hat. Das Ausmaß der übermittelten Daten sollte auf die im maschinenlesbaren Bereich des Passes oder sonstiger Reisedokumente beschränkt bleiben; biometrische Daten sollten nicht übermittelt werden. Passagiere sollten vor dem Kauf ihrer Flugtickets über die Übermittlung sowie über den Zeitpunkt der Erfassung informiert werden.

Die Rechtsgrundlage sollte außerdem angemessene Schutzmechanismen für betroffene Personen enthalten, darunter Modalitäten zur Ausübung ihrer Rechte, und könnte im Rahmen der Bewertung und Überarbeitung der Richtlinie 2004/82/EG eingeführt werden.

9.10.2013 Schreiben des Vorsitzenden der Artikel-29-Datenschutzgruppe Jacob Kohnstamm an die Mitglieder des LIBE-Ausschusses bezüglich des Vorschlags für einen Ratsbeschluss zum Abkommen zwischen Kanada und der Europäischen Union über die Übermittlung und Verarbeitung von Fluggastdatensätzen (PNR)

In dem Schreiben legt die Datenschutzgruppe ihre Meinung zum PNR-Abkommen zwischen der EU und Kanada dar. Die Datenschutzgruppe erachtet Datenminimierung als äußerst wichtig für den Datenschutz von Fluggästen und empfiehlt, dass die Notwendigkeit einer jeden Position auf der Datenliste von kanadischer Seite separat geprüft wird. Die Datenschutzgruppe rät außerdem zu einer Überarbeitung der Definitionen der Begriffe Verhütung, Aufdeckung, Aufklärung und Verfolgung von terroristischen Straftaten und schwerer grenzüberschreitender Kriminalität, da diese zu ungenau sind.

Die Arbeitsgruppe bedauert, dass das Abkommen die Verarbeitung sensibler Daten durch kanadische Behörden erlaubt, und empfiehlt, dass im Falle von Verstößen gegen den Datenschutz oder bei Datenschutzzwischenfällen die zuständigen EU-Datenschutzbehörden informiert werden.

Die Datenschutzgruppe macht Vorschläge bezüglich der Überwachung der Umsetzung des Abkommens und empfiehlt darüber hinaus, dass die Parteien Luftfahrtunternehmen dazu verpflichten, Fluggästen Informationen hinsichtlich Grund, Zweck, Verwendung, Recht auf Zugang, Recht auf Auskunft, Recht auf Berichtigung und Recht auf Rechtsschutz bezüglich der Verarbeitung ihrer personenbezogenen Daten bereitstellen.

Die Datenschutzgruppe schlägt viel genauere Verweise auf die Rechte auf Zugang und Rechtsschutz vor und ist mit der Verlängerung der Aufbewahrungsfrist gegenüber dem Abkommen von 2005 nicht einverstanden. Des Weiteren schlägt die Datenschutzgruppe vor, dass die Behörden, an die die Daten übermittelt werden könnten, in dem Abkommen oder im Anhang aufgelistet werden.

8.11.2013 Zweites Schreiben der Artikel-29-Datenschutzgruppe an Herrn López Aguilar, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, bezüglich des Vorschlags für eine neue Richtlinie zur Verhinderung von Geldwäsche und Terrorismusfinanzierung

Dieses Schreiben der Datenschutzgruppe vom 8. November 2013 folgte auf ein früheres Schreiben und griff darin die zuvor geäußerten Bedenken auf, die von den Mitgesetzgebern noch nicht berücksichtigt worden waren, unter anderem, dass die Vorschläge nicht spezifisch genug waren, um als klare Rechtsgrundlage zu dienen, sie neue Maßnahmen enthielten, die die Privatsphäre und den Datenschutz nicht berücksichtigen, und sie die Zusammenarbeit mit sowie die Rolle von Datenschutzbehörden ignorierten.

5.12.2013 Kommentare der Artikel-29-Datenschutzgruppe zum direkten Zugang durch Strafverfolgungsbehörden von Drittländern auf Daten, die in anderen Rechtsgebieten gespeichert sind, wie es in den Entwürfen für ein Zusatzprotokoll zum Budapester Übereinkommen über Computerkriminalität vorgeschlagen wird

Die Ad-hoc-Untergruppe des T-CY des Europarats für Rechtsgebiete und grenzüberschreitenden Zugriff auf Daten und Datenverkehr legte Vorschläge zur Änderung des Protokolls zum Budapester Übereinkommen über Computerkriminalität vor, um zusätzliche Möglichkeiten für den grenzüberschreitenden Datenzugang zu schaffen, darunter den grenzüberschreitenden Zugang ohne Einwilligung.

Die Datenschutzgruppe kommt zu dem Schluss, dass, wenngleich die Verarbeitung von Daten zu Strafverfolgungszwecken rechtmäßig ist, sofern sie nicht gegen geltendes Recht verstößt, und angesichts der Tatsachen, dass Cloud-Computing immer wichtiger wird, dass es dadurch immer schwerer wird, Daten bestimmten Standorten zuzuordnen, und dass es bei der Verarbeitung von Cloud-Computing-Daten an Kontrolle und Transparenz mangelt, der Datenzugang zu Strafverfolgungszwecken in einem anderen Rechtsgebiet gegen die Datenschutzgrundsätze Notwendigkeit, Verhältnismäßigkeit und Zweckbindung verstößt.

In Anbetracht des Umstands, dass es sich bei den Übereinkommen 108 und 185 des Europarates um internationale Übereinkommen handelt, bedeutet es ferner, dass im Falle einer Unvereinbarkeit mit der Europäischen Menschenrechtskonvention nur europäische Staaten unter die Zuständigkeit des Europäischen Gerichtshofs für Menschenrechte fallen würden und somit eine Nichteinhaltung von Nicht-Europarat-Staaten erlaubt würde.

11.12.2013 Schreiben der Artikel-29-Datenschutzgruppe an den Internationalen Luftverkehrsverband (IATA) zum Thema „New Distribution Capability“

Die Datenschutzgruppe legte dem IATA in einem Schreiben seine vorläufigen Beobachtungen zum neuen Datenstandard „New Distribution Capability“ des IATA dar und informierte ihn darüber, dass die Menge der angeforderten personenbezogenen Daten in einem angemessenen Verhältnis zum Verarbeitungszweck stehen sollte und dass die Verarbeitung gemäß Artikel 7 der Richtlinie 95/46/EG eine Rechtsgrundlage haben sollte.

Die Datenschutzgruppe war sich nicht sicher, ob die Verhältnismäßigkeitsprüfung erfolgreich war oder ob eine Rechtsgrundlage basierend auf der Erfüllung eines Vertrages im Falle einer allgemeinen Suchanfrage, die nicht auf eine bestimmte Fluggesellschaft beschränkt war, zur Anwendung kommt. Eine Verarbeitung kann basierend auf einer ausdrücklichen Einwilligung ohne Zwang und Zweifel erfolgen.

Zu weiteren Themen, die es zu berücksichtigen gilt, gehören die Rolle der Luftfahrtunternehmen beim Buchungsvorgang sowie die Frage, ob sie in manchen Fällen in Bezug auf die Datenaufbewahrung, die Bereitstellung von Informationen für Fluggäste, potenzielle Übermittlungen in Drittländer außerhalb der EU sowie die Risiken von Profiling als für die Datenverarbeitung Verantwortliche erachtet werden könnten.

1.2 Elektronische Kommunikation, Internet und neue Technologien

27.2.2013 Stellungnahme 02/2013 zu Apps auf intelligenten Geräten – WP 202

Die vorliegende Stellungnahme der Datenschutzgruppe verdeutlicht den Rechtsrahmen für die Verarbeitung personenbezogener Daten bei der Entwicklung, Verbreitung und Nutzung von Apps auf intelligenten Endgeräten. Dabei liegt der Schwerpunkt auf der Einwilligungsanforderung, den Grundsätzen der Zweckbindung und der Datenminimierung, der Notwendigkeit angemessener Sicherheitsmaßnahmen, der Verpflichtung zu einer korrekten Aufklärung der Endnutzer, den Rechten der Endnutzer, angemessenen Speicherfristen und insbesondere der angemessenen Verarbeitung der von Kindern und über Kinder erfassten Daten.

Die Datenschutzgruppe kommt zu dem Schluss, dass viele Arten von Daten, die auf einem intelligenten mobilen Endgerät verfügbar sind, personenbezogene Daten sind. Der einschlägige Rechtsrahmen ist die Richtlinie 95/46/EG zusammen mit der Einwilligungsanforderung nach Artikel 5 Absatz 3 der Datenschutzrichtlinie für elektronische Kommunikation. Diese Vorschriften gelten unabhängig vom Standort des App-Entwicklers oder des App-Stores für jede App, die an App-Nutzer in der EU vertrieben wird.

Die Fragmentierung des App-Ökosystems, das breite Spektrum technischer Möglichkeiten für den Zugriff auf Daten, die auf mobilen Endgeräten gespeichert sind oder von diesen erstellt werden, und die mangelnde Kenntnis der einschlägigen Rechtsvorschriften unter den Entwicklern führen zu einer Reihe ernsthafter Datenschutzrisiken für App-Nutzer. Diese Risiken reichen von einer mangelnden Transparenz und einem fehlenden Problembewusstsein der App-Nutzer bis hin zu unzureichenden Sicherheitsmaßnahmen, ungültigen Einwilligungsmechanismen, der Tendenz zur Datenmaximierung und einer ungenauen Festlegung der Verarbeitungszwecke.

Zwischen den Datenschutzverpflichtungen der verschiedenen, an der Entwicklung, der Verbreitung und der Konzeption der technischen Möglichkeiten von Apps beteiligten Parteien bestehen Überschneidungen. Die meisten Schlussfolgerungen und Empfehlungen sind an App-Entwickler gerichtet (da diese den größten Einfluss darauf haben, wie die Verarbeitung erfolgt bzw. wie Informationen in einer App dargestellt werden). Um die höchsten Standards für den Datenschutz und den Schutz der Privatsphäre zu erreichen, müssen App-Entwickler jedoch häufig mit anderen Akteuren im App-Ökosystem zusammenarbeiten, z. B. mit den Herstellern von Betriebssystemen und Endgeräten, den App-Stores und Dritten wie z. B. Analysedienstleistern und Online-Werbenetzen.

13.3.2013 Schreiben der Artikel-29-Datenschutzgruppe an Neelie Kroes, Vizepräsidentin der Europäischen Kommission, zum Vorschlag der Kommission für eine Regulierung elektronischer Identifikations- und Vertauensdienste für elektronische Binnenmarkttransaktionen

In diesem Schreiben bringt die Datenschutzgruppe ihre Bedenken bezüglich des Vorschlags der Kommission für eine Regulierung elektronischer Identifikations- und Vertrauensdienste für elektronische Binnenmarkttransaktionen zum Ausdruck. Diese Bedenken umfassen die Auslegung bestimmter, in dem Vorschlag gebrauchter Begriffe, die Verwendung von Pseudonymen, Datenminimierung und in Zertifikaten enthaltene personenbezogene Daten, die Anwendbarkeit der Richtlinie 95/46/EG; elektronische Vertrauensdienste und -siegel sowie Massensignaturen und qualifizierte Signaturen für Mitarbeiter; elektronische Identität und Datenminimierung sowie die Gefahr von Profiling durch Online-Autorisierungs- und -Validierungssysteme und die Sicherheit elektronischer Signaturen, Aufsichtsbehörden, Listen qualifizierter Vertrauensdienste und Definitionen von Sicherheitsniveaus.

18.6.2013 Schreiben an Google bezüglich Google Glass, einer Art tragbarem Computer in Brillenform

Die Arbeitsgruppe schrieb Google bezüglich Google Glass an und brachte ihre Bedenken im Hinblick auf die Einhaltung der Datenschutzvorschriften; Datenschutzmechanismen; die erfassten Daten und ob diese weiterverbreitet werden; den beabsichtigten Zweck der Daten; Gesichtserkennung; die breiteren sozialen und ethischen Probleme, die sich zum Beispiel durch die heimliche Erfassung von Daten über andere Individuen daraus ergeben; sowie die Ergebnisse von etwaigen Risikoeinschätzungen im Zusammenhang mit Datenschutz zum Ausdruck.

2.10.2013 Arbeitsunterlage 02/2013 mit Leitlinien für die Einholung der Einwilligung zur Verwendung von Cookies – WP 208

Seit Annahme der geänderten Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG im Jahr 2009 haben die Website-Betreiber eine Reihe von praktischen Lösungen für die Einholung der Einwilligung zur Verwendung von Cookies entwickelt, die für verschiedene Zwecke genutzt werden. Die Vielzahl der von Website-Betreibern genutzten Einwilligungsmechanismen ist Ausdruck der Vielfalt der Organisationen und ihrer Zielgruppen. Dem Website-Betreiber steht es frei, wie er die Einwilligung einholt, solange die Einwilligung im Rahmen der EU-Gesetzgebung als gültig anerkannt werden kann. Diese Stellungnahme geht der Frage nach, ob eine bestimmte, von einem Website-Betreiber umgesetzte Lösung sämtliche Auflagen für eine gültige Einwilligung erfüllt.

In der Praxis werden die gesetzlichen Auflagen von den Website-Betreibern in den Mitgliedstaaten der EU unterschiedlich umgesetzt. Sie stützen sich in der Regel auf eine Reihe von Praktiken, die einzeln jedoch kaum als gültige Einwilligung ausreichen dürften.

In Anbetracht der unterschiedlichen Auslegungen der Richtlinie präzisiert die Stellungnahme die Erfordernisse, die für eine gültige Einwilligung erfüllt sein müssen, sowie deren wesentliche Elemente:

1. Spezifische Informationen: Die Einwilligung muss für den konkreten Fall gegeben worden sein und auf angemessener Informationen beruhen. Eine pauschale Einwilligung ohne Angabe des genauen Zwecks der Verarbeitung ist nicht zulässig.

2. Zeitpunkt: Die Einwilligung ist vor Beginn der Verarbeitung einzuholen.

3. Aktive Entscheidung: Das Verfahren zur Einholung und zur Erteilung der Einwilligung darf keinen Zweifel an der Absicht der betroffenen Person lassen. Es muss eine aktive Willensbekundung des Nutzers erteilt werden.

4. Ohne Zwang: Eine Einwilligung kann nur dann gültig sein, wenn die betroffene Person eine echte Wahlmöglichkeit hat.

5. Website-Betreiber, die dafür sorgen möchten, dass ein Einwilligungsmechanismus für Cookies die Bedingungen in jedem Mitgliedstaat erfüllt, sollten all diese Elemente berücksichtigen.

1.3 ÜBERARBEITUNG DES RECHTSRAHMENS FÜR DEN DATENSCHUTZ

22.1.2013 Arbeitsunterlage 01/2013 – Beitrag zu den vorgeschlagenen Durchführungsrechtsakten – WP 200

In dieser Arbeitsunterlage geht die Datenschutzgruppe – wie in der Stellungnahme 08/2012 – näher auf die Unterschiede zwischen delegierten Rechtsakten und Durchführungsrechtsakten ein, listet die einschlägigen Kriterien auf, anhand derer sich bestimmten lässt, ob Durchführungsrechtsakte gerechtfertigt und erforderlich sind, und prüft alle etwaigen Durchführungsrechtsakte Artikel für Artikel.

26.2.2013Stellungnahme 01/2013 mit weiteren Beiträgen zur Diskussion über den Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr – WP 201

In dieser Stellungnahme legt die Datenschutzgruppe ihre Kommentare zum Vorschlag für eine Richtlinie aus der Perspektive der Verwendung von Daten von nicht verdächtigen Personen, der Rechte der von der Datenverarbeitung betroffenen Personen, der Verwendung von Datenschutz-Folgeabschätzungen im Strafverfolgungsbereich sowie der Befugnisse der Datenschutzbehörden dar.

27.2.2013 Erklärung der Datenschutzgruppe zu aktuell geführten Diskussionen bezüglich des Datenschutz-Reformpakets

Diese Erklärung, die auf die Stellungnahmen WP191 und WP199 der Datenschutzgruppe folgt, greift die bereits zum Ausdruck gebrachten Bedenken zu den Bereichen Flexibilität im öffentlichen Sektor; personenbezogene Daten und Pseudonymisierung; Einwilligung; Governance; internationale Übermittlungen sowie risikobasierter Ansatz auf. Die Themen „leitende Datenschutzbehörde und Kompetenz“ sowie „Ausnahmen für familiäre und persönliche Aktivitäten“ werden ebenfalls gründlicher besprochen.

Bezüglich Flexibilität im öffentlichen Sektor kommt die Datenschutzgruppe zu dem Schluss, dass eine Unterscheidung zwischen dem öffentlichen und dem privaten Sektor lediglich zu Rechtsunsicherheit führen würde. Dies wäre auch in praktischer Hinsicht aufgrund der Unterschiede zwischen den Mitgliedstaaten in Bezug auf die Art und Weise und das Ausmaß der von öffentlichen Stellen ausgeführten Aufgaben nicht umsetzbar.

Eine Pseudonymisierung von Daten ist die Unkenntlichmachung von Identitäten auf rückidentifizierbare Weise. Die Unkenntlichmachung von Identitäten ohne die Möglichkeit einer Rückidentifizierung stellt eine Anonymisierung dar. Wenn Pseudonymisierung oder Verschlüsselung jedoch so betrieben wird, dass Einzelpersonen rückverfolgt oder (indirekt) identifiziert werden können, gelten weiterhin die Datenschutzvorschriften.

Wann immer eine Einwilligung als Rechtsgrundlage dient, muss diese hinreichend klar sein. Sie kann auf vielerlei Weise erfolgen, doch es sollte eine unverzichtbare Voraussetzung sein, dass sie ausdrücklich erteilt wird. Indem der für die Datenverarbeitung Verantwortliche die Einwilligung nachweisen muss, werden die Rechte des Einzelnen gestärkt.

Die zusätzlichen Aufgaben des Europäischen Datenschutzausschusses und der EU-Datenschutzbehörden werden zwar für einen stärkeren Schutz personenbezogener Daten sorgen, für Letztere jedoch auch das Problem ausreichender Ressourcen aufwerfen. Darüber hinaus sollten sie in der Lage sein, ihre eigenen Prioritäten festzulegen und Maßnahmen wie z. B. Untersuchungen auf Eigeninitiative durchzuführen – trotz Verpflichtungen in Bezug auf Zusammenarbeit, Amtshilfe und Kohärenz.

Es ist wichtig, dass die personenbezogenen Daten von EU-Bürgern unabhängig davon, ob die Daten innerhalb der EU verarbeitet oder in Drittländer außerhalb der EU übermittelt werden, denselben Schutz genießen. Nicht verbindliche Instrumente und Selbsteinschätzungen im Zusammenhang mit Übermittlungen an Drittländer sollten die Ausnahme bleiben und nur unter besonderen Umständen und nur für nicht massive und einmalige Übermittlungen möglich sein. In Fällen von rechtswidrigen Offenlegungen sollten Rechtshilfeabkommen verpflichtend sein.

Einige der Bestimmungen der vorgeschlagenen Verordnung, die einigen der für die Datenverarbeitung Verantwortlichen Lasten auferlegen, könnten als ungerecht erachtet werden und sollten demnach auf die jeweiligen Verantwortlichen und die Verarbeitungsaktivitäten ausgerichtet werden. Bezüglich Compliance sollte dafür gesorgt werden, dass personenbezogene Daten hinreichend geschützt werden, und dies kann von Verantwortlichem zu Verantwortlichem variieren. Dies hängt nicht nur von der Größe des für die

Datenverarbeitung Verantwortlichen ab, sondern auch von der Art und Weise der Verarbeitung und den Datenkategorien.

Anhang 1: Vorschläge für Änderungen in den Bereichen Kompetenz und leitende Datenschutzbehörde

In diesem Anhang macht die Datenschutzgruppe Vorschläge für Änderungen in den Bereichen Kompetenz und leitende Datenschutzbehörde auf der Grundlage, dass alle Aufsichtsbehörden auf dem Gebiet ihres Mitgliedstaates kompetent sein müssen. Die „leitende Datenschutzbehörde" muss für ein Unternehmen der alleinige Ansprechpartner sein und sich um den Entscheidungsfindungsprozess kümmern, an dem sich alle involvierten Aufsichtsbehörden beteiligen. Das Ergebnis des Entscheidungsfindungsprozesses sollte für alle Aufsichtsbehörden verbindlich sein. Das Konzept der Hauptniederlassung sollte geklärt werden, und falls es weiterhin Unklarheiten darüber gibt, welche Behörde die „leitende Behörde" ist, muss ein Entscheidungsfindungsverfahren bereitgestellt werden, und zwar bevorzugt vom Europäischen Datenschutzausschuss. Außerdem müssen Einzelpersonen immer die Möglichkeit haben, bei Gerichten in ihrem eigenen Mitgliedstaat Rechtsmittel einzulegen.

Anhang 2: Vorschläge für Änderungen in Bezug auf Ausnahmen für persönliche und familiäre Aktivitäten

In diesem Anhang schlägt die Datenschutzgruppe Änderungen in Bezug auf Ausnahmen für persönliche und familiäre Aktivitäten vor und verweist auf Kriterien, anhand derer entschieden wird, ob eine Verarbeitung zu persönlichen oder familiären Zwecken geschieht; sonstige einschlägige gesetzliche Bestandteile wie Verleumdung, Belästigung, bösartige Kommunikation, Anstiftung zu bedrohlichem Verhalten und in einigen Fällen Verfolgung oder Diskriminierung; Gewinnorientierung; Verbindung mit einer beruflichen oder gewerblichen Aktivität; persönliche Datenverarbeitung und weltweite Verbreitung sowie Korrespondenz und Aufbewahrung von Adressen.

13.5.2013 Ratgeber zu den wesentlichen Elementen einer Definition von Profiling und einer diesbezüglichen Bestimmung in der Datenschutz-Grundverordnung der EU

Mit diesem Dokument legt die Datenschutzgruppe einen Ratgeber zu den wesentlichen Elementen einer Definition von Profiling und einer diesbezüglichen Bestimmung im Entwurf der Datenschutz-Grundverordnung vor. Ausgangspunkt ist dabei die Tatsache, dass die Verbindung und Verlinkung personenbezogener Daten zur Erstellung von Profilen erhebliche Auswirkungen auf den Datenschutz haben können. Profiling ermöglicht die Bestimmung, Analyse und Prognose der Persönlichkeit einer Person (oder bestimmter Aspekte davon) meist ohne das Wissen der betroffenen Person. Demzufolge haben betroffene Personen möglicherweise nicht genügend Kontrolle über die Verarbeitung ihrer personenbezogenen Daten.

Die Datenschutzgruppe hält es für notwendig, der Datenschutz-Grundverordnung eine Definition von Profiling hinzuzufügen, und schlägt eine solche Definition vor.

Die Datenschutzgruppe bevorzugt einen umfassenden Ansatz zur Bestimmung spezifischer gesetzlicher Bestimmungen, nicht nur für die Nutzung und Weiterverarbeitung von durch Profiling erhaltener personenbezogener Daten, sondern auch für die Erfassung von Profiling-Daten und die Erstellung von Profilen an sich. Des Weiteren schlägt sie das Hinzufügen weiterer Elemente vor, wie z. B. eine größere Transparenz und stärkere individuelle Kontrolle in Bezug auf die Entscheidung, ob die eigenen personenbezogenen Daten zu Profiling-Zwecken verarbeitet werden dürfen; ausdrückliche Einwilligung als Rechtsgrundlage für die Datenverarbeitung zu Profiling-Zwecken sowie das Recht auf Zugang zu den Profildaten, um diese zu modifizieren oder zu löschen, und ein höheres Maß an Verantwortung aufseiten der für die Datenverarbeitung Verantwortlichen bezüglich Profiling-Methoden.

Profiling sollte Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen unterliegen, die auf Grundlage einer Datenschutz-Folgenabschätzung ergriffen werden. Des Weiteren sollte Profiling datenschutzfreundliche Technologien und Standardeinstellungen, spezifische Maßnahmen zur Datenminimierung, Datensicherheit und in bestimmten Fällen menschliches Eingreifen umfassen.

Angesichts der Tatsache, dass Profiling verschiedene Auswirkungen auf die Privatsphäre Einzelner haben kann, sollte die Verordnung klare Regelungen zur Rechtmäßigkeit und zu den Bedingungen der Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling enthalten und bei der Beurteilung der tatsächlichen Auswirkungen auf betroffene Personen, die eine bestimmte Art der Verarbeitung hat, einen gewissen Ermessensspielraum einräumen. Die Datenschutzgruppe unterstützt daher einen Ansatz, der Profiling oder auf Profiling basierende Maßnahmen einschließt, nur in dem Maße, dass sie erhebliche Auswirkungen auf die Interessen, Rechte oder Freiheiten der betroffenen Personen haben. Die Formulierung „erhebliche Auswirkungen" sollte unter Berücksichtigung des Ausmaßes des Grundrechts auf Datenschutz sowie der Bewertung der Interessen von für die Verarbeitung Verantwortlichen und der Analyse der potenziellen Auswirkungen von Profiling-Technologien auf die Rechte und Freiheiten der betroffenen Personen ausgelegt werden. Dies erfolgt am besten durch den Europäischen Datenschutzausschuss.

1.4. PERSONENBEZOGENE DATEN

1.4.1 Zweckbindung

2.4.2013 Stellungnahme 03/2013 zur Zweckbindung – WP 203

Diese Stellungnahme hat zum Ziel, den Grundsatz der Zweckbindung zu analysieren, Leitlinien für die praktische Anwendung des Grundsatzes nach dem derzeitigen Rechtsrahmen zu liefern und Empfehlungen für die Zukunft aufzustellen. Zweckbindung schützt betroffene Personen, indem die Art und Weise, wie für die Datenverarbeitung Verantwortliche ihre Daten verwenden können, eingeschränkt wird, während auch den für die Datenverarbeitung Verantwortlichen ein gewisses Maß an Flexibilität eingeräumt wird. Personenbezogene Daten müssen zu festgelegten, expliziten und rechtmäßigen Zwecken (Zweckbestimmung) erfasst werden und dürfen nicht in einer Art und Weise, die mit diesen Zwecken unvereinbar ist, weiterverarbeitet werden (Vereinbarkeit der Nutzung).

Die Vereinbarkeit muss auf Einzelfallbasis, unter Berücksichtigung aller einschlägigen Umstände und mit besonderem Augenmerk auf der Beziehung zwischen dem Zweck, zu dem die personenbezogenen Daten erfasst wurden, und dem Zweck der Weiterverarbeitung beurteilt werden. Weitere zu berücksichtigende Faktoren sind der Kontext, in dem die personenbezogenen Daten erfasst wurden, und die angemessenen Erwartungen der betroffenen Personen im Zusammenhang mit ihrer weiteren Verwendung; die Beschaffenheit der personenbezogenen Daten und die Auswirkungen einer Weiterverarbeitung auf die betroffenen Personen sowie die von den für die Datenverarbeitung Verantwortlichen getroffenen Sicherheitsvorkehrungen zur Gewährleistung einer einwandfreien Verarbeitung und zur Vorbeugung unerwünschter Auswirkungen auf die betroffenen Personen.

Eine Verarbeitung personenbezogener Daten auf eine Weise, die mit den zum Zeitpunkt der Erfassung angegebenen Zwecken unvereinbar ist, ist unrechtmäßig und demnach verboten. Der für die Datenverarbeitung Verantwortliche kann eine unrechtmäßige Verarbeitung nicht durch Berufung auf eine andere Rechtsgrundlage gemäß Artikel 7 der Richtlinie 95/46/EG legitimieren. Der Grundsatz der Zweckbindung kann nur durch Artikel 13 der Richtlinie eingeschränkt werden.

Artikel 6 Absatz 4 der vorgeschlagenen Datenschutzverordnung erlaubt eine weit gefasste Ausnahme von der Vereinbarkeitsbestimmung, die ihre Anwendbarkeit erheblich einschränken würde und das Risiko birgt, diesen Kerngrundsatz auszuhöhlen. Die Datenschutzgruppe empfiehlt daher, dass der vorgeschlagene Absatz 4 gelöscht wird und die Gesetzgeber die oben aufgeführte Auflistung einschlägiger Faktoren zur Beurteilung der Vereinbarkeit berücksichtigen.

Stellungnahme 06/2013 zu den offenen Daten (‚Open Data') und der Weiterverwendung von Informationen des öffentlichen Sektors (‚PSI') (416 kB) – WP 207 (5.6.2013)

Diese Stellungnahme betrifft die Änderung der Richtlinie 2003/98/EG zur Weiterverwendung von Informationen des öffentlichen Sektors (‚PSI-Richtlinie'), die zwar die Bedingungen für diese Weiterverwendung von Informationen des öffentlichen Sektors harmonisiert, öffentlichen Stellen jedoch freistellt, ob sie Daten für die Weiterverwendung zur Verfügung stellen.

Der Zweck der Änderung bestand darin, dass alle öffentlichen Informationen sowohl für kommerzielle als auch nichtkommerzielle Zwecke weiterverwendet werden können, wofür jedoch Ausnahmen gelten, wie z. B. aus Gründen des Datenschutzes.

Die geänderte Richtlinie schreibt den öffentlichen Stellen jetzt zwingend vor, die Weiterverwendung aller bei ihnen vorhandenen, nach innerstaatlichem Recht öffentlich zugänglichen Informationen zu gestatten, und das nur dann, wenn keinerlei Vorschriften des geltenden Datenschutzrechts verletzt werden.

Eine größere Zugriffsmöglichkeit auf öffentliche Informationen ist nicht ohne Risiken. Um diese Risiken möglichst gering zu halten, muss in allen Fällen, in denen der Schutz der Privatsphäre und der personenbezogenen Daten auf dem Spiel steht, ein ausgewogenes Gesamtkonzept verfolgt werden – zwischen der Entwicklung des Weiterverwendungsmarktes einerseits und dem Recht auf Schutz der personenbezogenen Daten und dem Recht auf Privatsphäre andererseits. Der Schwerpunkt für ‚offene Daten' liegt auf der Transparenz und der Rechenschaftspflicht der öffentlichen Stellen sowie auf dem Wirtschaftswachstum und nicht auf der Durchsichtigkeit des einzelnen Bürgers. Statt personenbezogener Daten sind es häufig statistische Daten, die aus personenbezogenen Daten abgeleitet wurden und zu Zwecken der Weiterverwendung bereitgestellt werden und werden sollten.

In einigen Situationen können personenbezogene Daten gegebenenfalls nach Maßgabe rechtlicher, technischer oder organisatorischer Maßnahmen zum Schutz der betreffenden Personen weiterverwendet werden. In solchen Fällen ist eine klare Rechtsgrundlage erforderlich, wobei die Grundsätze der Verhältnismäßigkeit, der Datenminimierung und der Zweckbindung zu berücksichtigen sind.

Die Datenschutzgruppe empfiehlt, dass die Möglichkeit, dass einige Informationen personenbezogene Daten enthalten können, so früh wie möglich und unter Berücksichtigung des Datenschutzes bereits in der Planungs- und Entwicklungsphase (‚data protection by design') wie auch im Fall von bestehenden Verarbeitungssystemen nach Maßgabe der datensparsamsten Voreinstellungen (‚data protection by default') in Betracht gezogen werden sollte. Außerdem sollten Datenschutz-Folgenabschätzungen durchgeführt werden, bevor personenbezogene Daten oder daraus abgeleitete anonymisierte Daten zugänglich gemacht werden. Wenn Daten anonymisiert werden, ist es von großer Bedeutung, das Rückidentifizierungsrisiko zu bewerten, und eine bewährte Verfahrensweise, die Rückidentifizierung einem Testdurchlauf zu unterziehen. Das Ergebnis der Bewertung könnte dabei behilflich sein, die geeigneten Schutzmaßnahmen zur Risikominimierung zu ermitteln oder zu der Entscheidung führen, von der Veröffentlichung bzw. der Bereitstellung zu Zwecken der Weiterverwendung abzusehen. Die Lizenzbedingungen zur Weiterverwendung von Informationen sollten eine Datenschutzklausel umfassen. Kommt die Datenschutz-Folgenabschätzung zu dem Ergebnis, dass eine Lizenz nicht ausreicht, um auf die Datenschutzrisiken einzugehen, sollten keine personenbezogenen Daten offengelegt werden. Öffentliche Stellen sollten gegebenenfalls dafür Sorge tragen, dass personenbezogene Daten anonymisiert werden und die Lizenzbedingungen die Rückidentifizierung von natürlichen Personen sowie die Weiterverwendung von personenbezogenen Daten zu Zwecken, die die betroffenen Personen beeinträchtigen können, speziell verbieten. Schließlich sollten die Mitgliedstaaten in Betracht ziehen, Wissensnetze/Kompetenzzentren aufzubauen und zu unterstützen und damit den Austausch zu bewährten Praktiken im Zusammenhang mit Anonymisierung und offenen Daten zu ermöglichen.

6.6.2013 Schreiben der Artikel-29-Datenschutzgruppe an die ICANN bezüglich der Erklärung zur Auswirkung der Überarbeitung der ICANN RAA auf den Datenschutz

In diesem Schreiben befasst sich die Datenschutzgruppe mit der Frage, inwiefern die endgültige Vereinbarung über die Zulassung einer Registrierungsstelle (RAA) der ICANN die europäischen Datenschutzvorschriften einhält, und befasst sich dabei insbesondere mit der Rechtmäßigkeit der Verpflichtung der Registrierungsstellen zur Datenaufbewahrung.

Die ICANN hat für Registrierungsstellen ein Verfahren eingeführt, um, falls nötig, auf Antrag von diesen Bestimmungen ausgenommen zu werden und einen Verstoß gegen das geltende Datenschutzrecht zu vermeiden. Solch ein Antrag kann auf der schriftlichen Weisung einer Regierungsbehörde des zuständigen Rechtsgebiets beruhen, sofern die Einhaltung der Datenaufbewahrungsbestimmungen gegen das geltende Recht verstößt.

Die Datenschutzgruppe beobachtete, dass die vorgeschlagene neue Datenaufbewahrungsbestimmung auf keiner gesetzlichen Auflage in Europa beruht, und wies darauf hin, dass die Datenschutzrisiken unter Berücksichtigung der Vielfalt dieser Registrierungsstellen hinsichtlich Größe sowie technischen und organisatorischen Sicherheitsmaßnahmen und aufgrund der Tatsache, dass die Möglichkeit von Datenschutzverstößen negative Auswirkungen auf Einzelpersonen mit Domainnamen hat, im Vergleich zum Nutzen des Vorschlags unverhältnismäßig hoch sind.

Die Datenschutzgruppe hatte außerdem Einwände bezüglich der Datenaufbewahrung auf der Grundlage eines Vertrages anstelle eines nationalen Gesetzes, um z. B. ein dringliches soziales Anliegen auf dem Gebiet der Strafverfolgung anzusprechen. Die Tatsache, dass diese personenbezogenen Daten für die Strafverfolgung nützlich sein könnten, rechtfertigte nicht ihre Aufbewahrung nach Ablauf des Vertrages.

1.4.2 Intelligente Stromversorgungsnetze

Stellungnahme 04/2013 zum Muster für die Datenschutz-Folgenabschätzung („Muster") für intelligente Netze und intelligente Messsysteme, erstellt durch die Sachverständigengruppe 2 der Taskforce der Kommission für intelligente Netze (285 kB) – WP 205 (22.4.2013)

Die Europäische Kommission veröffentlichte 2012 eine Empfehlung zu Vorbereitungen für die Einführung intelligenter Messsysteme („Empfehlung der Kommission"), um den Mitgliedsstaaten unter anderem Hilfestellung bei der Einführung intelligenter Messsysteme auf den Strom- und Gasmärkten und Orientierungshilfen in Datenschutzfragen zu geben. Die Empfehlung lautete eingebauter und standardmäßiger Datenschutz und legte fest, dass Mitgliedstaaten ein Muster für die Datenschutz-Folgenabschätzung („Muster") annehmen und einsetzen, das von der Kommission zu entwickeln und der Datenschutzgruppe zur Stellungnahme vorzulegen ist.

Die Stellungnahme der Datenschutzgruppe kommt zu dem Schluss, dass trotz einer Verbesserung des Musters nach wie vor hinsichtlich Umfang, beteiligten Akteuren, Rechtsgrundlage und Wahlmöglichkeiten, Datenminimierung sowie Technologien zum besseren Schutz der Privatsphäre viel getan werden muss.

1.4.3 Grenzen und Inneres

23.4.2013 Schreiben der Artikel-29-Datenschutzgruppe an die IATA bezüglich Checkpoint of the Future und Anhang

Die Datenschutzgruppe schrieb der IATA bezüglich des vorgeschlagenen Projekts Checkpoint of the Future und wies darauf hin, dass es grundsätzliche Fragen im Hinblick auf die Einhaltung der EU-Datenschutzvorschriften und insbesondere der Grundsätze der Notwendigkeit und der Verhältnismäßigkeit; der Datenqualität, Datenminimierung und Zweckbindung; spezifischer Datenkategorien; der Rechtmäßigkeit der Verarbeitung; der Rechte der betroffenen Personen und der Transparenz; automatisierter Entscheidungen und Profiling; internationaler Übermittlungen personenbezogener Daten sowie der Datensicherheit und Vertraulichkeit aufwirft. Eingebauter

Datenschutz sollte ein Leitprinzip sein, und Datenschutzbedenken sollten von Beginn an berücksichtigt werden.

Im Anhang des Schreibens warf die Datenschutzgruppe spezifische Fragen zu den Themen Effektivität; Notwendigkeit und Verhältnismäßigkeit; Fluggastdifferenzierung; Data Controlling und Compliance; Zweckbindung; bekannte Reiseprogramme; Verhaltensanalyse; Datenzugang und Transparenz; Identitätsmanagement; Zugang zu und Austausch von Daten sowie Technologie auf.

6.6.2013 Stellungnahme 05/2013 zu intelligenten Grenzen – WP 206

Die Kommission legte 2013 Vorschläge für ein Einreise-/Ausreisesystem (EES) und ein Registrierungsprogramm für Reisende (RTP) für den Schengen-Raum vor, die zusammen als Vorschläge für „intelligente Grenzen" bezeichnet werden. Außerdem wurde ein Vorschlag für erforderliche Änderungen des Schengener Grenzkodizes vorgelegt.

Der Vorschlag für ein Einreise-/Ausreisesystem umfasst ein System zur zentralen Speicherung der Ein- und Ausreisedaten von Drittstaatsangehörigen, die für Kurzaufenthalte im Schengen-Raum zugelassen sind, unabhängig davon, ob sie einer Visapflicht für ein Schengen-Visum unterliegen. Anstatt die Reisepässe bei der Einreise in den Schengen-Raum und der Ausreise aus dem Schengen-Raum abzustempeln, werden Daten über die Identität des Besuchers sowie über Dauer und Zweck des Aufenthalts bei der Einreise in das System eingegeben und bei der Ausreise überprüft, um sicherzustellen, dass der Drittstaatsangehörige die höchstens zulässige Aufenthaltsdauer nicht überschritten hat. Da das EES ein zentrales System darstellt, ist bei der Prüfung der EES-Daten unerheblich, über welche Grenzübergangsstelle der Drittstaatsangehörige aus dem Schengen-Raum ausreist. In erster Linie soll mit dem System verhindert werden, dass Drittstaatsangehörige die zulässige Aufenthaltsdauer im Schengen-Raum überziehen. Der Vorschlag für ein EES umfasst ein System, in dem zunächst personenbezogene Daten erfasst werden, die zur Identifizierung von Personen benötigt werden (alphanumerische Daten). Nach drei Jahren sollen auch biometrische Daten erfasst werden. Nach zwei Jahren soll geklärt werden, ob Strafverfolgungsbehörden und Drittstaaten Zugang zu den im System gespeicherten Informationen erhalten sollten.

Der Vorschlag für ein RTP umfasst ein Programm zur freiwilligen Registrierung von Reisenden, die häufig in den Schengen-Raum einreisen (Vielreisende), beispielsweise Geschäftsreisende. Drittstaatsangehörige können den Status als registrierte Reisende beantragen, um die Grenzabfertigung zu beschleunigen. Grundlage des RTP bilden ein Zentralregister mit biometrischen Daten sowie ein an die Reisenden ausgehändigtes „Token", auf dem eine individuelle Kennung gespeichert ist.

Die Datenschutzgruppe bezweifelt, dass das EES beim Erreichen der eigenen erklärten Ziele wirksam sein kann. Doch selbst wenn das EES einen wesentlichen Mehrwert bieten würde, kam man zu dem Schluss, dass der Mehrwert des EES im Hinblick auf das Erreichen seiner Ziele das nötige Maß der Notwendigkeit nicht erfüllt, um die Beeinträchtigung bestehender Rechte gemäß Artikel 8 der EU-Charta zu rechtfertigen. Ferner ist man der Auffassung, dass der Mehrwert des EES in Bezug auf die einzelnen Ziele nicht im Verhältnis zum Ausmaß seiner Auswirkungen auf die Grundrechte steht und dass Alternativen existieren, um die Ziele zu erreichen.

9.12.2013 Schreiben der Artikel-29-Datenschutzgruppe an Herrn López Aguilar, Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, bezüglich des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über EUROPOL

In diesem Schreiben kommentierte die Datenschutzgruppe den Vorschlag der Europäischen Kommission für eine Verordnung über die Agentur der Europäischen Union für die Zusammenarbeit und die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (Europol-Verordnung), zu der sowohl der Europäische Datenschutzbeauftragte (EDSB) als auch die gemeinsame Kontrollinstanz von Europol Stellungnahmen abgegeben haben.

Die Datenschutzgruppe kommt zu dem Schluss, dass das in dem Vorschlag festgelegte Datenschutzniveau hinter den im Europol-Ratsbeschluss dargelegten Standards zurückbleibt und dass der Vorschlag verbessert werden muss, um zu einer verbesserten, stärkeren Datenschutzregelung für Europol beizutragen. Demnach erscheint es als notwendig, einige wichtige Bestimmungen im Entwurf der Europol-Verordnung umzuformulieren und, wo möglich, wirkungsvollere Datenschutzmechanismen einzuführen, die speziell auf die Aktivitäten von Europol abgestimmt sind.

Die Datenschutzgruppe kommt außerdem zu dem Schluss, dass für die Beschreibung des Ausmaßes der Europol-Kompetenzen und spezifischer Verbrechen, für die Europol in Zukunft zuständig sein wird, eine genauere Definition nötig ist.

Es gibt keine klare Zuständigkeitsverteilung, was die von Dritten bereitgestellten Informationen betrifft. Ebenso gibt es keine klare Zuweisung von Verantwortlichkeiten in Bezug auf die Ergebnisse der von Europol durchgeführten analytischen Aufgaben. Da eine Verbindung zwischen den Daten, die für die Vorbereitung eines Berichts verwendet werden, und dem Endergebnis besteht, sollte jeder auf ungenauen Daten basierende Bericht entsprechend aktualisiert werden. Dies kann nur mit einer genauen Zuständigkeitsverteilung geschehen.

Die Bestimmungen zu den Zwecken der Datenverarbeitungsaktivitäten scheinen Europol nicht in die Lage zu versetzen, seine derzeitigen und beabsichtigten zukünftigen Aufgaben zu erfüllen, und werden negative Auswirkungen auf die Privatsphäre des Einzelnen haben. Für die Einrichtung von Datenverarbeitungssystemen, mit denen nur bestimmte personenbezogene Daten verarbeitet werden, sollten Bedingungen definiert werden. Der Vorschlag würde von einer Aufnahme bestimmter Elemente des eingebauten Datenschutzes profitieren, nämlich dem Einbeziehen von Datenschutz-Folgenabschätzungen als verpflichtendes Hilfsmittel in bestimmten Fällen sowie Mechanismen, die datenschutzfreundliche Grundeinstellungen ermöglichen.

Die Datenschutzgruppe stellt das Fehlen einer Verpflichtung in Bezug auf Meldungen von Verstößen gegen den Schutz personenbezogener Daten an die Aufsichtsbehörde und in bestimmten Fällen an betroffene Personen fest, wie es im Datenschutzpaket und vor allem in den Artikeln 28 und 29 der vorgeschlagenen Richtlinie vorgesehen ist. Die Datenschutzgruppe empfiehlt unter Berücksichtigung der Besonderheiten der Aufgaben von Europol die Aufnahme dieser Verpflichtung in den Vorschlag.

1.4.4 Sport

5.3.2013 Schreiben der Artikel-29-Datenschutzgruppe an die Welt-Anti-Doping-Agentur bezüglich der dritten Phase der WADA-Konsultation im Zusammenhang mit der Überarbeitung des Welt-Anti-Doping-Kodizes und seiner Internationalen Standards sowie Beitrag zum Anhang

Seit ihren Stellungnahmen WP156 (2008) und WP162 (2009) zum Standard zum Schutz der Privatsphäre und personenbezogener Informationen, zu bestimmten einschlägigen Bestimmungen des Welt-Anti-Doping-Kodizes und des Standards für Doping-Kontrollen hat die Datenschutzgruppe den Überarbeitungsprozess des Welt-Anti-Doping-Kodizes überwacht und mit diesem Schreiben bezüglich der dritten und letzten Phase der von der WADA organisierten öffentlichen Konsultation eine Reihe von Beobachtungen und Bedenken im Zusammenhang mit den Problemen der Rechtmäßigkeit auf der Grundlage einer Einwilligung, der Verhältnismäßigkeit der Standortdaten, Aufbewahrungsfristen und (der Bedingungen für) die automatische Veröffentlichung von Sanktionen sowie die Eignung für internationale Datenübermittlungen zur Sprache gebracht.

1.4.5 Überwachung

18.4.2013 Schreiben der Artikel-29-Datenschutzgruppe an INDECT

Die Datenschutzgruppe schrieb den Projektkoordinator von INDECT, einem von der Kommission finanzierten Forschungsprojet, als Reaktion auf eine an die Datenschutzgruppe erteilte Erklärung des

Projekts INDECT aus dem Vorjahr an. Die Datenschutzgruppe stellte klar, dass Videomaterial in vielen Fällen aufgrund seiner besonderen Beschaffenheit als personenbezogene Daten erachtet werden muss, und gab INDECT eine kurze Übersicht darüber, was als personenbezogene Daten angesehen wird.

Die Datenschutzgruppe nahm zur Kenntnis, dass INDECT die Einwilligung aller an den Forschungsarbeiten Beteiligten eingeholt hatte, verwies jedoch darauf, dass nicht nur die Forschungsarbeiten selbst sowie die Art und Weise, wie diese durchgeführt werden, sondern auch die Ergebnisse der Forschungsarbeiten mit den Grundrechten und insbesondere mit dem Recht auf Privatsphäre und Datenschutz in Einklang stehen müssen, bevor die Ergebnisse in der Praxis zum Einsatz kommen, wenn das Forschungsprojekt die Verarbeitung personenbezogener Daten umfasst und die Wahrscheinlichkeit besteht, dass die Privatsphäre europäischer Bürger beeinträchtigt wird.

Die Datenschutzgruppe schlug für die Entwicklung neuer Technologien und Lösungen proaktive Maßnahmen wie „Datensparsamkeit“, „eingebauter Datenschutz“ und „datenschutzfreundliche Grundeinstellungen“ vor und würdigte damit die Tatsache, dass viele Technologien, die darauf abzielen, potenzielle Bedrohungen zu erkennen, die Aufmerksamkeit von Sicherheits- oder Überwachungsdiensten durch „innovative Algorithmen zur Unterstützung menschlicher Entscheidungen“, die die in dem Videomaterial gezeigten Personen nicht identifizieren müssen, auf mögliche gefährliche Ereignisse richten.

Die Datenschutzgruppe wies INDECT auf Datenschutzrisiken hin, die mit der Art und Weise der durchgeführten Forschungsarbeiten einhergehen.

Kapitel Zwei
Die wichtigsten Entwicklungen in den Mitgliedstaaten

BELGIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Änderungen des Gesetzes vom 8. Dezember 1992 zum Datenschutz bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz)

1. Aussetzung (mit Auflagen) des Rechts auf Zugang während einer Prüfung oder einer Steuerprüfung durch das Finanzministerium

Artikel 3 des Datenschutzgesetzes – das für bestimmte Datenverarbeitungsaktivitäten besondere Vorkehrungen enthält – sieht seit 2012 u. a. die Aussetzung des Rechts auf Zugang zu Daten im Zusammenhang mit der vom Finanzministerium verwalteten Verarbeitung während eines Zeitraums vor, in dem die betroffene Person einer Prüfung oder Untersuchung unterzogen wird oder diesbezüglich Vorbereitungen laufen.

Da diese Maßnahme insbesondere von der Datenschutzbehörde als inakzeptabel erachtet wurde[2], wurde dieser Artikel 2013 geändert. Eine Aussetzung des Rechts auf Zugang ist unter den oben genannten Umständen zwar nach wie vor vorgesehen, *jedoch nur, sofern die Umsetzung dieses Rechts auf Zugang die Prüfung, Untersuchung oder diesbezüglichen Vorbereitungen beeinträchtigen würde* **und** *lediglich während deren Durchführung*. Die Dauer dieser Vorbereitungen, während denen das Recht auf Zugang nicht gilt, *darf ein Jahr ab Zugangsersuchen nicht überschreiten*.

Die Ausnahme wird außerdem unmittelbar nach Abschluss der Prüfung oder Untersuchung oder bei Abbruch der Vorbereitungen, weil diese nicht zu einer Prüfung oder Untersuchung führen, aufgehoben. Das Ministerium für Informationssicherheit und Datenschutz (internes Prüfungsorgan), das dem Finanzministerium unterstellt ist, hat den betroffenen Steuerzahler unmittelbar zu benachrichtigen und über die im Beschluss des für die Datenverarbeitung Verantwortlichen enthaltenen *Motivation* hinter der Aussetzung zu unterrichten.

Wenn das Recht auf Zugang während dieses Zeitraums unter den oben genannten Bedingungen ausgesetzt ist, haben betroffene Personen – wie bei polizeilichen Angelegenheiten – ein indirektes Recht auf Zugang, das sie durch die Datenschutzbehörde (gemäß Artikel 13 des Datenschutzgesetzes) ausüben.

2. Schaffung eines Organs zur Prüfung der polizeilichen Informationsverwaltung durch die Datenschutzbehörde (Gesetz vom 18. März 2014)

Das Gesetz vom 18. März 2014 sieht neben der Datenschutzbehörde die Schaffung eines Organs zur Prüfung polizeilicher Informationen vor, das für die Prüfung der durch das Gesetz zur Regelung der polizeilichen Aufgaben vorgesehene Verarbeitung von Informationen und Daten verantwortlich ist. Dieses Organ geht seiner Arbeit unabhängig von der Datenschutzbehörde nach, teilt mit ihr jedoch ein Sekretariat. Es besteht hauptsächlich aus Mitgliedern der Bundes- und Regionalpolizei sowie aus Sachverständigen. Unter den Mitgliedern muss sich jedoch auch ein Prüfer der Aufsichtsbehörde (Datenschutzbehörde) befinden.

Die Aufsichtsbehörde ist insbesondere für die Überprüfung der Einhaltung der Regelungen für den direkten Zugang zur nationalen Polizeidatenbank (BNG) sowie für Direktabfragen derselben verantwortlich. Des Weiteren ist sie für die Überprüfung aller Mitarbeiter der Polizei zuständig, die für die Pflege dieser Datenbank verantwortlich sind. Sie sorgt durch betriebliche Untersuchungen dafür, dass der Inhalt der BNG sowie die Verarbeitung der darin gespeicherten Daten und Informationen den Bestimmungen des Gesetzes zur Regelung der polizeilichen Aufgaben entspricht, insbesondere die

[2] Datenschutzbehörde, Stellungnahme 32/2012 vom 17. Oktober 2012 (http://www.privacycommission.be). Das belgische Verfassungsgericht löschte diese Bestimmung per Anordnung vom 25. März 2014 infolge eines Antrags auf Annullierung der ursprünglichen Änderung (vor der Überarbeitung 2013).

Regulierung der Verarbeitungsaktivitäten wie z. B. Dateneingabe und Speicherung von Informationen gemäß ihrer Art und Zuverlässigkeit und sogar die Löschung und Archivierung von Daten und Informationen am Ende der Aufbewahrungsfristen. Besondere Datenbanken (z. B. solche mit begrenzter Laufzeit) werden ebenfalls überprüft. Das Organ hat Untersuchungsbefugnisse und erstattet dem Repräsentantenhaus auf Anfrage bzw. jährlich Bericht.

Bezüglich der Änderung der Artikel 3 und 9 (Auskunftsrecht) des Datenschutzgesetzes Institut professionnel des agents immobiliers gegen Englebert u. a. vor dem Verfassungsgericht Belgien und dem Europäischen Gerichtshof (EuGH)

Die Rechtssache befasste sich mit der Frage, ob diese Bestimmung korrekt in belgisches Recht umgesetzt wurde, da sie keine Ausnahmen für Privatdetektive ähnlich denen in Art. 13 Abs. 1 lit. d und g der Richtlinie 95/46 enthält. Da keinerlei Ausnahmen für Privatdetektive enthalten sind, bestehe sogar eine Informationspflicht. Daraufhin wurde die Frage aufgeworfen, ob nicht einerseits eine ungerechte Behandlung in Bezug auf Privatdetektive vorliege oder es andererseits nun nicht mehr möglich sei, unter diesen Bedingungen als Privatdetektiv zu arbeiten. In Belgien wird der Beruf des Privatdetektivs durch das Gesetz vom 19. Juli 1991 geregelt.

In Anbetracht dieser Fragen wandte sich das Handelsgericht 2012 an das belgische Verfassungsgericht. Letzteres wandte sich daraufhin an den EuGH.

Der EuGH kam am 7. November 2013 zu einem Urteil (C-473/12): http://curia.europa.eu/juris/document/document.jsf?text=&docid=144217&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=182002; das belgische Verfassungsgericht fällte seinen Beschluss am 3. April 2014: http://www.const-court.be/public/f/2014/2014-059f.pdf

Der belgische Verfassungsgerichtshof kam zu dem Schluss, dass die betreffende Bestimmung des belgischen Datenschutzgesetzes vom 8. Dezember 1992 gegen die Artikel 10 (Grundsatz der Gleichheit) und 11 (Grundsatz der Nichtdiskriminierung) der belgischen Verfassung insofern verstößt, als die Verpflichtung zur Information ohne Weiteres auf die Tätigkeit eines Privatdetektivs Anwendung findet, der dazu ermächtigt ist, seine Tätigkeiten für juristische Personen des öffentlichen Rechts gemäß Artikel 13 des Gesetzes vom 19. Juli 1991 „zur Regelung des Berufs des Privatdetektivs“ auszuüben, und der für eine Berufsorganisation des öffentlichen Rechts (Institut professionnel des agents immobiliers) handelt, die gesetzlich beauftragt ist, Verstöße gegen die berufsständischen Regeln eines reglementierten Berufs (Immobilienmakler) zu untersuchen.

Änderung des Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation – eine neue Kompetenz für die Datenschutzbehörde zum Thema *Verstöße gegen den Schutz personenbezogener Daten*

Seit April 2014 müssen sich Anbieter öffentlicher elektronischer Kommunikationsdienste bei Meldungen von Verstößen gegen den Schutz personenbezogener Daten nicht mehr an das Belgische Institut für Telekommunikation wenden, sondern an die Datenschutzbehörde. Diese erstattet wiederum beim Institut Meldung. Die Datenschutzbehörde muss außerdem dafür sorgen, dass diese Unternehmen gegebenenfalls die betroffenen Personen über die Verstöße informieren. Anschließend wird eine Partnerschaft zwischen dem Belgischen Institut für Telekommunikation und der Datenschutzbehörde gebildet.

Änderung der institutionellen Datenschutzlandschaft

Neben der *Vlaamse toezichtcommissie* (Kontrollkommission für den Datenaustausch zwischen flämischen öffentlichen Dienstleistungen im Zusammenhang mit elektronischer Verwaltung) wurde eine Kontrollkommission für den Datenaustausch der Regionen Wallonien und Brüssel eingerichtet.

Aktivitäten der Datenschutzbehörde

Der Jahresbericht der Datenschutzbehörde enthält genaue Informationen über ihre Aktivitäten. Einige davon verdienen besondere Aufmerksamkeit (siehe http://www.privacycommission.be):

- **Sensibilisierung Minderjähriger:** Die belgische Datenschutzbehörde organisierte für Grundschulkinder die Aufführung eines unterhaltsamen, belehrenden Theaterstücks (nur in niederländischer Sprache) zum Thema Datenschutz (Online-Aktivitäten und Privatsphäre). Sie erstellte ein komplettes pädagogisches Kit namens „Je suis jeune et je protège ma vie privée" (Datenschutz für junge Menschen). Ein Teil davon wird von dem Theaterstück bekräftigt. Genaueres erfahren Sie auf den zugehörigen Websites unter http://www.jeddecide.be und http://www.ikbeslis.be

- ***Verstöße gegen den Schutz personenbezogener Daten:*** Infolge mehrerer schwerwiegender Datenlecks (einschließlich der Duplikation einer Kundendatenbank der belgischen Bahn, welche die Daten von 1,4 Mio. Menschen betraf) gab die belgische Datenschutzbehörde mehrere Empfehlungen zur Vermeidung solcher Lecks heraus, die in der Regel auf unzureichende Datensicherheitsmaßnahmen zurückzuführen sind.

- **Arbeit am Entwurf der EU-Verordnung (*EU-Datenschutzreform*)**: Die Datenschutzbehörde gab zwei wichtige Stellungnahmen im Zusammenhang mit der Datenschutzreform der Europäischen Union heraus. Stellungnahme 35/2012 bezieht sich auf die vorgeschlagene Verordnung, die ursprünglich von der Europäischen Kommission vorgelegt wurde. Stellungnahme 10/2014 bezieht sich auf den Text, über den der LIBE-Ausschuss im Oktober 2013 abgestimmt hat.

Organisation	Datenschutzbehörde
Vorsitz und/oder Gremium	1. Januar 2013 bis einschließlich 2. Mai 2013 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 2012. 2. Mai 2013 bis 31. Dezember 2013 Vorsitzender: W. Debeuckelaere (Vorsitzender) Stellvertretender Vorsitzender: S. Verschuere Gremiumsmitglieder: A. Junion (Anwältin), F. Robben (Geschäftsführer der Banque Carrefour de la Sécurité Sociale sowie der E-Health-Plattform), J. Baret (Generalsekretärin der FÖD Justiz), E. Gheur (Geschäftsführer von Galaxia und Dozent an der Universität Luxemburg), G. Vermeulen (Professor für Rechtswissenschaften an der Universität Gent), S. Waterbley (Ratsmitglied der GD Telekommunikation und Informationsgesellschaft der FÖD Wirtschaft) Stellvertretende Mitglieder: M. Salmon (Beraterin des

	Berufungsgerichts Brüssel), S. Mertens de Wilmars (Dozent), F. Schuermans (Generalanwalt des Berufungsgerichts Gent), Y. Roger (Vorsitzender des sektoriellen Ausschusses für soziale Sicherheit und Gesundheitswesens) 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	6 840 000 EUR
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): 69 - Stellungnahmen und Initiativempfehlungen: 5 - Empfehlungen zur Weiterverarbeitung: 11
Meldungen	6 047 Meldungen von Datenspeichersystemen und insgesamt 5 252 Meldungen neuer Datenverarbeitungsaktivitäten. 436 Meldungen von Änderungen/Berichtigungen existierender Datenverarbeitungsaktivitäten und 359 Meldungen abgeschlossener Datenverarbeitungsaktivitäten
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 erhalten:

	- Sektorausschuss der Bundesbehörde: 44 Einzelgenehmigungen - Sektorausschuss für Statistik: 28 Einzelgenehmigungen - Sektorausschuss für das Nationalregister: 87 Einzelgenehmigungen - Sektorausschuss für soziale Sicherheit und Gesundheitswesen: Siehe Website der Banque Carrefour de la Sécurité Sociale https://www.ksz-bcss.fgov.be/fr/bcss/nodepage/content/websites/belgium/security/committee_03.html
Anträge betroffener Personen	Die Statistiken der belgischen Datenschutzbehörde unterscheiden nicht zwischen Auskunftsersuchen von betroffenen Personen oder von für die Datenverarbeitung Verantwortlichen: Die Datenschutzbehörde bearbeitete 3 532 Auskunfts- oder Vermittlungsanfragen (einschließlich Überprüfungen). Darunter: 2 871 Auskunftsersuche sowohl von öffentlichen Stellen und derzeitigen oder zukünftigen für die Verarbeitung verantwortlichen Personen sowie betroffenen Personen, 450 Vermittlungsanfragen und 211 Überprüfungen. Die Zentrale bearbeitete 2 868 Anträge zu den folgenden Themen: Einsatz von Überwachungskameras (14,85 %), Grundsätzliches zum Thema Datenschutz (8,12 %), Beschäftigung (5,47 %), Wirtschaft (3,35 %) (Fragen zu Verbraucherkrediten) sowie staatliche Behörden (2,24 %).
Beschwerden betroffener Personen	Bei der Datenschutzbehörde gingen 450 Beschwerden ein. Dies entspricht einem Zuwachs von 48,5 % im Vergleich zu 2012 (303). Diese Beschwerden betrafen hauptsächlich die folgenden Bereiche: - Grundsätzliches zum Thema Datenschutz (27,6 %), Grundsatz der Verhältnismäßigkeit, Missachtung des Grundsatzes der Zweckbindung, Informationspflicht - Registrierung von säumigen Kunden bei der Zentrale für Privatkredite (Centrale des crédits aux particuliers) der Belgischen Nationalbank (13,6 %) - Videoüberwachung (12,4 %) - Direktmarketing (5,1 %) - Internet (4 %)
Vom Parlament bzw. der Regierung angeforderte Beratung	Eine Auflistung der 2013 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	211 Prüfungen.

	Die Datenschutzbehörde führte im Jahr 2013 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 Informationen.

BULGARIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
Vorsitz und/oder Gremium	Gemäß Art. 7 Absatz 1 des Gesetzes zum Schutz personenbezogener Daten ist die Kommission für den Schutz personenbezogener Daten (CPDP) eine kollektive Behörde bestehend aus einem Vorsitzenden und vier Mitgliedern. 2013 war die CPDP wie folgt strukturiert: Veneta Shopova (Vorsitzende) und Krassimir Dimitrov, Valentin Enev, Mariya Mateva und Veselin Tselkov (vier Mitglieder).
Budget	2 700 000 BGN, davon wurden 2 693 530 BGN ausgegeben.
Personal	Anzahl der Beamten: 67
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2013 wurden insgesamt 357 Beschlüsse, Stellungnahmen und Anweisungen herausgegeben, davon: 252 Beschwerden 79 Stellungnahmen zur Anwendung des Datenschutzgesetzes 26 verbindliche Anweisungen
Meldungen	42 308 für die Datenverarbeitung Verantwortliche
Vorabprüfungen	2 613 Vorabprüfungen
Anträge betroffener Personen	123 Anträge von natürlichen und juristischen Personen sowie verschiedene Anfragen zu aktuellen Themen im Zusammenhang mit den Zuständigkeiten der CPDP.
Beschwerden betroffener Personen	450 Beschwerden – die meisten davon in den folgenden Bereichen: Telekommunikation: 333 Beschäftigung und Versicherungsdienstleistungen: 42 Bankwesen: 33 Gesundheit und Bildung: 13 Sonstige: 29
Vom Parlament bzw. der Regierung angeforderte Beratung	Im Berichtszeitraum gingen vom Ministerrat zwei Anträge auf Stellungnahmen ein: - Antrag auf Stellungnahme zu zwei Anträgen auf Zugang zu

	öffentlichen Informationen: Ein Medienunternehmen forderte eine Liste von Beamten und Verwaltungsangestellten des Ministerrats mit Namen, Berufsbezeichnungen und den vertraglich vereinbarten Gehältern an. - Antrag auf Stellungnahme zu einer Frage, die zwei Abgeordnete dem Premierminister der Republik Bulgarien gemäß Artikel 90 Absatz 1 der Verfassung der Republik Bulgarien und Artikel 89 der Vorschriften für die Organisation und Verfahren der Nationalversammlung über den Vorsitzenden der Nationalversammlung gestellt haben. Sie forderten Informationen zu einer Reihe von nach wie vor beschäftigten sowie ehemaligen Beamten der staatlichen Verwaltung für einen Zeitraum von sechs Monaten an, die von der Stelle wie folgt definiert wurden: Ministerien, staatliche Behörden, Exekutivagenturen, lokale Behörden sowie auf juristische Personen spezialisierte Behörden.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Es gingen 13 Meldungen und 12 Genehmigungsanträge für die Datenübermittlung an Drittländer ein. Erstmals wurde auch ein Antrag in Bezug auf verbindliche unternehmensinterne Vorschriften (BCR) eingereicht. Da dieses Instrument in der bulgarischen Gesetzgebung nicht vorgesehen war, genehmigte die Datenschutzbehörde in diesem Fall die Übermittlung unter Berufung auf Artikel 36b des Datenschutzgesetzes. Diese Genehmigung erfolgte auf der Grundlage von Informationen zu den vertraglichen Verpflichtungen zwischen dem für die Datenverarbeitung Verantwortlichen und dem Empfänger, die ausreichende Garantien für den Schutz der Daten boten. Bezüglich des bestehenden Verfahrens für verbindliche unternehmensinterne Vorschriften der Artikel-29-Datenschutzgruppe hat die CPDP leitende Datenschutzbehörden für 15 BCR genehmigt und deren Beschlüssen zu fünf BCR zugestimmt.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2013 wurden insgesamt 2 696 Prüfungen durchgeführt: 2 613 *ex-ante*; 39 laufend; *ex-post*: 44, größtenteils in den folgenden Bereichen: Gesundheitswesen: 1 510; Handel und Dienstleistungen: 310; Aus- und Weiterbildung: 225; Rechts- und sonstige Beratungsdienstleistungen: 136; Bauwesen und Architektur: 62; Tourismus: 51.
Sanktionsmaßnahmen	

Sanktionen	2013 erstellte die Datenschutzbehörde im Rahmen von verwaltungs- und strafrechtlichen Maßnahmen Folgendes: - 30 Feststellungen von Verwaltungsdelikten - 29 Bußgeldbescheide
Geldbußen	Die Datenschutzbehörde erließ 2013 Bußgeldbescheide und materielle Sanktionen im Wert von 76 800 BGN.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A. – das bulgarische Datenschutzgesetz sieht keine Ernennung von Datenschutzbeauftragten vor.

B. Rechtsprechung

1. Bezüglich der erlassenen verbindlichen Anweisungen und Bußgeldbescheide

2013 wurden 26 verbindliche Anweisungen erteilt, die meisten davon im staatlichen Verwaltungssektor, gefolgt von lokalen und kommunalen Behörden und den Sektoren Finanzen, Versicherung und Gesundheitswesen. Die wenigsten Anweisungen wurden in den folgenden Sektoren erteilt: Justiz, Aus- und Weiterbildung, Informationstechnologie, Handel und Dienstleistungen.

Die Anweisungen wurden im Zusammenhang mit den folgenden Themen erlassen:

- Mangel an nötigen organisatorischen und technischen Maßnahmen, um den Schutz personenbezogener Daten zu gewährleisten: 44 % der Beschlüsse;
- mangelndes Ergreifen erforderlicher Maßnahmen zur Aktualisierung der an das Register der für die Datenverarbeitung Verantwortlichen übermittelten Informationen: 18 %;
- unrechtmäßige Verarbeitung personenbezogener Daten: 25 %;
- Verarbeitung personenbezogener Daten ohne Einwilligung in Kenntnis der Sachlage durch betroffene Personen: 13 %;

Die CPDP hat 2013 29 Bußgeldbescheide erlassen. Keiner davon wurden aufgehoben; einer wurde mit einer Reduzierung der Geldbuße bestätigt. Von den 2011 und 2012 erlassenen Bescheiden, gegen die 2013 Berufung eingelegt und dies gerichtlich verhandelt wurde, wurden drei vollständig aufgeboben. Zwölf wurden bestätigt, und bei sechs wurde die Höhe der Geldbuße reduziert. Derzeit sind 25 Bußgeldbescheide noch anhängig. 2013 traten fünf Bußgeldbescheide ohne Berufung in Kraft.

Zu den häufigsten Verstößen gegen das Datenschutzgesetz gehörten:

- Verstöße gegen die Grundsätze der Rechtmäßigkeit, der Verhältnismäßigkeit und der Zweckbindung der Verarbeitung personenbezogener Daten: 15 Verstöße;
- Verarbeitung ohne gesetzliche Vorgaben für die Zulässigkeit der Verarbeitung: 20 Verstöße, für die materielle Sanktionen verhängt wurden;
- Versäumnis, technische und organisatorische Maßnahmen zum Schutz der Daten gegen versehentliche oder unrechtmäßige Zerstörung oder versehentlichen Verlust und unberechtigtes

Zugreifen, Berichtigen oder Verbreiten sowie gegen sonstige rechtswidrige Formen der Verarbeitung zu ergreifen: 19 Verstöße, für die materielle Sanktionen verhängt wurden;

- Verarbeitung der Daten, bevor der für die Datenverarbeitung Verantwortliche sich bei der zuständigen Behörde und bei der CPDP registriert hatte: 3 Verstöße, für die materielle Sanktionen und Geldbußen verhängt wurden;
- Verarbeitung zu Zwecken der kommerziellen Direktwerbung, ohne den betroffenen Personen das Recht auf Widerspruch einzuräumen: 5 Verstöße, für die materielle Sanktionen verhängt wurden;
- Weigerung, die Kommission bei der Ausübung ihrer Aufsichtsbefugnisse zu unterstützen: 4 Verstöße, für die materielle Sanktionen verhängt wurden;
- Versäumtes Entscheiden über Anträge auf Zugang zu personenbezogenen Daten: 2 Verstöße;
- Versäumte Meldung an das CCTV-Register: 4 Verstöße.

2. Bezüglich der Abgabe von Stellungnahmen zu Anträgen und Signalen

Neben den oben in der Tabelle aufgeführten Anträgen staatlicher Behörden, die bei der Datenschutzbehörde eingingen, waren die folgenden Stellungnahmen von Interesse:

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

2013 gingen verschiedene Anträge auf Stellungnahme zum Zugang zur Nationalen Bevölkerungsdatenbank (NBD) ein, die von der Generaldirektion „Zivile Registrierungs- und Verwaltungsdienstleistungen“ (CRAS) des Ministeriums für regionale Entwicklung und öffentliche Bauvorhaben (MRDPW) gepflegt wird, sowie zum Zugang zu den Personenstandsregistern.

Die für die Verarbeitung personenbezogener Daten Verantwortlichen beantragten weiterhin direkten Zugang zur NBD, was von rechtlichen Interessen oder von ihren Aktivitäten und der Ausübung gesetzlicher Verpflichtungen herrührte (wie z. B. Kreditinstitutionen, die im Zusammenhang mit den Identifikationsanforderungen der Kunden Zugang beantragten, da es sich dabei um eine Bestimmung des Gesetzes zur Bekämpfung von Geldwäsche handelt).

Im Zusammenhang mit den Anträgen auf direkten Zugang zur NBD geht die CPDP 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 Datenschutzbehörde ließ in einer Stellungnahme verlauten, dass der GD CRAS des MRDPW bei der Bereitstellung bestimmter personenbezogener Daten (ohne Direktzugang) an die Parteien, die sie beantragt haben, rechtlich nichts im Wege steht, wenn diese ihr rechtliches Interesse gemäß den etablierten Verfahren unter Beweis stellen.

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 2013 dennoch auf Anträge auf Stellungnahme der staatlichen und kommunalen Behörden im Zusammenhang mit Anträgen auf Zugang zu öffentlichen Informationen.

2.2.1. Anträge an die einschlägigen staatlichen Behörden (Ministerrat) auf Bereitstellung von Daten wie:

- Namen, Berufsbezeichnungen und Gehälter von Angestellten und Beamten sowie Kopien deren Arbeitsverträge. In diesem Fall war die CPDP der Meinung, dass bei einem derartigen Volumen die erforderlichen Informationen in die Kategorie „personenbezogene Daten" fallen, da Personen anhand dieser Daten identifiziert werden können, und eine Verarbeitung dieser Daten nur nach Einwilligung der betroffenen Personen erfolgen kann.

- Anzahl der beschäftigten und ehemaligen Beamten der staatlichen Verwaltung für einen Zeitraum von sechs Monaten, je nach Status der Behörde, wie z. B. Ministerien, staatliche Behörden, Exekutivagenturen, lokale Behörden sowie spezialisierte Behörden. Der Ministerrat wurde dazu aufgefordert, eine Liste mit Namen und Angaben zum Beschäftigungsgrund bereitzustellen. Außerdem wurde darauf hingewiesen, dass durch die Bereitstellung dieser Informationen bestimmte administrative Strukturen identifiziert werden. In diesem Fall könnten die Informationen (ohne die Namen der Einzelpersonen) bereitgestellt werden, um die rechtliche Verpflichtung des für die Datenverarbeitung Verantwortlichen einzuhalten.

2.2.2. Sonstige Anträge auf Zugang zu Informationen

Der stellvertretende Leiter der Exekutivagentur für Forstwirtschaft beantragte beim Ministerium für Land- und Forstwirtschaft die Bereitstellung von personenbezogenen Daten bezüglich der Nutzungsänderung und des Verkaufs von Grundstücken in Waldgebieten. Bevor die angeforderten Informationen bereitgestellt werden, sollten die gesetzlichen Anforderungen sowie das öffentliche Interesse sowohl in Bezug auf die von Parlamentsabgeordneten gestellten Fragen als auch in Bezug auf das Recht auf Privatsphäre und das Vorhandensein der Einwilligung durch die betroffenen Personen berücksichtigt werden. Die Datenschutzbehörde hat dazu wie folgt Stellung genommen: Der für die Datenverarbeitung Verantwortliche kann die Dateien mit Informationen zu Veräußerungen und Nutzungsänderungen von Grundstücken herausgeben, nachdem die darin enthaltenen personenbezogenen Daten in ein Format gebracht wurden, die eine Identifikation von Individuen unmöglich macht, wie z. B. durch Löschung oder Anonymisierung anhand von Initialen.

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

Eine weitere wichtige Frage im Zusammenhang mit dem Zugang zu Informationen, die personenbezogene Daten enthalten, wurde 2013 von der CPDP bearbeitet. Es handelte sich dabei um die Bekanntmachung der Erklärungen gemäß dem Gesetz zur Vermeidung und Offenlegung von Interessenkonflikten (LPDCI) auf den offiziellen Websites staatlicher Institutionen. Im Bemühen um Ausgewogenheit zwischen dem öffentlichen Interesse und dem Schutz personenbezogener Daten bestimmter Personen akzeptierte die CPDP, dass die Veröffentlichung von Erklärungen erst nach der ausdrücklichen schriftlichen Einwilligung der betroffenen Personen an separater Stelle der Erklärung erfolgen sollte. Die Bekanntmachung der LPDCI-Erklärungen im Internet ohne die ausdrückliche Einwilligung der betroffenen Personen wäre ein Verstoß gegen das Datenschutzgesetz. Demnach müssen alle Erklärungen, die ohne Einwilligung auf offiziellen Websites veröffentlicht wurden, solange entfernt werden, bis ausdrücklich eine Einwilligung erteilt wurde. Die Bekanntmachung darf nicht die Unterschrift des Erklärenden enthalten. In Fällen, in denen die Erklärung die personenbezogenen Daten anderer Personen enthält, müssen diese Daten anonymisiert werden, da die Einwilligung durch die betroffene Person nicht für die personenbezogenen Daten anderer gilt.

2.4. Bezüglich des Zugangs zu sensiblen, in speziellen Registern enthaltenen Daten

Weitere Stellungnahmen, die die CPDP 2013 abgegeben hat, bezogen sich auf Angelegenheiten im Zusammenhang mit dem Zugang zu sogenannten „sensiblen Daten", deren Verarbeitung gemäß Artikel 5 Absatz 1 des Datenschutzgesetzes in der Regel verboten ist.

Ein Beispiel wäre der Fall einer staatlichen psychiatrischen Klinik in einer bulgarischen Stadt, an die die Regionaldirektion des Innenministeriums mit der Bitte herangetreten war, eine „aktualisierte Liste der derzeit hospitalisierten Patienten mit psychischen Erkrankungen" bereitzustellen. In diesem Fall gab die Datenschutzbehörde eine Stellungnahme ab, die besagte, dass die Pflicht zur Pflege einer Liste psychisch Kranker durch die Polizei gemäß Artikel 20 Absatz 1 und 7 der Anweisung 13-2295 des Innenministeriums aus dem Jahr 2012 gegen die Bestimmungen für die Bereitstellung von Gesundheitsdaten gemäß Artikel 28 Absatz 1 des Gesundheitsgesetzes verstößt, das die Rechte der Patienten – in diesem Fall die Rechte der psychisch Kranken in der betroffenen staatlichen psychiatrischen Klinik – schützt.

Des Weiteren enthält die Verfassung der Republik Bulgarien mehrere Grundsätze in Bezug auf psychisch Kranke: Demnach bedürfen Personen mit physischen oder psychischen Störungen eines besonderen Schutzes durch den Staat und die Gesellschaft (Artikel 51 Absatz 3). Außerdem muss der Staat die Gesundheit seiner Bürger schützen (Artikel 52 Absatz 3). Darüber hinaus steht die Anweisung im Gegensatz zu den Bestimmungen von Artikel 157 Absatz 1 des Innenministeriumgesetzes, das die Erfassung von Bürgerdaten, die sich ausschließlich auf ihren Gesundheitszustand beziehen, ausdrücklich verbietet (Artikel 157 Absatz 1 des Innenministeriumgesetzes). Angesichts dieser Erwägungen ließ die Datenschutzbehörde in einer Stellungnahme verlauten, dass die beantragten Informationen (aktualisierte Liste der hospitalisierten Patienten mit psychischen Erkrankungen) nicht bereitgestellt werden dürfen. Solch eine Bereitstellung würde gegen Artikel 4 Absatz 1 und Artikel 5 Absatz 2 des Datenschutzgesetzes, gegen Artikel 28 des Gesundheitsgesetzes sowie gegen Artikel 157 Absatz 1 des Innenministeriumgesetzes verstoßen.

In diesem Fall würde eine Bereitstellung solcher Informationen zu Personen, die in dieser Klinik behandelt werden, gegen die Grundsätze der Zweckbindung und der Verhältnismäßigkeit gemäß Artikel 2 Absatz 2 des Datenschutzgesetzes verstoßen.

2.5. Stellungnahme zur Parlamentswahl

Die CPDP gab 2013 eine Stellungnahme zu einem Antrag des Vorsitzenden und des Sekretärs der zentralen Wahlkommission zur Parlamentswahl ab.

Zunächst wurde die Frage aufgeworfen, ob es nötig sei, sich bezüglich der Initiativkomitees für die Nominierung unabhängiger Kandidaten für die Nationalversammlung bei der Datenschutzbehörde zu registrieren. Laut der CPDP handelt es sich bei den Initiativkomitees für die Nominierung unabhängiger Kandidaten gemäß Artikel 96 Absatz 2 der Wahlordnung um für die Datenverarbeitung Verantwortliche, die demnach dazu verpflichtet sind, sich bei der Datenschutzbehörde zu registrieren.

Die zweite Angelegenheit betraf die Parlamentswahl sowie die Änderungen und Zusätze in der Wahlordnung vom Februar 2013, laut derer die zentrale Wahlkommission (ZWK) neue Verpflichtungen hat. Im Zusammenhang mit einer dieser Verpflichtungen (die Live-Übertragung der ZWK-Tagungen im Internet) gab die Datenschutzbehörde eine Stellungnahme ab, die besagt, dass dies in Anbetracht der gesetzlichen Verpflichtung, die sich aus den neuen Bestimmungen der Wahlordnung ergibt, sowie der Durchführung von Aufgaben im öffentlichen Interesse, d. h. zur Gewährleistung der Möglichkeit, die Öffentlichkeit über wichtige Themen zu informieren, die während der ZWK-Tagungen besprochen werden, rechtmäßig und zulässig sei.

2.6. Die Stellungnahme der CPDP zur Umsetzung des Foreign Account Tax Compliance Act für US-Steuerzahler in Bulgarien

Eine Frage von erheblichem finanziellen Interesse, zu der die CPDP eine Stellungnahme abgegeben hat, ist die Umsetzung des vom US-Kongress beschlossenen Foreign Account Tax Compliance Act (FATCA) für US-Steuerzahler in Bulgarien.

Der Antrag wurde von den Vertretern einer Bank mit Sitz in Bulgarien gestellt, die Teil eines multinationalen Unternehmens war. Der Hauptzweck von FATCA liegt in der Bekämpfung grenzüberschreitenden Steuerbetruges von US-Bürgern mit Konten und Finanzanlagen im Ausland durch die US-Steuerbehörden. Dieses Ziel wird durch den Aufbau eines globalen Systems für den automatischen Informationsaustausch erreicht, das alle ausländischen Finanzinstitutionen dazu verpflichtet, Informationen zu allen Konten von US-Steuerzahlern oder ausländischen Unternehmen, die sich im Besitz von US-Steuerzahlern besitzen, an das US-Finanzministerium zu übermitteln. FATCA schafft demnach zahlreiche neue Verpflichtungen für alle ausländischen Finanzinstitutionen. Nach einer gründlichen Analyse geht die CPDP davon aus, dass aufgrund der Tatsache, dass für die bulgarische Bank derzeit keine gesetzliche Verpflichtung besteht, die personenbezogenen Daten ihrer Kunden, die dem US-Steuerrecht unterliegen, bezüglich der Umsetzung von FATCA an einen anderen für die Datenverarbeitung Verantwortlichen in den Vereinigten Staaten zu übermitteln, und es demnach für die CPDP keine Rechtsgrundlage gibt, um eine Übermittlung der Daten in die USA zu genehmigen. Eine Datenübermittlung, die ausschließlich auf der Einwilligung der betroffenen Personen beruht, wäre exzessiv und würde aufgrund der fehlenden Einwilligungsregelung gegen den Grundsatz der Rechtmäßigkeit der Verarbeitung personenbezogener Daten verstoßen.

C. Sonstige wichtige Informationen

Im Berichtszeitraum verabschiedete die CPDP 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 CPDP eine neue Verordnung über ein Minimum an technischen und organisatorischen Maßnahmen 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. 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 von Datenschutzverstößen ein angemessener Schutz personenbezogener Daten gewährleistet werden. Als wichtigste Zwecke des Schutzes personenbezogener Daten wurden Vertraulichkeit, Integrität und Verfügbarkeit definiert. Es werden fünf verschiedene Ebenen des Schutzes personenbezogener Daten eingeführt: physischer Schutz, persönlicher Schutz, dokumentarischer Schutz, der Schutz vor automatisierten Informationssystemen bzw. Netzwerken sowie kryptografischer Schutz. Des Weiteren führte die Verordnung den Grundsatz „Kenntnis erforderlich“ ein.

Um das angemessene Niveau der technischen und organisatorischen Maßnahmen und die zulässige Art des Datenschutzes zu bestimmen, sind die für die Datenverarbeitung Verantwortlichen dazu verpflichtet, regelmäßig eine Folgenabschätzung der Datenverarbeitung durchzuführen.

Mit der Folgenabschätzung sollen die Auswirkungsebenen und die entsprechenden Datenschutzniveaus definiert werden. Für jedes Schutzniveau werden die nötigen technischen und organisatorischen Maßnahmen bestimmt, die von den für die Datenverarbeitung Verantwortlichen ergriffen werden müssen.

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

Seit Inkrafttreten der Verordnung bietet die CPDP Schulungen und Beratungsdienste an, die sich an für die Datenverarbeitung Verantwortliche richten, um sie für die neuen Datenschutzregelungen zu sensibilisieren.

Die Verordnung (https://www.cpdp.bg/en/index.php?p=element&aid=632) ist auf der Website der Datenschutzbehörde in englischer Sprache verfügbar.

Die CPDP legt entsprechend dem dafür vorgesehenen jährlichen Schulungsplan den Schwerpunkt auf Schulungen, die sich an für die Verarbeitung Verantwortliche richten. Die Sachverständigen der Datenschutzbehörde beteiligten sich bei den Kursen des Instituts für öffentliche Verwaltung, welches das einzige nationale Ausbildungszentrum für Beamte ist, als Dozenten für Fragen des Schutzes personenbezogener Daten.

DÄNEMARK

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
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	Rund 22,5 Millionen DKK
Personal	Rund 35
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A. (in den folgenden Zahlen enthalten)
Meldungen	2 777
Vorabprüfungen	2 777
Anträge betroffener Personen	2 221 Diese Zahl umfasst alle bei der dänischen Datenschutzbehörde eingegangenen Anfragen und Beschwerden
Beschwerden betroffener Personen	Siehe oben
Vom Parlament bzw. der Regierung angeforderte Beratung	468
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	14 Fälle im Zusammenhang mit Sicherheitsfragen
Prüfmaßnahmen	
Prüfungen, Untersuchungen	45
Sanktionsmaßnahmen	
Sanktionen	Die dänische Datenschutzbehörde kritisiert jedes Jahr eine Reihe von für die Datenverarbeitung Verantwortlichen für die Nichteinhaltung des Gesetzes über die Verarbeitung personenbezogener Daten.
Geldbußen	k. A.

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

B. Rechtsprechung

Öffentliche Institutionen mit Social-Media-Präsenzen

Im Oktober 2013 erhielt die dänische Datenschutzbehörde (DSB) eine Anfrage von einer öffentlichen Institution bezüglich ihrer Social-Media-Präsenz – vor allem auf Twitter und Facebook. Die Institution plante ein Pilotprojekt zur Erhöhung der öffentlichen Präsenz auf Social-Media-Websites.

Für diese Situation hat die dänische DSB zwei Hauptpunkte anzumerken. Zunächst sollten die Beiträge der Behörde auf Social-Media-Websites keine personenbezogenen Daten enthalten. Als Hauptregel gilt, dass Einzelpersonen die für die Datenverarbeitung Verantwortlichen ihrer eigenen Social-Media-Beiträge sind.

Zweitens können solche Behörden, falls es Bürgern möglich ist, die Behörden durch interne Mailing-Systeme auf Social-Media-Websites zu kontaktieren, zu für die Datenverarbeitung Verantwortlichen werden, ebenso wie es möglich ist, die Social-Media-Websites als Datenverarbeiter zu erachten. Demnach müssen die Behörden die Verwaltung des internen Mailing-Systems berücksichtigen.

Wenn die Behörden als für die Datenverarbeitung Verantwortliche und die Social-Media-Websites als Datenverarbeiter erachtet werden, so tragen diese Behörden die Verantwortung für den Datenschutz und müssen möglicherweise mit den Social-Media-Websites eine Datenverarbeitungsvereinbarung abschließen. Des Weiteren müssen die Behörden die Bestimmungen bezüglich der Übermittlung von Daten an Drittländer berücksichtigen.

Personenbezogene Daten bei sich aufspaltenden Unternehmen

Im März 2013 erhielt die dänische DSB die Anfrage einer Anwaltskanzlei bezüglich der Aufspaltung eines Unternehmens in mehrere unabhängige Unternehmen im Rahmen einer Umstrukturierung. Die Frage lautete, ob das Unternehmen als Nachfolger angesehen werde oder ob es sich um eine Übermittlung personenbezogener Kundendaten an ein anderes Unternehmen handele.

Die dänische DSB kam zu dem Schluss, dass es sich dabei im Allgemeinen um eine Übermittlung von Daten handelt, da die Daten von einem Unternehmen an ein anderes weitergegeben werden. In manchen Fällen ist es jedoch möglich, dies als Nachfolge des Unternehmens zu betrachten.

In solchen Situationen muss Folgendes beachtet werden: Die Beziehungen zum Kunden (Rechte und Pflichten) werden übertragen, die übertragenen Vermögenswerte bleiben weiterhin bestehen, die erfolgreiche Teilung des Unternehmens ist genau definiert, das Unternehmen kann unabhängig agieren, und der einzige Zweck der Übermittlung ist die Umstrukturierung.

Falls diese Situation zutrifft, kann dies als Nachfolge in Bezug auf die personenbezogenen Daten angesehen werden. Diese vorläufige Einschätzung liegt beim für die Datenverarbeitung Verantwortlichen.

C. Sonstige wichtige Informationen

Videoüberwachung in Taxis

Seit 2010 sind dänische Taxiunternehmen gesetzlich dazu verpflichtet, Taxis mit Videoüberwachungskameras auszustatten. Demzufolge führte die dänische DSB bei Taxiunternehmen eine Reihe von Prüfungen durch, um zu bestätigen, ob die Videoüberwachung mit den Datenschutzbestimmungen in Einklang stehen, sowie um Informationen über die Handhabung der Videoüberwachung durch die für die Datenverarbeitung Verantwortlichen zu erfassen.

Die DSB kam zu dem Schluss, dass die Taxiunternehmen die Datenschutzbestimmungen ausreichend verstanden hatten, da bei den Prüfungen keine schwerwiegenden Verstöße ermittelt wurden.

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.

DEUTSCHLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Bundesbeauftragter für Datenschutz und Informationsfreiheit

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 (bis 17. Dezember 2013) und Andrea Voßhoff[3]
Budget	9 090 000 EUR
Personal	85
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	-
Meldungen	-
Vorabprüfungen	-
Anträge betroffener Personen	12 074
Beschwerden betroffener Personen	Keine Unterscheidung zwischen Beschwerden und Anträgen
Vom Parlament bzw. der Regierung angeforderte Beratung	-
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	-
Prüfmaßnahmen	
Prüfungen, Untersuchungen	104
Sanktionsmaßnahmen	
Sanktionen	-

[3]Andrea Voßhoff wurde am 19. Dezember 2013 zur neuen Bundesbeauftragten für Datenschutz und Informationsfreiheit ernannt und trat zum 6. Januar 2014 ihr Amt an.

Geldbußen	0
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	-

Im Berichtszeitraum hat es in Deutschland keine wesentlichen Änderungen oder Weiterentwicklungen hinsichtlich des Datenschutzes auf Gesetzesebene gegeben.

Als Beispiel für eine Entwicklung auf internationaler Ebene mit Konsequenzen für die Umsetzung auf nationaler Ebene sei der Vorschlag der OECD für einen globalen Informationsaustausch zur Bekämpfung von Steuerhinterziehung und Steuervermeidung genannt, der im Folgenden näher beschrieben werden soll:

Die weltweite Finanzkrise, die Skandale um sogenannte Steuerdaten-CDs sowie die wachsende Verlagerung von privaten Vermögen ins Ausland haben auf internationaler Ebene dazu geführt, dass die G20, die OECD, das Global Forum für einen effektiven und transparenten Informationsaustausch sowie die EU Steuerhinterziehung und Steuervermeidung entschlossen bekämpfen.

Am 20. Juli 2013 billigten die Finanzminister und Notenbankgouverneure der G20 einen OECD-Vorschlag zu einem globalen Modell für den automatischen Austausch im multilateralen Rahmen. Die Entscheidung der G20 ist auch vor dem Hintergrund des einstimmigen Beschlusses des Europäischen Rates vom 22. Mai 2013 zu sehen, durch den der Ausweitung des automatischen Informationsaustausches auf EU-Ebene und globaler Ebene Priorität eingeräumt wird.

Am 13. Februar 2014 hat die OECD einen globalen Standard für den automatischen Informationsaustausch vorgelegt. Darin ist u. a. festgelegt, welche Informationen ausgetauscht werden müssen und welche Finanzdienstleister und Steuerpflichtigen erfasst werden. Der internationale Standard umfasst ein Modellabkommen, einen Common Reporting Standard (CRS), einen Kommentar zur Auslegung sowie Mindeststandards für die Informatiklösung.

Für die Arbeiten zur Kommentierung des Standards ist ein Zeitraum bis Mitte des Jahres 2014 vorgesehen. Das Bundesministerium der Finanzen hat hierzu die deutsche Datenschutzklausel einschließlich Haftungs- und Todesstrafenklausel in die Diskussion eingeführt. Das auf OECD-Ebene entwickelte Modell beruht weitgehend auf dem zwischenstaatlichen Ansatz für die Umsetzung des von den USA initiierten FATCA-Abkommens (Foreign Account Tax Compliance Act).

Die G5 haben sich inzwischen darauf geeinigt, den Standard zum Jahreswechsel 2015/16 einzuführen (FATCA plus eineinhalb Jahre). Dies bedeutet, dass die Finanzinstitute mit Datum 31.12.2015 ihren Datenbestand in Bezug auf die Bestandskonten auf Steueransässige in anderen Staaten durchsuchen und ab dem 1.1.2016 bei Neukonten die Steueransässigkeit der Kontoinhaber nach einem vorgegebenen Verfahren (Due Diligence Procedure) ermitteln müssen. Die erste Meldung an das Bundeszentralamt für Steuern erfolgt entsprechend im September 2017. Im Rahmen der Revision der Amtshilferichtlinie strebt die Europäische Kommission an, innerhalb der EU das sogenannte CAA/CRS (Competent Authority Agreement/Common Reporting Standard) ohne inhaltliche Änderung im Rahmen europäischen Rechts umzusetzen.

Die nationale Umsetzung eines CAA/CRS-Abkommens soll nach Auffassung des Bundesministeriums der Finanzen zur Vereinfachung der Rechtsetzung im Rahmen einer Verordnung erfolgen. Die dazu erforderliche Verordnungsermächtigung müsse gemäß Artikel 80 Absatz 1 GG Inhalt, Zweck und Ausmaß präzise bestimmen. § 117c der Abgabenordnung werde dieser Vorgabe nicht gerecht, da dort auf ein in nationales Recht transformiertes internationales Abkommen verwiesen werde und das CAA/CRS lediglich ein Verwaltungsabkommen wäre. Insbesondere aus datenschutzrechtlichen Gründen sei für einen automatischen Informationsaustausch jedoch eine den Datenaustausch genau bezeichnende gesetzliche

Grundlage erforderlich. Angedacht sei deshalb, einen § 117d Abgabenordnung zu schaffen, der die auszutauschenden Informationen präzise definiere und vorgebe, zu welchem Zweck und in welchem Ausmaß diese Informationen genutzt werden dürfen.

Durch eine solche Regelung wird dem Grundsatz der Zweckbindung Rechnung getragen. Des Weiteren sollte im Hinblick auf die Durchführung des automatischen Informationsaustausches die Gewährleistung einer angemessenen Datensicherheit gesetzlich abgesichert werden. Überdies müsste unter anderem noch geklärt werden, in welcher Form eine Absicherung der datenschutzrechtlichen Betroffenenrechte erfolgt. Hierbei bietet sich an, entweder eine Regelung in der Ermächtigungsgrundlage oder in der Verordnung zu schaffen. Maßgeblich für die konkrete Ausgestaltung ist, dass der Betroffene hinreichend transparent über seine Betroffenenrechte informiert wird.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat im Rahmen seiner Stellungnahme gegenüber dem Bundesministerium der Finanzen deutlich gemacht, dass die nationale Umsetzung des CAA/CRS-Abkommens zur Implementierung des von der OECD entwickelten neuen Standards für den automatischen Informationsaustausch das Recht auf informationelle Selbstbestimmung aus Artikel 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 GG betrifft und daher einer gesetzlichen Grundlage bedarf, die dem rechtsstaatlichen Gebot der Normenklarheit entspricht und verhältnismäßig ist.

Die Umsetzung des CAA/CRS-Abkommens, das vom Bundesministerium der Finanzen als Verwaltungsabkommen im völkerrechtlichen Sinne gemäß Artikel 59 Absatz 2 Satz 2 GG eingestuft wird, muss sich im Rahmen der gesetzlichen Ermächtigung bewegen, die vorliegend noch zu schaffen ist. Hierbei muss das verordnungsspezifische Bestimmtheitsgebot hinreichend beachtet werden. So müssen nach Artikel 80 Absatz 1 Satz 2 GG Inhalt, Zweck und Ausmaß der erteilten Ermächtigung in dem ermächtigenden Gesetz bestimmt werden. Von Seiten des Bundesbeauftragten wird dem Bundesministerium der Finanzen darin zugestimmt, eine eigene gesetzliche Grundlage (§ 117d Abgabenordnung) zu fordern, um den datenschutzrechtlichen Anforderungen Genüge zu tun.

B. Rechtsprechung

2013 sind drei gerichtliche Entscheidungen bekannt geworden, die sich u. a. mit der Anwendbarkeit des deutschen Rechts auf ausländische Internet-Anbieter befasst haben. Dabei sind z. T. Wertungswidersprüche aufgetreten. Im Einzelnen handelt es sich um folgende Entscheidungen:

Landgericht Berlin vom 30.4.2013 (Az. 15 O 92/12)

Im Rahmen der Inhaltskontrolle der Datenschutzrichtlinie von Apple Sales International, Irland, nach dem Bürgerlichen Gesetzbuch prüft das Gericht die vom Unternehmen verwendeten Klauseln zur Verarbeitung personenbezogener Daten. Als Prüfungsmaßstab werden dabei die Vorschriften des Bundesdatenschutzgesetzes herangezogen.

Bundesgerichtshof vom 14.5.2013 (Az. VI ZR 269/12)

Das Gericht hat auf einen Anspruch des Geschädigten auf Unterlassung der Anzeige bestimmter persönlichkeitsrechtsverletzender Suchergänzungsvorschläge („Autocomplete“-Funktion) gegen den in den USA ansässigen Suchmaschinenbetreiber Google entschieden.

3. Oberverwaltungsgericht Schleswig vom 22.4.2013 (Az. 4 MB 11/13)

Das Gericht hat in einem nicht anfechtbaren Beschluss festgestellt, dass auf die Datenverarbeitung bei Facebook Ireland Limited auch in Bezug auf deutsche Nutzer nicht deutsches, sondern ausschließlich irisches Datenschutzrecht anwendbar ist. Begründet wurde dies damit, dass Facebook Ireland Ltd. eine Niederlassung von Facebook in Europa darstelle.

C. Sonstige wichtige Informationen

Nachdem die Überwachungsaktivitäten der USA und Großbritannien ans Licht kamen, hat der Bundesbeauftragter für Datenschutz und Informationsfreiheit sie letzten Sommer zu einer Sitzung des Ausschusses für Innere Angelegenheiten eingeladen. Während der Besprechung wurden wichtige Fragen des Datenschutzes diskutiert.

Zudem hat der Bundesbeauftrage eine schriftliche Stellungnahme zu diesem Thema für alle Parlamentsmitglieder für eine Anhörung im November 2013 verfasst. Diese Stellungnahme wurde in die offizielle Dokumentation des Parlaments aufgenommen (BT Drs. 18/59). Auf diese Weise konnte das Bewusstsein zu Datenschutzfragen gestärkt werden.

ESTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Die Entwicklung der Informations- und Kommunikationstechnologie und der Informationsgesellschaft schreitet rasch voran. Beim Schutz personenbezogener Daten und bei der Erfassung öffentlicher Informationen gibt es daher eine weitreichende „Grauzone".

Undefinierte rechtliche Konzepte (z. B. übermäßiger Schaden, öffentliches Interesse) müssen demnach ständig neu ausgelegt werden. Wenn man bedenkt, wie klein das estnische Recht und der estnische Sprachraum ist, braucht die Entwicklung unserer spezialisierten Rechtsterminologie und unserer juristischen Praktiken etwas länger als die größerer Länder.

Demnach muss sich die Datenschutzbehörde vermehrt auf die Erstellung von Leitlinien und die Entwicklung juristischer Verfahren konzentrieren, um für rechtliche Klarheit und Rechtssicherheit zu sorgen, die für die öffentliche Verwaltung und für die Wirtschaft wesentlich sind.

Jedes Jahr widmet sich die Datenschutzbehörde einer wichtigen „Grauzone", organisiert Beobachtungen, Prüfungen und Gespräche mit den betroffenen Parteien und entwickelt Richtlinien auf Grundlage der Ideen von Fachleuten und der praktischen Probleme.

*

Letztes Jahr war der Einsatz von Überwachungs- und Aufzeichnungsausrüstung das zentrale Thema. Wir haben versucht, es auf komplexe Weise anzugehen: Nutzung von Kameras zu Privatzwecken, Aufzeichnungen an öffentlichen Orten und auf einer öffentlichen Veranstaltung, Sicherheitskameras, Aufzeichnungen zur Vertragsdurchsetzung und zu journalistischen Zwecken, Kameras in Kinder-, Bildungs- und öffentlichen Einrichtungen usw. Debattiert wurde zum Beispiel die Frage, ob es sich bei Kindergärten und Schulen um öffentliche Orte handelt, an denen keine Einwilligung nötig ist, was Videoaufnahmen und Fotografien betrifft, und falls doch, inwieweit.

Die Rechtsberaterin der Datenschutzbehörde, Maris Juha, leitete die Erstellung der „Leitlinien zur Kameranutzung" in die Wege. Hierbei handelte es sich um unsere ersten Leitlinien, die im geplanten Gesetzesinformationssystem veröffentlicht werden.
*

Neben der Erstellung neuer Leitlinien versuchen wir außerdem, unsere anderen wichtigen Leitlinien „aktiv" zu halten, uns bei unserer täglichen Arbeit darauf zu beziehen und im Auge zu behalten, ob Änderungsbedarf besteht. Wie sich herausgestellt hat, besteht neben der 2011 verfassten Leitlinie zur Verarbeitung personenbezogener Daten in Beschäftigungsverhältnissen der Bedarf an einer gründlicheren Behandlung des Themas Datenschutz bei der Nutzung von Computern und intelligenten Geräten durch Arbeitnehmer.

Während Nachrichten zwischen Einzelnen normalerweise durch Vertraulichkeit geschützt sind und Offenlegung durch ein Unternehmen durch die Verpflichtung zu Datenschutz und Geheimhaltung geregelt wird, ist die Beziehung zwischen Arbeitgeber und Arbeitnehmer eine völlig andere und wird nicht durch die oben aufgeführten Regelungen abgedeckt. Die Leitlinie „Datenschutz bei der Computernutzung durch Arbeitnehmer", die vom IT-Berater der Datenschutzbehörde Urmo Parm angestoßen wurde, vereint Informationstechnologie und rechtliche Erläuterungen.

Neben der Veröffentlichung von Antworten auf Fragen, die für Arbeitnehmer und Arbeitgeber am interessantesten sind, im Abschnitt „Häufig gestellte Fragen" auf unserer Website werden wir diese außerdem im Portal für das Berufsleben veröffentlichen, das vom Arbeitsamt verwaltet wird.

*

Im vergangenen Jahr wurden mehrere Fragen zum Thema Versicherung bearbeitet: Nutzung von Daten Dritter, Speicherung von Einwilligungen zur Verarbeitung personenbezogener Daten sowie Bewegung von Kundendaten bei einem Broker, der den Arbeitgeber wechselt. Auf Initiative der leitenden Prüferin Merit Valgjärv überwachten wir außerdem Leasing-Unternehmen im Zusammenhang mit der Übermittlung personenbezogener Daten an Versicherungsunternehmen.

Im Bankenwesen untersuchten wir Fälle von Datenverarbeitung auf vertraglicher und Einwilligungsbasis und führten außerdem Überwachungen durch, um uns einen Überblick über die gängige Praxis zu verschaffen. Die Hauptprobleme traten im Zusammenhang mit der Einwilligung in Direktmarketing auf. Die Banken haben ihre Verfahren in diesem Bereich nun angepasst.

Basierend auf Problemen, die in der Praxis aufgetreten sind, konnten wir die Leitlinie zur Veröffentlichung von Zahlungsausfällen erheblich verbessern.

*

Die Gründung der IT-Gruppe hat die Aufklärungs- und Sensibilisierungsmaßnahmen der Datenschutzbehörde im Bereich Informations- und Kommunikationstechnologie erheblich verbessert. Wir werden über die Presse und im Internet praktische Erklärungen und Anweisungen veröffentlichen. Neun praktische, vom IT-Berater Urmo Parm erstellte Empfehlungen für die sichere Nutzung von Smartphones wurden auf der Facebook-Seite der Datenschutzbehörde über 21 000 Mal aufgerufen. Anweisungen für Facebook-Anwendungen wurden über 10 000 Mal aufgerufen. Die Anweisungen für die Einrichtung von Browsern auf Computern von Kindern (die an die Eltern gerichtet waren) wurde fast 10 000 Mal aufgerufen; die für das Löschen von Ausweisdaten aus dem Browserverlauf auf Computern 4 000 Mal.

Des Weiteren führten wir Sensibilisierungsmaßnahmen anhand verschiedener Formen der Zusammenarbeit durch, wie z. B. mit dem Projekt Targalt Internetis (Internet intelligent nutzen) mit dem Verband der Geschichts- und Sozialkundelehrer und Internetbeauftragten. Auf Initiative der Beraterin Silver Sarapuu erstellten wir Comic-Hefte zum Thema Datenschutz, die Lehrkräfte an Schulen als Begleitmaterial für den Unterricht nutzen können.

*

In Zusammenarbeit mit der Universität Tatu organisierten wir die Konferenz „Ethische Dimensionen des Datenschutzes und der Privatsphäre. Globale und lokale Herausforderungen“ , die am 9. und 10. Januar 2013 stattfand. Die Auswahl der Redner war beeindruckend, darunter mehrere erstklassige Wissenschaftler aus Estland sowie international bekannte Redner aus dem Ausland, wie Prof. Beate Rössler und der Europäische Datenschutzbeauftragte Peter Hustinx. Schirmherr der Konferenz war der Präsident der Republik, der auch den ersten Vortrag zum Thema hielt. In Zusammenarbeit mit dem Ethikzentrum der Universität Tartu wurde eine Konferenz über Aufklärungs- und Sensibilisierungsmaßnahmen für den Finanzsektor abgehalten.

Für eine derart hochrangige und gleichzeitig umfangreiche Forschungsveranstaltung müssen wir uns vor allem bei Prof. Margit Sutrop, der Leiterin des Ethikzentrums der Universität Tartu, sowie bei Ihrem Team bedanken. Die Konferenzteilnehmer kamen vorwiegend aus dem Sektor Rechtswissenschaften oder Informationstechnologie. Ich bin mir sicher, dass alle von der Konzeptualisierung ihrer täglichen Arbeit anhand von ethischen Werten beeindruckt waren.

*

Das Genehmigen von Datenbanken im staatlichen Managementsystem für Informationssysteme ist ein zwischenbehördliches Verfahren, das von außen trocken und langweilig wirkt und die Öffentlichkeit nicht sonderlich interessiert. Als Ausnahme stellte sich die Genehmigung des Informationssystems für den Fahrkartenverkauf für öffentliche Verkehrsmittel in Tallinn heraus.

Da die Kommunalregierung die Anmerkungen von der Datenschutzbehörde und der staatlichen Informationssystembehörde zur rechtlichen Situation und Informationssicherheit ignorierte und eine unkoordinierte Datenbank einsetzte, leiteten wir separate Überwachungsverfahren in die Wege, bei denen wir Sachverständige der Informationssystembehörde und des Zentrums für Registrierungsstellen und Informationssysteme einbezogen. Demzufolge wurden die Zeiträume für eine Speicherung personenbezogener Daten verkürzt, die Sicherheit erhöht, die für die Kommunalregierungen relevanten Gesetze geändert und die Datenbank einem Konzertierungsverfahren unterzogen.

All diese Änderungen, die infolge der Überwachung durchgeführt wurden, wären ohnehin während der Genehmigung der Datenbankplanungsphase oder spätestens während der Genehmigung der Umsetzungsphase ans Licht gekommen.

Wir sind der Ansicht, dass dies eine Lektion für alle staatlichen und kommunalen Regierungsbehörden ist: Datenschutzprobleme in Datenbanken rückwirkend zu ändern, ist teurer und mühseliger, als sie bereits während der Planung und Genehmigung zu vermeiden.

Wir stellten „Datenbank-Leitlinien“ zusammen, um praktische Probleme im Zusammenhang mit der Regulierung und Verwaltung von Datenbanken zu lösen.

*

Im Rahmen von grenzüberschreitenden Aktivitäten setzten wir die Zusammenarbeit zwischen den Datenschutzbehörden der baltischen Länder fort und führten mithilfe einer gemeinsamen Methodik Aufsichtsaktivitäten zu vereinbarten Themen durch.

Wir schlossen die dreigliedrige Überwachung der Hotels der Kette Radisson Blue Hotels ab. Bei der Überwachung von Kasinos entdeckten wir ein Schlupfloch im estnischen Recht bezüglich der maximalen Speicherzeit von Videoaufnahmen und Kundendaten, für dessen Korrektur wir in Zusammenarbeit mit Strafverfolgungsbehörden und der Gewerkschaft für Glücksspielanbieter eine Empfehlung herausgaben.

Datenschutzbehörden führten im Rahmen des globalen Netzwerks für die Durchsetzung des Rechts auf Datenschutz (Global Privacy Enforcement Network, GPEN) im Mai 2013 anlässlich des Internet Sweep Day Kontrollen durch. Hierbei untersuchten wir die Existenz und Verständlichkeit der Datenschutzrichtlinien der 40 größten Einzelhändler Estlands.

Laut der Richtlinie 95/46/EG liegt der Zweck der Artikel-29-Datenschutzgruppe in der Verbesserung der harmonisierten Umsetzung der Richtlinie. Bis heute ist die mit Abstand umfangsreichste Aktivität der Datenschutzgruppe das Verfassen von Stellungnahmen (Leitlinien), worin wir sehr gut geworden sind. Des Weiteren wurde politische Beratung bereitgestellt – kürzlich insbesondere im Zusammenhang mit der Reform des EU-Datenschutzgesetzes zur Koordinierung der Lösung von Fällen, die für internationales Aufsehen gesorgt haben. Falls nötig, wurde einigen Behörden von Mitgliedstaaten das Recht eingeräumt, im Namen der gesamten Arbeitsgruppe zu agieren.

Im Oktober 2013 präsentierte die Datenschutzbehörde bei der Plenarsitzung der Datenschutzgruppe eine Initiative, die vorsah, regelmäßig die Organisation praktischer Zusammenarbeit auf die Agenda zu setzen, um Managementerfahrung auszutauschen und auf reibungslosere Verfahren der grenzüberschreitenden Zusammenarbeit hinzuarbeiten. An der Initiative beteiligten sich Kollegen aus Großbritannien. In allen folgenden Plenarsitzungen wurden alle gemeinsam vorbereiteten Punkte der Tagesordnung besprochen.

*

Als Reaktion auf Verstöße liegt die Priorität der Datenschutzbehörde nach wie vor auf der schnellstmöglichen Beendigung der Verstöße und nicht auf Strafen.

Unterstützt wird dieser Ansatz außerdem von der Studie „Zugang zu Rechtsmitteln im Zusammenhang mit Datenschutz in EU-Mitgliedsstaaten“ (Access to data protection remedies in EU member states) der

Agentur der Europäischen Union für Grundrechte im Januar 2014. Betroffene Personen, deren Rechte verletzt wurden, sind vorwiegend daran interessiert, dass diese Verstöße schnell beendet werden.

Laut der Datenschutzbehörde dienen Dispute im Zusammenhang mit der Verfügbarkeit öffentlicher Informationen demselben Zweck: Personen, die Anträge stellen, sind an schnellen, unkomplizierten Zugangsverfahren interessiert.

Als Vergleich: Bei Aufsichtsaktivitäten im Zusammenhang mit dem Schutz personenbezogener Daten und öffentlichen Informationen wurden 287 Vorschläge/Empfehlungen und nur 53 Vorschriften erstellt. Bei den meisten Fällen endet der Verstoß nach Erhalt eines Vorschlags oder einer Empfehlung.

Die Anzahl der Ordnungswidrigkeitsverfahren wurde reduziert und beinhaltet hauptsächlich den Missbrauch professioneller Zugangsrechte zu sensiblen Datensätzen. Da der Verstoß bereits stattgefunden hat, ist eine Überwachung durch Vorlage von Vorschlägen/Vorschriften nicht mehr relevant. Daher reagiert die Datenschutzbehörde bei solchen Fällen stets mit der Einleitung von Ordnungswidrigkeitsverfahren.

Die Situation beim Bevölkerungsregister hat sich bedeutend verbessert. Wir erkennen die jahrelange systematische Nutzungsüberwachung durch das Innenministerium an, das für die Registrierung verantwortlich ist. Vermutlich war es auch hilfreich, dass in den Medien über dieses Thema berichtet wurde.

Bei der Datenschutzprüfung der Straßenverwaltungsbehörde untersuchten wir die Schwachstellen beim Datenschutz des verschlossenen Teils des Verkehrsregisters. Dieses enthält Kontaktdaten auf der Grundlage des Bevölkerungsregisters. Heute hat die Straßenverwaltungsbehörde technische Maßnahmen umgesetzt und eine interne Kontrolle eingeführt, um Missbrauch zu vermeiden. Von nun an wird sie auf Grundlage einer im Vorjahr abgeschlossenen Vereinbarung die Datenschutzbehörde bei vermuteten Verstößen informieren, damit diese ein Ordnungswidrigkeitsverfahren in die Wege leiten kann.

Organisation	Estnische Datenschutzbehörde
Vorsitz und/oder Gremium	Generaldirektor
Budget	631 329 EUR
Personal	18
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	601
Meldungen	602 Registrierungen von Verarbeitungen sensibler personenbezogener Daten
Vorabprüfungen	15
Anträge betroffener Personen	1 370
Beschwerden betroffener Personen	550
Vom Parlament bzw. der	52

Regierung angeforderte Beratung	
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten: Genehmigungen von Datenbanken des öffentlichen Sektors (einschließlich Ablehnungen)	89
Prüfmaßnahmen	
Prüfungen, Untersuchungen	463
Sanktionsmaßnahmen	
Sanktionen	22 Fälle
Geldbußen	3 206 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	121

FINNLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Zuge der Umsetzung der Strategie der Datenschutzbehörde im Berichtszeitrum führten wir eine Umstrukturierung unseres Personalplanungssystems durch und integrierten unser internes Kompetenzmanagementprogramm gründlicher in das System. Um in einem volatilen Betriebsumfeld für dauerhaften Erfolg zu sorgen, müssen wir die Qualität und Quantität der internen Kompetenzen sichern. Zu weiteren Eckpfeilern unserer Strategie gehören die Fähigkeit, die Auswirkungen neuer Phänomene abzuschätzen und unsere Maßnahmen zu priorisieren, die Nutzung von Informationen als Steuerungsinstrument sowie die Bildung nötiger Allianzen bei gleichzeitiger Aufrechterhaltung unserer Unabhängigkeit und Neutralität.

Die Datenschutzbehörde hat außerdem das per Regierungsverordnung für Informationssicherheit vorgegebene Niveau erreicht. Im Rahmen dieser Bemühungen war das gesamte Personal dazu verpflichtet, einen Informationssicherheitstest zu absolvieren. Informationssicherheitsschulungen sind ein fester Bestandteil unseres Kompetenzmanagementprogramms.

Wir haben Maßnahmen in die Wege geleitet, um eine völlig neue Servicefunktion und Informationsdienste einzuführen sowie unser Personal umzustrukturieren. Die Entwicklung eines internen Informationsmanagements bildet einen Bestandteil dieses Weges. Ich bin der Ansicht, dass ein Großteil der an uns herangetragenen Themen bereits zu einem früheren Zeitpunkt kommentiert oder bearbeitet wurde. Ein effizientes Ressourcenmanagement und die fortlaufende Beibehaltung des Serviceniveaus erfordert, dass wir uns auf wesentliche Themen konzentrieren.

Unabhängig vom Abschluss der Datenschutzregulierung oder -richtlinie sind wir uns bewusst, dass bezüglich der Kompetenz in unserem Land ein sehr großer Bedarf besteht, um die zunehmende Anzahl an Stellen, die sich für Datenschutzbeauftragte eröffnen, besetzen zu können. Aus diesem Grund haben wir eine interne Umfrage durchgeführt, um das Potenzial zu untersuchen, das für die Erschaffung eines Gütesiegels für die erforderlichen Schulungen besteht. Diese Produktentwicklungsmaßnahme soll in Zusammenarbeit mit Bildungseinrichtungen im Einklang mit unserer Strategie durchgeführt werden.

Im Zuge unseres Strebens nach maximaler Effektivität setzten wir unsere wirtschaftssektor- und phänomenspezifischen Umfragen fort. Diese Umfragen bezogen sich auf Ziele wie durch Werbung finanzierte Telefondienste, Kurzzeitkreditindustrie, kommerzielle Nutzung personenbezogener Daten sowie bei internationaler Zusammenarbeit untersuchte Website-Informationssicherheit (Sweep Day).

Konsistenzmechanismen und internationale Zusammenarbeit wurden zusammen mit unseren norwegischen Kollegen praktiziert, indem eine gemeinsame Prüfung eines globalen Online-Musikdienstkonglomerats durchgeführt wurde. Die Prüfung wurde während des laufenden Jahres abgeschlossen.

Eines unserer Schwerpunktthemen war der Datenschutz für Unternehmer. Unternehmer waren einer Reihe von aggressiven Verkaufstaktiken ausgesetzt. Um ihren Rechtsschutz zu garantieren, ist ein ausgeglichener Informationsaustausch zwischen den Streitparteien wichtig. Im Rahmen unserer Kompetenzen unterstützten wir den finnischen Unternehmensverband bei diesem Problem.

Biobanken wurden den Datenschutzverpflichtungen der Datenschutzbehörde als neue Zielgruppe hinzugefügt. Die nationale Aufsichtsbehörde für Wohlstand und Gesundheit (Valvira) wird als oberste Aufsichtsbehörde fungieren.

Organisation	
Vorsitz und/oder Gremium	Reijo Aarnio ist seit dem 1. November 1997 der Datenschutzbeauftragte.
Budget	Das Jahresbudget liegt bei 1 708 000 EUR
Personal	Insgesamt 20 Mitarbeiter.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	3 157
Meldungen	535
Vorabprüfungen	siehe Meldungen
Anträge betroffener Personen	958
Beschwerden betroffener Personen	(Zugang und Korrekturen) 269
Vom Parlament bzw. der Regierung angeforderte Beratung	127
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	119
Sanktionsmaßnahmen	233
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	>1 000

B. Rechtsprechung

Polizeifälle

Es wurde öffentlich bekannt, dass die personenbezogenen Daten des russischen Präsidenten sich im Informationssystem der finnischen Polizei befanden. Zur selben Zeit wurden Prüfungen bezüglich der unautorisierten Einsicht der Daten eines verstorbenen olympischen Goldmedaillengewinners

durchgeführt. Die Untersuchung führte dazu, dass Dutzende von Polizeimitarbeiter des Verstoßes gegen das Datenschutzgesetz für schuldig befunden wurden. Die Situation drohte das öffentliche Vertrauen in die Polizei und die Position der finnischen Polizeikommandanten zu schädigen. Ich persönlich bin der Meinung, dass die Befehlskette innerhalb der Polizei bis zu den Informationen verarbeitenden Daten zu lang ist und eine Überwachung näher an den eigentlichen Abläufen erforderlich ist.

Lebensmittelsicherheit

Kundenkartensysteme erfassen seit jeher Informationen zu den allgemeinen Einkaufsgewohnheiten der Verbraucher, die dazu ihre Einwilligung erteilt haben. Produktspezifische Informationen wurden bislang nicht erfasst. Die finnische Behörde für Lebensmittelsicherheit Evira wurde darüber informiert, dass ein von einer Einzelhandelskette mit Kundenkartensystem verkauftes Produkt möglicherweise das giftige Datura stramonium enthält und dazu führt, dass Kunden im Krankenhaus behandelt werden mussten. Gemäß Artikel 19 der allgemeinen EU-Lebensmittelverordnung (Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates) hielt Evira den Einzelhändler dazu an, Maßnahmen zu ergreifen, um die Daten des Kundenkartensystems mit den Verkaufsdaten des Ladens zu verknüpfen, um die Verbraucher zu warnen, die das betroffene Produkt gekauft hatten. Wie sich herausstellte, war das Geschäft tatsächlich in der Lage, diese Daten zu verknüpfen. Dies führte zu einer lebhaften Diskussion bezüglich der Glaubwürdigkeit des Kundenkartensystems und auch der Beziehung zwischen Datenschutz und Produktsicherheit.

Affiliate-Marketing

Das Gesetz zum Schutz der Privatsphäre in der elektronischen Kommunikation sieht vor, dass bei auf Verbraucher ausgerichtetem elektronischen Direktmarketing eine vorherige Einwilligung erforderlich ist. Um diese eindeutige Vorschrift zu umgehen, wurde Affiliate-Marketing entwickelt. Bei Affiliate-Marketing wird die eigentliche Marketing-Maßnahme von einem Unternehmen getroffen, das zum Beispiel in einem Opt-out-Land ansässig ist. Das Unternehmen, das seine Produkte verkaufen will, kauft Marketing-Dienstleistungen von dem anderen Unternehmen, behauptet jedoch, keine Dienste zur Verarbeitung personenbezogener Daten oder personenbezogene Dateninhalte zu kaufen. Bei einer Art von Affiliate-Marketing wird von den Marketing-Kommunikationsmaterialien oder sonstigen Kommunikationsmaterialien eines anderen Unternehmens Werbefläche gekauft. Die Datenschutzbehörde griff in diese Vorgänge ein. In Zusammenarbeit mit der Direktmarketingindustrie werden nun Verhaltenskodizes für solche Marketing-Maßnahmen erstellt.

Definition eines für die Verarbeitung personenbezogener Daten Verantwortlichen

Mir wurde mitgeteilt, dass die Vertreter einer religiösen Gruppierung Haushalte besucht und unter Missachtung des Datenschutzgesetzes personenbezogene Daten erfasst haben. Dabei ging es nicht um die Frage, ob die Religionsgemeinschaft Daten erfassen darf oder nicht, sondern darum, wer für die Verarbeitung der Daten verantwortlich ist. Die Religionsgemeinschaft stritt ihre Verantwortung ab und erklärte, dass es sich in dem Fall um die Nutzung personenbezogener Daten zu privaten Zwecken gehandelt habe, was vom Datenschutzgesetz unberührt bliebe. Ich sowie der Datenschutzausschuss, der bei der Angelegenheit die zuständige Behörde war, waren anderer Meinung. Die Religionsgemeinschaft legte bei einem Verwaltungsgericht Berufung ein.

C. Sonstige wichtige Informationen

Das neue Ökosystem der mobilen Kommunikation stellte den Datenschutz sowie die Stellung und die Rechte der Verbraucher auf allgemeinerer Ebene vermehrt vor Herausforderungen. Smartphones haben das Zeitalter der Applikationen (Apps) eingeläutet. Die Verarbeitung personenbezogener Daten bewegt sich von herkömmlichen Zentralregistern hin zu immer komplizierteren Systemen, bei denen eine Vielzahl von Applikationen über die Betriebssysteme von in eine Netzwerk-Infrastruktur integrierten Geräten betrieben wird.

In diesem Zusammenhang wurde in Finnland eine nationale Strategie für Cybersicherheit eingeführt.

Das Ministerium für Verkehr und Kommunikation führte eine Studie zum aktuellen Thema Big Data durch, und das Finanzministerium ernannte eine Arbeitsgruppe für die Umsetzung eines Open-Data-Programms. Die Betreiber litten weiterhin unter der mangelhaften zwischenbehördlichen Datenübermittlung. Um den Teil des Problems zu beheben, der auf dem Fehlen einer umfassenden Informationssystemarchitektur beruht, kam man zu der Entscheidung, dass als Korrekturmaßnahme eine neue Behörde (Valtori) gegründet werden solle, die mehr als eintausend Personen beschäftigt. Auf ähnliche Weise wurde ein Kanal für Bürgerdienste ins Leben gerufen, der zum Teil auf den Erfahrungen in Estland beruht.

Ein Rechtsrahmen bezüglich des Schutzes personenbezogener Daten befindet sich weiterhin im Entstehen. Dieser Prozess hat jedoch auch unsere Aufsichtsverpflichtungen erhöht. Der angemessene Umfang oder, genauer gesagt, der Mangel an Ressourcen scheint auf Grundlage einer Studie, die im Zusammenhang mit dem NETSO-Projekt durchgeführt wurde und noch nicht erschienen ist, ein dauerhafter Zustand zu sein.

Das Gesetzgebungsprojekt zum Informationsgesellschaftskodex ist unter der Leitung des Ministeriums für Verkehr und Kommunikation schnell vorangeschritten. Das Projekt warf auch die Frage der Netzneutralität auf bzw. ob die gesamte Internetkommunikation weiterhin frei ablaufen sollte oder ob Betreiber zum Beispiel das Recht haben sollten, einigen Nachrichten, d. h. diejenigen, für die mehr bezahlt wird, bevorzugt zu behandeln.

In dem Bericht von Professor Ahti Saarenpää wurde auftragsgemäß der potenzielle Bedarf an positiven Bonitätsbeurteilungen erörtert. Der Verfasser kam zu dem Schluss, dass es besser wäre, zuerst die Auswirkungen der europäischen Datenschutzverordnung auf die Verarbeitung finanzieller Daten zu beobachten. Er stellte jedoch auch fest, dass Bonitätsbeurteilungen zu den grundsätzlichen Datensätzen eines Unternehmens gehören sollten, was zur Einräumung besonderer gesetzlicher Vorrechte führen würde.

Die Arbeit der Arbeitsgruppe zur Besteuerung des Straßenverkehrs unter der Leitung von Herrn Ollila erregte außerdem die Gemüter. Ich sprach mich gegen die Nachverfolgung von Fahrzeughaltern in Echtzeit aus und schlug vor, dass Daten dezentralisiert erfasst werden sollten, wenn sie als Grundlage für eine Besteuerung herangezogen werden müssen.

Eine von uns durchgeführte Studie zeigte, dass fast alle Telekommunikationsanbieter, die Mobilfunkverträge für Verbraucher anbieten, auch eine Option mit teilweiser Finanzierung durch Werbung zur Verfügung stellen. Der Verbraucher willigt ein, als Gegenleistung für einen Rabatt auf Telefongebühren Werbung zu erhalten. Laut Verbraucherschutzbehörden ist ein Telefon eine Notwendigkeit. Die Datenschutzrichtlinie definiert eine Einwilligung als einen einseitigen, widerrufbaren Rechtsakt. Verbraucher schlossen häufig Verträge ab, die teilweise durch den Erhalt von Werbung finanziert wurden, und zogen unmittelbar danach ihre Einwilligung zurück. Die Datenschutzbehörde kam zu dem Schluss, dass im Falle eines solchen notwendigen Produkts eine Einwilligung kein Bestandteil der Kundenvereinbarung sein dürfe, sondern stattdessen als separate Absichtserklärung erachtet werden müsse. Infolgedessen entwickelten die Anbieter ein spezielles Doppelpreissystem.

Die Inkenntnissetzung der Öffentlichkeit stellt eines der größten Herausforderungen des Datenschutz dar. Um korrekte und zeitgerechte Informationen weiterzugeben, wurde 2013 unsere Website umstrukturiert. Außerdem beteiligten wir uns an der Entwicklung eines Gesamtkonzepts des Magazins Tietosuoja und trafen einen Beschluss zur Gründung einer Informationsdienstgruppe.

FRANKREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2013 war einmal mehr von einem beträchtlichen Anstieg der Aktivitäten geprägt, woran zu erkennen ist, welchen bedeutenden Stellenwert personenbezogene Daten im digitalen Zeitalter einnehmen und dass sich die Bevölkerung diesem Thema immer bewusster wird. Angesichts dieses Zuwachses ergreift die französische Datenschutzbehörde (Commission nationale de l'informatique et des libertés, CNIL) diesbezüglich auch weiterhin Maßnahmen und hat sich entsprechend angepasst, um noch schneller reagieren zu können.

Entwicklung von Compliance-Tools

Die CNIL hat 2013 ihre Strategie fortgesetzt und Fachkräfte mit verschiedenen Compliance-Tools unterstützt, wie z. B. „Datenschutzkorrespondenten", Gütezeichen, verbindliche unternehmensinterne Vorschriften (BCR) und sektorielle Compliance-Pakete.

„Datenschutzkorrespondenten" an Koregulierung beteiligt

Jedes Jahr nimmt die Bedeutung von Datenschutzkorrespondenten als zentrale Akteure hinsichtlich Compliance zu.

Ende 2013 hatten 13 000 Stellen einen Datenschutzkorrespondenten ernannt. Im Vorjahr waren es noch 11 000 gewesen. Der Mehrwert, der durch Ernennen eines Datenschutzkorrespondenten entsteht, ist an neuen Projekten, die eine Verarbeitung personenbezogener Daten umfassen, aufgrund der erteilten Ratschläge, des Umgangs mit Beschwerden oder CNIL-Prüfungen und zu guter Letzt aufgrund der erleichterten Ausübung des Rechts auf Zugang und Widerspruch besonders groß.

Der zukünftige Datenschutzbeauftragte, der aus dem Datenschutzkorrespondenten hervorgeht und dessen Zuständigkeitsbereich sich erweitert, steht im Mittelpunkt eines im Entwurf der Europäischen Datenschutzverordnung vorgesehenen Modells.

Gütezeichen: Vertrauen wecken

Das Datenschutzgesetz ermöglicht es der CNIL, Produkten oder Verfahren Gütezeichen auszustellen. Mit dem CNIL-Gütezeichen können Unternehmen sich hinsichtlich Servicequalität von der Konkurrenz abheben. Den Nutzern vermitteln die Gütezeichen Vertrauen in die damit ausgezeichneten Produkte und Verfahren und sorgen dafür, dass diejenigen leicht erkannt werden, die ein hohes Schutzniveau für ihre personenbezogenen Daten garantieren.

Auf Anfrage von Berufsverbänden wurden drei Bezugssysteme entwickelt: das Gütezeichen „Ausbildung", das 2012 eingeführte Gütezeichen „geprüfte Verarbeitung" sowie das erste Produktgütezeichen, das 2014 für digitale sichere Dienstleistungen eingeführt wurde. Seit 2012 hat die CNIL 29 Gütezeichen vergeben.

Compliance-Pakete

Nach ausführlichen Gesprächen mit betroffenen Fachkräften wurden verschiedene sektorielle Pakete entwickelt: ein „Versicherungspaket", ein „Sozialwohnungspaket", ein „Smart-Meter-Paket" und ein „Kommunalbehördenpaket".

Empfehlungen:

Die CNIL hat 2013 mehrere Empfehlungen herausgegeben, die Fachkräften die praktischen Bedingungen für die Umsetzung des Datenschutzgesetzes vermitteln. Diese Empfehlungen bezogen sich auf Cookies

und andere Tracking-Technologien, die Aufbewahrung von Bankkartendaten durch Einzelhändler und digitale Tresore.

Beratung für Behörden

Im Jahr 2013 gab die CNIL 74 Stellungnahmen zu Verordnungs- oder Gesetzentwürfen heraus, darunter:

- der Entwurf des Verbraucherschutzgesetzes mit Bestimmungen für die Einführung eines nationalen Privatkreditregisters;
- die Transparenz der Interessenkonflikte im Gesundheitswesen;
- die Transparenz des politischen Lebens;
- die Nationale Plattform für richterliche Überwachung (Plateforme nationale des interceptions judiciaires, PNIJ): Die Rechtsvorschrift wurde noch nicht veröffentlicht;
- der Entwurf des Gesetzes über die Nutzung von Ortungssystemen bei strafrechtlichen Ermittlungen;
- das zentrale Vorstrafenregister (Traitement des antécédents judiciaires, TAJ);
- lokale öffentliche Teledienste.

Darüber hinaus stand die CNIL Parlamentsabgeordneten mit rechtlichen und technischen Ratschlägen zur Seite und empfahl Informations- und Sensibilisierungsmaßnahmen.

Innovationsförderung

Im Rahmen seiner Innovations- und Vorausplanungsaktivitäten arbeitet die CNIL verstärkt mit Akteuren verschiedener Hintergründe zusammen. Dadurch kann sie technologische Entwicklungen besser voraussehen und so früh wie möglich neue Einsatzmöglichkeiten fördern, um für nachhaltige Innovationen zu sorgen, welche die Rechte der Nutzer respektieren.

Die CNIL hat demnach 2013 ein Innovationslabor ins Leben gerufen, in dem innovative Produkte und Anwendungen getestet, Tools wie z. B. Cookieviz – das 62 500 Mal heruntergeladen wurde – für die Öffentlichkeit entwickelt sowie Forschungs- und Entwicklungsprojekte wie das Projekt Mobilitics in Zusammenarbeit mit Inria koordiniert werden.

Überwachung der Meldungen von Verstößen gegen den Schutz personenbezogener Daten

Infolge des Inkrafttretens der europäischen Verordnung zu Maßnahmen im Zusammenhang mit Meldungen von Verstößen gegen den Schutz personenbezogener Daten im August 2013 führte die CNIL ein Fernverfahren ein, das über ihre Website zugänglich ist und es Betreibern ermöglicht, Meldungen auf sicherem Wege zu erstatten.

Erleichterte Ausübung von Rechten

Beschwerden

Bei der CNIL gingen 2013 rund 5 640 Beschwerden ein, womit das Beschwerdeaufkommen konstant blieb. Dies ist hauptsächlich auf exaktere Anträge und eine Konzentration auf praktische Inhalte zurückzuführen, welche die Situationen genauer beschreiben, in denen die CNIL eingreifen kann (z. B. Merkblätter zum Schutz personenbezogener Daten am Arbeitsplatz und bei der Videoüberwachung).

Der Widerspruch gegen Datenverarbeitungsaktivitäten und die Ausübung des Rechts auf Zugang waren sektorübergreifend die Hauptgründe für Beschwerden. Gleichzeitig bestätigte das Jahr 2013 den Trend, der seit 2011 zu beobachten ist, nämlich die hohe Anzahl an Beschwerden im Zusammenhang mit dem Internet-/Telekommunikationssektor (34 % der Beschwerden) und insbesondere das Thema Online-Reputation.

Bei der CNIL gingen 1 917 Beschwerden bezüglich der Löschung von Texten, Fotos, Videos, Kontaktdaten, Kommentaren, falschen Online-Profilen, der Weiterverwendung öffentlich im Internet zugänglicher Daten usw. ein.

Recht auf indirekten Zugang

Bei der CNIL gingen 4 305 Anträge auf indirekten Zugang ein. Im Vergleich zum Vorjahr entspricht dies einem Anstieg von 17 %. Diese Anträge erforderten insgesamt 7 148 Prüfungen im Zusammenhang mit Bankkonten- und ähnlichen Formularen (Fichiers des comptes bancaires et assimilés, FICOBA) der Steuerbehörde, dem Strafregister (zentrales Vorstrafenregister ab dem 1. Januar 2014) und der Überwachung durch Nachrichtendienste.

Sanktionen

Am 10. Juni 2013 schrieb die Vorsitzende der CNIL ein Aufforderungsschreiben an Google Inc. Die CNIL (die Vorsitzende und die zwei stellvertretenden Vorsitzenden) beschlossen, diesen Beschluss öffentlich zu machen, und zwar insbesondere aufgrund des Status und der Größe des beteiligten Konzerns sowie aufgrund der großen Anzahl der von der Datenverarbeitung betroffenen Personen.

Dieses Aufforderungsschreiben folgte auf die Entscheidung von Google Inc., die verschiedenen Vertraulichkeitsrichtlinien der rund sechzig Dienste des Unternehmens zu einer einzigen Richtlinie zu vereinen.

In ihrem Beschluss betonte die Vorsitzende der CNIL, dass Google Inc. seinen Nutzern nicht ausreichend Informationen über die Bedingungen zur Verfügung stellte, unter denen ihre personenbezogenen Daten erfasst werden.

Dem Unternehmen wurde außerdem am Ende einer Verhältnismäßigkeitsprüfung zwischen seinem legitimen Interesse auf der einen Seite und den Rechten und Interessen der Internetnutzer auf der anderen Seite vorgeworfen, nicht vor der Zusammenführung ihrer Daten die Einwilligung der Nutzer eingeholt zu haben. Die Vorsitzende wies darauf hin, dass aufgrund des Aus- und Übermaßes der Datenzusammenführung das Risiko besteht, dass die Datenschutzrechte der Nutzer missachtet werden.

Darüber hinaus wurden Mängel in Bezug auf die Verpflichtung, eine Aufbewahrungspflicht der erfassten Daten festzulegen, sowie auf die Inkenntnissetzung der Nutzer vor der Platzierung von Cookies auf deren Computern erwähnt.

Da das Unternehmen nicht auf das Aufforderungsschreiben reagierte, wurde ein Sanktionsverfahren eingeleitet. Am 3. Januar 2014 verkündete die CNIL eine Geldbuße in Höhe von 150 000 EUR und ordnete Google außerdem an, zu diesem Beschluss auf www.google.fr eine Pressemitteilung zu veröffentlichen.

Am 14. Januar 2014 beantragte Google eine teilweise Aufhebung der Sanktionsabsichten gegen den Konzern durch die CNIL. Das Oberste französische Verfassungsgericht lehnte den Antrag per Anordnung am 7. Februar 2014 ab.

Überwachung der extraterritorialen Anwendung der Gesetze von Drittstaaten, die Auswirkungen auf europäische Bürger haben

Massenüberwachungssysteme

Im März 2013 rief die CNIL sogar noch vor Veröffentlichung der Enthüllungen von Edward Snowden eine Arbeitsgruppe ins Leben, die Anhörungen durchführen und sich mit der Frage des Zugangs ausländischer Behörden auf die Daten europäischer Bürger befassen soll.

Die CNIL nahm aktiv an den Vorbereitungsarbeiten der Artikel-29-Datenschutzgruppe zu elektronischen Massenüberwachungsprogrammen teil. Diesbezüglich kam sie im Juli 2013 zu Gesprächen mit ihren Amtskollegen zusammen.

Die Vorsitzende der CNIL wurde außerdem im Oktober 2013 vom LIBE-Ausschuss des Europäischen Parlaments im Rahmen von Diskussionen zur Bedeutung gesetzlicher Tools zur Überwachung von Übermittlungen im Prism-Fall angehört.

Die Angelegenheit ist nicht nur mit dem Thema Datenschutz verbunden, sondern wirft auch Bedenken außerhalb des Zuständigkeitsbereichs nationaler Datenschutzbehörden auf.

Aus diesen Gründen kam die CNIL zu dem Schluss, dass eine mögliche Lösung die Schaffung eines spezifischen Tools in Form eines internationalen Abkommens ist, das garantieren soll, dass die Nachrichtendienste von Drittländern ein angemessenes Datenschutzniveau bieten.

Ein solches zwischenstaatliches Abkommen darf jedoch angesichts der an die Öffentlichkeit geratenen Informationen unter keinen Umständen ein elektronisches Massenüberwachungsprogramm wie Prism legitimieren. Ein derartiges Abkommen sollte mit der Charta der Grundrechte der Europäischen Union und der Europäischen Menschenrechtskonvention in Einklang stehen. Ein Verstoß gegen die Datenschutzrechte der Bürger müsse demnach dringend und nachweisbar notwendig sein und durch einen rechtmäßigen, verhältnismäßigen Zweck gerechtfertigt werden.

Des Weiteren unterstützt die CNIL die Wiedereinführung von Artikel 42 des ursprünglichen Entwurfs in die geplante europäische Datenschutzverordnung. Dieser Text sieht vor, dass die Übermittlung von Daten in Drittländer außerhalb der Europäischen Union auf Anfrage einer ausländischen Behörde nur mit der Genehmigung der nationalen Datenschutzbehörde ausgeführt werden darf.

Schwarze Listen

Die CNIL beleuchtete bestimmte Gesetze genauer, die Behörden und Unternehmen dazu verpflichten, dafür Sorge zu tragen, dass ihre Mitarbeiter, Lieferanten oder Subunternehmer nicht aus irgendwelchen Gründen auf „schwarzen Listen“ stehen.

Einige Staaten – vor allem die USA – versuchen seit mehreren Jahren, sich selbst vor verschiedenen Risiken zu schützen (z. B. durch die Bekämpfung der Terrorismusfinanzierung und strategisch sensible Exporte), indem sie per Gesetz Handelssanktionen erlassen oder bestimmte Beschränkungen einführen.

Die Handhabung dieser Risiken hat zur Schaffung und Nutzung internationaler oder nationaler schwarzer Listen geführt, auf denen bestimmte Staaten, natürliche und juristische Personen, Organe oder Konzerne geführt werden, denen Verbote (z. B. Handelsverbote) auferlegt werden sollen oder denen besondere Aufmerksamkeit zu widmen ist. Diese Gesetze erfordern oftmals eine Prüfung aller Aktivitäten, an denen diese Länder, Personen, Unternehmen, Organe oder Konzerne direkt oder indirekt beteiligt sind.

Die CNIL hat sich darüber Gedanken gemacht und empfiehlt die Einführung einiger minimaler Vorkehrungen im Zusammenhang mit der Nutzung solcher Listen.

Regulatorische Entwicklungen

Die vorgeschlagenen Änderungen des Datenschutzgesetzes im Zusammenhang mit dem Entwurf eines Digitalgesetzes

Nachdem die Regierung im Februar 2013 den Entwurf eines Digitalgesetzes angekündigt hatte, hat die CNIL mehrere Vorschläge für Gesetzesänderungen aufgesetzt, die bezüglich des Entwurfs nötig sein könnten.

Diese Vorschläge betreffen die vier Hauptakteure auf dem Gebiet des Datenschutzes: Einzelpersonen, Unternehmen, Behörden und die CNIL.

Die CNIL schlägt insbesondere Folgendes vor:

- eine verstärkte Effektivität der individuellen Rechte (z. B. elektronische Ausübung von Rechten usw.) sowie den spezifischen Schutz Minderjähriger;
- eine fortlaufende Vereinfachung der Verfahren für Unternehmen;
- Ausweitung der Befugnisse der CNIL auf Nachrichtendienstinformationen im Einklang mit dafür angemessenen Bedingungen;
- direkter Zugang zu Strafregistereinträgen von Angeklagten (Opfer, Kläger usw.);
- eine Erhöhung der Höchststrafen und schnelleres Auslösen von Bußgeldverfahren.

Beteiligung an Arbeiten am EU-Verordnungsentwurf

Angesichts der Größte der technologischen, politischen, wirtschaftlichen und internationalen Herausforderungen des Verordnungsentwurfs wurde dieser 2013 im Europäischen Parlament und im EU-Rat ausgiebig debattiert.

In diesem Zusammenhang teilte die CNIL den Behörden weiterhin ihre Bedenken mit.

Bezüglich einer einzigen Anlaufstelle fördert die CNIL ein ausgeglichenes Governance-Modell im Interesse aller Beteiligten. Demnach wurde in enger Zusammenarbeit mit der französischen Regierung eine alternative und glaubwürdige Lösung zu der von der Europäischen Kommission vorgeschlagenen einzigen Anlaufstelle entwickelt. Dieser Alternativvorschlag basiert auf den folgenden Punkten:

- gemeinsame Kompetenzen für eine „transnationale“ Verarbeitung zwischen den Behörden des Wohnsitzlandes der betroffenen Personen und der Behörden in dem Land, in dem das Unternehmen seinen Hauptsitz hat;
- Organisation der Zusammenarbeit zwischen den Datenschutzbehörden durch die Ernennung einer federführenden Behörde basierend auf dem Kriterium der Hauptniederlassung;
- Verabschiedung der Beschlüsse im Rahmen eines gemeinsamen Beschlussverfahrens;
- effektiver gerichtlicher Rechtsschutz für betroffene Personen vor dem Gericht ihres Wohnsitzlandes vor Beschlüssen ihrer Behörde sowie aufseiten der für die Datenverarbeitung Verantwortlichen vor dem Gericht des Landes der federführenden Behörde, das für ihre Hauptniederlassung zuständig ist;
- eine neue Rolle für den Europäischen Datenschutzausschuss, der für die Beilegung von Streitigkeiten zwischen Datenschutzbehörden verantwortlich ist.

Im Zusammenhang mit der Anonymisierung von Daten ist die CNIL der Ansicht, dass die Anonymisierung von Daten als Sicherheitsmaßnahme ein System reduzierter Verpflichtungen für die Datenverarbeitung Verantwortliche rechtfertigen kann, warnt jedoch vor der Schaffung spezieller Vorkehrungen für anonymisierte Daten.

Bezüglich des risikobasierten Ansatzes kommt die CNIL zu dem Schluss, dass der risikobasierte Ansatz unter keinen Umständen Rechte verletzen oder dazu führen darf, dass für die Datenverarbeitung Verantwortliche (oder den Verarbeiter) von ihrer allgemeinen Verpflichtung zur Einhaltung der Bestimmungen der Verordnung ausgenommen werden dürfen.

Organisation	Französische Datenschutzbehörde
Vorsitz und/oder Gremium	Vorsitz: Isabelle FALQUE-PIERROTIN Stellvertretende Vorsitzende: Marie-France Mazars (seit Februar 2014), Eric Peres (seit Februar 2014). 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 2013 (in Mio. EUR): 16,9
Personal	Anzahl der Mitarbeiter: 178
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	2 542 Beschlüsse/129 Stellungnahmen/3 Empfehlungen
Meldungen	Bei der CNIL gingen 92 351 Meldungen ein, darunter: 11 085 Meldungen von Videoüberwachungssystemen 5 483 Meldungen von Ortungssystemen 29 Gütezeichen
Vorabprüfungen	Genehmigungen: 2 615 im Jahr 2013, darunter: 247 im Plenum angenommene Genehmigungen, 1 078 Genehmigungen von Datenübermittlungen an Nicht-EU-Staaten, 3 Rahmengenehmigungen, 416 Genehmigungen biometrischer Systeme, 656 Genehmigungen von Datenverarbeitungen zu medizinischen Forschungszwecken sowie 215 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 2013 35 524 schriftliche und 124 595 telefonische Anfragen
Beschwerden betroffener Personen	Bei der CNIL gingen 2013 5 640 Beschwerden ein Anfragen betroffener Personen: 4 305 Anträge auf indirekten Zugang in Bereichen, in denen eine Datenverarbeitung der Staatssicherheit,

	Verteidigung oder öffentlichen Sicherheit dient
Vom Parlament bzw. der Regierung angeforderte Beratung	Die CNIL nahm 2013 129 Stellungnahmen an. Des Weiteren wurde die CNIL über 20 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	414 Untersuchungen, davon 130 Untersuchungen bzgl. Videoüberwachungssystemen.
Sanktionsmaßnahmen	
Sanktionen	14 durch die CNIL im Jahr 2013 verhängte Sanktionen. Rechtsstreite gegen Verantwortliche von Datenverarbeitungen: 56 (57 Mahnungen, 7 Geldstrafen, 5 Verwarnungen), 1 Kündigung.
Geldbußen	Die CNIL verhängte 2013 Geldbußen im Gesamtwert von 43 000 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	12 953 Institutionen ernannten 2013 einen DPO, was 3 679 DPO darstellt

B. Rechtsprechung

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

- Oberstes Verwaltungsgericht, Untersektion 10, Herr B. A. gegen CNIL 345408 (4.11.2013)
- Oberstes Verwaltungsgericht, Richter im Verfahren des vorläufigen Rechtsschutzes, SAS Paris Saint-Germain Fußball und Handball gegen CNIL 373061 (20.11.2013)
- Oberstes Verwaltungsgericht, Untersektionen 10 und 9, Herr B. A. gegen CNIL, 328634 (3.6.2013)
- Oberstes Verwaltungsgericht, Richter im Verfahren des vorläufigen Rechtsschutzes, Herr B. A. 365459 (14.2.2013)
- Oberstes Verwaltungsgericht, Untersektion 10, Langlois, Association Internet sans Frontières, das Unternehmen OVH SAS gegen SGG, Ministerium für Wirtschaft und Finanzen 347349 (20.11.2013)
- Oberstes Verwaltungsgericht, Untersektionen 10 und 9, Herr A. / Oberstes Verwaltungsgericht 359417 (17.7.2013)

- Oberstes Verwaltungsgericht, Untersektionen 10 und 9, La Poste / Oberstes Verwaltungsgericht 342372 (17.4.2013)
- Oberstes Verwaltungsgericht, Untersektionen 10 und 9, Ausschuss für Hygiene, Sicherheit und Arbeitsbedingungen des Unternehmens Lyondell Chimie France gegen Innenministerium 337982 (24.4.2013)
- Kassationsgericht Paris, Kammer für Handelssachen, SARL Google France gegen das Unternehmen Cobrason 1121011112471394 (29.1.2013)
- Kassationsgericht, 1. zivile Kammer, Unternehmen Agence du Palais gegen Rose Marie V, 1119530 (10.4.2013)
- Kassationsgericht, 1. zivile Kammer, Unternehmen Google Inc. et al. gegen Société Lyonnaise de Garantie 1217591 (19.6.2013)
- Kassationsgericht, Kammer für Handels-, Finanz- und Wirtschaftssachen, Herr X. gegen das Unternehmen Bout-Chard 1217037 (25.6.2013)
- Kassationsgericht, Kammer für Strafsachen, Mohamed X. gegen Staatsanwaltschaft 1381945 (22.10.2013)
- Kassationsgericht, Kammer für Strafsachen, Unternehmen Biotronik France 1280346 (24.4.2013)
- Kassationsgericht, Kammer für Soziales, Verband für Kinder- und Jugendschutz des Départements Alpes-Maritimes (Association départementale pour la sauvegarde de l'enfance, de l'adolescence et des jeunes adultes des Alpes-Maritimes, ADSEA 06) gegen Herrn CARTON, 1126099 (23.4.2013)
- Kassationsgericht, Kammer für Soziales, Herr Dubos gegen das Unternehmen Distribution Casino France 1216564 (26.6.2013)
- Kassationsgericht, 1. zivile Kammer, Verbraucherverband Isère Union fédérale des consommateurs de l'Isère gegen Caisse régionale de Crédit agricole mutuel Sud Rhône-Alpes 10283972 (23.1.2013)

GRIECHENLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Das griechische Parlament verabschiedete das Drogengesetz 4139/2013, das u. a. Bestimmungen im Hinblick auf die Offenlegung der personenbezogenen Daten von Straftätern enthält und dadurch Änderungen des Gesetzes 2472/1997 zum Schutz personenbezogener Daten herbeiführte.

Die Datenschutzbehörde veröffentlichte insgesamt 158 Beschlüsse und 6 Stellungnahmen, von denen einige in Abschnitt B „Rechtsprechung" aufgeführt werden.

Des Weiteren brachte die Datenschutzbehörde schriftlich seine Ansichten zu a) der Verarbeitung personenbezogener Daten durch Kreditratingagenturen, b) den beiden Abkommensentwürfen – „Statement of Protocol" und „Absichtserklärung" – zwischen der griechischen Prüfaufsichtsbehörde Accounting & Auditing Standards Oversight Board und der US-amerikanischen Prüfaufsichtsbehörde Public Company Accounting Oversight (PCAOB) für den grenzüberschreitenden Informationsaustausch im Zusammenhang mit der Aufsicht von Wirtschaftsprüfern, c) dem griechischen Aktionsplan für Open Government im Rahmen der griechischen Beteiligung an der Open Government Partnership (OGP) sowie d) dem „Cl@rity-Programm" (http://diavgeia.gov.gr/en), laut dem alle Ministerien und öffentlichen Stellen im Allgemeinen dazu verpflichtet sind, ihre Beschlüsse ins Netz zu stellen, zum Ausdruck.

Am Europäischen Tag des Datenschutzes 2013 veröffentlichte die Datenschutzbehörde auf ihrer Website die Broschüre und das Video „Kontrolle über die eigenen personenbezogenen Daten übernehmen", die von der Europäischen Kommission (GD Justiz) produziert wurden und nützliche Informationen zur Reform des Datenschutzgesetzes enthalten. Des Weiteren organisierte die Behörde zur Feier ihres 15. Jubiläums zu Sensibilisierungszwecken eine zweitägige Konferenz, deren Hauptthema der Beitrag der griechischen Datenschutzbehörde zur Schaffung eines datenschutzfreundlichen Umfeldes in Griechenland war.

Die Behörde veröffentlichte außerdem vier Ausgaben des vierteljährlich erscheinenden elektronischen Newsletters mit Informationen zu aktuellen Entwicklungen auf dem Gebiet des Datenschutzes auf nationaler, europäischer und internationaler Ebene. Zu guter Letzt veröffentlichte die Datenschutzbehörde auf ihrer Website die Ergebnisse der 2012 durchgeführten Online-Befragung zu Themen im Zusammenhang mit dem Schutz personenbezogener Daten.

Zum wiederholten Mal konnte jedoch das schwerwiegende Problem der Unterbesetzung der Datenschutzbehörde, das seit ihrer Gründung besteht, aufgrund der andauernden schlechten Finanzlage Griechenlands auch 2013 nicht gelöst werden. Darüber hinaus beeinträchtigt die fortlaufende Reduzierung des Budgets, das der Datenschutzbehörde für betriebliche Zwecke zugeteilt wird, die Fähigkeit der Behörde, ihren Verpflichtungen ausreichend nachzukommen.

Organisation	
Vorsitz und/oder Gremium	Petros Christoforos (Vorsitzender des Gremiums).
Budget	1 816 500 EUR.
Personal	Abteilung Audit: 14 Juristen und 11 IT-Fachkräfte (davon drei (3) unbezahlte Beurlaubungen und zwei (2) im Mutterschutz); Abteilung Kommunikation und PR: 5 (davon wurde eine (1) für einen Teil des Jahres an eine andere Stelle des öffentlichen Dienstes abgestellt und dann dorthin versetzt, eine (1) für einen Teil des Jahres im Mutterschutz, eine (1) ging in Ruhestand); Personal- und Finanzabteilung: 16 Personen (davon wurde eine (1) an eine andere

	Stelle des öffentlichen Dienstes versetzt, eine (1) wurde von einer anderen Stelle des öffentlichen Dienstes versetzt, nachdem sie an die Datenschutzbehörde abgestellt worden war, und eine (1) im Mutterschutz, drei (3) wurden ebenfalls von einer anderen Stelle des öffentlichen Dienstes versetzt, davon eine (1) unbezahlte Beurlaubung).
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die Datenschutzbehörde veröffentlichte 158 Beschlüsse und 6 Stellungnahmen.
Meldungen	Die Datenschutzbehörde erhielt 650 Meldungen (381 davon betrafen die Installation und den Betrieb von Überwachungskameras, 92 betrafen die Übermittlung von Daten in Länder außerhalb der EU).
Vorabprüfungen	Die Datenschutzbehörde bewilligte bzw. erneuerte 127 Genehmigungen zur Verarbeitung sensibler Daten, zur Verknüpfung von Dateien sowie zu Datenübermittlungen in Länder außerhalb der EU.
Anträge betroffener Personen	1 144.
Beschwerden betroffener Personen	692 (Strafverfolgungsbehörden und Ordnungsamt: 20, öffentliche Verwaltung und lokale Behörden: 19, Landesverteidigung: 5, Besteuerung/Finanzministerium: 3, Gesundheitswesen: 5, Sozialversicherung: 13, Bildung und Forschung: 9, Bankwesen: 111, Privatwirtschaft: 107, elektronische Kommunikation: 264, Arbeitsbeziehungen: 22, Massenmedien: 3, Sonstige: 111).
Vom Parlament bzw. der Regierung angeforderte Beratung	4 – siehe Abschnitt (A) „Zusammenfassung der Aktivitäten und Neuerungen“.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Am Europäischen Tag des Datenschutzes 2013 veröffentlichte die Datenschutzbehörde Folgendes auf ihrer Website: Broschüre und Video „Kontrolle über die eigenen personenbezogenen Daten übernehmen“, die von der Europäischen Kommission (GD Justiz) produziert wurden, nützliche Informationen zur Reform des Datenschutzgesetzes. Des Weiteren organisierte die Behörde zur Feier ihres 15. Jubiläums zu Sensibilisierungszwecken eine zweitägige Konferenz (23. und 24. Mai), die in der Konzerthalle von Athen stattfand. Das Hauptthema war der Beitrag der griechischen Datenschutzbehörde zur Schaffung eines datenschutzfreundlichen Umfeldes in Griechenland. Die Behörde veröffentlichte außerdem vier Ausgaben des vierteljährlich erscheinenden elektronischen Newsletters mit Informationen zu aktuellen Entwicklungen auf dem Gebiet des Datenschutzes auf nationaler, europäischer und internationaler Ebene. Zu guter Letzt veröffentlichte die Datenschutzbehörde 2013 auf ihrer Website die Ergebnisse der 2012 durchgeführten Online-Befragung zu Themen im Zusammenhang mit dem Schutz personenbezogener Daten.

Prüfmaßnahmen	
Prüfungen, Untersuchungen	10 Prüfungen von für die Datenverarbeitung Verantwortlichen im privaten Sektor. Genauer wurden vier (4) Prüfungen bei Unternehmen durchgeführt, um ihre Verfahren in Bezug auf die Rechtmäßigkeit der Erfassung und Verarbeitung personenbezogener Daten im Rahmen der Bereitstellung von Bonitätsprüfungsdienstleistungen zu überprüfen. Zwei (2) zusätzliche Prüfungen wurden bei zwei Banken im Zusammenhang mit angeblichen Verstößen gegen das Datenschutzgesetz durchgeführt, die sich jedoch als unbegründet herausstellten. Zwei (2) weitere Prüfungen wurden im Hinblick auf Spam und das Verschicken unerwünschter E-Mails zur Werbung für Produkte und Dienstleistungen zweier Unternehmen durchgeführt. Zu guter Letzt wurden zwei (2) Prüfungen zum Einsatz von Videoüberwachungssystemen an einem Arbeitsplatz (Pizzalieferservice-Kette) zur Überwachung von Verhalten und Leistung der Arbeitnehmer durchgeführt. Außerdem unterstützte die Behörde die Einheit für Cyberkriminalität der griechischen Polizei in zwei Fällen (angeblicher Verstoß gegen das Datenschutzgesetz in einem Unternehmen sowie illegale Verarbeitung personenbezogener Daten, die über eine Website erfasst wurden).
Sanktionsmaßnahmen	
Sanktionen	Die Datenschutzbehörde verhängte 26 Sanktionen (6 Verwarnungen, 20 Geldbußen). Bei sechs (6) Beschlüssen erlegte die Datenschutzbehörde eine Verwarnung und eine Geldbuße auf. Die Sanktionen bezogen sich auf folgende Themen: Öffentlicher Sektor (3), Marketing – Werbung für Produkte und Dienstleistungen (2), Finanzsektor (4), Verletzungen des Schutzes personenbezogener Daten (2), Massenmedien (1), Videoüberwachung (2), Bildung und Forschung (1) sowie elektronische Kommunikation (10).
Geldbußen	Bußgelder: Der Gesamtwert der von der griechischen Datenschutzbehörde auferlegten Geldbußen belief sich auf 311 735 EUR.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Stellungnahme 2/2013

Die Datenschutzgruppe gab eine Stellungnahme bezüglich Angaben auf der Website der Journalistenkrankenkasse (E.D.O.E.A.P.) ab, da dort die Schulden natürlicher Personen im Zusammenhang mit Versicherungsbeiträgen und Werbesteuer veröffentlicht worden waren. Infolge einer Anfrage der Journalistenkrankenkasse kam die Behörde zu dem Schluss, dass diese im Internet eingestellten Angaben der Schulden natürlicher Personen keine rechtmäßige Verarbeitung personenbezogener Daten darstellen. Genauer gesagt, ist dies in keinem Gesetz und in keinem Präsidialdekret vorgesehen und steht auch nicht mit dem Grundsatz der Verhältnismäßigkeit im Einklang.

Stellungnahme 4/2013

Die Datenschutzbehörde kam zu dem Schluss, dass die Erfassung und Verarbeitung der Führungszeugnisse von Mitarbeitern durch die Versicherung, bei der sie tätig sind, keine rechtmäßige Verarbeitung darstellt, da dies dem Grundsatz der Verhältnismäßigkeit widerspricht. Als Alternative schlug die Behörde vor, dass eine Erklärung an Eides statt ausreichen würde.

Stellungnahme 5/2013

Die Datenschutzbehörde ging einer Anfrage vom Generalsekretär für Staatseinnahmen betreffend des Entwurfs eines ministeriellen Beschlusses zum System der Bank- und Zahlkontenregistrierungsstellen nach, das derzeit entwickelt wird. Das System soll die Übermittlung von Ersuchen um Verzicht auf das Bankgeheimnis durch zuständige Justizbehörden und Diensten an Finanzinstitutionen sowie den direkten Empfang der relevanten Antworten vereinfachen, ohne gegen das für den Verzicht auf das Bank- und Berufsgeheimnis geltende Recht zu verstoßen. Die Datenschutzbehörde kam zu dem Schluss, dass die Verarbeitung durch ein Gesetz oder ein Präsidialdekret vorgesehen sein sollte, in dem der für die Datenverarbeitung Verantwortliche, die Ziele, die Daten, die Aufbewahrungsfrist, die Empfänger der Daten, die technischen Spezifikationen der für den Betrieb des Systems erforderlichen Anwendungen sowie die organisatorischen und technischen Maßnahmen für die Sicherheit der Verarbeitung der personenbezogenen Daten aufgeführt werden. Die Datenschutzbehörde urteilte außerdem, dass „sensible Daten“ nach dem Erhalt der Antwort von den zuständigen staatlichen Behörden und Diensten aus dem System gelöscht werden und zusätzliche technische Maßnahmen ergriffen werden sollten, die gewährleisten, dass Datenantworten von den anfragenden Behörden empfangen werden. Schließlich wies die Behörde darauf hin, dass es für den Schutz personenbezogener Daten und für die Bereitstellung einer effektiven Lösung am besten wäre, wenn die Finanzinstitutionen und nicht das Generalsekretariat für Informationssysteme des Finanzministeriums (G.S.I.S.) zur Aufbewahrung der Daten verpflichtet wären und dass die Aufbewahrungsfrist außerdem so festgelegt werden sollte, dass sie dem Grundsatz einer effektiven Lösung entspricht. Darüber hinaus muss der für die Datenverarbeitung Verantwortliche die Behörde über die beabsichtigte Verarbeitung benachrichtigen, bevor diese beginnt.

Beschluss 42/2013

Nach Beschwerden und der Durchführung von Verwaltungsprüfungen erlegte die Datenschutzbehörde einem Unternehmen für die unrechtmäßige Erfassung und darauffolgende Nutzung personenbezogener Daten für das Versenden unerwünschter E-Mails zu Direktmarketing- und Werbezwecken eine Geldbuße in Höhe von 2 000 EUR auf. Außerdem ordnete die Behörde die Vernichtung der Datei mit den E-Mail-Adressen an. Zur Ermittlung der Bußgeldsumme wurden unter anderem die schwierige wirtschaftliche Situation des Unternehmens und die Zusammenarbeit der Vertreter während der von der Datenschutzbehörde durchgeführten Verwaltungsprüfung berücksichtigt.

Beschluss 109/2013

Mit ihrem Beschluss 109/2013 erlegte die griechische Datenschutzbehörde einer Bank eine Geldbuße in Höhe von 75 000 EUR auf, da diese zu Werbezwecken Datensätze mit unrechtmäßig erfassten personenbezogenen Daten erworben hatte. Insbesondere wurden die Daten ohne die Einwilligung der betroffenen Personen erfasst. Diese stammten weder aus öffentlich zugänglichen, für diese Zwecke vorgesehenen Quellen noch hatten die betroffenen Personen ihre Daten zu ähnlichen Zwecken offengelegt. All dies war der Bank bekannt. Die Datenschutzbehörde ordnete außerdem die Vernichtung aller relevanten Banklisten an. Im Rahmen desselben Beschlusses sprach die Datenschutzbehörde eine Empfehlung an die Bank aus, die Bestimmungen von Artikel 11 der geltenden Fassung des Gesetzes 3471/2006 zum Schutz personenbezogener Daten und der Privatsphäre im Sektor der elektronischen Telekommunikation in Bezug auf Werbung für Produkte und Dienstleistungen sowie die einschlägigen Gesetze und Verordnungen der Datenschutzbehörde einzuhalten.

Beschluss 58/2013

Die Datenschutzbehörde urteilte, dass die Verarbeitung einfacher und sensibler Daten von Menschen mit Behinderung zum Zwecke der Ausnahme von der Mautgebühr ein rechtmäßiger Zweck für eine Verarbeitung darstellt. Die Erfassung und Pflege der personenbezogenen Daten von Menschen mit Behinderung per Sonderantragsformular, wie es derzeit praktiziert wird, stellt jedoch eine unrechtmäßige Verarbeitung personenbezogener Daten dar. Das Unternehmen sollte weniger personenbezogene Daten erfassen, um Menschen mit Behinderung von Mautgebühren auszunehmen, und außerdem dafür sorgen, dass Menschen mit Behinderung über die Erfassung personenbezogener Daten sowie über die Vertraulichkeit und Sicherheit der Verarbeitung informiert werden.

Beschluss 98/2013

Die Datenschutzbehörde erlegte dem Generalsekretariat für Informationssysteme (G.S.I.S.) das höchstmögliche Bußgeld auf und urteilte, dass es seine Verpflichtung, angemessene Sicherheitsvorkehrungen zu ergreifen, verletzt und dies zu einem besonders schwerwiegenden Durchsickern personenbezogener Daten – fast aller Steuerzahler in Griechenland – geführt hat. Die Behörde urteilte, dass die G.S.I.S. trotz der von ihm verwalteten Datenmenge und der Sensibilität der Daten bis Juli 2013 keine angemessenen technischen und organisatorischen Sicherheitsvorkehrungen getroffen hat, um den unrechtmäßigen Zugang zu den Daten und deren Verbreitung zu verhindern, bzw. keine Maßnahmen für die Identifizierung potenzieller Datenschutzzwischenfälle ergriffen hat.

Beschluss 136/2013

Die Datenschutzbehörde urteilte, dass die Bereitstellung des Dienstes „Street View“ von Google, Inc. – unter den in Beschluss 53/2011 genannten Bedingungen – in Bezug auf den Dienst Google Maps sowie unter bestimmten Bedingungen, wie die Inkenntnissetzung der betroffenen Personen vor Beginn der Datenverarbeitung und die Wahrung der Rechte auf Zugang und Widerspruch, rechtmäßig ist. Das Unternehmen muss diese Rechte innerhalb einer Frist von fünf Tagen wahren.

Beschluss 138/2013

Die Datenschutzbehörde untersuchte das elektronische Verschreibungssystem im Hinblick auf den Schutz und die Sicherheit personenbezogener Daten. Da der Betrieb und die Pflege des elektronischen Verschreibungssystems unter der Aufsicht des Ministeriums für soziale Sicherheit (GGKA) vollständig an ein Unternehmen ausgelagert wurde, fand die Prüfung ausschließlich in den Räumen von IDIKA und seinen Subunternehmern statt. Die Datenschutzbehörde bat den für die Datenverarbeitung Verantwortlichen (GGKA), innerhalb von zwei Monaten ab Beschlussdatum einen genauen Zeitplan für die Umsetzung der Empfehlungen, die im Rahmen des Beschlusses erteilt wurden, einzureichen sowie die im vertraulichen Anhang dargelegten Themen zu bearbeiten. Der Zeitplan muss außerdem alle Abhilfemaßnahmen abdecken, die in der laufenden Ausschreibung für das neue elektronische Verschreibungssystem enthalten sind und noch nicht umgesetzt wurden. Des Weiteren forderte die Datenschutzbehörde den für die Datenverarbeitung Verantwortlichen auf, vierteljährliche Fortschrittsberichte einzureichen. Schließlich bat die Datenschutzbehörde den für die Datenverarbeitung Verantwortlichen, im einzureichenden Antrag auf Erneuerung der Erlaubnis für die Verarbeitung sensibler Daten die neuen Maßnahmen zu beschreiben, die in der Zwischenzeit ergriffen worden sein werden.

Videoüberwachungssysteme:

Beschluss 49/2013

Drei Privatschulen installierten Videoüberwachungssysteme, um auf ihrem Gelände Diebstählen und Vandalismus vorzubeugen und die Sicherheit der Schüler und Mitarbeiter zu gewährleisten. Die Schulen

wollten das System rund um die Uhr betreiben und beantragten die Ausnahme von Artikel 18 der Richtlinie 1/2011 der Datenschutzbehörde zur Installation von Videoüberwachungssystemen, die vorsieht, dass Videoüberwachungssysteme in Schulen nur außerhalb der Schulzeiten betrieben werden dürfen. Die Datenschutzbehörde lehnte den Antrag ab, da die Schulen keine neuen Vorschläge unterbreiteten, die eine Ausnahme von dieser Bestimmung rechtfertigen würden. Des Weiteren wurde das, was sie beantragten, bereits bei der Erarbeitung des Entwurfs besagter Richtlinie durch die Datenschutzbehörde berücksichtigt.

Beschluss 78/2013

In diesem Fall prüfte die Datenschutzbehörde die Beschwerde eines Elternteils bezüglich eines Kindergartens, der ein Videoüberwachungssystem in den Gruppenräumen, im Hof, im Eingangsbereich und im Büro der Kindergartenleitung installiert hatte, das den ganzen Tag in Betrieb war. Hierüber wurden weder die Eltern noch die Datenschutzbehörde informiert. Die Kindergartenleitung erstattete bei der Datenschutzbehörde Meldung und erklärte, dass ein solches System aufgrund der Größe der Anlage installiert worden sei, weil es bereits mehrere Unfälle mit Kindern gegeben habe, und dass die Eltern ordnungsgemäß informiert worden seien. Die Datenschutzbehörde kam zu dem Schluss, dass der Grundsatz der Verhältnismäßigkeit nicht eingehalten wurde, und sprach dem Kindergarten eine Verwarnung aus, die Kameras aus den Gruppenräumen zu entfernen und dafür zu sorgen, dass die Kameras im Hof am Rand installiert werden, dass es keine Überwachungsbildschirme gibt und dass die Daten (außer im Falle von Zwischenfällen) am nächsten Werktag gelöscht werden. Des Weiteren riet die Datenschutzbehörde dem Kindergarten, die Rechte auf Zugang und Widerspruch zu respektieren.

Beschluss 59/2013

Bei diesem Fall ging es um ein Videoüberwachungssystem, das in einem öffentlichen Gebäude (Rathaus) installiert worden war, um staatliches Eigentum und insbesondere eine Reihe von Denkmälern in der Umgebung vor Vandalismus zu schützen, da diese in den vergangenen zwei Jahren stark beschädigt worden waren. Das System wurde als notwendig erachtet, da im Vorfeld bereits mildere Maßnahmen wie eine bessere Beleuchtung und Polizeipatrouillen ergriffen worden waren, diese jedoch keine Wirkung zeigten. Die Datenschutzbehörde forderte den für die Datenverarbeitung Verantwortlichen dazu auf, das aktuelle Videoüberwachungssystem so zu modifizieren, dass Folgendes gegeben ist: i) nur die Denkmäler sollen aufgezeichnet werden, ii) die Monitore sollen entfernt und lediglich das Aufzeichnungssystem beibehalten werden, iii) die Systempasswörter sollen nur einer bestimmten Person bekannt sein, der die Sicherheitsleitung für das Videoüberwachungssystem übertragen wird, iv) der Zugang zu den Bilddaten und eine Installation von Monitoren soll nur möglich sein, wenn sich ein Zwischenfall ereignet hat und dies schriftlich vom Bürgermeister beantragt wird.

IRLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

2013 eröffnete das Amt des Datenschutzbeauftragten 910 Verfahren zur Untersuchung von Beschwerden (viele Beschwerden werden informell bearbeitet, indem Beschwerdeführer angemessen über ihre Rechte informiert werden). 2013 wurden 1 290 Beschwerdeverfahren abgeschlossen. Wie in den Jahren zuvor konnte die überwiegende Mehrheit der Beschwerden gütlich beigelegt werden; nur 29 Beschwerden gaben Anlass zu formellen Beschlüssen. Die Verfahren richteten sich gegen Unternehmen, die sich im Bereich Marketing nicht an die Regelungen zur Privatsphäre in der elektronischen Kommunikation (Rechtsverordnung 336/2011 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 2013 sind in Abschnitt B dieses Berichts enthalten. Die Anzahl der Meldungen von Verstößen gegen den Schutz personenbezogener Daten blieb konstant (1 507 im Jahr 2013). Somit setzt sich die Entwicklung infolge der Einführung des Verhaltenskodex für Verstöße gegen den Schutz personenbezogener Daten im Jahr 2010 fort. Bei einem schwerwiegenden Verstoß gegen die Datensicherheit, an dem ein in Irland ansässiger für die Datenverarbeitung Verantwortlicher beteiligt war, der mit einer Reihe von für die Datenverarbeitung Verantwortlichen in ganz Europa Verträge abgeschlossen hatte, erteilte der Datenschutzbeauftragte einen Vollstreckungsbescheid, der den für die Datenverarbeitung Verantwortlichen an der Datenverarbeitung hinderte, bis bestimmte Anforderungen im Zusammenhang mit der Datensicherheit erfüllt sind. Das Amt des Datenschutzbeauftragten führte außerdem gemäß den Anforderungen der Verordnung 611/2013 der Europäischen Kommission ein Online-Formular zur Meldung von Verstößen gegen das Datenschutzgesetz durch Telekommunikations- und Internetserviceanbietern ein.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Billy Hawkes
Budget	Budget: 1 727 000 EUR. Ausgegeben: 1 960 999 EUR.
Personal	30 (Stand: 31. Dezember 2013)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	29 formelle Beschlüsse
Meldungen	5 778
Vorabprüfungen	k. A.
Anträge betroffener Personen	12 000 Anfragen per E-Mail. Außerdem schriftliche Anträge.
Beschwerden betroffener Personen	910
Vom Parlament bzw. der Regierung angeforderte Beratung	Regelmäßige informelle Konsultationen zu Gesetzesvorschlägen/Vorschlägen von Rechtsvorschriften.
Sonstige Informationen zu einschlägigen allgemeinen	1 507 Meldungen über Verletzungen der Datensicherheit.

Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	44 Audits (Prüfungen)
Sanktionsmaßnahmen	
Sanktionen	101 Verfahren gegen 14 Rechtssubjekte
Geldbußen	Es wurden Geldbußen in Höhe von 35 600 EUR zuzüglich Kosten verhängt. Des Weiteren wurden Spenden zu wohltätigen Zwecken gemäß dem Probation Act in Höhe von 27 750 EUR zuzüglich Kosten gerichtlich angeordnet.
Datenschutzbeauftragte (DPO)	k. A.
Zahlenangaben zu DPO	

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 Datenverarbeitung Verantwortliche die Zugriffsrechte betroffener Personen missachten. In einem Fall (siehe Abschnitt A) wurde ein Vollstreckungsbescheid erteilt, der einen für die Datenverarbeitung Verantwortlichen an der Datenverarbeitung hindern sollte, bis bestimmte Anforderungen im Zusammenhang mit Datensicherheit erfüllt sind. In einigen Fällen werden für die Datenverarbeitung Verantwortliche in Fallstudien erwähnt, die im Jahresbericht des Datenschutzbeauftragten enthalten sind. Im Jahr 2013 beteiligte sich der Datenschutzbeauftragte an mehreren erfolgreichen strafrechtlichen Verfolgungen 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 Zusammenhang mit unerwünschten Marketing-SMS und -E-Mails. 2013 wurden 101 Verfahren gegen 14 Rechtssubjekte eingeleitet.

C. Sonstige wichtige Informationen

Der Datenschutzbeauftragte tauschte sich auch weiterhin mit großen öffentlichen Organisationen über den Datenschutz aus. Das Amt des Datenschutzbeauftragten hat jetzt die Prüfungen dreier großer staatlicher Stellen abgeschlossen, die personenbezogene Daten speichern: das Ministerium für Sozialschutz, das Finanzamt und die irische Polizei An Garda Síochána.

Die Prüfung des Datenschutzes bei der An Garda Síochána fand von 2011 bis Oktober 2013 statt. Der Bericht wurde von der An Garda Síochána im März 2014 veröffentlicht. Ein Schwerpunkt der Prüfung lag auf dem IT-Hauptsystem PULSE, das die An Garda Síochána zur Speicherung von Daten nutzt.

Die Prüfung zeigte Bereiche auf, in denen Verbesserungen erforderlich sind. Im Großen und Ganzen zeigten die meisten überprüften Bereiche, dass die irische Polizei professionell und im Einklang mit dem Datenschutzgesetz agiert. Das Amt des Datenschutzbeauftragten begann 2013 außerdem eine Prüfung von LinkedIn Ireland.

ITALIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetzesänderungen

Datenschutzgesetz (Rechtsverordnung Nr. 196 vom 30. Juni 2003)

Abschnitt 19 Absatz 3-bis des Datenschutzgesetzes wurde durch Abschnitt 53 Absatz 1 lit e) der Rechtsverordnung Nr. 33 vom 14. März 2013 aufgehoben. Die Formulierung dieses Absatzes wurde jedoch auf Abschnitt 4 Absatz 5 der besagten Rechtsverordnung verlegt („Der staatliche Arbeitgeber muss die Informationen betreffend der Erledigung der Aufgaben eines Angestellten des öffentlichen Diensts sowie die jeweilige Beurteilung verfügbar machen. Nach Maßgabe des Rechts dürfen keine Informationen über die Art der Erkrankungen bzw. persönliche oder familiäre Umstände, die sich aus der Abwesenheit einer Person vom Arbeitsplatz ergeben, oder die Elemente der Beurteilung oder jegliche Informationen zum Beschäftigungsverhältnis zwischen dem oben genannten Angestellten des öffentlichen Diensts und dem staatlichen Arbeitgeber offengelegt werden, falls diese für eine Offenlegung von Informationen gemäß Abschnitt 4 Absatz 1 lit d) geeignet sind.

Die aktuelle Version des Datenschutzgesetzes ist über folgenden Link in englischer Sprache einsehbar: http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf

Hauptaktivitäten

Datenverarbeitung im öffentlichen Sektor

Die Datenschutzbehörde gab am 7. Februar 2013 ihre Stellungnahme zum Entwurf der Rechtsverordnung Nr. 14 (angenommen am 14. März 2013) ab, die spezifische Transparenzvorschriften für öffentliche Stellen enthält (wie z. B. Veröffentlichungen auf der Website der jeweiligen Stelle). Der Garante wies auf einige kritische Punkte des Entwurfs hin und machte spezifische Vorschläge zur Abstimmung von Transparenz und Schutz personenbezogener Daten, wie zum Beispiel: Vermeidung der Verbreitung bestimmter Datenkategorien, wie solche zur Gesundheit der betroffenen Personen; Vermeidung der Auffindbarkeit von im Internet veröffentlichten Daten durch allgemeine Suchmaschinen wie Google (interne Suchmaschinen sind zu bevorzugen); Festlegung des Zeitraums, in dem das Veröffentlichen von Daten auf Websites im Hinblick auf Transparenz als verhältnismäßig angesehen werden kann; Beschränkung der Veröffentlichung von Daten auf Mitarbeiter des öffentlichen Sektors auf streng relevante Daten; Einschränkung der Veröffentlichung von Daten von Personen, die politische Ämter bekleiden, unter Berücksichtigung der Anforderungen an die Verhältnismäßigkeit.

Bekämpfung von Steuerhinterziehung

Die Datenschutzbehörde ordnete infolge von spezifischen Untersuchungen Maßnahmen im Zusammenhang mit Verarbeitung durch die Steuerbehörde zur genauen Beurteilung des Einkommens natürlicher Personen zur Bekämpfung von der Steuerhinterziehung (21. November 2013) an. Mit den Maßnahmen sollte erreicht werden, dass die betreffende Aktivität zur Betrugsbekämpfung unter Einhaltung des Schutzes personenbezogener Daten durchgeführt wird. Sie bestanden insbesondere aus spezifischen Anpassungen durch die Behörde hinsichtlich der Kriterien für das Erstellen von Steuerzahlerprofilen und für die Auswahl der zu prüfenden Einzelpersonen. Des Weiteren wurden Vorkehrungen bezüglich der Datenqualität, der Datenaufbewahrung, der Informationen, die betroffenen Personen bezüglich der Datenverarbeitung bereitgestellt werden, sowie der Möglichkeit, von der Steuerbehörde angehört zu werden, festgelegt.

Justiz

Die Datenschutzbehörde legte Maßnahmen und Vorkehrungen fest, die Staatsanwälte in Italien umsetzen müssen, um die Sicherheit der von ihnen erfassten und von ihnen im Rahmen von Abhörungen genutzten Daten zu erhöhen (24. Juli 2013). Zu den Maßnahmen gehörten sowohl physische Sicherheitsmaßnahmen (wie z. B. der Zugang zu Räumlichkeiten nur durch individuell zugewiesene Ausweisen und dazugehörigen numerischen Codes oder auf biometrischen Daten beruhenden Geräten; die Aufzeichnung aller Zugänge; Videoüberwachung der Räumlichkeiten) als auch IT-Sicherheitsvorkehrungen (wie z. B. die Nutzung spezieller Arbeitsplätze und strenge Autorisierungsverfahren für den Zugang zu Systemen und Servern; Aufzeichnung aller Abhöraktivitäten; verschlüsseltes Kopieren auf tragbare Medien; verschlüsselte Speicherung der Originaldokumente und Sicherungskopien; Nutzung sicherer Netzwerkprotokolle beim Datenaustausch zwischen Justizbehörden und Internetanbietern).

Nachrichtendienste

Infolge der Enthüllungen durch Edward Snowden wurde von der italienischen Datenschutzbehörde und der Abteilung für Informationssicherheit des Präsidiums des Ministerrats eine Absichtserklärung unterzeichnet (11. November 2013). Damit sollen umfassende Schutzmechanismen für die Rechte des Einzelnen gewährleistet werden, dessen personenbezogene Daten zu Nachrichtendienstzwecken verarbeitet werden, insbesondere hinsichtlich der folgenden Punkte: Überwachung durch den Garante bezüglich Nachrichtendiensten und Mechanismen für die Beurteilung des Zugangs von Nachrichtendiensten zu personenbezogenen Daten in Datenbanken des öffentlichen Sektors.

Marketing

Die Datenschutzbehörde musste mehrmals im Bereich Marketing eingreifen. Sie gab Leitlinien zu Marketing und Spam (einschließlich des sogenannten Social Spams, viralen Marketings und zielgerichteten Marketings) heraus. Darin war ein gebündeltes Maßnahmen- und Vorkehrungspaket enthalten, das sowohl Unternehmen, die eine Marketingkampagne für ihre Produkte und Dienstleistungen planen, als auch Einzelpersonen zugute kommt, die sich gegen unerwünschte Werbung zur Wehr setzen möchten (4. Juli 2013). Die Datenschutzbehörde stellte in einem separaten Beschluss klar, dass es für alle Marketingaktivitäten – wie z. B. Versendung von Werbe-E-Mails oder Durchführung von Marktbefragungen – ausreicht, die Einwilligung ein einziges Mal einzuholen. Die Einwilligung in den Erhalt automatisierter Werbenachrichten (E-Mails, SMS) gilt auch für Nachrichten, die über weniger in die Privatsphäre eingreifende Kanäle, wie z. B. per Post oder durch Anrufe mit Unterstützung durch das Vermittlungspersonal, übermittelt werden, vorausgesetzt, dass Nutzer angemessen darüber informiert werden und die Möglichkeit erhalten, ihre jeweiligen Präferenzen frei zum Ausdruck zu bringen (15. Mai 2013). Genaue Regelungen wurden für öffentliche und private Stellen festgelegt, die den Einsatz von Call-Centern außerhalb der EU planen. Neben der Erinnerung an die Anforderungen, die für eine Übermittlung personenbezogener Daten (insbesondere Kundendaten) an Drittländer erfüllt werden müssen, wies die Datenschutzbehörde den betroffenen für die Datenverarbeitung Verantwortlichen an, den Kunden des Unternehmens spezifische Informationen bereitzustellen und ihnen die Möglichkeit zu geben, sich bezüglich eingehender Anrufe für Betreiber zu entscheiden, die in Italien ansässig sind (10. Oktober 2013). Der Garante legte spezifische Maßnahmen zur Vermeidung von stillen Anrufen fest, die einen wesentlichen Anlass für Besorgnis der Nutzer darstellen, und hielt diesbezüglich eine öffentliche Konsultation ab. Zu den Maßnahmen gehören insbesondere die Beendigung stiller Anrufe (d. h. Anrufe, bei denen kein Telefonist zum Annehmen des Anrufs verfügbar ist) innerhalb von drei Sekunden nach Abheben durch den Angerufenen; eine Obergrenze von drei stillen Anrufen pro 100 erfolgreichen Anrufen (pro Telemarketing-Kampagne); ein Verbot von wiederholten Anrufen vor Ablauf einer Woche nach dem stillen Anruf sowie die Speicherung von Statistiken zu stillen Anrufen für mindestens zwei Jahre, um Aufsichtsführung zu ermöglichen.

Profiling durch Telefongesellschaften

Telefongesellschaften erhielten von der Datenschutzbehörde die Erlaubnis, anhand von Aggregatdaten über einen kürzeren Zeitraum (zwei Tage anstatt des bisherigen Monats) Profiling-Aktivitäten durchzuführen. Der Hauptgrund für diesen Beschluss war der wachsende Gebrauch von Nummernübertragbarkeitsoptionen und die breitere Palette an Datenangeboten (und -profilen), die Kunden zur Verfügung stehen. Die betreffenden Aggregatdaten umfassen Ursprungs- und Zielverkehr-Volumina (in Minuten oder Bytes), die Anzahl der Aufladungen (pro Verkaufskanal, d. h. online, Geldautomat, Bankkarten) sowie die Gesamtanzahl der Aufladungen. Alle weiteren, von der Datenschutzbehörde in früheren Beschlüssen festgelegten Schutzmechanismen behalten ihre Gültigkeit – einschließlich der Nutzung spezieller IT-Systeme für Profiling sowie strenge Sicherheitsmaßnahmen für den Datenzugang.

Mobile Zahlungen

Die Datenschutzbehörde verabschiedete einen Beschluss zu mobilen Zahlungen (12. Dezember 2013) und führte damit spezifische Mechanismen zum Schutz personenbezogener Daten von Nutzern ein, die durch direkte Belastung ihrer Telefonrechnungen über so genannte mobile Fernzahlungssysteme Zahlungen vornehmen. Diese Zahlungsweise verbreitet sich immer weiter und zieht die Verarbeitung mehrerer personenbezogener (und manchmal sensibler) Daten, wie z. B. Zensusdaten, die Art der gekauften Dienstleistung oder des gekauften Produkts sowie das Datum und die Uhrzeit des Kaufs, nach sich. Die Schutzmechanismen – die eine spezifische Informationsmeldung, Einwilligung im Falle von Marketing und Profiling, Sicherheitsmechanismen und Datenaufbewahrungsrichtlinien umfassen – richten sich an die drei größten Interessenvertreter, die an mobilen Zahlungsdiensten beteiligt sind (die Anbieter, d. h. Anbieter elektronischer Kommunikationsdienste; zentrale Zahlungsstellen, welche die technologischen Plattformen für mobile Zahlungsdienste bereitstellen und verwalten; Händler, die digitale Inhalte, Multimedia- und andere Produkte anbieten und verkaufen).

Google Street View

Die Datenschutzbehörde erlegte Google aufgrund seines Street-View-Dienstes eine Geldbuße in Höhe von einer Millionen Euro auf. Grund dafür war insbesondere ein Vorfall, bei dem unrechtmäßig erfasste Daten in einer großen Datenbank gespeichert wurden, die von Google im Zusammenhang mit dem Street-View-Dienst eingerichtet worden war. Angesichts Googles Konzernumsatzes in Höhe von über 50 Milliarden Dollar im Jahr 2012 berief sich der Garante des Weiteren auf die Bestimmung des Datenschutzgesetzes, die vorsieht, dass großen Unternehmen effektive Sanktionen auferlegt werden.

Verstöße gegen den Schutz personenbezogener Daten

Die Datenschutzbehörde nahm einen allgemeinen Beschluss an, der die bislang geltenden Leitlinien laut Absatz 6 des Abschnitts 32-bis des Gesetzes (Umsetzung der Richtlinie 136/2009/EG) ersetzt, um Leitlinien und Anweisungen im Hinblick auf Umstände, unter denen Anbieter elektronischer Kommunikationsdienste dazu verpflichtet sind, Verstöße gegen den Schutz personenbezogener Daten zu melden, sowie das Format solcher Meldungen und die einschlägigen Durchführungsbestimmungen bereitzustellen (4. April 2013).

Methoden der graphometrischen Authentifizierung

Die Datenschutzbehörde genehmigte zwei Anträge auf Vorabprüfung von Banken, die beabsichtigten, zu Kundenauthentifizierungszwecken graphometrische Authentifizierungsmethoden zu nutzen. Die Datenschutzbehörde forderte die strikte Einhaltung des Grundsatzes der Zweckbindung und die Verfügbarkeit von Alternativverfahren für Nutzer, die diese Authentifizierungsmethode nicht nutzen wollen oder können. Außerdem müssen die Datenaufbewahrungsmaßnahmen mit dem Grundsatz der Verhältnismäßigkeit in Einklang stehen.

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 sich seine Sachverständigen in der italienischen Delegation an der DAPIX-Arbeitsgruppe des Rates beteiligten.

Die Datenschutzbehörde wirkte aktiv an der Arbeit der OECD und des Europarats mit, insbesondere über die Arbeitsgruppe zu Informationssicherheit und Datenschutz (vormals WPISP, jetzt WPSPDE) 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 so genannten Berlin Group (Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation).

Sowohl auf europäischer als auch auf internationaler Ebene war das Jahr 2013 außerdem durch die wichtige Arbeit der Datenschutzbeauftragten hinsichtlich einer engeren und effektiveren Kooperation gekennzeichnet, insbesondere im Durchsetzungsbereich spezifischer Arbeitsgruppen, an denen die italienische Datenschutzbehörde beteiligt ist (GPEN, IECWG, Phaedra-Projekt usw.). Die Datenschutzbehörde setzte ihre Arbeit im Rahmen der Programme IPA, TAIEX und Twinning der Europäischen Kommission für neue Beitrittsländer, Beitrittskandidaten (Türkei, Kroatien bis Juni 2013, ehemalige jugoslawische Republik Mazedonien) und die ENP-Länder fort.

Organisation	Italienische Datenschutzbehörde
Vorsitz und/oder Gremium	Vorsitzender des Gremiums: Dr. Antonello SORO Gremium: Augusta IANNINI Giovanna BIANCHI CLERICI Licia CALIFANO
Budget	Ungefähr 8,4 Mio. EUR (von der Regierung bereitgestellt)
Personal	122
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Anzahl der Beschlüsse des Gremiums: **606**
Meldungen	**1 656**
Vorabprüfungen	**24**
Anträge betroffener Personen	Anfragen insgesamt: etwa **4 700** Auskunftsersuchen („questiti“): **311** 2012 von betroffenen Personen eingereichte Berichte und Forderungen („segnalazioni“ und „reclami“): **4 393**
Beschwerden betroffener Personen	(durch das Datenschutzgesetz speziell geregelte formelle Beschwerden betreffend den Zugang zu den eigenen

	personenbezogenen Daten): 222
Vom Parlament bzw. der Regierung angeforderte Beratung	22
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Im Frontoffice der Datenschutzbehörde gingen 2013 rund 31 000 Anrufe und E-Mails ein
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen bzw. Untersuchungen (vor Ort): 411
Sanktionsmaßnahmen	
Sanktionen	Etwa 850
Geldbußen	Betrag: etwa 4 Mio. EUR, im Namen der Datenschutzbehörde von der für Kontrollen zuständigen Finanzpolizei verhängt
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Oberster Gerichtshof – Rechtssache Google Vividown – Keine strafrechtliche Verantwortlichkeit aufseiten von Hostingdienstleistern

Die dritte Kammer für Strafsachen des italienischen Obersten Gerichtshofs veröffentlichte (per Beschluss Nr. 8611/2013) die Begründung ihres Freispruchs dreier Führungskräfte von Google, die 2010 in erster Instanz zu sechs Monaten Gefängnis verurteilt worden waren, nachdem auf der Videoplattform von Google ein Video hochgeladen worden war, das einen minderjährigen Behinderten zeigte, der von Klassenkameraden gedemütigt wurde. Laut Oberstem Gerichtshof können Internet-Hostinganbieter im Falle eines Verstoßes gegen das Datenschutzgesetz aufgrund hochgeladener Videos nicht strafrechtlich verantwortlich gemacht werden. Dieser äußerst wichtige Beschluss erklärt, dass „die vorliegenden Vergehen gemäß Abschnitt 167 des Datenschutzgesetzes als Pflichtverstöße auszulegen sind, da wir es hier mit einem Verhalten zu tun haben, das nur zu einem Verstoß gegen die Verpflichtungen des Besitzers der verarbeiteten Daten und keiner anderen Person, die in irgendeiner Weise mit den verarbeiteten Daten umgeht, jedoch ohne eine damit verbundene Entscheidungsbefugnis ist, geführt hat“. Der Oberste Gerichtshof wies außerdem darauf hin, dass der Hostingdienstleister „weder die Kontrolle über die gespeicherten Daten hat noch in irgendeiner Weise zur Auswahl oder Recherche der Daten oder zur Erstellung der die Daten enthaltenen Datei beiträgt. Solche Daten sind einzig und allein den Nutzern des Dienstes zuzuschreiben, die sie auf die Plattform laden, die ihnen zur Verfügung gestellt wird“.

Kassationsgericht (Oberster Gerichtshof) – Verbraucher haben das Recht, zeitnah über negative, sie betreffende Meldungen informiert zu werden

In einer Entscheidung der Zivilkammer des Kassationsgerichts (Nr. 349/2013), die sich mit Verbraucherrechten befasst, wurde geurteilt, dass Verbraucher das Recht haben, zeitnah über negative, sie betreffende Meldungen informiert zu werden. Das Gericht befand die Beschwerde eines Finanzunternehmens gegen das Urteil der Mailänder Vorinstanz – aus Gründen der gerichtlichen Zustellung – als unzulässig. In dieser Rechtssache stellte die betroffene Person, nachdem diese von einer „negativen Meldung" im Zusammenhang mit einem Kredit, der ihr 2003 gewährt worden war, 2008 einen entsprechenden Antrag auf Zugang zur Datenbank des Unternehmens und legte daraufhin beim Gericht in Mailand Klage ein, als sie diesbezüglich keine Antwort erhalten hatte. Der Oberste Gerichtshof bestätigte das Recht des Verbrauchers, prompt über seine Position in den Archiven des Finanzunternehmens informiert zu werden, und wies insbesondere darauf hin, dass der für die Datenverarbeitung Verantwortliche dazu verpflichtet ist, den Login-Antrag „ohne Verzögerung" zu prüfen. Dementsprechend berücksichtigte das erstinstanzliche Gericht die 15-tägige Frist, die dem für die Datenverarbeitung Verantwortlichen im Gesetz für eine Bearbeitung des Antrages eingeräumt wird, und kam zu dem Schluss, dass eine solche Frist hierfür angemessen ist.

Kassationsgericht (Oberster Gerichtshof) – Unrechtmäßiger Eingriff in die Privatsphäre

Die Strafkammer des Kassationsgerichts lehnte (per Beschluss Nr. 8762/2013) ein Rechtsmittel gegen das Urteil des Berufungsgerichts Florenz ab, das den Beklagten wegen eines Verstoßes gegen Artikel 615-bis des italienischen Strafgesetzbuches verurteilt hatte, nachdem dieser ein Gespräch zwischen seiner Schwester und seiner Freundin mit einem in der Wohnung versteckten Aufnahmegerät aufgenommen hatte. Das Gericht erklärte unter Berufung auf die ständige Rechtsprechung, dass das Vergehen eines unrechtmäßigen Eingriffs in das Privatleben auch im Falle einer unfairen Aufzeichnung wie dieser besteht, und wies darauf hin, dass zu Zwecken der Anwendung von Artikel 615-bis des Strafgesetzbuches mit „Zuhause (dem Privatwohnort) auch der Ort gemeint ist, an dem sich ein großer Teil des emotionalen Lebens abspielt, selbst wenn dies nicht gewöhnlich …". Aus dem Urteil ging besonders hervor, dass eine Person davon ausgeht, dass an einem solchen Ort in der Regel ihre Privatsphäre geschützt ist, und sie demnach besonders anfällig ist für böswilliges, unfaires Verhalten von Personen, denen sie emotional nahesteht.

C. Sonstige wichtige Informationen

Die Datenschutzbehörde brachte ihr Interesse daran zum Ausdruck, den italienischen Staat in der Rechtssache C-46/13 des Europäischen Gerichtshofs (Vorabentscheidungsersuchen gemäß Artikel 267 TFEU) zur Auslegung von Artikel 7 lit c) der Richtlinie 2006/24/EG anzuhören: Mit den Fragen an den Europäischen Gerichtshof wollte die österreichische Datenschutzkommission u. a. insbesondere klarstellen, ob Artikel 7 lit c) der Richtlinie 2006/24/EG dahingehend auszulegen ist, dass eine von der Vorratsspeicherung betroffene natürliche Person nicht zum Kreis der „besonders ermächtigten Personen" im Sinne dieser Bestimmung zählt und ihr kein Recht auf Auskunft über ihre eigenen Daten gegenüber dem Anbieter eines öffentlich zugänglichen Kommunikationsdienstes oder dem Betreiber eines öffentlichen Kommunikationsnetzes eingeräumt werden darf. Die italienische Datenschutzbehörde unterstrich, dass betroffene Personen gemäß Abschnitt 7 und 8 des italienischen Datenschutzgesetzes auf alle eigenen personenbezogenen Daten, die von einem Dienstleister verarbeitet werden, zugreifen kann, außer auf eingehende Anrufe, es sei denn, dass dies tatsächlich und konkret für die Leistung der Untersuchungen durch den Verteidiger abträglich sein könnte.

KROATIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	
Vorsitz und/oder Gremium	Anto Rajkovača
Budget	5 482 847 HRK (1 EUR = 7,5 HRK)
Personal	28
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	1 091
Meldungen	21 978 (1 648 im Jahr 2013)
Vorabprüfungen	
Anträge betroffener Personen	Die Anträge werden nicht separat registriert.
Beschwerden betroffener Personen	212
Vom Parlament bzw. der Regierung angeforderte Beratung	17
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Nach einer Umstrukturierung konzentriert sich die Datenschutzbehörde nun vermehrt auf Prüfmaßnahmen.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	330
Sanktionsmaßnahmen	
Sanktionen	87
Geldbußen	2
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	2 037 registrierte DPO (643 im Jahr 2013)

Im Berichtszeitraum engagierte sich die kroatische Datenschutzbehörde stark für eine Sensibilisierung der Öffentlichkeit zum Thema Datenschutz. Im Folgenden informieren wir Sie über die wichtigsten Aktivitäten, die in diesem Zeitraum durchgeführt wurden:

- Die Einführung der „Roten Taste“, eines Online-Formulars zur Meldung sexuellen Missbrauchs oder der Ausbeutung von Kindern, das das Innenministerium in Zusammenarbeit mit der Partnerschaft zur Schaffung eines funktionierenden „Zentrums für sichereres Internet“ (bei der die kroatische Datenschutzbehörde einer der strategischen Partner ist) ins Leben gerufen hat, um die Öffentlichkeit in Bezug auf eine sichere Nutzung des Internets zu sensibilisieren und eine sichere, verantwortungsvolle, angemessene und effiziente Nutzung des Internets durch Kinder und Jugendliche zu fördern.

- Am Tag des Datenschutzes 2013 organisierte die Datenschutzbehörde eine Gala-Pressekonferenz mit verschiedenen Aktivitäten, wie z. B. die Ernennung der neuen Datenschutz-Botschafter (berühmte Persönlichkeiten, die trotz ihrer Popularität einen sehr guten Ruf genießen), deren Aufgabe es ist, die Privatsphäre und den Schutz personenbezogener Daten zu fördern

- Anlässlich des 10-jährigen Jubiläums organisierte die Datenschutzbehörde (im Mai 2013) zahlreiche Aktivitäten, die von der kroatischen Öffentlichkeit sehr gut aufgenommen wurden. Hierbei handelte es sich um Folgendes:

  1) **Die Gala-Pressekonferenz „10 Schritte zur Bekämpfung von Hassreden im Internet“** fand im kroatischen Parlament in Gegenwart vieler bedeutender Persönlichkeiten des politischen und kulturellen Lebens Kroatiens statt. Darunter befanden sich die Datenschutz-Botschafter, die äußerst dramatische Berichte zweier kroatischer Jugendlicher vortrugen, die aufgrund sehr aggressiven Cyber-Mobbings während ihrer Jugend – also einer ohnehin sehr heiklen Phase des Lebens – schwere Traumata erlitten. Auf diese Weise konnte der Öffentlichkeit eine sehr wichtige Botschaft zu den Folgen von Hassreden vermittelt werden. Ein detaillierter Bericht dieser Konferenz wurde zur besten Sendezeit im Rahmen des zentralen Informationsprogramms von NOVA TV ausgestrahlt, das in Kroatien die höchsten Einschaltquoten hat.Des Weiteren hielten Vertreter des Innenministeriums, des Akademischen Forschungsnetzwerks (CARNET) und des kroatischen Journalistenverbandes Vorträge und schilderten dabei ihre Sichtweisen zu diesem Thema.

  2) Die Datenschutzbehörde ist sehr stolz auf sein **Informationsmaterial** mit Aufklärungsbotschaften in Bezug auf das Thema Hassreden im Internet:

     - Aufklärungsplakat „10 Schritte zur Bekämpfung von Hassreden im Internet“;

     - Roll-up-Poster 1: „Lass uns auf positiven Wellen surfen“;

     - Roll-up-Poster 2: „Jeder trägt Verantwortung!“.

  3) **Die Konferenz der Datenschutz- und Informationsbeauftragen** mit fünf renommierten Gastrednern (Sachverständigen), die äußerst informative Vorträge zu den neuesten Trends im Bereich Datenschutz und verwandten Themen hielten.Die Datenschutzagentur wurde für ihre Initiative, eine solche Konferenz zu organisieren, sehr gelobt, da diese den mehr als 100 Besuchern viele nützliche Informationen lieferte.

LETTLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Als eine der Hauptentwicklungen wurde die Änderung des Datenschutzgesetzes ausgearbeitet (seit dem 7. März 2014 in Kraft). Die Änderungen sehen eine klarere Einbeziehung der betroffenen Personen in die Verarbeitung personenbezogener Daten vor, um damit einhergehende Probleme zu lösen (z. B. bei Fällen, in denen die betroffene Person den für die Datenverarbeitung Verantwortlichen um eine große Menge an Informationen bittet usw.). Die Änderungen betreffen außerdem den Bereich Videoüberwachung: Die Meldung einer solchen Datenverarbeitung bei der Datenschutzbehörde ist nur dann verpflichtend, wenn durch die Videoüberwachung erfasste personenbezogene Daten gespeichert werden. Mehrere Gesetzesänderungen haben die Arbeitsbelastung der Datenschutzbehörde, hauptsächlich in Bezug auf die Meldung von Videoüberwachung, erhöht.

Angesichts des weit verbreiteten Einsatzes von Videoüberwachung in Lettland hat die lettische Datenschutzbehörde gemeinsam mit dem Amt des Ombudsmanns zu diesem Thema eine breitere Diskussion angestoßen.

Organisation	DATENSCHUTZBEHÖRDE
Vorsitz und/oder Gremium	Vorsitzende: Signe Plūmiņa
Budget	2013: 265 317 LVL (oder 377 512 EUR)
Personal	19 (einschließlich Verwaltungspersonal)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Beschlüsse: keine statistischen Daten vorhanden; Stellungnahmen: keine statistischen Daten vorhanden; Empfehlungen: 2.
Meldungen	532
Vorabprüfungen	493
Anträge betroffener Personen	6
Beschwerden betroffener Personen	362
Vom Parlament bzw. der Regierung angeforderte Beratung	Keine statistischen Daten vorhanden; die Beratung des Parlaments bzw. der Regierung erfolgte häufig durch das Justizministerium, das auch die Meinung der Datenschutzbehörde berücksichtigt.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Gegen 8 Beschlüsse der Datenschutzbehörde wurde beim Leiter der Datenschutzbehörde Einspruch erhoben. Gegen 4 Beschlüsse der Datenschutzbehörde wurde bei einem Gericht Berufung eingelegt. Die wichtigsten Beschwerdegründe: Verstöße gegen das Zugangsrecht betroffener Personen (sowohl bezüglich der bereitzustellenden Informationen zu Beginn der Verarbeitung personenbezogener Daten als auch bezüglich der auf Antrag der betroffenen

	Person bereitzustellenden Informationen); Identitätsdiebstahl (sowohl online als auch offline).
Prüfmaßnahmen	
Prüfungen, Untersuchungen	677 (nur rund 5 % aus Eigeninitiative)
Sanktionsmaßnahmen	
Sanktionen	In 36 Fällen – 14 Verwarnungen und 22 Geldbußen – wurden Verwaltungssanktionen verhängt.
Geldbußen	20 476 55 LVL (29 135,50 EUR).
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	42 DPOs, die von für die Datenverarbeitung Verantwortlichen ernannt wurden

B. Rechtsprechung

Keine nennenswerten Ergebnisse.

C. Sonstige wichtige Informationen

Zur Förderung der Zusammenarbeit nahm die lettische Datenschutzbehörde am jährlichen Treffen der drei baltischen Staaten teil, wo für 2014 eine jährliche gemeinsame Prüfung des Schutzes personenbezogener Daten in Spas und Freizeiteinrichtungen beschlossen wurde. Im Jahr 2013 wurde eine jährliche gemeinsame Prüfung von Glücksspieleinrichtungen und Kasinos durchgeführt.

LITAUEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Da Litauen vom 1. Juli bis zum 31. Dezember 2013 die EU-Ratspräsidentschaft inne hatte, konzentrierte sich die Datenschutzbehörde der Republik Litauen auf die Reform des Datenschutzgesetzes und nahm an Sitzungen der Arbeitsgruppe DAPIX teil.

Am 25. Januar 2013 wurde der Europäische Datenschutztag gefeiert. Im Seimas der Republik Litauen fand an diesem Tag eine Pressekonferenz zum Thema „Datenschutz in der Europäischen Union und in Litauen“ statt. Am 4. Februar 2013 wurde der Datenschutztag außerdem an der Schule Biržiška in Mykolas begangen. Die Datenschutzbehörde organisierte für die Schüler ein Seminar zu den Themen privater und öffentlicher Bereich in der Informationsgesellschaft, Reisepässe der Republik Litauen, soziale Netzwerke und ähnlichen Fragen.

Die Datenschutzbehörde nahm an der Konferenz „Schutz personenbezogener Daten für Privatpersonen und Unternehmen“ teil, die am 9. Mai 2013 vom litauischen Unternehmerverband veranstaltet wurde.

Die Datenschutzbehörden Lettlands, Litauens und Estlands kamen im März 2013 im lettischen Riga zusammen, um die Zusammenarbeit der baltischen Staaten fortzusetzen.Die Datenschutzbehörden der baltischen Länder führten zum zweiten Mal eine gemeinsame Prüfung der Verarbeitung und des Schutzes personenbezogener Daten im Glücksspielsektor durch. Insgesamt wurden 2013 in den baltischen Ländern 13 Kasinos überprüft.

Im Jahr 2013 wurde das Informationssystem „HELP“ eingeführt, das den Zugang zur Datenschutzbehörde über elektronische Kommunikationsnetze ermöglicht. Somit haben betroffene Personen und für die Datenverarbeitung Verantwortliche die Möglichkeit, überall und jederzeit Beschwerden oder sonstige Anträge elektronisch an die Datenschutzbehörde zu übermitteln und auf die gleiche Weise eine Antwort zu erhalten. Betroffene Personen und für die Datenverarbeitung Verantwortliche sehen jetzt, wer ihr Anliegen bearbeitet, wie die Bearbeitung abläuft und in welcher Phase sich die Bearbeitung befindet.

Dr. Algirdas Kunčinas wurde zum zweiten Mal für eine Amtszeit von fünf Jahren zum Leiter der Datenschutzbehörde ernannt. Die neue Amtszeit begann zum 1. Januar 2014.

Organisation	
Vorsitz und/oder Gremium	Dr. Algirdas Kunčinas
Budget	1 919 000 Litas (555 781 EUR)
Personal	30
Allgemeine Aktivitäten	
Stellungnahmen, Empfehlungen	k. A.
Meldungen	1 409
Vorabprüfungen	338
Anfragen von Bürgern	23

Beschwerden von Bürgern	327
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	3 845 Konsultationen; 100 öffentliche Mitteilungen; 4 Zusammenfassungen der Ergebnisse der Untersuchungen von Beschwerden und der Rechtsprechung; 29 Schlussfolgerungen zu Dokumenten der EU und des Europarates; 65 Antworten auf Anfragen von Parteien im Zusammenhang mit dem Übereinkommen (ETS Nr. 108); 309 koordinierte Rechtsakte und Dokumente von für die Datenverarbeitung Verantwortlichen; 11 vorbereitete Rechtsakte; 6 öffentliche Konsultationen.
Prüfmaßnahmen	
Prüfungen	51
Sanktionsmaßnahmen	
Sanktionen	Die Datenschutzbehörde erstellte 41 Protokolle zu Verwaltungsverstößen.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Verarbeitung der persönlichen Identifikationsnummer

Eine Person reichte eine Beschwerde ein, da ein Unternehmen für Internetdienste und Kabelfernsehen den Beschwerdeführer aufgefordert hatte, einen Standardvertrag zu unterzeichnen und die persönliche Identifikationsnummer anzugeben. Laut Artikel 7 Absatz 2 des Datenschutzgesetzes der Republik Litauen ist es nur mit der Einwilligung der betroffenen Person erlaubt, bei der Verarbeitung personenbezogener Daten die persönliche Identifikationsnummer mitzuverarbeiten. In Absatz 3 des Artikels werden Ausnahmen dieser Regelung genannt. Die Datenschutzbehörde stellte fest, dass die Einwilligung des Beschwerdeführers nicht aus freien Stücken erfolgte, da dieser sonst nicht die gewünschte Dienstleistung erhalten hätte, und erteilte dem Unternehmen die rechtsverbindliche Anweisung, das Formular des Standardvertrages zu ändern und die Kunden nicht um die Angabe der persönlichen Identifikationsnummer zu bitten. Diese Anweisung wurde vom Unternehmen vor dem Bezirksverwaltungsgericht Vilnius angefochten. Das Gericht wies das Berufungsgesuch als unbegründet ab und kam zu dem Schluss, dass die Feststellung der Datenschutzbehörde, die Einwilligung des Beschwerdeführers sei nicht frei erteilt worden, korrekt sei. Der Beschwerdeführer legte gegen dieses Urteil vor dem Obersten Verwaltungsgericht Berufung ein, welches ebenfalls zu dem Schluss kam, dass die Anweisung der Datenschutzbehörde korrekt gewesen sei und dass die Argumentierung des Unternehmens, dass die Angabe der persönlichen Identifikationsnummer auf dem Vertrag notwendig sei, in diesem Fall unwichtig sei.

Offenlegung personenbezogener Daten gegenüber Medien

Eine Person legte eine Beschwerde ein, da das Finanzamt ihre personenbezogenen Daten über eine andauernde Steuerprüfung den Medien zugänglich gemacht hatte. Laut Artikel 38 Absatz 1 des Steuerverwaltungsgesetzes der Republik Litauen hat der Steuerverwalter die Daten der Steuerzahler vertraulich zu behandeln und nur zu rechtmäßigen Zwecken zu verwenden. Laut Artikel 38 Absatz 2 Unterabsatz 6 des Gesetzes müssen Daten zu Verstößen gegen das Steuerverwaltungsgesetz nicht vertraulich bleiben, wenn die Schuld des Verstoßes nachweislich beim Steuerzahler liegt. Die Datenschutzbehörde beschloss, dass das Finanzamt die personenbezogenen Daten des Beschwerdeführers über die Steuerprüfung, die zu dem Zeitpunkt zwar begonnen hatte, aber noch nicht abgeschlossen war, unrechtmäßig veröffentlicht hat und dass es dafür in Artikel 5 des Datenschutzgesetzes keine Rechtsgrundlage oder sonstige Kriterien für die rechtmäßige Offenlegung personenbezogener Daten gibt. Die Datenschutzbehörde wies das Finanzamt an, die bisherige Praxis des Informierens der Medien (auf Anfrage der Medien) über noch andauernde Steuerprüfungen von natürlichen Personen einzustellen, da ein Verstoß gegen das Steuerverwaltungsgesetz durch den Steuerzahler erst noch nachgewiesen werden muss.

Das Finanzamt legte gegen diese Anweisung beim Bezirksverwaltungsgericht Vilnius Berufung ein, da es der Meinung war, dass die Offenlegung der Fakten einer noch andauernden Steuerprüfung eine der Maßnahmen zur Prävention von Verstößen gegen das Steuerverwaltungsgesetz und zur Bereitstellung von Informationen über die Aktivitäten der Institution sei. Das Gericht wies dies auf der Grundlage von Artikel 38 des Steuerverwaltungsgesetzes als unbegründet ab und stellte fest, dass die Offenlegung der personenbezogenen Daten von Steuerzahlern nicht mit dem Ziel der Prävention von Verstößen und der Bereitstellung von Informationen über die Aktivitäten der Institution zu rechtfertigen sei.

Das Finanzamt legte beim Obersten Verwaltungsgericht gegen dieses Urteil Berufung ein, welche ebenfalls abgewiesen wurde.

LUXEMBURG

A. Zusammenfassung der Aktivitäten und Neuerungen

Gesetzesänderungen

Im Jahr 2013 gab es keine Gesetzesänderungen auf dem Gebiet des Datenschutzes.

Wichtige Themen

Eine der Aufgaben der CNPD ist die Beratung der luxemburgischen Regierung zu Themen in Bezug auf Privatsphäre und Datenschutz. Im Jahr 2013 wurden 10 formale Stellungnahmen zu Gesetzen und Vorschriften abgegeben. Die wichtigsten Themen waren:

- die Organisation des nationalen Nachrichtendienstes;
- der Status, das Ausweisungsverfahren und die Befugnisse des koordinierenden Arztes („*médecin coordinateur*“);
- die Reform des Gesetzes über den öffentlichen Dienst;
- die Reform der Urteilsvollstreckung und der Vollzugsverwaltung;
- der grenzüberschreitende Austausch von Daten zu Verkehrsdelikten;
- das nationale Krebsregister.

Auf dem Gebiet der intelligenten Verbrauchsmessung („Smart Metering“) unterstützt die CNPD Luxmetering bei der Umsetzung seiner Betriebsabläufe und -verfahren im Rahmen einer Datenschutz-Folgenabschätzung. Luxmetering ist eine wirtschaftliche Interessenvereinigung („*Groupement d'intérêts économique*“) aus sieben luxemburgischen Strom- und Gasversorgungsunternehmen. Sie ist für die Implementierung der Infrastruktur und des landesweiten Einsatzes von 350 000 intelligenten Verbrauchszählern verantwortlich.

Neuerungen

Die CNPD und CNIL (Frankreich) führten auf Anfrage der Artikel-29-Datenschutzgruppe eine Prüfung der Servicevereinbarung und der Online-Datenschutzrichtlinie von Microsoft durch, nachdem das Unternehmen seine vertraglichen Nutzungsbedingungen geändert hatte. Frühere Beispiele für die Änderung der Nutzungsbedingungen von Unternehmen wie Google oder Facebook haben gezeigt, dass diese Änderungen in Europa weitreichende Auswirkungen haben und den Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen schwächen können.

Nach den Enthüllungen in der internationalen Presse in Bezug auf das PRISM-Programm erhielt die luxemburgische Datenschutzbehörde zwei Anträge von europäischen Bürgern auf Prüfung, ob Skype und Microsoft Luxembourg ihre Daten rechtmäßig verarbeitet und ob die Unternehmen ihre Daten an die Nationale Sicherheitsagentur der Vereinigten Staaten weitergegeben haben.

Als leitende Datenschutzbehörde genehmigte die CNPD nach einer 18-monatigen Diskussion die verbindlichen unternehmensinternen Vorschriften des in Luxemburg ansässigen multinationalen Stahlkonzerns ArcelorMittal. Dies erfolgte gemeinsam mit den Datenschutzbehörden der 25 anderen europäischen Länder, in denen ArcelorMittal tätig ist. Es handelte sich hierbei um das zweite Verfahren zur Genehmigung verbindlicher unternehmensinterner Vorschriften der CNPD, die bereits 2009 bei den verbindlichen unternehmensinternen Vorschriften von eBay als leitende Datenschutzbehörde fungierte.

Wichtige Veranstaltungen und Sensibilisierung

Anlässlich ihres zehnjährigen Jubiläums veranstaltete die CNPD am 28. Januar 2013 (Datenschutztag) eine Konferenz mit Dean Spielmann (Präsident des Europäischen Gerichtshofs für Menschenrechte) zum Thema „*Datenschutz in der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte*".

Neben dieser großen Veranstaltung nahm die luxemburgische Datenschutzbehörde außerdem an mehreren Sensibilisierungsveranstaltungen für die breite Öffentlichkeit und entsprechenden Schulungen für ein stärker fachspezifisches Publikum teil. Ein Beispiel dafür ist die von der AFCDP (*Association Française des Correspondants à la Protection des Données à caractère Personnel*) in Luxemburg ausgerichtete Konferenz für Datenschutzbeauftragte.

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	1 552 000 EUR
Personal	Gremium: 3 Rechtsabteilung: 5 Meldungen und Vorabprüfungen: 2 Allgemeine Verwaltung: 2 Kommunikation und Dokumentation: 1 IT und Logistik: 1 Gesamt: 14
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	693
Meldungen	1 072
Vorabprüfungen	725
Anträge betroffener Personen	270
Beschwerden betroffener Personen	177
Vom Parlament bzw. der Regierung angeforderte Beratung	10
Sonstige Informationen zu	Treffen und Konsultationen (öffentlicher/privater Sektor) 177

einschlägigen allgemeinen Aktivitäten	Informationssitzungen und Konferenzen: 18
Prüfmaßnahmen	
Prüfungen, Untersuchungen	26
Sanktionsmaßnahmen	
Sanktionen	1
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Im Laufe des Jahres 2013 ernannte DPOs: 20 (Zum Zeitpunkt der Erstellung des Berichts) insgesamt ernannte DPO: 49

B. Rechtsprechung

Gericht erster Instanz, Kammer für Arbeitsrecht, 7. März 2013, zur Gültigkeit von Nachweisen (E-Mail-Korrespondenz), die ohne eine vorherige Genehmigung durch die CNPD gesammelt wurden

Die wichtigste Frage bei dieser Rechtssache bezog sich auf die Festlegung, ob die fristlose Kündigung eines Mitarbeiters des Unternehmens X gerechtfertigt war oder nicht. Der Arbeitgeber berief sich auf Praktiken des unlauteren Wettbewerbs durch den Mitarbeiter und legte als Beweis u. a. eine Liste von E-Mails vor, die der Arbeitnehmer geschrieben und versendet hatte. Der Arbeitnehmer beantragte den Ausschluss dieser Nachweise vom Verfahren, da im Vorfeld keine Genehmigung der CNPD eingeholt worden war. (N.B.: nach luxemburgischem Recht muss die Überwachung der E-Mail-Korrespondenz von Arbeitnehmern vorher von der CNPD genehmigt werden).

Nachdem geklärt wurde, dass in diesem Fall im Vorfeld keine Genehmigung erteilt worden war, befand das Gericht erster Instanz unter Berufung auf das Grundrecht des Briefgeheimnisses und das Recht auf Privatsphäre, dass die besagten Dokumente vom Verfahren ausgeschlossen werden müssen.

Dieses Urteil ist dahingehend äußerst interessant, als das Gericht erster Instanz auf dem Gebiet der E-Mail-Überwachung einen gegenteiligen Standpunkt einnimmt zu dem auf dem Gebiet der Videoüberwachung, wo die meisten Urteile erklären, dass Bilder auch ohne vorherige Genehmigung der CNPD als Beweismaterial zugelassen werden können. Es muss jedoch darauf hingewiesen werden, dass dies nur das Gericht erster Instanz ist und Unternehmen X möglicherweise Berufung eingelegt hat. Zum Zeitpunkt des Verfassens dieses Berichts lag jedoch noch kein Urteil vor.

C. Sonstige wichtige Informationen

Im Jahr 2013 wurde in Luxemburg der erste Verband für Privatsphäre und Datenschutz ins Leben gerufen. Die Mitglieder der APDL *(„Association pour la protection des données au Luxembourg“)* sind hauptsächlich Datenschutzbeauftragte, IT-Sicherheitsfachleute und Richtlinienbeauftrage sowie Rechtsanwälte und Berater.

MALTA

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Jahr 2013 verfolgte das Amt des Informations- und Datenschutzbeauftragten einen proaktiven Ansatz, um den Sektoren mit dem Ziel zu begegnen, ihre Betriebsabläufe zu besprechen und auftretende Datenschutzprobleme, die ein Eingreifen des Datenschutzbeauftragten erfordern würden, in Angriff zu nehmen. Die Datenschutzbehörde bedient sich eines Ansatzes zur Koordinierung solcher Besprechungen mit der breiten Vertretung des jeweiligen Sektors. Dieser Ansatz hat zu zufriedenstellenden Ergebnissen geführt, vor allem dort, wo Leitlinien oder Verhaltenskodizes entwickelt werden mussten, um bestimmte Bereiche des Sektors zu regulieren.

Obwohl von gesetzgeberischer Seite nicht in das Datenschutzgesetz oder in damit zusammenhängende Gesetze eingegriffen wurde, hat die Datenschutzbehörde im Laufe des Jahres interne Überprüfungen durchgeführt, um die übergreifende Politik der Regierung zur Gewährleistung einer besseren Regulierung umzusetzen.

Im März wurde ein neues Parlament gewählt. Während der Wahlkampagne verzeichnete die Datenschutzbehörde einen beträchtlichen Anstieg der eingehenden Beschwerden. Ein Großteil davon wurde von betroffenen Personen eingereicht, die einen Verstoß gegen ihre Datenschutzrechte durch politische Parteien oder Kandidaten vermuteten, als Letztere ihre politischen Wahlkampfbotschaften per E-Mail oder SMS verschickten. Die Beschwerden wurden von Personen eingereicht, die weder als Parteimitglieder registriert waren noch im Vorfeld ihre Einwilligung für den Erhalt solcher unerwünschten Nachrichten erteilt hatten.

Nach der Wahl berief der Datenschutzbeauftragte diesbezüglich eine Besprechung mit den großen politischen Parteien ein, um sie darüber zu informieren, dass es an der Zeit sei, Leitlinien zur Verarbeitung personenbezogener Daten im politischen Wahlkampf zu erstellen. Diese Leitlinien sollen eine deutliche, allgemein gültige Auslegung des Datenschutzgesetzes in einem politischen Umfeld bereitstellen, in dem politische Parteien und Kandidaten personenbezogene Daten natürlicher Personen zu Zwecken des Wahlkampfs und der Verbreitung ihrer politischen Ideologien verarbeiten. Nach einer Reihe von Besprechungen und schriftlichen Beiträgen der beteiligten Parteien setzte die Datenschutzbehörde einen endgültigen Entwurf auf, der im dritten Quartal 2014 verabschiedet werden soll.

Die Datenschutzbehörde wurde im Berichtszeitraum durch die Teilnahme an verschiedenen Datenschutzforen weiterhin ihren europäischen und internationalen Verpflichtungen gerecht. Am 28. Januar bereitete die Datenschutzbehörde ähnlich wie in den Jahren zuvor Informations- und Büromaterial zum Thema Sicherheit im Internet vor, das an Schüler vorher festgelegter Jahrgangsstufen verteilt wurde.

Bezüglich der Umsetzung des Gesetzes über die Informationsfreiheit sammelten die staatlichen Behörden 2013 Erfahrungen bei der Umsetzung des Gesetzes und der Verarbeitung von Anträgen zur Dokumentation durch spezielle IT-Systeme. Die von der Koordinierungsstelle für Informationsfreiheit (die von dem Ministerium ins Leben gerufen wurde, dem auch die Datenschutzbehörde untersteht) bereitgestellte Intervention und Unterstützung war dabei entscheidend, dass die staatlichen Behörden diese Ziele erreichen konnten.

Die staatlichen Behörden bearbeiteten insgesamt 130 Auskunftsersuchen, von denen 10 noch aus dem Jahr 2012 stammten. Davon wurden 71 (54,6 %) angenommen und 51 (39,2 %) abgelehnt. Die Anzahl der Ersuchen, bei denen ein Beschluss noch aussteht, belief sich Ende des Jahres auf 4 (3,1 %). Weitere 4 Ersuchen (3,1 %) wurden von den Antragstellern zurückgezogen. Von den abgelehnten Fällen stellten 14 (27,4 %) beim Datenschutzbeauftragten einen Berufungsantrag. Der Datenschutzbeauftragte entschied in einem Fall zugunsten des Antragstellers und lehnte die anderen 13 ab. Von diesen 13 Fällen legten 3 vor dem Berufungsgericht für Datenschutz Berufung ein. Eine vierte Person fühlte sich bezüglich

der Datenschutzbeschwerde durch den Beschluss des Datenschutzbeauftragten benachteiligt und legte vor dem Gericht Berufung ein.

Zum Jahresende waren die Urteile für alle diese Fälle noch ausstehend, da die Richter aufgrund einer Änderung der Regierung ihre Ämter niedergelegt hatten.

Organisation	Amt des Informations- und Datenschutzbeauftragten
Vorsitz und/oder Gremium	Informations- und Datenschutzbeauftragter
Budget	ca. 280 000 EUR
Personal	Beauftragter – 1 Fachpersonal – 3 Technische Unterstützung – 2 Administrative Unterstützung – 3
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Der Beauftragte für Datenschutz und Informationsfreiheit erließ 81 Beschlüsse. Der Datenschutzbeauftragte gab 28 an für die Datenverarbeitung Verantwortliche gerichtete Stellungnahmen/Empfehlungen in Bezug auf Datenschutzangelegenheiten ab.
Meldungen	240 neue Meldungen
Vorabprüfungen	6 Anträge auf Vorabprüfung
Anträge betroffener Personen	Täglich gingen durchschnittlich 10 Anrufe und 250 E-Mails ein
Beschwerden betroffener Personen	144 Beschwerden zum Thema Datenschutz und 14 zum Thema Informationsfreiheit.
Vom Parlament bzw. der Regierung angeforderte Beratung	1 Antrag stammte vom Ministerium für Bildung und Beschäftigung und bezog sich auf den Entwurf eines Rechtsinstruments, das die personenbezogenen Daten von Schülern zum Zweck der Entwicklung zielgerichteter Strategien zur Lösung des wachsenden Problems leistungsschwacher Schüler beantragte.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Es wurden 10 Vor-Ort-Prüfungen vorwiegend im Rahmen von Beschwerdeermittlungsverfahren durchgeführt.

Sanktionsmaßnahmen	
Sanktionen	Für die Datenverarbeitung Verantwortliche wurden offiziell ermahnt. Gerichtsverfahren wurden jedoch nicht eingeleitet.
Geldbußen	Einem für die Datenverarbeitung Verantwortlichen wurde nach wiederholten Vergehen, die bei Abschluss einer Untersuchung festgestellt wurden, eine Geldbuße auferlegt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Es wurden 14 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 wir Signale aus verschiedenen Quellen innerhalb der Gesellschaft auf unterschiedlichen Wegen, wie z. B. Telefonanrufe, E-Mails oder Medienberichte, erhalten. 2011 wurde ein neues Signalregistrierungssystem eingeführt, das eine Erfassung von Signalen nach Sektoren durch die niederländische Datenschutzbehörde 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 in Betracht gezogen.

Die Schwerpunkte der niederländischen Datenschutzbehörde lagen 2013 u. a. auf folgenden Bereichen: Profiling, angemessener Schutz medizinischer Daten sowie Datenverarbeitung im Rahmen von Beschäftigungsverhältnissen. Darüber hinaus konzentrierten sich die Aktivitäten der niederländischen Datenschutzbehörde 2013 auf die Grundsätze der Zweckbindung, Einwilligung, Transparenz und insbesondere der Datensicherheit.

Eine der wichtigsten Untersuchungen des Jahres 2013 betraf den Schutz medizinischer Daten. Jeder hat das Recht auf denselben Schutz vor unbefugtem Zugang zu seinen medizinischen Daten. Eine Untersuchung der niederländischen Datenschutzbehörde bei verschiedenen Gesundheitseinrichtungen, Notdienstkliniken und Apotheken hat jedoch gezeigt, dass es bei den Sicherheitsmaßnahmen, die zum Schutz der Patientendaten vor unbefugtem Zugang ergriffen werden, viele Probleme gibt. Unzureichende Sicherheitsmaßnahmen bergen das Risiko, dass Mitarbeiter, die nicht an der Behandlung des Patienten beteiligt sind, auf dessen medizinische Daten zugreifen können. Die niederländische Datenschutzbehörde kam zu dem Schluss, dass auf der Grundlage der Untersuchungen, der erhaltenen Signale und der Gespräche mit Branchenverbänden die aufgedeckten Probleme im Gesundheitswesen relativ weit verbreitet sind.

Die Übermittlung von Patientendaten zwischen Erbringern von Gesundheitsleistungen, zum Beispiel von einer Arztpraxis an eine Versicherungsgesellschaft oder ein Pharmaunternehmen, ist sehr strengen Schutzmechanismen unterworfen. Diese Übermittlungen sind nur mit der Einwilligung der betroffenen Personen erlaubt. Die niederländische Datenschutzbehörde untersuchte die Übermittlung medizinischer Daten durch Apotheker an ein Unternehmen, das Produkte für Patienten mit Inkontinenz herstellt, und kam zu dem Schluss, dass die Apotheker keine ausreichenden Maßnahmen zum Schutz der Patientendaten ergriffen hatten. Des Weiteren hatten nicht alle Patienten ihre Einwilligung für die Übermittlung ihrer Daten an das Pharmaunternehmen erteilt.

Eine weitere Untersuchungsreihe, die 2013 durchgeführt wurde, betraf Online-Daten und Profiling. Daten zu angesehenen Fernsehprogrammen, besuchten Websites und heruntergeladenen Apps sagen viel über das Verhalten und die Vorlieben einer Person aus. Oft ist jedoch nicht klar, was mit diesen Daten passiert, die von Telekommunikationsanbietern und App-Entwicklern erfasst werden. Die meisten Menschen sind sich der Tatsache nicht bewusst, dass sie diese sogenannten „kostenlosen“ Dienste im Grunde mit ihren personenbezogenen Daten bezahlen. Unternehmen und Organisationen müssen Nutzern ausreichend Informationen über die Nutzung ihrer Daten bereitstellen und falls nötig um ihre Einwilligung bitten.

Eine der Untersuchungen, die 2013 in diesem Bereich durchgeführt wurden, betraf die unrechtmäßige Datenanalyse („Packet Inspections") von vier Telekommunikationsanbietern. Die Unternehmen speicherten Daten über das Aufrufen von Websites und Apps durch den Kunden und verstießen damit gegen das Gesetz. Außerdem wurden die Kunden nicht ordnungsgemäß darüber informiert.

Des Weiteren führten parlamentarische Fragen zur Nutzung von Cookies auf den Websites des niederländischen öffentlich-rechtlichen Rundfunkveranstalters (Nederlandse Publieke Omroep, NPO) dazu, dass die niederländische Datenschutzbehörde diesbezüglich weitere Leitlinien zum Rechtsrahmen herausgegeben hat, die erklärten, dass NPO nicht das Recht hat, Besuchern den Zugang zu seiner Website zu verweigern, wenn diese sich gegen die Nachverfolgung ihres Surfverhaltens im Internet entschieden haben.

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 2013 erteilte die Datenschutzbehörde Ratschläge bezüglich des Entwurfs des Jugendschutzgesetzes (Jeugdwet). Beim Entwurf des Jugendschutzgesetzes geht es um die Zuweisung administrativer und finanzieller Aufgaben durch die Regierung an die Kommunen in Bezug auf die Bereitstellung von Unterstützung und Fürsorge bei der Erziehung von Kindern und Jugendlichen mit psychischen Problemen. Die exakte Aufgabenteilung steht zwar noch nicht fest, doch die niederländische Datenschutzbehörde geht davon aus, dass Dezentralisierung – ein Trend, der bereits bei anderen Gesetzentwürfen zu beobachten war – zu einer höheren Menge an Daten führen wird, die von Kommunen verarbeitet werden. Ferner wird davon ausgegangen, dass eine umfassende Herangehensweise an Jugend- und Familienprobleme zu einem erhöhten Informationsaustausch zwischen den verschiedenen Interessenvertretern und außerdem zu einem erhöhten Risiko übermäßiger Datenverarbeitung, (unrechtmäßiger) Nutzung von Daten zu einem anderen (nicht kompatiblen) Zweck sowie unzureichender Sicherheitsmaßnahmen führen wird.

Angesichts der öffentlichen Informationen, die zur Dezentralisierung der Jugendhilfe verfügbar sind, scheint es, als würden Gemeinden und andere Beteiligte keine Maßnahmen ergreifen, um dieses Risiko zu mindern. Der Gesetzentwurf enthält anscheinend auch nicht die nötigen Ressourcen, um ein System aufzubauen, das eine sorgfältige, rechtmäßige Datenverarbeitung gewährleistet. Die niederländische Datenschutzbehörde ist daher der Meinung, dass Kommunen dazu verpflichtet sein sollten, in Bezug auf (aktuelle und geplante) Datenverarbeitungsaktivitäten Datenschutz-Folgenabschätzungen und Prüfungen durchzuführen. Dies sollte beim Entwurf des Jugendschutzgesetzes oder in der Sekundärgesetzgebung berücksichtigt werden.

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: 7 586 000 EUR Ausgegeben: 7 827 000 EUR

Personal	74,9 Vollzeitmitarbeiter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	109 (Leitlinien, Stellungnahmen, Verhaltenskodizes, internationale Fälle, Ausnahmen, Sanktionen und internationale Übermittlungen)
Meldungen	3 523
Vorabprüfungen	86
Signale ([4]) betroffener Personen	6 879
Vom Parlament bzw. der Regierung angeforderte Beratung	30
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	k. A.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	73
Sanktionsmaßnahmen	
Sanktionen	19
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	369 (in 362 Organisationen)

B. Rechtsprechung

Während des Berichtszeitraums befassten sich die niederländischen Gerichte mit mehreren Rechtssachen im Zusammenhang mit dem Datenschutz. Eine der Rechtssachen betraf eine Klägerin, die beim Nationalen Forensischen Institut (NFI) anfragte, ob sie einen Tropfen Blut einer verstorbenen Person verwenden könne, den die NFI in einem seiner Archive aufbewahrte, um die Familienzugehörigkeit festzustellen. Nach Einwänden der Töchter des Verstorbenen wurde ihr der Zugang zu dem Blutstropfen verwehrt. Sie legte diesbezüglich beim Staatsanwalt und beim NFI Berufung ein, woraufhin der Staatsanwalt antwortete, dass der Beschluss nicht als rechtskräftiger Beschluss im Sinne des Strafgesetzbuches erachtet werden könne und ihr Rechtsmittel daher ungültig sei.

Sie legte vor dem Gericht Rotterdam Berufung ein, das prüfte, ob der Beschluss tatsächlich keine rechtlichen Auswirkungen im Sinne des Strafgesetzbuches hat. Das Gericht kam zu dem Schluss, dass

[4] 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 des betroffenen Sektors registriert.

weder das Strafgesetzbuch noch das Bestattungsgesetz in dieser Situation zur Anwendung käme. Angesichts der Tatsache, dass es sich um Körpermaterial handelt, greift das niederländische Datenschutzgesetz. Die Frau hätte sich demnach an ein Zivilgericht wenden und unter Berufung auf das Datenschutzgesetz Rechtsmittel einlegen sollen, anstatt in einer Verwaltungssache beim Staatsanwalt und beim NFI Berufung einzulegen.

In einer anderen Rechtssache des Jahres 2013 wandte sich ein Kläger an das Obersten Verwaltungsgericht, da ihm unrechtmäßig das Recht auf Zugang, Berichtigung oder Löschung von Daten, welche die niederländische Einwanderungsbehörde über ihn gespeichert hatte, verwehrt worden war.

Der Kläger war in Besitz einer Aufenthaltsgenehmigung auf Grundlage der Tatsache, dass er mit Person X verheiratet war. Der Justizminister erhielt daraufhin ein anonymes Schreiben, in dem erklärt wurde, dass der Kläger nicht der Ehepartner von Person X war, sondern ihr Bruder. Daraufhin schickte er dem Kläger ein Schreiben, in dem er erklärte, dass der Minister aufgrund anonymer Informationen die Absicht habe, die Aufenthaltsgenehmigung des Klägers zu widerrufen, und bot die Möglichkeit einer freiwilligen Zusammenarbeit an, um zur Ermittlung des Sachverhalts einen DNA-Test durchzuführen. Der Kläger lehnte den DNA-Test ab. Dies machte es technisch unmöglich zu bestimmen, ob die Informationen in dem anonymen Schreiben der Wahrheit entsprachen. Aus diesem Grund focht der Minister die Aufenthaltsgenehmigung an.

Der Kläger wollte daraufhin den Verfasser des anonymen Schreibens wegen Verleumdung anklagen und bat daher um Zugang zu dem Dokument, um die Daten zu berichtigen oder zu löschen. Er war der Ansicht, dass er Zugang zu dem Dokument erhalten und es ihm möglich sein sollte, das Schreiben zu vernichten, da es personenbezogene Daten über ihn enthielt. Der Minister verwehrte ihm den Zugang mit der Begründung, dass es nötig sei, einen Dritten zu schützen und dessen Rechte und Freiheiten zu wahren. Außerdem habe er eine Zusammenfassung über den Inhalt des Schreibens erhalten. Das Gericht bestätigte dies und ließ ferner verlauten, dass der Inhalt des Schreibens nicht die personenbezogenen Daten des Klägers betraf. Der Kläger legte beim Obersten Verwaltungsgericht unter Berufung auf Artikel 8 der Europäischen Menschenrechtskonvention Rechtsmittel ein.

Das Oberste Verwaltungsgericht kam zu dem Urteil, dass das im niederländischen Datenschutzgesetz verankerte Recht auf Berichtigung nicht dazu da ist, Informationen zu berichtigen oder zu löschen, die dem Kläger nicht gefallen. Ob die Informationen in dem Schreiben richtig sind oder nicht, soll in einem angemessenen Verfahren ermittelt werden. Diesbezüglich wurde ein Ermittlungsverfahren im Zusammenhang mit der Aufenthaltsgenehmigung des Klägers durchgeführt. Die Tatsache, dass die Ermittlung ergab, dass es technisch unmöglich war, den wahren Sachverhalt festzustellen, hat keinen Einfluss auf die Tatsache, dass der Minister das Schreiben als relevant erachtete und dass er es zu Recht aufbewahrte, nachdem er seine Interessen gegen die des Klägers, nämlich die Vernichtung des Schreibens, abgewogen hatte. Ferner urteilte das Gericht, dass der Schutz des Verfassers des Schreibens als wichtiger erachtet wurde als die Interessen des Klägers. Die Entscheidung, das Schreiben nicht zu vernichten, wurde demnach vom niederländischen Datenschutzgesetz gemäß Art. 8 Abs. 2 der Europäischen Menschenrechtskonvention gerechtfertigt, da dies ein Verstoß gegen selbigen Artikel dargestellt hätte.

ÖSTERREICH

A. Neue Entwicklungen und Aktivitäten

Im Berichtszeitraum wurde im Parlament die **DSG-Novelle 2014**[5] beschlossen. Diese sieht die Neueinrichtung einer **monokratischen Datenschutzbehörde** vor, die an die Stelle der Datenschutzkommission tritt. Weiters ist ein Rechtszug von der Datenschutzbehörde an das (ebenfalls ab 2014 neue) Bundesverwaltungsgericht vorgesehen.

Die Datenschutzkommission hat daher ihre Tätigkeit als Datenschutzkontrollstelle im Sinne des Artikels 28 der Datenschutzrichtlinie[6] am 31.12.2013 eingestellt.

Organisation	Österreichische Datenschutzkommission
Vorsitz und/oder Gremium	Vorsitz: Dr. Anton SPENLING Geschäftsführendes Mitglied: Dr. Eva SOUHRADA-KIRCHMAYER Gremiumsmitglieder: Dr. Anton SPENLING, Dr. Eva SOUHRADA-KIRCHMAYER, Mag. Helmut HUTTERER, Dr. Claudia ROSENMAYR-KLEMENZ, Dr. Klaus HEISSENBERGER, Mag. Daniela ZIMMER.
Budget	Kein eigenes Budget im Jahr 2013. Die Ausgaben werden aus dem Budget des Bundeskanzleramts gedeckt.
Personal	16 Vollzeit- und 8 Teilzeitbeschäftigte (entspricht 21,85 Vollzeitbeschäftigten)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	107 formale Beschlüsse (Beschwerden), 326 Fälle für den Bürgerbeauftragten und 49 Genehmigungen (Datenübermittlung in Drittländer, Forschung und Gutachten).
Meldungen	11 404
Vorabprüfungen	4 193
Anträge betroffener Personen	Schriftlich: 1 136 Telefonisch: nicht schriftlich dokumentiert, bis zu 100 Anrufe täglich
Beschwerden betroffener Personen	Beschwerden, denen eine formale Entscheidung folgte: 107 Beschwerden, denen eine Klärung oder Empfehlung folgte: 326
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	Es wurden 160 Millionen bereichsspezifische Personenkennzeichen

[5] BGBl. I Nr. 83/2013.

[6] 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

einschlägigen allgemeinen Aktivitäten	herausgegeben. Des Weiteren wurden von der zur Datenschutzbehörde gehörenden E-Government-Registerbehörde 546 elektronische Vollmachten genehmigt sowie über 10 000 neue Personen und rund 1,4 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	16, 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. Datensicherheit bei Gaszählern

Im Berichtsjahr hat die Datenschutzkommission in einer **Empfehlung** einem Gaslieferanten empfohlen, bei frei zugänglichen **Gaszählern** geeignete Datensicherheitsmaßnahmen zu ergreifen, um den **Zugriff** auf personenbezogene, im Gaszählgerät gespeicherte Daten **durch Unbefugte zu unterbinden**.

Der Einschreiter hatte sich darüber beschwert, dass im Zuge des Neueinbaus von Gasleitungen im denkmalgeschützten Haus, in dem er wohnhaft ist, die Gaszählgeräte auf den Gang verlegt würden, sodass der Zählerstand, Verbrauch (ob und wie viel) etc. einem unbegrenzten Kreis von unbekannten Personen (Mieter und Angehörige, Zusteller etc.) zugänglich wären.

Der Gaslieferant entgegnete, für den Montageort des Zählers seien sicherheitstechnische (Richtlinie der ÖVGW, Allgemeine Verteilernetzbedingungen) und gesetzliche Vorgaben sowie die räumliche Situation vor Ort zu berücksichtigen. Ein „massiver Eingriff" in das Recht auf Datenschutz des Einschreiters sei aber nicht gegeben, das Vorliegen personenbezogener Daten werde bezweifelt, die An- bzw. Abwesenheiten in der Wohnung könne man anhand des Zählerstandes nicht eruieren.

Die Datenschutzkommission stellte fest, dass für alle Organisationseinheiten eines Auftraggebers, die (personenbezogene) Daten verwenden, **Maßnahmen zur Gewährleistung der Datensicherheit** zu treffen sind. Dabei ist je nach Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit (u. a.) sicherzustellen, dass die Daten Unbefugten nicht zugänglich sind.

Wird Unbefugten – durch den allgemein zugänglichen Montageort wie hier – **ohne jede Beschränkung** der **Zugriff auf personenbezogene Daten** ermöglicht, die dem Grundrecht auf Datenschutz (§ 1 DSG 2000) unterliegen, wird der Betroffene (Verbraucher) in diesem Grundrecht verletzt.

2. Personenbezug bei Statistiken

Im Berichtsjahr hat die Datenschutzkommission in einer **Empfehlung** einer Krankenkasse, die an interessierte Unternehmen mit mehr als 50 Arbeitnehmern auf Anfrage eine Krankheitsgruppen-Statistik der Arbeitnehmer für ein Berichtsjahr übermittelte, empfohlen, die Krankengruppen-Statistiken so zu gestalten, dass diese für jeden anfragenden Betrieb individuell angepasst werden.

Die statistischen Auswertungen waren so gestaltet, dass in einer Spalte diverse Krankheitsgruppen angeführt waren und daneben, in weiteren Spalten, die Krankenstandsfälle, getrennt nach Männern und Frauen, sowie die sich daraus ergebende Gesamtzahl der betroffenen Arbeitnehmer, und die Krankenstandstage, wiederum getrennt nach Männern und Frauen, sowie die sich daraus ergebende Gesamtzahl der betroffenen Arbeitnehmer.

Der Zweck der Übermittlung der Krankheitsgruppen-Statistik bestand darin, Maßnahmen zur betrieblichen Gesundheitsförderung zu ermöglichen.

Die Beschwerdeführerin hatte Bedenken, dass es für den einzelnen Unternehmer im einen oder anderen Fall möglich sei, einen direkten Personenbezug zwischen Diagnose und Mitarbeitern herzustellen, sodass es sich bei den übermittelten Daten nicht bzw. nicht in jedem Fall um indirekt personenbezogene oder anonymisierte Daten handle.

Diesen Bedenken folgte die Datenschutzkommission und empfahl der Krankenkasse, eine Trennung in männliche und weibliche Mitarbeiter – und damit einhergehend auch die Ausweisung der für diese Gruppe typischen Krankheiten (wie bspw. Krankheiten betreffend die Geschlechtsorgane) – erst dann vorzunehmen, wenn zu einer dieser Gruppen mehr als fünf Personen zu zählen sind. Diese Anzahl gewährleistet nach Ansicht der Datenschutzkommission, dass ein Rückschluss auf bestimmte Arbeitnehmer/innen nicht möglich ist.

Ist es einem Arbeitgeber aufgrund der übermittelten Krankengruppen-Statistik nämlich möglich, den Bezug zu einem bestimmten Arbeitnehmer herzustellen, so wird der betroffene Arbeitnehmer durch den von seinem Arbeitgeber gezogenen Rückschluss in seinem schutzwürdigen Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten gemäß § 1 Absatz 1 DSG 2000 verletzt. Da es sich bei Gesundheitsdaten gemäß § 4 Z 2 DSG 2000 um sensible Daten handelt, ist diesbezüglich ein besonders strenger Maßstab anzulegen.

Damit bestätigte die Datenschutzkommission zudem den vom Verfassungsgerichtshof ausgesprochenen Grundsatz, dass auch bei grundsätzlich nicht personenbezogenen Statistiken sichergestellt sein muss, dass aufgrund der Veröffentlichung keine Rückschlüsse auf (schutzwürdige und durch das Grundrecht auf Datenschutz auch geschützte) Daten gezogen werden können (vgl. dazu VfSlg 12.228/1989). Dieser Grundsatz ist auch im § 46 Absatz 1 DSG 2000 wiederzufinden, der eine Privilegierung der Verwendung zulässigerweise für andere Untersuchungen oder auch andere Zwecke ermittelter Daten nur dann vorsieht, wenn die angestrebte wissenschaftliche Untersuchung oder die Statistik keine personenbezogenen Ergebnisse zum Ziel hat.

POLEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Ab dem 22. März 2013 war die Behörde des Generalinspektors für den Schutz personenbezogener Daten (GIODO) für Meldungen von Verstößen gegen den Datenschutz durch Anbieter öffentlich verfügbarer Telekommunikationsdienste zuständig. Diese neue Verpflichtung folgt auf eine Änderung des Telekommunikationsgesetzes, welche die Bestimmungen der Richtlinie 2002/58/EG zum Schutz der Privatsphäre in der elektronischen Kommunikation, wie eingeführt durch Richtlinie 2009/136/EG vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst – die sogenannte Richtlinie „Rechte der Bürger" – in polnisches Recht umsetzt.

Bezüglich der oben genannten Verpflichtung wurde ein elektronisches Formular zur Meldung von Verstößen gegen den Datenschutz erstellt und ein Team zusammengestellt, das die Verstöße gegen den Datenschutz analysiert. Hierzu gehört die Beurteilung der Angemessenheit der von den Betreibern im Zusammenhang mit den gemeldeten Verstößen ergriffenen Maßnahmen.

2013 erhielt der GIODO 139 Meldungen von Verstößen gegen den Datenschutz durch Telekommunikationsanbieter.

Der GIODO modifizierte und verbesserte im Jahr 2013 regelmäßig die elektronische Kommunikation mit Bürgern und für die Datenverarbeitung Verantwortlichen. Des Weiteren stellte der GIODO die existierenden IT-Technologien von einer Client-Server-Architektur auf eine cloudbasierte Architektur um.

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

1. Am 1. März 2013 fand ein Treffen des Generalinspektors mit Françoise Le Bail, Generaldirektorin der GD Justiz der Europäischen Kommission, statt. Bei dem Treffen ging es um eine Fortschrittsanalyse der Reform des EU-Datenschutzrahmens sowie um Themen, die bei der andauernden Debatte für die größten Kontroversen sorgen oder für die zukünftige Form der Vorkehrungen zum Schutz personenbezogener Daten in Europa von großer Bedeutung sind.

2. Am 16. April 2013 wurde im Senat (obere Kammer des polnischen Parlaments) in Zusammenarbeit mit dem GIODO eine gemeinsame Sitzung der Senatsausschüsse abgehalten. Es wurden die Hauptrichtungen der Änderungen des EU-Datenschutzrahmens, die Auswirkungen der allgemeinen Verordnung zur Situation der polnischen Unternehmer und Verbraucher sowie deren Beziehung zu den nationalen Bestimmungen angesichts der Herausforderungen der Globalisierung und zeitgemäßer Geschäftsmodelle besprochen.

3. Am 4. April 2013 beteiligten sich der GIODO sowie Vertreter der EG, der ständigen Vertretung der Republik Polen in der EU, MdEP, Vertreter der Ministerien, NRO, der Wirtschaft und Universitäten sowie unabhängige Sachverständige an einer Diskussion der Reform des Datenschutzgesetzes, die vom Ministerium für Verwaltung und Digitalisierung – einer führenden Behörde für die Arbeit an der allgemeinen Verordnung in Polen – organisiert wurde. Am 13. Mai 2013 fand im Rahmen der Debatte „Digitale Identität: Wer sind wir online und wie verbreiten wir Wissen über uns selbst?" eine ähnliche Sitzung zum Thema Datenschutzreform statt. Kommissarin Viviane Reding, Vizepräsidentin der Europäischen Kommission und Leiterin der Arbeit am Entwurf der neuen Verordnung des Europäischen Parlaments und des Rates, war als Ehrengast anwesend.

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	135 Mitarbeiter.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	1 358 Beschlüsse (504 im Zusammenhang mit Anmeldeverfahren, 74 im Zusammenhang mit Prüfungen, 646 zu Verfahren infolge von Beschwerden, 134 zu Genehmigungen von Datenübermittlungen in Drittländer und 109 im Zusammenhang mit Verwaltungsvollstreckungen). In 121 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 16 866 Datenspeichersysteme gemeldet.
Vorabprüfungen	Infolge der Anmeldeverfahren (Vorabprüfungen) wurden 2 279 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.
Anträge betroffener Personen	Der polnischen Datenschutzbehörde wurden 4 911 rechtliche Fragen zugeschickt. Über die Informations-Hotline der GIODO wurden außerdem 11 908 Erklärungen bereitgestellt.
Beschwerden betroffener Personen	Beschwerden über Verletzungen des Schutzes personenbezogener Daten, unter anderem in folgenden Bereichen: - Öffentliche Verwaltung (126 Beschwerden), - Gerichte, Staatsanwaltschaft, Polizei, Gerichtsvollzieher (56 Beschwerden); - Banken und andere Finanzinstitute (127 Beschwerden); - Internet (124 Beschwerden), - Marketing (31 Beschwerden), - wohnungsbezogen (57 Beschwerden), - Sozial-, Sach- und Personenversicherungen (50 Beschwerden), - soziale Organisationen (12 Beschwerden),

	- Telekommunikation (24 Beschwerden), - Beschäftigung (11 Beschwerden), - Inkassoverfahren (42 Beschwerden), - Bildungswesen (21 Beschwerden), - Gesundheitswesen (34 Beschwerden), - sonstige (386 Beschwerden).
Vom Parlament bzw. der Regierung angeforderte Beratung	Dem GIODO wurden 617 Gesetzentwürfe zur Prüfung vorgelegt.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	60 – Anzahl der durch den GIODO durchgeführten Schulungen zu den Bestimmungen zum Schutz personenbezogener Daten, insbesondere für öffentliche Einrichtungen. 209 Bildungseinrichtungen, darunter Grund-, Mittel- und weiterführende Schulen sowie Berufsausbildungszentren für Lehrer, nahmen an der vierten Ausgabe des landesweiten Programms „Deine Daten, deine Verantwortung. Bildungsinitiative für Schüler und Lehrer" für das Schuljahr 2013/14 teil.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2013 wurden 173 Prüfungen durchgeführt. Die sektorspezifischen Prüfungen bezogen sich auf die folgenden Themen: - Online-Dienstleistungen (einschließlich Online-Shopping) – 10 Prüfungen, - Unternehmen mit Treueprogrammen – 7 Prüfungen, - Megastores mit RFID – 8 Prüfungen, - territoriale Selbstverwaltungsbehörden, die (im Zusammenhang mit der Ausübung des Gesetzes für Ordnung und Sauberkeit) Daten zum Zwecke der Müllentsorgung erfassten – 15 Prüfungen, - Polizeieinheiten, die (zur Erleichterung der Polizeiarbeit) das elektronische System „e-posterunek" (E-Polizeiwache) nutzen – 8 Prüfungen, - Behörden mit der Befugnis, die im nationalen Informationssystem und dem Visa-Informationssystem enthaltenen Daten zu verarbeiten – 14 Prüfungen, - Anbieter von Telekommunikationsdiensten (im Zusammenhang mit Verstößen gegen den Datenschutz) – 14 Prüfungen.
Sanktionsmaßnahmen	
Sanktionen	Der GIODO führt keine allgemeine Statistik über Sanktionen. Im Zusammenhang mit der Befugnis des GIODO als

	Durchsetzungsbehörde wurden jedoch 109 Verwaltungsverfahren eingeleitet. In Verbindung mit Prüfungen leitete der GIODO 2013 Verwaltungsverfahren gegen für die Datenverarbeitung Verantwortliche ein und erließ 74 Beschlüsse, die eine Anordnung zur Wiederherstellung eines rechtmäßigen Zustandes umfassten. Des Weiteren erließt der GIODO 92 Beschlüsse zu unterlassenen Meldungen von Datenspeichersystemen. Im Berichtszeitraum wurden keine Sanktionen verhängt.
Geldbußen	2013 wurden keine Geldbußen verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Im Jahr 2013 wurde gegen 52 der 646 Verwaltungsbeschlüsse des GIODO beim Verwaltungsgericht der Woiwodschaft Warschau Berufung eingelegt. Im Vergleich dazu wurde 2012 gegen 70 Beschlüsse Berufung eingelegt – ein Rückgang von 18.

Von den Urteilen, die zu den gegen die Beschlüsse der Datenschutzbehörde eingelegten Berufungen gefällt wurden, ist das Urteil des Obersten Verwaltungsgerichts vom 21. August 2013 (Nr. I OSK 166/12) besonders hervorzuheben. Bei diesem Urteil kam das Gericht zu dem Schluss, dass Art. 18 Abs. 6 des Gesetzes über die Bereitstellung von Dienstleistungen auf elektronischem Wege lediglich dazu verpflichtet, Daten zu Zwecken der durchgeführten Verfahren an staatliche Behörden bereitzustellen. Es besteht keine Verpflichtung, diese Daten Personen bereitzustellen, deren Rechte verletzt wurden. Sowohl die Behörde, welche die Offenlegung von Daten angeordnet hat, als auch das Verwaltungsgericht, das sich jedes Mal mit der Berufung gegen einen solchen Beschluss auseinandersetzen muss, müssen in Anbetracht der individuellen Umstände eines gegebenen Falles die Interessen abwägen, d. h. das Recht auf Schutz personenbezogener Daten und das Recht auf Würde, den Ruf oder das Unternehmensimage. Hierbei müssen die sich aus dem Grundsatz der Verhältnismäßigkeit ergebenden Anforderungen berücksichtigt werden, damit die ergriffenen Maßnahmen dem Risiko für das Interesse, das in einem Fall mehr Schutz erfordert, gerecht werden. Das Oberste Verwaltungsgericht betonte, dass die aktuellen rechtlichen Gegebenheiten die Schlussfolgerung zulassen, dass man die Offenlegung der von dem Online-Service erfassten Daten über ein weniger restriktives Gesetz als das über die Bereitstellung von Dienstleistungen auf elektronischem Wege beantragen könne, und zwar über das Datenschutzgesetz und insbesondere Art. 23 (durch Datenverarbeitung, einschließlich deren Offenlegung). Hierfür müssten jedoch bestimmte Bedingungen erfüllt sein, wie z. B. die Verhältnismäßigkeit der Maßnahmen und Zwecke sowie die Wahrung der verschiedenen Interessen: Recht auf freie Meinungsäußerung und das Recht auf Wahrung der persönlichen Interessen. Die Partei, welche die Offenlegung der personenbezogenen Daten beantragt, muss ihren Standpunkt rechtfertigen. Gemäß Art. 23 Abs. 1 und 5 muss hierfür ein „legitimes Interesse“ bestehen. Falls sich eine Partei weigert, die Daten offenzulegen, sie jedoch die für die Datenverarbeitung Verantwortliche ist, kann die Partei beim GIODO einen Antrag stellen, damit dieser nach Durchführung der einschlägigen Verfahren per Beschluss die Offenlegung der personenbezogenen Daten anordnen kann. In dieser Hinsicht ist die Beurteilung des GIODO entscheidend und sollte von den Umständen des jeweiligen Falles abhängen, da sowohl das Gesetz zur Bereitstellung von Dienstleistungen auf elektronischem Wege als auch das Datenschutzgesetz zur Anwendung kommen. Bei seinem Beschluss muss der GIODO in jedem Fall individuell beurteilen, welche rechtlich geschützten Interessen wichtiger sind – die personenbezogenen Daten oder die wirtschaftlichen Interessen des Unternehmens.

Das Oberste Verwaltungsgericht wies 2013 in letzter Instanz ein vom Gemeindevorsteher W. gegen das Urteil des Verwaltungsgerichts der Woiwodschaft vom 24. November 2011 (Nr. II SA/Wa 1828/11) eingelegtes Rechtsmittel ab. In seinem Urteil vom 14. März 2013 (Nr. I OSK 620/12) bestätigte das Oberste Verwaltungsgericht die im Rahmen seiner Verwaltungsverfahren getroffenen Beschlüsse des GIODO. Das Oberste Verwaltungsgericht betonte in seinem Urteil Folgendes: „Bei der Untersuchung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten (...) machten sowohl der GIODO als auch das Gericht erster Instanz auf angemessene Weise von den in Art. 23 Abs. 1 des Gesetzes vorgesehenen Grundsätzen zur Bestimmung der Zulässigkeit der Verarbeitung personenbezogener Daten Gebrauch. Dies unter der Annahme, dass es sich bei der Voraussetzung zur Legitimierung der Verarbeitung solcher Daten um die in Punkt 2 der oben genannten Bestimmung handelt." Letztere lässt die Verarbeitung personenbezogener Daten zu, falls dies zur Ausübung von Rechten und Pflichten aufgrund der gesetzlichen Vorschriften notwendig ist. In diesem Fall konnte die Verpflichtung, die sich aus einer rechtlichen Bestimmung für den Gemeindevorsteher im Zusammenhang mit den Inhalten des Gemeinderatsbeschlusses in der offiziellen Online-Publikation – Öffentlicher Informationsbulletin (BIP) – ergab, ohne die Offenlegung der personenbezogenen Daten des Klägers erfüllt werden. Wenn die öffentlichen Informationen einschließlich der Beschlüsse im BIP zum Zwecke der Transparenz der öffentlichen Aktivitäten des Gemeinderates veröffentlicht werden, so kann dieser Zweck auch dann erreicht werden, wenn die Daten von Privatpersonen zu Datenschutzzwecken aus den Informationen gelöscht werden.

C. Sonstige wichtige Informationen

Im Berichtszeitraum wurde bei der Anzahl der für eine Registrierung gemeldeten Dateien ein Anstieg beobachtet (um 40 % im Vergleich zu 2012, um 81 % im Vergleich zu 2011 und um ganze 242 % im Vergleich zu 2010). Erwähnenswert ist außerdem, dass der GIODO immer mehr Meldungen von privaten Stellen erhält – 2013 erhöhte sich die Anzahl der Meldungen von solchen Stellen im Vergleich zu 2012 um 95 %; die Anzahl der Meldungen von öffentlichen Stellen erhöhte sich dagegen nur um 3 %. Demzufolge stammten im Berichtszeitraum ganze 46 % aller Meldungen von privaten Stellen, während sich dieser Wert in 2012 und 2011 auf 31 bis 32 % belief. Im Jahr 2013 bearbeitete der GIODO 3 709 von für die Verarbeitung Verantwortlichen erstatteten Aktualisierungsmeldungen. Außerdem beschloss der GIODO in 340 Fällen eine Löschung von Datenspeichersystemen aus dem landesweiten offenen Register für Systeme zur Speicherung personenbezogener Daten.

Anlässlich des Europäischen Datenschutztages am 28. Januar 2013 organisierte der Generalinspektor wie jedes Jahr für alle Bürger einen Tag der offenen Tür sowie eine Konferenz mit dem Titel „Datenschutz im Gesundheitswesen und bei klinischen Studien". Außerdem wurde der Europäische Datenschutztag wie üblich auch in Brüssel gefeiert. Des Weiteren übernahm der GIODO eine aktive Rolle bei der 5. Internationalen Konferenz zu Computern, Privatsphäre und Datenschutz (23. bis 25. Januar), in deren Rahmen die polnische Datenschutzbehörde am 23. Januar 2013 eine Sonderdiskussionsrunde zur polnischen Gesetzgebung mit dem Titel „*Von ‚Solidarität' zur Überwachungsgesellschaft. Datenschutzdilemmas in Polen*" organisierte.

Der GIODO setzte seine Initiative fort und organisierte auch in anderen polnischen Städten zusätzliche Tage der offenen Tür, darunter der 3. Tag der offenen Tür in Poznán am 6. und 7. Mai 2013, der u. a. eine wissenschaftliche Konferenz zu den rechtlichen und wirtschaftlichen Aspekten der Verarbeitung personenbezogener Daten zu wirtschaftlichen Zwecken sowie eine Reihe von Seminaren und Schulungen für die öffentliche Verwaltung umfasste.

Vom 23. bis 26. September 2013 richtete der GIODO in Warschau die 35. Internationale Konferenz der Datenschutzbeauftragten mit dem Titel „Datenschutz: Ein Kompass in einer turbulenten Welt" aus. Die Konferenz trug weltweit zu einer Sensibilisierung beim Thema Datenschutz bei und legte zudem den Grundstein für den Austausch von Erfahrungen und Ansichten auf diesem Gebiet. Außerdem bot sie eine bessere Erklärung der Probleme im Zusammenhang mit Datenschutz. Zur geschlossenen Sitzung der 35. Internationalen Konferenz begrüßten wir 66 Delegierte aus aller Welt. Die Erfahrung und das Fachwissen

derart vieler Teilnehmer bot die einzigartige Gelegenheit, ganze 8 Beschlüsse zu verschiedenen Bereichen des Datenschutzes zu verabschieden, wie z. B. Akkreditierung, Profiling, die strategische Richtung der Konferenz, die internationale Durchsetzungskoordinierung, Offenheit bezüglich Datenschutzpraktiken, digitale Bildung für alle sowie Web-Tracking und Privatsphäre. Darüber hinaus wurde die „Warschauer Erklärung zur ‚Appifizierung' der Gesellschaft" verabschiedet. Auf der Offenen Konferenz kamen Vertreter verschiedener Bereiche wie Politik, Wissenschaft, Wirtschaft sowie nationale und internationale NRO zusammen, die in nach drei Themen aufgeteilten Gruppen debattierten: „Weltweite Reformen. Interoperabilität zwischen den Regionen", „Datenschutz und Technologie" und „Akteure: Perspektiven, Rollen, Interessen". Auf der Offenen Konferenz wurde die „Warschauer Erklärung 2013: Forderung nach Anreizen zur Förderung der Ernennung von DPOs" von der Confederation of European Data Protection Organisations und den nationalen Verbänden der Datenschutzbeauftragten in Europa verabschiedet.

2013 wurde das **PHAEDRA-Projekt** zur Verbesserung praktischer und hilfreicher Zusammenarbeit zwischen den Datenschutzbehörden gegründet, das von der Europäischen Kommission im Rahmen des Programms Grundrechte und Bürgerschaft mitfinanziert wird. Der GIODO beteiligt sich als Mitglied des Konsortiums an dem Projekt. Das Projekt wird in Zusammenarbeit mit der Vrije Universiteit Brüssel (Projektkoordinator), UK Trilateral Research & Consulting LLP (Partner) und der spanischen Universität Jaume I (Partner) realisiert. Das grundlegende Ziel des Projekts ist die Identifizierung der Probleme, welche die Zusammenarbeit zwischen bestimmten Datenschutzbehörden und anderen staatlichen, mit diesem Thema befassten Stellen behindern, sowie die Ausarbeitung von Empfehlungen, die zu einer Verbesserung der Situation beitragen. Demnach wird das Projekt zur Verbesserung der Kooperation und Koordination zwischen allen Interessenvertretern beitragen. Das Projekt soll 2015 abgeschlossen werden.

PORTUGAL

A. Zusammenfassung der Aktivitäten und Neuerungen

Im Mai 2013 veranstaltete die portugiesische Datenschutzbehörde in Lissabon die Data Protection Spring Conference, an der rund 130 Delegierte teilnahmen, um das Thema *Schutz der Privatsphäre: zukünftige Herausforderungen* zu diskutieren. Mitten in der EU-Datenschutzreform und der Modernisierung der Konvention 108 wurden auf der Konferenz der europäischen Kommissionsmitglieder wichtige Themen rund um die Zukunft des Datenschutzes besprochen, wie z. B. das Konzept personenbezogener Daten, die Rechte betroffener Personen im Internet, Informationssicherheit als Priorität, die Stärkung der Aufsicht sowie Kooperation.

Die portugiesische Datenschutzbehörde unterzeichnete ein Protokoll über die Zusammenarbeit mit dem Forschungszentrum der juristischen Fakultät der Universität Lissabon, um gemeinsam das Bewusstsein für Datenschutz und Privatsphäre zu schärfen und sich gegenseitig bei Initiativen zu unterstützen.

Die Datenschutzbehörde veröffentlichte neue Leitlinien zur Überwachung der Nutzung von IKT am Arbeitsplatz und aktualisierte damit ihre Leitlinien von 2002. Hierbei wurden das neue Arbeitsrecht sowie neue Entwicklungen in diesem Bereich berücksichtigt. Es war daher eine Aktualisierung und genauere Darstellung bestimmter Aspekte der privaten Nutzung von IKT durch Mitarbeiter erforderlich http://www.cnpd.pt/bin/orientacoes/Delib_controlo_comunic.pdf

Die Datenschutzbehörde überprüfte außerdem die Entwicklung des Projekts zu elektronischen Gesundheitsdaten und gab grünes Licht für Phase II der Plattform für Gesundheitsdaten. Die Behörde gab hiermit wichtige Bedingungen für die Verarbeitung personenbezogener Daten vor und bezog die Implementierung von Instrumenten mit eingebautem Datenschutz ein, um die Privatsphäre der Bürger zu verbessern und ihnen die Kontrolle über den Zugang zu ihren Daten und deren Nutzung zu verschaffen.

Infolge der praktischen Umsetzung der aktualisierten Datenschutzrichtlinie für elektronische Kommunikation berief die portugiesische Datenschutzrichtlinie wichtige Treffen mit Interessenvertretern aus Wirtschaft und Marketing ein, um mit ihnen über den neuen Rechtsrahmen, insbesondere über Cookies, zu sprechen.

Was die elektronischen Meldungen betrifft, erstellte die Datenschutzbehörde detailliertere Meldeformulare für bestimmte Fälle der Datenverarbeitung per Videoüberwachung und erhöhte somit die Anzahl der vollständig elektronischen Verfahren.

Organisation	Comissão Nacional de Protecção de Dados – CNPD
Vorsitz und/oder Gremium	Prof. Dr. Filipa Calvão (Vorsitzende)
Budget	2 356 436 EUR
Personal	Reduzierung von 25 auf 18 (bis Ende des Jahres) aufgrund rechtlicher Beschränkungen des öffentlichen Dienstes
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	12 285
Meldungen	11 170

Vorabprüfungen	10 280
Anträge betroffener Personen	89 Anträge auf Zugang zu und Löschung von Daten im Schengener Informationssystem
Beschwerden betroffener Personen	652
Vom Parlament bzw. der Regierung angeforderte Beratung	88
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	259 Anträge auf Zugang zu personenbezogenen Daten durch Dritte 910 Anträge auf Stellungnahme zur Aufhebung der Vertraulichkeit von Anrufen aufgrund störender Anrufe 2 585 schriftlich über die Website an die Zentrale geschickte Auskunftsersuchen (von für die Datenverarbeitung Verantwortlichen und betroffenen Personen)
Prüfmaßnahmen	
Prüfungen, Untersuchungen	246
Sanktionsmaßnahmen	
Sanktionen	158
Geldbußen	± 205 000 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

RUMÄNIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Organisation	Nationale Aufsichtsbehörde für den Schutz personenbezogener Daten
Vorsitz und/oder Gremium	Ancuta Gianina Opre
Budget	3 460 000 RON (ungefähr 772 321 EUR)
Personal	43 sowie Präsidentin und Vizepräsident der Datenschutzbehörde
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	632, davon 5 Beschlüsse zur Löschung personenbezogener Daten, 1 Beschluss zur Beendigung der Datenverarbeitung und die Löschung der verarbeiteten personenbezogenen Daten sowie 1 Empfehlung
Meldungen	7 499
Vorabprüfungen	-
Anträge betroffener Personen	156
Beschwerden betroffener Personen	721
Vom Parlament bzw. der Regierung angeforderte Beratung	32
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	-
Prüfmaßnahmen	
Prüfungen, Untersuchungen	229 vor Ort und 44 schriftlich
Sanktionsmaßnahmen	
Sanktionen	66 Geldbußen in Höhe von insgesamt 134 500 RON (ca. 30 022 EUR)
Geldbußen	124 Verwarnungen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	-

B. Rechtsprechung

Rechtsprechung 1

Ein Gericht veröffentlichte in einer von einem Sprecher des Gerichts präsentierten Pressemitteilung die personenbezogenen Daten des Opfers einer Straftat ohne dessen Einwilligung.

Die Pressemitteilung wurde zur gleichen Zeit in einer Nachrichtensendung im Fernsehen übertragen und eine Aufzeichnung davon auf der Website des Rundfunkveranstalters veröffentlicht, auf die öffentlich zugegriffen werden konnte.

Laut dem für die Datenverarbeitung Verantwortlichen las der Sprecher des Gerichts ein Dokument vor, das gemäß dem Tatsachenbestand erstellt wurde und den Vor- und Nachnamen des Opfers enthielt. In den daraufhin veröffentlichten Pressemitteilungen wurde das Opfer anhand der Initialen des Vor- und Nachnamens anonymisiert.

Dem für die Datenverarbeitung Verantwortlichen wurde für diesen Verstoß gemäß Art. 32 des Gesetzes Nr. 677/2001 eine Sanktion auferlegt.

Gleichzeitig wurde dem für die Datenverarbeitung Verantwortlichen empfohlen, ein Dokument vorzulegen, aus dem hervorgeht, dass die Sprecher bezüglich Datenschutz betroffener Personen im Zusammenhang mit Massenmedien geschult wurden.

Rechtsprechung 2

Ein Petent behauptete, von einem Reisebüro wiederholt unerwünschte Werbe-E-Mails erhalten zu haben, dessen Dienste er nach seiner Aussage noch nie in Anspruch genommen habe. Der Petent wies außerdem auf die Tatsache hin, dass die Werbe-E-Mails nicht die vollständigen Kontaktdaten des Reisebüros enthielten, das ihm auch dann noch Werbe-E-Mails zuschickte, nachdem er mittels der Abmeldefunktion in den Nachrichten darum gebeten hatte, solche E-Mails nicht mehr zu erhalten.

Infolge der Prüfung der Werbe-E-Mails, die der Petent erhalten hatte, kam die Datenschutzbehörde zu dem Schluss, dass diese nicht den exakten Namen eines Unternehmens enthielten. Die Datenschutzbehörde führte schriftlich und am Hauptsitz des Unternehmens mehrere Untersuchungen durch. Es konnte festgestellt werden, dass Vertreter des Reisebüros sich weigerten, die von der Datenschutzbehörde im Rahmen ihrer Untersuchungen angeforderten Informationen bereitzustellen, und dass die Werbe-E-Mails trotz des wiederholten Widerspruchs weiterhin beim Petenten eingingen.

Unter Berücksichtigung dieser Ergebnisse wurden dem für die Datenverarbeitung Verantwortlichen gemäß Gesetz Nr. 677/2001 und Gesetz Nr. 506/2004 Sanktionen auferlegt, da das Unternehmen sich weigerte, die Informationen bereitzustellen und an der angekündigten Untersuchung teilzunehmen, und es dem Petenten weiterhin wiederholt Werbe-E-Mails zuschickte, obwohl dieser ausdrücklich Widerspruch eingelegt hatte. Darüber hinaus enthielten die meisten E-Mails nicht die vollständigen Kontaktdaten der wahren Identität des Absenders.

Rechtsprechung 3

Das Innenministerium informierte die Datenschutzbehörde über die Offenlegung mehrerer Kategorien personenbezogener Daten im Internet und schickte als Nachweis ein optisches Gerät, auf dem Dokumente mit personenbezogenen Daten gespeichert waren.

Mit dieser Nachricht wurde die Datenschutzbehörde über notarische Dokumente im Internet (ein ODC-Netzwerk) informiert, welche die Adressen verschiedener Notariate, zentraler/lokaler Behörden, Verträge, Mandate, Erklärungen natürlicher Personen, Erklärungen bestimmter Richter in Bezug auf ihre Verweigerung der Kooperation mit Nachrichtendiensten oder deren Nicht-Mitgliedschaft bei der politischen Polizei, Authentifizierungsdokumente usw. enthielten.

Im Zuge der Untersuchung räumte der Notar, von dem diese Dokumente stammten, ein, dass die Dokumente echt und auf dem Computer seiner Mitarbeiter verfasst worden seien, er sich jedoch nicht erklären könne, wie sie im Internet veröffentlicht wurden. Laut dem Notar gab es infolge eines Virus einige Probleme mit den Computern.

Am Tag der Untersuchung stellte sich heraus, dass das Notariat nicht die Mindestanforderungen für den Schutz personenbezogener Daten gemäß Anordnung Nr. 52/2002 erfüllte.

Am Tag der Untersuchung war keine Authentifizierungsmethode erforderlich, um auf die Computer zuzugreifen, auf denen die notariellen Dokumente aufgesetzt wurden. Außerdem hätten die Dokumente kopiert und von jeder Personen, die Zugang zu dem Computer hat, ausgedruckt werden können. Aufgrund der fehlenden Authentifizierungsmethoden hätte sich jeder Zugang zu den auf den Computern des Notariats befindlichen personenbezogenen Daten verschaffen können. Demnach war es nicht möglich, anhand von Zugangsprotokollen die Personen zu identifizieren, die Zugang zu den IT-Geräten hatten. Des Weiteren bestand die Möglichkeit, Dokumente auf ein externes Gerät zu kopieren und dadurch die Computer über externe Speichermedien mit Viren zu infizieren.

Dem für die Datenverarbeitung Verantwortlichen wurden aufgrund des Verstoßes gegen Art. 33 des Gesetzes Nr. 677/2001 Sanktionen auferlegt, da der für die Datenverarbeitung Verantwortliche bis zum Tag der Untersuchung keine ausreichenden Sicherheits- und Vertraulichkeitsmaßnahmen ergriffen hatte, um die personenbezogenen Daten der Kunden, Mitarbeiter und Partner (einschließlich sensibler Daten) vor unbefugtem Zugriff und Veröffentlichen sowie gemäß Art. 19 und 20 des Gesetzes Nr. 677/2001 vor jeder Form der illegalen Datenverarbeitung, wie der Veröffentlichung derartiger personenbezogener Daten im Internet, zu schützen.

SCHWEDEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Die Aufmerksamkeit, die Datenschutzfragen in den Medien, bei für die Datenverarbeitung Verantwortlichen und in der Öffentlichkeit zukommt, hat 2013 zugenommen. Die schwedische Datenschutzbehörde (*Datainspektionen*) ist in den Nachrichten noch sichtbarer geworden und wir konnten einen Anstieg der Abonnenten unserer Pressemitteilungen und unseres Magazins verzeichnen. Wir hielten im Berichtszeitraum 62 Seminare und Vorlesungen ab, was einem Anstieg von 20 % entspricht. Des Weiteren stieg die Anzahl der Gesetzentwürfe, zu denen die Datenschutzbehörde um Stellungnahmen gebeten wurde, was eine Gesamtzahl von 116 Stellungnahmen ergab. Auch auf internationaler Ebene wurde die Arbeit der Behörde umfassender. Der Vorschlag der Kommission für ein neues Datenschutzgesetz wurde weiterhin diskutiert, und die Datenschutzbehörde hat diese Arbeit genau verfolgt. Die Zusammenarbeit zwischen den Datenschutzbehörden der EU-Mitgliedstaaten hat sich ebenfalls weiterentwickelt, und die schwedische Datenschutzbehörde beteiligte sich an zahlreichen Arbeitsgruppen auf diesem Gebiet.

Ein wichtiges Ereignis des Jahres 2013 war ein neues Videoüberwachungsgesetz, das am 1. Juli in Kraft trat. Das neue Gesetz überträgt der Datenschutzbehörde eine zentrale Verantwortung für die Aufsicht der Videoüberwachung und außerdem die Befugnis, gegen Genehmigungen solcher Videoüberwachungsaktivitäten durch die Bezirksverwaltungsbehörden Berufung einzulegen. Die Datenschutzbehörde hat hierfür viele Ressourcen aufgewendet. Im zweiten Halbjahr 2013 arbeiteten vier Mitarbeiter ausschließlich an Videoüberwachungsfragen.

Edward Snowdens Enthüllungen über die Überwachung der Internetkommunikation durch die NSA waren 2013 in Schweden und in anderen Ländern ein heiß diskutiertes Thema. Anschuldigungen, dass die schwedische Polizei Daten von Personen mit Roma-Herkunft gespeichert habe, sorgten ebenfalls für eine hitzige Debatte und führten zu einer Vor-Ort-Prüfung durch den speziellen Aufsichtsrat der Polizei.

Im Rahmen unserer Aufsichtsaktivitäten lag ein Schwerpunkt auf der Verarbeitung personenbezogener Daten durch staatliche Behörden. Dies umfasste die Aufsicht des zwischenbehördlichen Informationsaustauschs, der Nutzung mobiler Geräte und Cloud-Dienste durch staatliche Behörden sowie der Entwicklungen zum Thema E-Government. Ein weiterer Schwerpunkt war die Polizei, bei der wir Informationen über deren Verarbeitung personenbezogener Daten sammelten, indem wir an alle 21 regionalen Polizeibehörden Fragebögen schickten. Außerdem führten wir bei einigen dieser regionalen Behörden Vor-Ort-Prüfungen durch. Zudem prüften wir erstmals die Verarbeitung personenbezogener Daten beim militärischen Nachrichtendienst im Rahmen geheimdienstlicher Aktivitäten.

Organisation	Schwedische Datenschutzbehörde
Vorsitz und/oder Gremium	Kristina Svahn Starrsjö. Vorsitzende
Budget	42 583 000 SEK = 4 288 750 EUR
Personal	Ungefähr 45 Mitarbeiter (entspricht 41 Vollzeitstellen)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	26 Beschlüsse zu Genehmigungen der Datenverarbeitung im Rahmen von strafrechtlichen Verurteilungen (größtenteils im Zusammenhang mit OFAC-Listen) 64 Stellungnahmen in Absprache mit Datenschutzbeauftragten

	214 Beschlüsse in Prüfungsfällen (siehe unten) 2 Checklisten; Verarbeitung personenbezogener Daten im Zusammenhang mit Personalbeschaffungsdatenbanken und Forschungsaktivitäten
Meldungen	3 378
Vorabprüfungen	44 (bezüglich der Verarbeitung personenbezogener Daten im Zusammenhang mit Forschungsaktivitäten)
Anträge betroffener Personen	230 formelle Anträge, 6 100 Fragen per E-Mail, 7 100 Anrufe
Beschwerden betroffener Personen	352
Vom Parlament bzw. der Regierung angeforderte Beratung	116 formelle Anträge, rund 70 informelle Konsultationen
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	53 Pressemitteilungen, 62 Vorträge und Seminare
Prüfmaßnahmen	
Prüfungen, Untersuchungen	214
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	7 047 für die Datenverarbeitung Verantwortliche haben Datenschutzbeauftragte ernannt

B. Rechtsprechung

Im März 2013 wies das Bezirksverwaltungsgericht in Stockholm die Berufung eines Sicherheitsunternehmens ab, das eine Datenbank – eine Art „schwarze Liste“ – erstellen wollte, um Menschen davon abzuhalten, die Tankstelle ohne zu bezahlen zu verlassen. Die Datenschutzbehörde hatte 2011 entschieden, dass eine solche Datenbank aufgrund der übermäßigen Datenerfassung, dem Risiko inkorrekter Informationen und dem Mangel an Mitteln zur Berichtigung der Informationen nicht genehmigt werden könne. Das Bezirksverwaltungsgericht bestätigte diesen Beschluss.

Im Bereich Kreditinformationen stimmte das Bezirksverwaltungsgericht dem früheren Beschluss der Datenschutzbehörde zu, für Nutzer, die Zugang zu Kreditinformationen im Internet haben, eine sichere Autorisierung erforderlich zu machen. Zwei Kreditauskunfteien legten Informationen über das Internet offen und baten um Benutzernamen und Passwörter, um Zugang zu erhalten. Laut Datenschutzbehörde

und Bezirksverwaltungsgericht erfordert diese Art der Offenlegung eine sicherere Autorisierung, wie z. B. einen elektronischen Ausweis oder Einmalpasswörter.

Eine weitere Rechtssache im Zusammenhang mit Kreditinformationen betraf die Verpflichtung, der Person, auf die sich die Informationen beziehen, eine Kopie der offengelegten Informationen zukommen zu lassen. Die Auskunfteien stellten bei der Offenlegung von Kreditinformationen über das Internet lediglich einen Link auf eine Website zur Verfügung, auf der die Informationen eingesehen werden konnten. In ihrem Beschluss kam die Datenschutzbehörde zu dem Schluss, dass ein solches Verfahren nur angemessen ist, wenn es als Alternative angeboten würde und die betroffene Person es akzeptiert, und dass anderenfalls eine schriftliche Kopie per Post verschickt werden muss. Das Bezirksverwaltungsgericht war derselben Ansicht.

C. Sonstige wichtige Informationen

Anfang 2013 gab die Datenschutzbehörde eine Stellungnahme zu einem Bericht einer Untersuchungskommission ab, die den Bedarf nach einer Überarbeitung der verfassungsrechtlichen Bestimmungen zur Meinungsfreiheit untersucht hatte. In ihrer Stellungnahme schlug die schwedische Datenschutzbehörde die Einführung einer allgemeinen Bestimmung vor, die schwere Verstöße gegen die Privatsphäre im Internet unter Strafe stellt. Wir erhalten eine große Anzahl an Beschwerden von Personen, die der Ansicht sind, dass ihre Privatsphäre aufgrund von Veröffentlichungen im Internet verletzt wurde. In vielen Fällen sind wir machtlos, da diese Veröffentlichungen aufgrund der Meinungsfreiheit vom Datenschutzgesetz ausgenommen sind. In unserer Stellungnahme brachten wir die Ansicht zum Ausdruck, dass eine Bestimmung, die strafrechtliche Sanktionen für schwere Verstöße gegen die Privatsphäre auf Websites usw. enthält, zu einer Prävention dieses Verhaltens beitragen würde. Im Laufe des Jahres haben wir Lehrkräften Informationen zu den Rechten und Pflichten im Internet bereitgestellt, die sie an ihre Schüler verteilen können. Wir haben außerdem Seminare für die Polizei und Staatsanwälte organisiert, um sie bei Ermittlungen von schweren Verstößen gegen die Privatsphäre im Internet zu unterstützen.

Im November 2013 feierte die Datenschutzbehörde ihr 40-jähriges Jubiläum. Die schwedische Datenschutzbehörde wurde 1973 gegründet und war die erste nationale Datenschutzbehörde der Welt.

SLOWAKEI

A. Zusammenfassung der Aktivitäten und Neuerungen

Das erste Halbjahr 2013 stand im Zeichen fortlaufender Bemühungen zur Änderung des Datenschutzrechts und das zweite Halbjahr im Zeichen der Umsetzung der verabschiedeten Gesetze in die Praxis. 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 Anwendersicht. Dieser Gesetzgebungsprozess endete im April 2013, als das slowakische Parlament ein neues Datenschutzgesetz mit der Nr. 122/2013 Coll. verabschiedete.

Das Gesetz trat am 1. Juli 2013 in Kraft und führte mehrere wichtige Veränderungen herbei, wie z. B. eine bessere Spezifikation des Status von für die Datenverarbeitung Verantwortlichen und betroffenen Personen sowie deren Beziehungen untereinander; eine Regulierung der Verarbeitung biometrischer Daten; eine eindeutige Definition des Umfangs und der Dokumentation von Sicherheitsmaßnahmen; die Festlegung des Instituts der befugten Person (einer Person, die beim für die Datenverarbeitung Verantwortlichen Kontakt mit den personenbezogenen Daten hat); eine neue Regelung der Ernennung eines Datenschutzbeauftragten (das neue Datenschutzgesetz setzt eine verpflichtende Prüfung voraus); eine Stärkung der Mechanismen für den Schutz der Rechte betroffener Personen; eine Änderung der Bedingungen für die grenzüberschreitende Übermittlung personenbezogener Daten; die Festlegung von Bedingungen für die Meldung und besondere Registrierung von Datenspeichersystemen; die Einführung einer Verwaltungsgebühr für besondere Registrierungen; die Bestimmung der Position der Behörde; die Erweiterung der Kompetenzen im Bereich des Datenschutzes usw.

Die Datenschutzbehörde setzte seine wöchentlichen Überwachungs- und Beurteilungsdienste für Material fort, das im Gesetzgebungsprozess im Rahmen des interministeriellen Überprüfungsverfahrens enthalten ist. Das Ziel dieses Verfahrens ist die Erfassung jeglichen Materials des interministeriellen Überprüfungsverfahrens und damit eine effektive Beurteilung und Kommentierung dieses Materials. Die Datenschutzbehörde beurteilte sämtliches Material im Hinblick auf die Einhaltung des Datenschutzgesetzes, um den gesetzlich Schutz der grundlegenden Anforderungen des gesellschaftlichen Lebens zu gewährleisten 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.

Die Verabschiedung und Umsetzung eines neuen Datenschutzgesetzes erhöhte das Interesse all jener, die mit Datenschutz zu tun haben. Die Anzahl der Auskunftsersuchen zu diesem Thema stieg im zweiten Halbjahr 2013 enorm. Die Datenschutzbehörde musste schriftlich insgesamt 2 263 Anträge beantworten, von denen sich 1 671 auf das neue Gesetz bezogen. Täglich gingen Dutzende telefonische Anfragen ein. Die Tatsache, dass Personen, die als Datenschutzbeauftragte fungieren möchten, dazu verpflichtet sind, bei der Datenschutzbehörde eine Prüfung abzulegen, hat ebenfalls für ein erhöhtes Interesse sowie für Diskussionen und einen besseren Datenschutz gesorgt. Die Datenschutzbehörde organisierte landesweit Schulungen für Datenverarbeiter, für die Datenverarbeitung Verantwortliche, DPOs und befugte Mitarbeiter, um den Bedarf an rechtlichem Fachwissen zu decken.

Landesweite Prüfungen durch die Datenschutzbehörde

Im Laufe des Jahres 2013 führte die Datenschutzbehörde gemäß dem jährlichen Prüfplan sowie auf Anfrage betroffener Personen, staatlicher Behörden und sonstiger Personen mehrere landesweite

Prüfungen durch. Der jährliche Prüfplan konzentrierte sich auf die Prüfungen von Datenverarbeitungsaktivitäten in Datenspeichersystemen, wie z. B. in den Bereichen Sozialwesen, kommunale Selbstverwaltung, Finanzdienstleistungen oder Videoüberwachung. Aufgrund der Gesetzesänderung zum Halbjahr 2013 wurden die Prüfungen in zwei Teile untergliedert. Aufgrund der Tatsache, dass sich die Bestimmungen für Prüfungen und Kontrollverfahren unterscheiden, wurde der erste Teil nach Gesetz Nr. 428/2002 Coll. und der zweite Teil nach Gesetz Nr. 122/2013 Coll. zum Schutz personenbezogener Daten durchgeführt.

Die nationale Einheit SIRENE

Auf Grundlage der dritten Bestimmung des Schengen-Aktionsplans der slowakischen Republik überprüfte die Datenschutzbehörde die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch das Schengen-Informationssystem der zweiten Generation, dem die slowakische Republik am 9. April 2014 beitrat. Die Prüfung bezog sich auf die Konformität der Datenschutzvorschriften innerhalb eines angemessenen Rechtsrahmens sowie auf die Sicherheit der verarbeiteten personenbezogenen Daten. Die Datenschutzbehörde kontrollierte außerdem das Ausmaß der verarbeiteten personenbezogenen Daten von Personen, die zum Zwecke der Auslieferung festgenommen werden sollen, von Drittstaatsangehörigen im Zusammenhang mit einer Einreise- oder Aufenthaltsverweigerung sowie von Personen und Dingen zum Zwecke der verdeckten Überwachung oder gezielten Kontrolle. Die Datenschutzbehörde kam zu dem Schluss, dass die Sicherheit der Verarbeitung von personenbezogenen Daten auf einem hohen Niveau liegt und in vollem Umfang dem einschlägigen Rechtsrahmen entspricht.

Sozialwesen

Die Datenschutzbehörde richtete ihre Aufsichtsaktivitäten 2013 auf Bereiche aus, in denen die für die Datenverarbeitung Verantwortlichen nicht nur allgemeine personenbezogene Daten, sondern auch Daten spezieller Kategorien verarbeiten. Der Bereich Sozialwesen erfordert die besondere Aufmerksamkeit der Datenschutzbehörde, da alle in diesem Bereich tätigen Organisationen (für die Datenverarbeitung Verantwortlichen) eine erhebliche Menge an Daten spezieller Kategorien verarbeiten. Die Prüfungen in diesem Bereich folgten auf die Prüfungen des Vorjahrs und zeigten, dass die für die Datenverarbeitung Verantwortlichen einige administrative Verpflichtungen gemäß Gesetz Nr. 428/2002 Coll. vernachlässigten, wie z. B. die Einweisung der verantwortlichen Personen, die mit personenbezogenen Daten umgehen, bezüglich ihrer Verpflichtungen, das Führen eines Registers bei Nutzung eines Datenspeichersystems, das Versäumnis, einen Datenschutzbeauftragten zu ernennen usw. Die Datenschutzbehörde wies Korrekturmaßnahmen an und leitete in fünf Fällen ein Bußgeldverfahren ein.

Kommunale Selbstverwaltung

Kommunale Selbstverwaltungen gehören zu einer Art der für die Datenverarbeitung Verantwortlichen, die spezielle Datenkategorien verarbeiten, die vielen nationalen Gesetzen unterliegen. Sie führen Bürgerregister, ziehen lokale Abgaben und Gebühren ein, bieten soziale Unterstützung und Leistungen sowie sonstige kommunale Dienstleistungen an usw. All diese Aktivitäten erfordern die Verarbeitung spezieller Datenkategorien und setzen voraus, dass die kommunale Selbstverwaltung dazu in der Lage ist, die wirtschaftlichen, sozialen, ethnischen oder gesundheitlichen Situationen in Bezug auf die betroffenen Personen in vollem Umfang zu erfassen. Die Datenschutzbehörde führte 10 Prüfungen durch, von denen 9 mit einem Protokoll für Korrekturmaßnahmen abgeschlossen wurden. Abgesehen von dem Versäumnis administrativer Verpflichtungen hatten die für die Datenverarbeitung Verantwortlichen auf ihren Websites die persönlichen Identifikationsnummern betroffener Personen veröffentlicht, bei Gemeinderatssitzungen Informationen über die wirtschaftliche Situation betroffener Personen offengelegt und es versäumt, über die Anbringung von Videoüberwachungskameras an öffentlichen Plätzen zu informieren. In einem Fall erfüllte der für die Datenverarbeitung Verantwortliche außerdem keinerlei gesetzliche Verpflichtungen.

Finanzdienstleistungen

Die Datenschutzbehörde führte im Bereich Finanzdienstleistungen drei Prüfungen gemäß Gesetz Nr. 428/2002 Coll. und acht Prüfungen gemäß Gesetz Nr. 122/2013 Coll. durch. Die für die Datenverarbeitung Verantwortlichen verarbeiteten personenbezogene Daten hauptsächlich gemäß Sondergesetz Nr. 186/2009 Coll. über finanzielle Vermittlung und Beratung. Dieses Gesetz regelt die Verarbeitung spezieller Datenkategorien, weshalb die Datenschutzbehörde ihre Aufsichtsaktivitäten in diesem Sektor verstärkte. Probleme bestanden hauptsächlich im Zusammenhang mit der Datenverarbeitung durch Auftragsverarbeiter, der Bestimmung des Umfangs und der Bedingungen der Verarbeitung, der rechtswidrigen Erfassung und Verarbeitung sowie der Nutzung von Daten zu anderen Zwecken ohne Benachrichtigung der betroffenen Personen.

Grenzüberschreitende Übermittlung personenbezogener Daten

Mit dem Gesetz Nr. 122/2013 Coll. wurden außerdem die Bedingungen für grenzüberschreitende Datenströme geändert. Das Konzept wurde genauer an die moderne Version angepasst, die ein höheres Maß an Flexibilität ermöglicht und den Verwaltungsaufwand reduziert. Das Gesetz unterscheidet natürlich zwischen Übermittlungen an Mitgliedstaaten der Europäischen Union und an die Länder, die zum Europäischen Wirtschaftsraum gehören, und ermöglicht Übermittlungen an Drittländer, deren angemessenes Datenschutzniveau von der Europäischen Kommission per Beschluss garantiert wurde. Es enthält außerdem Bestimmungen bezüglich der Datenübermittlung an Drittländer mit unangemessenen Datenschutzniveaus. Fälle grenzüberschreitender Datenströme innerhalb der EU sowie in Drittländer müssen ebenfalls ein angemessenes Datenschutzniveau aufweisen. Das Gesetz erfordert lediglich die Existenz einer angemessenen Rechtsgrundlage für die Durchführung solcher Datenverarbeitungsaktivitäten, und der für die Datenverarbeitung Verantwortliche muss die betroffenen Personen über die Übermittlung informieren und dafür sorgen, dass ihre Daten während der Übermittlung geschützt sind. Für diese Art von grenzüberschreitender Übermittlung gibt es keine weiteren Einschränkungen. Daten können nur dann an Drittländer übermittelt werden, die kein angemessenes Datenschutzniveau aufweisen, wenn der für die Datenverarbeitung Verantwortliche den Schutz der Privatsphäre und der Grundrechte und Freiheiten der betroffenen Personen ausreichend garantieren kann. Verbindliche unternehmensinterne Vorschriften und Standardvertragsklauseln gelten als ausreichende Garantien für solche Übermittlungen.

Der Verwaltungsaufwand wurde durch einen neuen Mechanismus der vorherigen Autorisierung von grenzüberschreitenden Übermittlungen an Drittländer ohne ausreichenden Datenschutz verringert. Früher musste der für die Datenverarbeitung Verantwortliche vor allen Übermittlungen an Drittländer ohne eine angemessene Entscheidung nach Gesetz Nr. 428/2002 Coll. eine Genehmigung einholen. Heute ist es nur dann nötig, die Genehmigung der Datenschutzbehörde einzuholen, wenn der für die Datenverarbeitung Verantwortliche Standardvertragsklauseln ändert oder eine offensichtliche Diskrepanz vorliegt.

Organisation	Behörde für den Schutz personenbezogener Daten der Slowakischen Republik
Vorsitz und/oder Gremium	Eleonóra Kročianová, Vorsitzende
Budget	876 324 EUR
Personal	33 Mitarbeiter
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Die Datenschutzbehörde gab 2013 die folgenden sechs Empfehlungen heraus: 1/2013 Das Konzept personenbezogener Daten

	2/2013 Grundlegende Konzepte – Menschen und die Verarbeitung personenbezogener Daten 3/2013 Videoüberwachung in Pkws 4/2013 Grenzüberschreitende Übermittlung personenbezogener Daten 5/2013 Das Konzept der Datenspeichersysteme 6/2013 Die Verarbeitung biometrischer Daten
Meldungen	387
Vorabprüfungen	28
Anträge betroffener Personen	160 Beschwerden und Anträge betroffener Personen 34 Beschwerden und Anträge sonstiger Personen
Beschwerden betroffener Personen	
Vom Parlament bzw. der Regierung angeforderte Beratung	108
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Die Datenschutzbehörde hielt 7 Reden im Radio und 9 im Fernsehen und veröffentlichte 58 Beiträge in gedruckten Medien.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	163 Prüfungen
Sanktionsmaßnahmen	
Sanktionen	151 Beschlüsse von Korrekturmaßnahmen
Geldbußen	11 Geldbußen in Höhe von insgesamt 25 160 EUR 9 Geldbußen wegen Verwaltungsverstößen in Höhe von insgesamt 20 360 EUR 2 Geldbußen in Höhe von insgesamt 3 500 EUR
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	Die Datenschutzbehörde führte während der Gründung der Datenschutzbehörde 253 DPO-Prüfungen und 47 in anderen Teilen des Landes durch. Insgesamt bewarben sich 3 073 Personen. Die Datenschutzbehörde stellte 1 705 Zertifikate für das Bestehen der Tests aus.

B. Rechtsprechung

Die Rechtsordnung der Slowakischen Republik beruht wie in mehreren anderen Mitgliedstaaten nicht auf Rechtsprechung.

C. Sonstige wichtige Informationen

Internationale Zusammenarbeit

Internationale Aktivitäten resultierten größtenteils aus der EU-Mitgliedschaft und erfolgten in Arbeitsgruppen unter der Schirmherrschaft und gemäß den Rechtsakten der Europäischen Gemeinschaften sowie auf Anfragen auf Partnerschaft und Zusammenarbeit der Datenschutzbehörde. Die Datenschutzbehörde nahm 2013 an allen vom Europarat, vom Rat der Europäischen Union und von der Europäischen Kommission organisierten Sitzungen teil. Neben regelmäßigen Sitzungen der Arbeitsgruppen nahm die Datenschutzbehörde an der Konferenz der mittel- und osteuropäischen Datenschutzbehörden, an der Frühjahrskonferenz in Lissabon und an einem Workshop über die Bearbeitung von Fällen in Sarajewo teil und organisierte eine bilaterale Sitzung mit der Datenschutzbehörde der Tschechischen Republik. Beide Datenschutzbehörden suchten nach Fällen mit gemeinsamen Problemen, die auf koordinierte Weise untersucht werden könnten, und unterzeichnete am Ende der Sitzung eine Absichtserklärung.

SLOWENIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Jahr 2013 markierte das zehnte Jubiläum der Datenschutzbeauftragten, deren Rolle sich in diesen Jahren von einer kleinen Beschwerdeinstanz unter der Leitung des Beauftragten für den Zugang zu öffentlichen Informationen zu einem wichtigen Garanten für Transparenz und Schützer personenbezogener Daten entwickelt hat. Darüber hinaus gab es 2013 einige wichtige Meilensteine zu verzeichnen, die es uns bewusst machten, wie viel wir zu verlieren haben, wenn wir unseren Datenschutz aufgeben. Nennenswerte Zwischenfälle im Zusammenhang mit Verstößen gegen die Privatsphäre zeigten, wie es täglich zu Verstößen gegen unsere Privatsphäre kommt und wie machtlos wir als Individuen sind, wenn der Staat in diesem Bereich die Kontrolle verliert.

2013 erhielt die Datenschutzbeauftragte 106 Anträge auf Stellungnahme zu Gesetzentwürfen und anderen Verordnungen, welche die Erfassung und Verarbeitung personenbezogener Daten betreffen (26 mehr als 2012). Wir stellten eine beunruhigend hohe Zahl an Gesetzesänderungen und Gesetzentwürfen fest, die ernsthafte Eingriffe in die Privatsphäre des Einzelnen hinsichtlich der Verarbeitung personenbezogener Daten nach sich ziehen würden und die im Schnellverfahren ohne sachgerechte Analysen und Beurteilungen der Konsequenzen zur Gewährleistung des grundgesetzlich garantierten Schutzes der Privatsphäre und der personenbezogenen Daten betroffener Personen verabschiedet werden. Zu den Gesetzen, die geändert werden sollen, zählen die Strafprozessordnung, das Gesetz über die Entfernung und Transplantation von menschlichen Körperteilen zu medizinischen Zwecken, das Gesetz über elektronischen Geschäftsverkehr, das Gesetz zur Prävention von Schwarzarbeit und -beschäftigung, das Gesundheits- und Krankenversicherungsgesetz, das Gesetz über Patientenrechte, das Gesetz über geringfügige Straftaten sowie das allgemeine Gesetz zur Datenaufbewahrung gemäß Art. 165 Abs. 4 des Gesetzes über den Schutz der Privatsphäre in der elektronischen Kommunikation.

Im vergangenen Jahr erhielt die Datenschutzbeauftragte in ihren beiden Tätigkeitsbereichen eine hohe (Rekord-) Zahl an Anträgen betroffener Personen, darunter Anträge auf Stellungnahmen, Beschwerden und Berufungen. Einerseits ist dies erfreulich, da daran deutlich zu erkennen ist, dass sich die Menschen immer mehr des Zwecks und der Relevanz beider Menschenrechte bewusst sind, die in den Kompetenzbereich der Datenschutzbeauftragten fallen. Gleichzeitig kann die Tatsache nicht ignoriert werden, dass die in diesem Jahr zum wiederholten Mal gestiegene Anzahl der Beschwerden und durchgeführten Untersuchungen auf den zunehmenden Trend hin zu problematischen Praktiken der verantwortlichen Behörden auf dem Gebiet des Zugangs zu öffentlichen Informationen zurückzuführen ist, während wir es andererseits mit einem zunehmend unersättlichen Bedürfnis vieler verschiedener privater wie staatlicher für die Datenverarbeitung Verantwortlicher nach der Erfassung und Verarbeitung von Daten zu tun haben.

Die Reaktionen von natürlichen Personen zeigen, dass die Arbeit der Datenschutzbeauftragten Wirkung zeigt. Das Meinungsforschungsinstitut Politbarometer führte im Januar 2013 eine Meinungsumfrage durch, die eine Beurteilung der Leistung nationaler Aufsichtsbehörden umfasste. Die Ergebnisse haben gezeigt, dass die Leistung mehrerer unabhängiger Aufsichtsbehörden (einschließlich der der Datenschutzbeauftragten) von den Befragten als extrem und äußerst positiv wahrgenommen wird (im Gegensatz zur Beurteilung der zentralstaatlichen Behörden wie der Nationalversammlung, der Regierung und des Regierungspräsidenten). Es darf nicht außer Acht gelassen werden, dass die Datenschutzbeauftragte auch bei den Befragungen von 2010, 2011 und 2012 unter den Zentralregierungs- und Sozialinstitutionen zu denen gehörte, denen die slowenische Bevölkerung am meisten vertraut. Dies zeigt, dass die Bevölkerung der Arbeit der Datenschutzbeauftragten ein fundiertes Vertrauen entgegenbringt.

Im Hinblick auf den Datenschutz wurden 2013 von der Datenschutzbeauftragten 712 Prüfungen und 106 Strafverfahren bearbeitet. Der Datenschutzbeauftragten wurde 2013 die Kompetenz für die Beobachtung und Prüfung des Cookie-Gesetzes übertragen. Mitte Juni 2013 traten die Bestimmungen

des Cookie-Gesetzes in Kraft, das die Aufbewahrung von Informationen oder den Zugang zu auf den Endgeräten von Teilnehmern oder Nutzern gespeicherten Daten betrifft. Nach Inkrafttreten des Cookie-Gesetzes erhielt die Datenschutzbeauftragte bis Ende 2013 35 Beschwerden betreffend 141 verantwortlichen Organisationen (Website-Betreiber). Die Beschwerden bezogen sich größtenteils auf eine unzureichende oder fehlende Benachrichtigung sowie auf unangemessene Mechanismen für die Einholung von Einwilligungen. Websites stellten nicht immer angemessene Kontrollmechanismen zur Verfügung, welche das Setzen von Cookies erlauben oder verbieten. Insbesondere gab es mehrere Fälle, bei denen eine Website Cookies setzte, wofür seit Inkrafttreten des neuen Gesetzes zum Schutz der Privatsphäre in der elektronischen Kommunikation die ausdrückliche Einwilligung der Nutzer erforderlich ist. Besonders problematisch erwiesen sich dabei nicht nur Cookies zu Werbe- oder Analysezwecken, sondern auch Cookies bestimmter Plug-Ins, die in der Regel von Dritten installiert werden und eine Aufzeichnung der tagtäglichen Online-Aktivitäten des Nutzers auf mehreren verschiedenen Websites ermöglichen (sogenannte „Tracking-Cookies"). Die überwiegende Mehrheit der verantwortlichen Organisationen, gegen die die Datenschutzbeauftragte Prüfungsverfahren einleitete, korrigierte die identifizierten Regelwidrigkeiten oder Verstöße, nachdem sie darüber informiert worden waren. Daher musste die Datenschutzbeauftragte diesbezüglich keine Beschlüsse herausgeben. In Zusammenarbeit mit den verantwortlichen Stellen entwickelte die Datenschutzbeauftragte Leitlinien für die Nutzung von Cookies sowie Antworten auf häufig auf den Websites der Datenschutzbeauftragten gestellten Fragen. Website-Betreiber stellten zahlreiche Fragen zum Thema Web-Analytik, insbesondere hinsichtlich einer derartigen Implementierung, dass sie auf Grundlage einer implizierten Einwilligung beim ersten Besuch der Website erlaubt sind. Die Datenschutzbeauftragte entfernte vorwiegend auf Websites des öffentlichen Sektors und auf großen slowenischen Medienwebsites erfolgreich einige der Plug-Ins, die vergleichsweise stärker in die Privatsphäre eingreifen.

Neben den Beschwerden im Zusammenhang mit Cookies richtete sich im Berichtszeitraum 2013 wie schon in den Vorjahren der Großteil der Beschwerden gegen Videoüberwachungsaktivitäten und die Nutzung personenbezogener Daten zu Direktmarketingzwecken. Abgesehen von den bereits genannten Beschwerden muss den Beschwerden besondere Aufmerksamkeit zukommen, die im Zusammenhang mit der Zustellung und dem anschließenden Lesen von E-Mails an die Unternehmens-E-Mail-Adressen von Mitarbeitern; im Hinblick auf die Veröffentlichung personenbezogener Daten auf Websites der für die Datenverarbeitung Verantwortlichen; bezüglich dem Verschicken kostenpflichtiger SMS-Nachrichten sowie im Zusammenhang mit der Verarbeitung falscher und veralteter Daten eingelegt wurden.

Neue Herausforderungen für den Schutz personenbezogener Daten ergaben sich weiterhin im Bereich der modernen Informations- und Kommunikationstechnologien. Dies betrifft vorwiegend die umfassendere Nutzung ferngesteuerter Automationssysteme, die eine verborgene, schwer aufzudeckende und übermäßige Erfassung personenbezogener Daten ermöglichen und einen schwerwiegenden Eingriff in die Privatsphäre darstellen. Da diese ferngesteuerten Automationssysteme mit einer breiten Vielfalt an Sensoren ausgestattet werden können, welche die Aufnahme von Videos, Bildern, Tonspuren sowie Daten zu Temperatur, Bewegung und Standort ermöglichen, wird deren Nutzung die Aufsichtsbehörden und die Wächter des Datenschutzes vor große Herausforderungen stellen.

Ein wichtiger Bestandteil der Aktivitäten der Datenschutzbeauftragten bezieht sich außerdem auf die Erteilung neuer Befugnisse an Strafverfolgungsbehörden, insbesondere im Hinblick auf die sehr häufigen Änderungen der Strafprozessordnung.

Die Datenschutzbeauftragte merkt an, dass es nach wie vor große Schwierigkeiten mit der Auslegung des Datenschutzes in der Kommunikation gibt, und weist darauf hin, dass ein schriftlicher Antrag einer staatlichen Behörde nicht ausreicht, um Informationen über die personenbezogenen Daten kommunizierender Individuen zu erhalten, da dies unter die Bestimmungen von Art. 37 der Verfassung der Republik Slowenien fällt. Dieser Artikel sieht vor, dass die Vertraulichkeit von Korrespondenz und anderer Kommunikationsmittel garantiert sein muss und dass der Schutz der Vertraulichkeit von Korrespondenz und sonstiger Kommunikationsmittel sowie die Unantastbarkeit der persönlichen Privatsphäre nur auf gerichtliche Anordnung hin aufgehoben werden kann, falls dies für den Anstoß oder den Verlauf strafrechtlicher Verfahren oder aus Gründen der nationalen Sicherheit erforderlich ist. Ende

2013 veröffentlichte die Datenschutzbeauftragte einen Bericht, der beunruhigende Polizeipraktiken ans Licht brachte, die 2012 trotz der eindeutigen Bestimmungen des Gesetzes über elektronischen Geschäftsverkehr und der Strafprozessordnung auf der Grundlage von 35 schriftlichen Anträgen bei Dienstleistern der Informationsgesellschaft die Daten von Nutzern von Websites mit Inhalten, die von Nutzern des Dienstes bereitgestellt oder übermittelt werden, beantragt hatte. In 31 Fällen geschah dies ohne erforderliche gerichtliche Anordnung, während bei 30 % der schriftlichen Anträge im Bezug auf die jeweilige Straftat nicht mit einer gerichtlichen Anordnung zu rechnen gewesen wäre.

Organisation	Informationsbeauftragte der Republik Slowenien
Vorsitz und/oder Gremium	Nataša Pirc Musar
Budget	1 291 010 EUR
Personal	32 Angestellte: Kabinett (2 bis 6 der Mitarbeiter sind auch Datenschutzbeauftragte und 2 Rechtsberater), Verwaltung (3), Rechtsberater für den Zugang zu öffentlichen Informationen und Datenschutz (10), Datenschutzforscher (2), Datenschutzbeauftragte (10) und 1 Systemadministrator.
Allgemeine Aktivitäten	Datenschutz und Zugang zu öffentlichen Informationen
Beschlüsse, Stellungnahmen, Empfehlungen	71 umfassende und 2 389 kurze Stellungnahmen und Empfehlungen auf der Grundlage von Anfragen betroffener Personen und für die Datenverarbeitung Verantwortlicher.
Meldungen	134 Meldungen zu Datenspeichersystemen mit personenbezogenen Daten.
Vorabprüfungen	23 Vorabprüfungen: 11 zu Biometrik, 16 zur Übermittlung von Daten an Drittländer, 5 zur Verknüpfung von Speichersystemen.
Anträge betroffener Personen	2 460 Anträge auf Stellungnahmen/Klärungen von betroffenen Personen.
Beschwerden betroffener Personen	Insgesamt 852 Beschwerden betroffener Personen. Bereiche: 68 betreffend die unrechtmäßige Übermittlung oder Offenlegung von Daten, 43 betreffend die unrechtmäßige Datenerfassung, 28 betreffend Cookies, 26 betreffend unzureichende Datensicherheit, 15 betreffend unrechtmäßiger Videoüberwachung und unangemessener Nutzung von Videomaterial sowie 7 betreffend Direktmarketing. Darüber hinaus 63 Beschwerden zum Umgang mit Rechten betroffener Personen.
Vom Parlament bzw. der Regierung angeforderte Beratung	Der Gesetzgeber und für die Gesetzentwürfe zuständige Behörden konsultierten die Datenschutzbeauftragte in Bezug auf 106 Gesetze und andere Rechtstexte, wie z. B. die Strafprozessordnung, das Gesetz über die Entfernung und Transplantation von menschlichen Körperteilen zu medizinischen Zwecken, das Gesetz über elektronischen Geschäftsverkehr, das Gesetz zur Prävention von Schwarzarbeit und -beschäftigung, das Gesundheits- und Krankenversicherungsgesetz, das Gesetz über Patientenrechte, das Gesetz über geringfügige Straftaten sowie das allgemeine Gesetz zur Datenaufbewahrung gemäß Art. 165

	Abs. 4 des Gesetzes über den Schutz der Privatsphäre in der elektronischen Kommunikation.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Weitere Tätigkeiten der Datenschutzbeauftragten im Jahr 2013: - Fortsetzung der Präventivarbeit (Vorträge, Konferenzen) zur sicheren Internetnutzung durch Kinder, Schüler, deren Eltern und Lehrkräfte gemeinsam mit dem Zentrum für ein sichereres Internet; - Fortsetzung der Aufklärung verantwortlicher Stellen und Teilnahme an verschiedenen Aufklärungskonferenzen, -workshops und Podiumsdiskussionen; - Veröffentlichung von Leitlinien zu intelligenter Videoanalytik und Leitlinien zur Nutzung von Website-Cookies; - Konsultationen bzgl. einer Reihe von Gesetzen; - Fortsetzung der starken internationalen Beteiligung.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	712 Prüfungen: 253 im öffentlichen Sektor, 459 im privaten Sektor.
Sanktionsmaßnahmen	
Sanktionen	Es wurden 106 Verfahren eingeleitet (18 im öffentlichen Sektor, 62 im privaten Sektor, 26 zu Privatpersonen), davon wurden 26 Verwarnungen und 72 Beschlüsse zu Verstößen (36 Ermahnungen und 36 Geldbußen) verhängt.
Geldbußen	Die Datenschutzbehörde verhängte Geldbußen in Höhe von 224 592 329 EUR (zuzüglich Verwaltungssteuern).
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Informationen zur Rechtsprechung

Aufzeichnung von Telefongesprächen durch eine öffentliche Institution

Die Datenschutzbeauftragte leitete ein Prüfungsverfahren gegen eine öffentliche Institution ein, nachdem bekannt worden war, dass diese als zuständige Behörde ein automatisches Informationssystem für Anrufe unter der Telefonnummer ihres Kontaktzentrums installiert hatte, das den Anrufer vor der Verbindung mit einem Telefonisten darüber informierte, dass sein Anruf zur Verbesserung der Servicequalität aufgezeichnet würde. Die Prüfung ergab, dass die zuständige Behörde die Aufzeichnung von Anrufen mit dem Ziel der Sicherung und Verbesserung der Servicequalität eingeführt hatte. Die Tonaufnahmen der Telefonate wurden zum Erarbeiten von Vorschlägen für ein an Telefonisten gerichtetes Schulungsprogramm (Rhetorikausbildung, Umgang mit Kunden in schwierigen Situationen usw.) verwendet. Die Datenschutzbeauftragte kam zu dem Schluss, dass es trotz der Inkenntnissetzung der Anrufer vor dem eigentlichen Gespräch keine Rechtsgrundlage für diese Tonaufnahmen gibt. Demnach wies die Datenschutzbeauftragte die Behörde an, die Aufnahmen von Telefonaten unter ihrer

Callcenter-Nummer einzustellen, die gespeicherten Aufnahmen zu löschen und die Benachrichtigung über die Aufnahme der Anrufe im automatischen Informationssystem zu entfernen.

Unzureichende Sicherung sensibler personenbezogener Daten durch eine Gesundheitseinrichtung

Die Datenschutzbeauftragte führte bei einer Gesundheitseinrichtung eine Prüfung der Verfahren und Maßnahmen zum Schutz personenbezogener Daten durch. Die Prüfung ergab, dass interne Dokumente zur Regelung der Sicherheit personenbezogener Daten kein Verfahren zur Führung und Nutzung von Protokollen über den Zugang zu personenbezogenen Daten vorsahen. Die Datenschutzbeauftragte kam zu dem Schluss, dass die Behörde in ihrer Datenbank eine große Menge personenbezogener Daten verarbeitete, bei denen es sich angesichts des Tätigkeitsbereichs der Behörde größtenteils um sensible personenbezogene Daten handelte, deren Missbrauch für die betroffenen Personen ernsthafte, zeitaufwändige und in einigen Fällen unumkehrbare Konsequenzen haben könnte. Aufgrund der Sensibilität der verarbeiteten Daten durch die Behörde hätte jede Risikoanalyse zeigen müssen, dass für die Daten ein hohes, wenn nicht das höchste Risiko besteht. Demnach hätten Maßnahmen und Verfahren zum Schutz solcher personenbezogenen Daten vorhanden sein müssen, um das Risiko zu mindern. Die Datenschutzbeauftragte wies die Behörde daher an, in einem internen Dokument ein Protokoll für die Umsetzung interner Prüfungen aufzusetzen, das den Umfang, die Häufigkeit, die verantwortlichen Personen, die Ziele, die Art der Umsetzung, die Berichterstattung und die erforderlichen Maßnahmen im Falle einer unrechtmäßigen Verarbeitung personenbezogener Daten festlegt.

Die Prüfung ergab außerdem, dass die Behörde zum Zwecke des Zugangs zum Informationssystem, das wiederum die Rückverfolgbarkeit der Datenverarbeitung ermöglichte, ein System mit permanenten Benutzernamen und Passwörtern einsetzte und alle Ärzte und Krankenschwestern dieselben Zugangsrechte besaßen. Jeder Arzt war in der Lage, die Daten aller Patienten einzusehen, die in der Einrichtung behandelt werden oder wurden. Darüber hinaus gab es keine Vorgaben hinsichtlich der Komplexität der gewählten Passwörter, was von bewährten Verfahren im Bereich IT und Informationssicherheit abwich. Angesichts der Beschaffenheit der von der Behörde über das Informationssystem verarbeiteten personenbezogenen Daten sowie unter Berücksichtigung der potenziellen Risiken sind solche Praktiken inakzeptabel. Entsprechend wies die Datenschutzbeauftragte die Behörde an, eine interne Passwortrichtlinie einzuführen und diese umzusetzen.

Polizeiliche Befugnisse im Falle eines Zugangs zu den Daten von Internetnutzern

Die Datenschutzbeauftragte erhielt eine Beschwerde bezüglich polizeilicher Befugnisse im Zusammenhang mit der Erfassung von Daten zu Nutzern von Websites, deren Inhalte von Leistungsempfängern oder Nutzern bereitgestellt werden (hierbei handelt es sich um Websites wie Online-Foren, Medien-Websites usw.). Die Beschwerde weckte den Verdacht, dass bei einer unbekannten Anzahl von Fällen die personenbezogenen Daten von Online-Forum-Nutzern ohne Rechtsgrundlage erfasst worden waren. Auf Grundlage der Analysen von Daten, die von der Polizei bereitgestellt wurden, stellte die Datenschutzbeauftragte fest, dass die Polizei für die Erfassung der personenbezogenen Daten von Online-Forum-Betreibern, bei denen es sich um Dienstleister der Informationsgesellschaft (und nicht um Betreiber elektronischer Kommunikationsnetze) handelt, nicht die richtigen Gesetze heranzieht. Man berief sich auf Bestimmungen der Strafprozessordnung, des Polizeigesetzes oder sogar des Datenschutzgesetzes anstelle des Gesetzes über elektronischen Geschäftsverkehr, das die Erfassung von Daten von Dienstleistern der Informationsgesellschaft regelt. In einigen Fällen wurde überhaupt keine Rechtsgrundlage angegeben. Des Weiteren mangelte es offensichtlich an der Kenntnis der Unterschiede zwischen den Betreibern (Betreiber öffentlich verfügbarer, elektronischer Kommunikationsnetze und -dienste), deren Aktivitäten vorwiegend dem Gesetz zum Schutz der Privatsphäre in der elektronischen Kommunikation unterliegen, und Betreibern von Websites (Dienstleister der Informationsgesellschaft), deren Aktivitäten vorwiegend dem Gesetz über elektronischen Geschäftsverkehr unterliegen. Die Datenschutzbeauftragte informierte das Innenministerium und die Staatsanwaltschaft der Republik Slowenien über die Ergebnisse der Prüfung und schlug diesbezüglich das Erstellen eines Berichts vor, der

eine Liste der Maßnahmen zur Behebung der identifizierten Mängel enthält. Ende 2013 erhielt die Datenschutzbeauftragte einen internen Bericht des Innenministeriums. Der Fall wurde ins Jahr 2014 übernommen.

Verlust von Wählerunterschriften bei einem Aufruf zu einer Volksabstimmung

Nach Medienberichten über fehlende Listen mit Unterschriften, die zu einer Volksabstimmung über das Gesetz zu den Maßnahmen der Republik Slowenien zur Stärkung der Bankenstabilität aufriefen, leitete die Datenschutzbeauftragte von Amts wegen eine Prüfung bei der Nationalversammlung und dem Innenministerium im Zusammenhang mit der Umsetzung des Datenschutzgesetzes ein. Die Prüfung ergab, dass die Anzahl der Unterschriften bzw. die Anzahl der Blätter, aus der sich die Liste der Initiatoren (d. h. der Unterzeichner) zusammensetzte, von der Nationalversammlung zum Zeitpunkt des Eingangs bzw. beim Fotokopieren und bei der Weitergabe der Liste an das Innenministerium nicht ordnungsgemäß geprüft bzw. dokumentiert worden war. Des Weiteren konnte die Authentizität der zu prüfenden Unterschriften nicht bestätigt werden. Der genaue Umfang der Liste mit den personenbezogenen Daten wurde bei Erhalt der Kopien, der Verteilung an die Mitarbeiter zur Prüfung oder bei ihrer Rückgabe nach der Prüfung vom Ministerium ebenfalls weder angemessen dokumentiert noch überprüft. Erst nach dem Eingreifen des Initiators infolge der offensichtlich unzureichenden Anzahl an Unterschriften wurde von der Nationalversammlung eine interne Überprüfung durchgeführt und die Blätter gezählt. Dies ergab, dass die Originalliste mit den Unterschriften aus 307 Seiten bestand, während das Innenministerium 271 Seiten geprüfter Kopien zurückgab. Somit stellte sich heraus, dass 36 Seiten der kopierten Liste mit den personenbezogenen Daten von 361 Unterzeichnern abhanden gekommen waren. Die Datenschutzbeauftragte kam zu dem Schluss, dass die beiden Behörden gegen die Anforderungen des Datenschutzgesetzes hinsichtlich Verfahren und Maßnahmen zum Schutz personenbezogener Daten verstoßen haben, da sie die Größe und den Inhalt der Unterschriftenliste für die Volksabstimmung nicht überprüft und dokumentiert haben. Darüber hinaus konnten die Behörden keine so genannte externe Rückverfolgbarkeit vorweisen, da sie nicht für die Möglichkeit gesorgt hatten, später nachzuvollziehen, welche personenbezogenen Daten der Unterzeichner der Initiative an die andere zuständige Behörde übermittelt worden waren. Aufgrund der festgestellten Regelwidrigkeiten erlegte die Datenschutzbeauftragte den Verantwortlichen bei der Nationalversammlung und dem Innenministerium eine Sanktion auf.

Vorzeitige Vernichtung von Gesundheitsdaten

Die Datenschutzbeauftragte leitete infolge einer Beschwerde ein Prüfungsverfahren gegen eine verantwortliche Einrichtung (ein Kurbad) ein, da diese angeblich die unrechtmäßige Löschung der Gesundheitsdaten einer betroffenen Person nach nur drei Jahren nach Abschluss der Behandlung veranlasst hatte. Die Prüfung ergab, dass die internen Regelungen der verantwortlichen Einrichtung für die personenbezogenen Daten von Patienten unterschiedliche Aufbewahrungsfristen (5 bis 15 Jahre) vorsahen. Trotz dieser Aufbewahrungsfristen bewahrte die verantwortliche Einrichtung, aufgrund von Platzmangel und beschränkten technischen Möglichkeiten zur Aufbewahrung sehr großer Mengen an Gesundheitsdaten in schriftlicher Form, Gesundheitsdaten nur drei Jahre ab Ende der Kurortbehandlung auf. Die zu löschenden Gesundheitsdaten wurden zwar gewogen, jedoch wurde aufgrund der sehr großen Anzahl der Fälle (ungefähr 2 500 bis 3 000) keine Liste mit den Namen der Patienten erstellt, deren Daten vernichtet wurden.Die Datenschutzbeauftragte kam zu dem Schluss, dass es sich bei Kurbädern laut geltendem Recht um Erbringer von Gesundheitsleistungen handelt, die sich daher an die Bestimmungen eines bestimmten Gesetzes (ZZPPZ) zur Speicherung personenbezogener Daten zu halten haben. Laut ZZPPZ müssen die Patientendaten und die Krankengeschichte nach dem Tod des Patienten weitere 10 Jahre aufbewahrt werden. Sonstige grundlegende Gesundheitsdaten müssen 15 Jahre aufbewahrt werden. Bei der Datenschutzbeauftragten ging außerdem eine Stellungnahme des Gesundheitsministeriums ein, die besagt, dass die in Kurbädern erstellte medizinische Dokumentation als Bestandteil der Patientendaten und Krankengeschichte erachtet und nach dem Tod des Patienten weitere 10 Jahre aufbewahrt werden muss. Die Datenschutzbeauftragte wies die verantwortliche

Einrichtung an, dafür zu sorgen, dass die personenbezogenen Daten ihrer Patienten gemäß ZZPPZ aufbewahrt und vernichtet werden (d. h. 10 Jahre nach dem Tod des Patienten). Die Einrichtung wurde außerdem angewiesen, Rückverfolgbarkeit so sicherzustellen, dass für jede Löschung der Zeitpunkt und die Zuordnung zu den Inhabern der Daten (Vor- und Nachname der Patienten, Patientennummer) hervorgeht. Die Probleme Platzmangel und Rückverfolgbarkeit können mühelos durch das Speichern elektronischer Daten gelöst werden, da das ZZPPZ nicht die Form der von den Erbringern von Gesundheitsleistungen gewählten Speicherform vorgibt.

Veröffentlichung personenbezogener Kundendaten auf dem „Willkommensbildschirm" einer Reparaturwerkstatt

Die Datenschutzbeauftragte stellte fest, dass eine Fahrzeugreparaturwerkstatt (die verantwortliche Einheit) ein elektronisches Buchungssystem nutzte und die folgenden personenbezogenen Daten von Kunden auf dem „Willkommensbildschirm" erschienen: Vor- und Nachname des Kunden, Uhrzeit der Annahme des Kunden, Hersteller des Kundenfahrzeugs, Nummernschild sowie Vor- und Nachname des Kundenbetreuers. Laut dem Unternehmen sollten Kunden auf dem Willkommensbildschirm ablesen können, wann ihr Fahrzeug zur Reparatur angenommen wurde und mit welchem Kundenbetreuer sie Kontakt aufnehmen sollen. Die Kunden waren mit der Einführung des Willkommensbildschirms zufrieden. Daher stellte er nach Ansicht des Unternehmens eine notwendige organisatorische Maßnahme dar, durch die Kunden Zeit und Geld sparen und mit der die Reparaturtechniker sich besser auf die Arbeit vorbereiten und somit den Service verbessern konnten. Die Datenschutzbeauftragte wies darauf hin, dass die Nutzung von Technologien, die eine Verarbeitung personenbezogener Daten umfasst, auch bezüglich ihres Zwecks überdacht werden muss. Falls der Zweck des für die Datenverarbeitung Verantwortlichen eine Verarbeitung personenbezogener Daten (Vor- und Nachname des Kunden sowie Nummernschild des Fahrzeugs) ist, so stellt dies von Natur aus die Verarbeitung personenbezogener Daten dar, für die eine angemessene Rechtsgrundlage bestehen muss. Die Veröffentlichung personenbezogener Daten auf dem „Willkommensbildschirm" gilt als Kommunikation, Verbreitung und Zugänglichmachung personenbezogener Daten an all diejenigen, die sich zum Zeitpunkt der Veröffentlichung der Daten auf dem Gelände der Werkstatt befinden. Eine solche Verarbeitung ist für die Erfüllung vertraglicher oder anderweitiger Verpflichtungen des verantwortlichen Unternehmens weder notwendig noch angemessen noch ist dies für die Erfüllung gesetzlicher Verpflichtungen des privaten Sektors erforderlich, was bedeutet, dass es hierfür keine Rechtsgrundlage gibt. Des Weiteren konnte sich das Unternehmen für eine derartige Verarbeitung weder auf eine Rechtsgrundlage noch auf die persönliche Einwilligung der betroffenen Personen berufen. Die Datenschutzbeauftragte wies das verantwortliche Unternehmen an, die Veröffentlichung der personenbezogenen Kundendaten (Vor- und Nachname der Kunden und Fahrzeugkennzeichen) auf dem so genannten „Willkommensbildschirm" in allen Serviceeinheiten einzustellen oder stattdessen die ausdrückliche Einwilligung aller Kunden für eine derartige Verarbeitung ihrer Daten einzuholen.

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.

Aufgrund von Budgetkürzungen nahm die Datenschutzbeauftragte 2013 lediglich an den dringlichsten Plenarsitzungen der Europäischen Union und gelegentlich an Sitzungen von vier der vielen Untergruppen der Artikel-29-Datenschutzgruppe teil. Insgesamt beteiligte sich die Datenschutzbeauftragte an acht 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;
- gemeinsame Kontrollinstanz für Zölle;
- Koordinationssitzungen des Europäischen Datenschutzbeauftragten (EDSB) mit nationalen Behörden für den Schutz personenbezogener Daten zur Überwachung des SIS II;
- 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 zur Überwachung des VIS;
- Koordinationssitzungen des Europäischen Datenschutzbeauftragten (EDSB) mit nationalen Behörden für den Schutz personenbezogener Daten (Eurodac).

Im März 2013 wurde die Datenschutzbeauftragte zur Vorsitzenden der gemeinsamen Kontrollinstanz für Europol gewählt. Des Weiteren beteiligte sich die Datenschutzbeauftragte aktiv an der Internationalen Arbeitsgruppe Datenschutz in der Telekommunikation (IWGDPT), die Vertreter der Datenschutzbeauftragten und -behörden aus aller Welt zusammenbringt. Ein Vertreter der Datenschutzbeauftragten beteiligte sich 2013 erneut am Beratenden Ausschuss des Europarates (T-PD) zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention 108).

Am 19. Juli 2013 wurde die Datenschutzbeauftragte Nataša Pirc Musar von der Europäischen Kommission in die Sonderarbeitsgruppe EU-USA berufen, deren Aufgabe es war, das aktuelle Aktivitätsniveau der Nationalen Sicherheitsagentur der Vereinigten Staaten (NSA) im Zusammenhang mit der Massenerfassung von Informationen und personenbezogenen Daten von EU-Bürgern zu bestimmen. Nataša Pirc Musar beteiligte sich an der Sonderarbeitsgruppe als eine der fünf führenden europäischen Sachverständigen auf dem Gebiet des Schutzes personenbezogener Daten. Am Ende dieses Mandats erstellte die Gruppe für die Europäische Kommission einen Bericht mit ihren Ergebnissen.

Auf Grundlage von Art. 60 des Beschlusses 2007/533/JI des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation sowie von Art. 44 der Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) ist die Datenschutzbeauftragte für die unabhängige Überwachung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten über SIS II auf ihrem Gebiet sowie deren Übermittlung aus ihrem Gebiet verantwortlich. Die Datenschutzbeauftragte erhielt 2013 keine Beschwerden im Hinblick auf die Umsetzung dieser Rechte in erster Instanz.

Im Jahr 2013 führte die Republik Slowenien eine Beurteilung der Umsetzung des Schengen-Besitzstandes bezüglich Datenschutz durch, an der sich die Datenschutzbeauftragte aktiv beteiligte.

Die Datenschutzbeauftragte begrüßte 2013 Vertreter ähnlicher Behörden aus Kroatien, Bosnien, Herzegowina und Mazedonien. Sie wurden mit der Arbeit und den bewährten Verfahren der Datenschutzbeauftragten innerhalb ihres Tätigkeitsbereichs vertraut gemacht.

2013 schloss die Datenschutzbeauftragte als führende Partnerin das Partnerschaftsprojekt SR/2009/IB/JH/01 zur Verbesserung des Datenschutzes in Serbien erfolgreich ab. Im Kontext der internationalen Zusammenarbeit auf dem Gebiet des Zugangs zu öffentlichen Informationen begann die

Datenschutzbeauftragte 2013 ihre zweijährige Teilnahme am internationalen Konsortium des Projekts LAPSI 2.0, das die Arbeit des Projekts LAPSI 1.0 fortsetzen und ein thematisches Netzwerk aus Sachverständigen auf dem Gebiet der Weiterverwendung öffentlicher Informationen zur Beseitigung von Hindernissen bei seiner praktischen Umsetzung bilden soll.

Am 24. Oktober 2013 veranstaltete die Datenschutzbeauftragte eine internationale Konferenz zum Thema Weiterverwendung öffentlicher Informationen. Die Konferenz wurde im Rahmen des europäischen, von der Europäischen Kommission geförderten LAPSI-Projekts (Legal Aspects of Public Sector Information, rechtliche Aspekte von Informationen im öffentlichen Sektor, http://www.lapsi-project.eu/) organisiert, dessen Ziel es ist, ein thematisches Netzwerk auf dem Gebiet der Weiterverwendung öffentlicher Informationen zu bilden, und an dem sich die Datenschutzbeauftragte als Partnerin beteiligt. Der Zweck der in Ljubljana abgehaltenen Konferenz war die Präsentation neuer Trends und Herausforderungen, die sich aus der Änderung der Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors, mit besonderem Augenmerk auf personenbezogenen Daten, ergeben. Die Veranstaltung wurde live im Internet übertragen.

SPANIEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Nach dem stetigen Anstieg der letzten Jahre blieb die Tätigkeit der Datenschutzbehörde 2013 auf dem Stand des Vorjahres, vor allem hinsichtlich Beschwerden und Prüfungsaktivitäten. Obwohl die Zahlen etwas geringer ausfallen, bleiben sie mit 10 600 Beschwerden von Bürgern und über 10 700 endgültigen Beschlüssen der Datenschutzbehörde nach wie vor hoch.

Das ganze Jahr über arbeiteten wir an Maßnahmen zur Sensibilisierung, zur Förderung der Bürgerrechtsausübung und zur einfacheren Einhaltung der Vorschriften. Die Datenschutzbehörde eröffnete diesbezüglich einen neuen Themenkanal auf seiner Website namens „Datenschutz und Internet“ mit einer Reihe von Aufklärungsvideos, die Schritt für Schritt zeigen, wie man die Datenschutzeinstellungen von Browsern, sozialen Netzwerken und allgemeinen Betriebssystemen ändert. In Zukunft werden auf diesem Kanal weitere Materialien veröffentlicht. An dieser Stelle sei insbesondere auf die Dienste hingewiesen, die auf unserer 2012 eingeführten E-Services-Plattform angeboten werden, sowie auf die Verbesserungen der Informationsdienste auf unserer Website, darunter die Aktualisierung der beliebtesten Leitlinien, die sich an die für die Datenverarbeitung Verantwortlichen verschiedener Sektoren richten.

Bezüglich der Prüfungen und der Ausübung der Sanktionsbefugnis ist es erwähnenswert, dass ein beträchtlicher Anstieg des prozentualen Anteils der Beschlüsse (84 % der Gesamtzahl) verzeichnet wurde, bei denen das Bußgeld durch die Anwendung der neuen, in einem 2011 verabschiedeten Gesetz eingeführten Kriterien zur Minderung der Schwere von Sanktionen unter Berücksichtigung von Aspekten wie dem Verhalten des für die Datenverarbeitung Verantwortlichen, der Ausübung der Rechenschaftspflicht oder der realen Konsequenzen des Verstoßes, wenngleich die Zahlen der Geldbußen nahezu unverändert geblieben sind. Andererseits ging die Anzahl an Beschlüssen leicht zurück, bei denen die Geldbuße durch eine „vorbeugende Warnung“ ersetzt wurde, sodass sich der prozentuale Anteil an allen Sanktionsbeschlüssen nun auf 24 % beläuft.

Die Datenschutzbehörde setzte außerdem ihre Bemühungen für einen besseren Schutz von Kindern fort. In dieser Hinsicht ging die Datenschutzbehörde im Oktober 2013 mit ihrer neuen, aufklärenden Website online, deren Ziel es ist, sowohl Kindern als auch Pädagogen einschlägige Informationen und Hilfsmittel bereitzustellen. Die Website vereint alle bisherigen pädagogischen Materialien der Datenschutzbehörde und enthält neue Hilfsmittel, die eigens für diese Website entwickelt wurden.

Organisation	Spanische Datenschutzbehörde
Vorsitz und/oder Gremium	José Luis Rodríguez Álvarez
Budget	13 524 070 EUR
Personal	158
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	
Meldungen	602 531
Vorabprüfungen	k. A.

Anträge betroffener Personen	102 064
Beschwerden betroffener Personen	10 604
Vom Parlament bzw. der Regierung angeforderte Beratung	318
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	2 299
Sanktionsmaßnahmen	
Sanktionen	874
Geldbußen	22 339 440
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Im Jahr 2013 erließ die Audiencia Nacional (das Berufungsgericht für Beschlüsse der Datenschutzbehörde) 274 Beschlüsse, von denen:

- 188 die gegen Beschlüsse der Datenschutzbehörde eingelegte Berufungen abwiesen (68 %)
- 33 dem Berufungskläger teilweise recht gaben (12 %)
- 53 der Berufung stattgaben (20 %)

Der Oberste Gerichtshof fällte 12 Urteile in Rechtssachen, bei denen gegen Urteile der Audiencia Nacional Berufung eingelegt wurde. In allen Rechtssachen bestätigten die Urteile im Grunde die Position der Datenschutzbehörde.

Die Audiencia Nacional beschloss außerdem, in einer Rechtssache, bei der es um das sogenannte „Recht auf Vergessenwerden" ging, beim Europäischen Gerichtshof eine Vorabentscheidung zu beantragen. Die Rechtssache ist eine von knapp zweihundert anhängigen Fällen des Gerichts und bezieht sich auf die Beschwerde, die ein Bürger bei der Datenschutzbehörde über Google eingelegt hat. Die Datenschutzbehörde wies Google per Beschluss an, eine Reihe von Suchergebnissen zu löschen. Google legte dagegen Berufung ein.

Bei dem Antrag auf Vorabentscheidung ging es um zwei Hauptfragen:

a. Einerseits um die Anwendbarkeit der Richtlinie 95/46 bezüglich der Dienste, die EU-Bürgern von Google Inc. bereitgestellt werden. Vor diesem Hintergrund legte das Gericht einen Fragenkatalog

bezüglich der Anwendbarkeit 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 Bürgern 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. 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.

C. Sonstige wichtige Informationen

Im Jahr 2013 stellte die Datenschutzbehörde der Autonomen Region Madrid ihre Aktivitäten ein. Ihre Befugnisse wurden an den Staat zurückgegeben und von der spanischen Datenschutzbehörde übernommen.

Im Rahmen der Aktivitäten der Datenschutzbehörde modifiziert die Änderung des Gesetzes zur Regelung der Judikative (Gesetz 4/2013) die Befugnisse seines leitenden Organs (Generalrat der rechtsprechenden Gewalt), einschließlich die der „Zusammenarbeit mit der Datenschutzbehörde im Bereich der Rechtsprechung. Er wird außerdem die Kompetenzen dieser Behörde nur im Hinblick auf die Aktivität der Richter im Zusammenhang mit der Nutzung der Gerichtsakten übernehmen".

Ferner schloss die Datenschutzbehörde 2013 ein Sanktionsverfahren gegen Google im Zusammenhang mit der neuen Datenschutzrichtlinie des Unternehmens ab. Das Verfahren wurde im Juni 2013 im Rahmen der koordinierten Durchsetzungsreaktion eröffnet, die von der Arbeitsgruppe vereinbart worden war und unter der Leitung der französischen Datenschutzbehörde CNIL stand. Der endgültige Beschluss stellte drei schwere Verstöße gegen das spanische Datenschutzgesetz fest, erlegte Google für jede davon eine Geldbuße in Höhe von 300 000 EUR auf und ordnete die unverzügliche Umsetzung der nötigen Maßnahmen durch den Konzern an, um die geltenden rechtlichen Anforderungen zu erfüllen. Die drei Verstöße beziehen sich auf die unrechtmäßige Erfassung und Verarbeitung personenbezogener Daten authentifizierter, nicht authentifizierter und passiver Nutzer; die Speicherung und Aufbewahrung von Daten über unbestimmte oder ungerechtfertigte Zeiträume sowie das Fehlen von Mechanismen zur Ausübung der Rechte auf Zugang, Berichtigung, Löschung und Widerspruch.

TSCHECHISCHE REPUBLIK

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Schwerpunkt der Überwachungsaktivitäten lag auf dem Prüfplan der Datenschutzbehörde und auf den Bürgerbeschwerden. Im Folgenden werden ausgewählte Fälle genauer erläutert. Die Bereiche der geplanten Überwachungen lauteten demnach wie folgt: Datenschutz im nationalen Schengener Informationssystem, Verarbeitung von Daten in Bezug auf Spendenbegünstigte (z. B. ESF-Mittel), Umgang mit Daten öffentlicher Verwaltungsstellen, Verarbeitung personenbezogener Daten im Dienstleistungssektor und im Handel.

Am 11. und 12. Februar 2013 veranstaltete unser Amt für die moldauische Datenschutzbehörde einen **Studienbesuch**. Die Veranstaltung wurde von TAIEX finanziert und logistisch unterstützt. Thema: Datenschutz in Print-, visuellen und audio-visuellen Medien.

Am 21. und 22. Mai 2013 veranstaltete unser Amt für die mazedonische Datenschutzbehörde einen TAIEX-finanzierten **Studienbesuch**. Die Veranstaltung wurde von TAIEX finanziert und logistisch unterstützt. Thema: Datenschutz im Schengener Informationssystem.

Des Weiteren beteiligten sich zwei unserer Sachverständigen als Redner an TAIEX-Workshops in Moldau, Bosnien und Herzegowina.

Am 15. und 16. April 2013 richteten wir in Prag die **53. Tagung** der Internationalen Arbeitsgruppe „Datenschutz in der Telekommunikation“ (**IWGDPT**) aus. Dort wurden zwei Dokumente angenommen:

- Arbeitspapier zu Webtracking und Privatsphäre: Die Beachtung von Kontext, Transparenz und Kontrolle bleibt unverzichtbar
- Arbeitspapier und Empfehlungen zu der Veröffentlichung personenbezogener Daten im Web, der Indexierung des Inhalts von Websites und dem Schutz der Privatsphäre.

Die Umsetzung des Projekts „Raising awareness of data protection issues among employees working in the EU“ (Verbessern des Bewusstseins zu Datenschutzthemen unter den in der EU tätigen Arbeitnehmern) des **Leonardo-da-Vinci-Partnerschaftsprogramms** wurde fortgesetzt. Im Rahmen des Projekts wird ein umfassendes Handbuch für ein breites Publikum europäischer Arbeitnehmer erstellt. Außerdem werden Sensibilisierungsveranstaltungen organisiert. Am Projekt beteiligt sind Datenschutzbeauftragte aus Polen (Projektkoordinator), der Tschechischen Republik, Bulgarien und Kroatien. Das Projekt soll im Juli 2014 abgeschlossen werden.

Organisation	Amt für Datenschutz
Vorsitz und/oder Gremium	Igor Němec (Präsident des Amtes für Datenschutz)
Budget	128 731 000 CZK (= 4 694 785 EUR, Wechselkurs: 1 EUR = 27,42 CZK)
Personal	100
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	6 Stellungnahmen (die meisten davon mehr oder weniger im Zusammenhang mit der Überwachung der Bürger) 1 umfangreiche Empfehlung – Methodologie für E-Shop-Betreiber

Meldungen	6 570 Meldungen (davon 5 994 registriert; 576 laufend oder ausgesetzt)
Vorabprüfungen	85
Anträge betroffener Personen	2 994 (davon 15 aus dem Ausland)
Beschwerden betroffener Personen	1 336 (sowie weitere 7 428 im Zusammenhang mit Spam)
Vom Parlament bzw. der Regierung angeforderte Beratung	k. A.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	79 Anträge unter Berufung auf das Informationsfreiheitsgesetz. 69 Gesetzentwürfe und 95 Durchführungsverordnungen, zu denen im Rahmen des interministeriellen Stellungnahmeverfahrens Stellung genommen wurde Genehmigung internationaler Übermittlungen: 25 Anträge, davon 20 gestattet, 1 abgelehnt und 4 aus verfahrensrechtlichen Gründen ausgesetzt
Prüfmaßnahmen	
Prüfungen, Untersuchungen	90 (davon 74 abgeschlossen) + 91 Untersuchungen im Zusammenhang mit Spam (alle abgeschlossen)
Sanktionsmaßnahmen	
Sanktionen	ca. 61 Sanktionen 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	ca. 155 Geldbußen
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Nach zahlreichen Beschwerden führten wir bei **drei Skiliftbetreibern** an drei Wintersportorten eine **Untersuchung** durch. Die Skifahrer wurden beim Kauf von Tickets und Liftpässen fotografiert und mit einem Laserchip gemessen (die Beschwerden bezogen sich größtenteils auf Saisonpässe). Die Fotografien wurden zusammen mit Vor- und Nachnamen, Körpergröße und Ticketnummer in einer Datenbank gespeichert. Als Zweck nannte man die Vermeidung von Missbrauch dieser Liftpässe (da sie häufig von mehr als nur einer Person benutzt wurden). Am Lift wurde kontrolliert, ob die Daten der Skifahrer mit dem Ticket übereinstimmten. Die Daten wurden nach Saisonende gelöscht. Die

Untersuchungen zeigten, dass alle Betreiber (die alle zur gleichen Zeit für die Datenverarbeitung Verantwortliche waren) in zwei Fällen gegen das Gesetz verstießen: 1. Unterlassene Inkenntnissetzung der betroffenen Personen über die jeweilige Datenverarbeitung, 2. Unterlassene Meldung der Datenverarbeitung und Registrierung bei der tschechischen Datenschutzbehörde. Daher erlegten wir allen drei Betreibern nichtfinanzielle Sanktionen auf (sie wurden dazu verpflichtet, angemessene Abhilfemaßnahmen zu ergreifen).

Wir veranlassten eine Untersuchung der tschechischen Standorte von **EURODAC**. Der Prüfer wählte per Zufall eine Reihe von Datensätzen aus, prüfte die Verfahren vor Ort (es gibt drei Standorte in der Tschechischen Republik, an denen Fingerabdrücke und weitere relevante Daten erfasst und gespeichert werden). Die Untersuchung ergab keine Verstöße gegen das Datenschutzgesetz. Das tschechische Innenministerium begrüßte unsere Empfehlung bezüglich des Erfordernisses einer besseren Feedback-Kommunikation zwischen dem EURODAC-Betreiber und den Registrierungsstellen (z. B. Informationen für den Fall, dass Asylsuchende durch Heirat die Staatsbürgerschaft erhalten).

Aufgrund zahlreicher Beschwerden (welche die Offenlegung falscher oder unvollständiger Daten und das Versäumnis betrafen, unrechtmäßig erfasste Daten auf Antrag zu löschen) führten wir **eine Untersuchung der Zentralen Erfassungsstelle von Schuldnern (CERD)** durch. Es wurde festgestellt, dass die untersuchte Stelle nur für die Verarbeitung zuständig ist, während sich der für die Datenverarbeitung Verantwortliche in den USA befindet. Die Untersuchung ergab in zwei Fällen einen Verstoß gegen das Datenschutzgesetz: 1. Zweckfremde und unverhältnismäßige Datenerfassung, 2. Verletzung der Rechte der betroffenen Personen in Fällen einer unrechtmäßigen Datenverarbeitung. Wir erlegten dem Verarbeiter Abhilfemaßnahmen auf und verpflichteten ihn dazu, uns über deren Erfüllung zu informieren. Außerdem empfahlen wir, die Verständlichkeit der angebotenen Dienstleistungen zu verbessern, um weiteren Beschwerden vorzubeugen.

Wir untersuchten die Sicherheit der Datenverarbeitung im einheitlichen **Informationssystem für Arbeit und Soziales**. Für die Datenverarbeitung ist das tschechische Ministerium für Arbeit und Soziales verantwortlich. Die Untersuchung ergab, dass mehrere Beamte das System mit demselben Benutzernamen und Passwort nutzten. Außerdem funktionierte es auch ohne Anmeldung. Daher wurden zwei Abhilfemaßnahmen auferlegt: 1. Bereitstellung eines eigenen Nutzernamens und Passworts an alle befugten Beamten, 2. Einführung eines verpflichtenden Anmeldeverfahrens durch den Software-Hersteller.

C. Sonstige wichtige Informationen

Unser Aufsichtspersonal führte bei drei Botschaften mehrere Prüfungen durch, manche davon im Rahmen einer Geschäftsreise zu einer Konferenz oder anderen Veranstaltung.

2013 begannen wir mit einer Prüfung im Zusammenhang mit der Umstellung von SIS 1+ auf SIS II. Es sollte überprüft werden, wie die Polizei der Tschechischen Republik als für die Datenverarbeitung Verantwortliche in diesem System für den Schutz personenbezogener Daten sorgt. Die Prüfung konzentriert sich auf Verfahren sowie auf die technische und physische Sicherheit der Daten. Die Prüfung dauert bis 2014 an.

Sensibilisierung: Unsere Sachverständigen hielten 33 Vorlesungen zum Datenschutzgesetz in öffentlichen Institutionen, lokalen Verwaltungsbehörden und privaten Einrichtungen.

Im Jahr 2013 bereiteten wir den Go-live der neuen Website der Datenschutzbehörde vor. Die Website wurde neu gestaltet und deren Funktionen verbessert. Die Struktur blieb dabei unverändert, um Stammnutzer nicht zu verwirren.

UNGARN

A. Zusammenfassung der Aktivitäten und Neuerungen

Bei der Nationalen Behörde für Datenschutz und Informationsfreiheit (NAIH) gingen 2013 über 3 000 Fälle ein. Einem Großteil davon wurde im Rahmen eines informellen Verfahrens (Untersuchung) nachgegangen. Die NAIH stieß 40 formale (Verwaltungs-) Verfahren an und verhängte in 31 Fällen Geldbußen. Einige dieser Beschlüsse wurden von für die Datenverarbeitung Verantwortlichen vor Gericht angefochten. Die Gerichte bestätigten die überwiegende Mehrheit der geprüften Beschlüsse.

Organisation	Nationale Behörde für Datenschutz und Informationsfreiheit
Vorsitz und/oder Gremium	Präsident: Attila Péterfalvi
Budget	467 500 000 HUF
Personal	56
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Verwaltungsbeschlüsse: Die Datenschutzbehörde bearbeitete 2013 40 Datenschutzfälle. Zum Redaktionsschluss des Jahresberichts waren 4 davon noch anhängig. 35 der 40 Datenschutzfälle führten zu einem Verwaltungsbeschluss. Einige der Fälle waren Ende 2013 noch anhängig. Stellungnahmen zu Gesetzentwürfen: 311 Fälle Stellungnahmen zu Sprachaufzeichnungen: Die NAIH stellte eine steigende Zahl an Beschwerden im Zusammenhang mit Sprachaufzeichnungsaktivitäten fest. Laut dem Datenschutzgesetz handelt es sich bei Sprachaufzeichnungen insofern um personenbezogene Daten, als sie mit der betroffenen Person in Verbindung gebracht werden können. Mehrere Gesetze enthalten Bestimmungen für die verpflichtende Aufzeichnung von Gesprächen. Gesetz CCXXXVII von 2013 zu Kreditinstituten und Finanzunternehmen sieht vor, dass solche Institutionen Beschwerdeanrufe aufzeichnen. Für Versicherungsunternehmen gilt diese Verpflichtung gemäß Gesetz LX von 2003 über Versicherungsgesellschaften und die Versicherungsbranche ebenfalls. Diese beiden Gesetze besagen, dass betroffene Personen die Möglichkeit erhalten müssen, auf Anfrage Zugang zu ihren Sprachaufzeichnungen zu erhalten. Die offizielle Stellungnahme der NAIH lautet, dass beide Parteien das Recht auf Zugang zu Sprachaufzeichnungen haben. Der Zugang durch die betroffenen Personen muss demnach ebenfalls gewährleistet sein. Sie müssen in der Lage sein, sich die Aufzeichnung anzuhören und kostenlos eine Kopie davon zu erhalten. Beschlüsse Die Datenschutzbehörde veröffentlichte 1 549 Beschlüsse zu spezifischen Datenschutzangelegenheiten (informelle Verfahren).
Meldungen	Wir bearbeiteten 11 686 Meldungen von Verarbeitungen

	personenbezogener Daten zur Eintragung im Datenverarbeitungsregister.
Vorabprüfungen	Keine Daten.
Anträge betroffener Personen	Diese Interventionsanträge werden als „konsultative Anträge“ gehandhabt und umfassen Anträge von für die Datenverarbeitung Verantwortlichen. Von den 932 Anträgen betrafen 790 Datenschutzfragen. 140 bezogen sich auf Angelegenheiten zum Thema Informationsfreiheit.
Beschwerden betroffener Personen	Die NAIH erhielt 1 239 Beschwerden betroffener Personen. Von den 1 239 Beschwerden betrafen 978 Fälle Datenschutzfragen, und 261 Fälle bezogen sich auf Angelegenheiten bezüglich der Informationsfreiheit.
Vom Parlament bzw. der Regierung angeforderte Beratung	Die NAIH wird regelmäßig zu Gesetzentwürfen konsultiert.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Internationale Fälle: 106
Prüfmaßnahmen	
Prüfungen, Untersuchungen	<u>Datenschutzverfahren</u> Formale Datenschutzverfahren werden von Amts wegen angestoßen. In den meisten Fällen folgen formale Verfahren auf informelle Untersuchungen. Die bei letzteren erfassten Informationen können für die formalen Verfahren verwendet werden. <u>Untersuchungsstrategie 2013</u> Die Datenschutzbehörde ermittelte drei Bereiche besonderer Relevanz, die sie als ihre Prioritäten für das Jahr 2013 angab: 1. Datenverarbeitungsaktivitäten durch Websites, einschließlich Registrierungsprozesse unter dem Aspekt der Nutzerrechte. Der Schwerpunkt wurde vor allem auf die Verarbeitung der personenbezogenen Daten von Kindern gelegt. 2. Die elektronische Offenlegung von Informationen zu lokalen Steuern. 3. Die Verarbeitung personenbezogener Daten durch Schuldenverwaltungsunternehmen. <u>Untersuchungen</u> Die wichtigste Aufgabe der Datenschutzbehörde besteht darin, eingehenden Beschwerden nachzugehen. Daneben beantwortet sie Konsultationsanfragen, um die Durchsetzung von Datenschutzleitlinien zu unterstützen.

	Prüfungen 2013 nahm der Datenschutz-Prüfdienst der Datenschutzbehörde seine Arbeit auf. Für die Datenverarbeitung Verantwortliche können gegen eine Gebühr eine Prüfung beantragen. Die NAIH führte 2013 zehn Prüfungen durch.
Sanktionsmaßnahmen	
Sanktionen	Die NAIH kann verschiedene Arten von Sanktionen verhängen. Bei informellen Verfahren kann die NAIH den für die Datenverarbeitung Verantwortlichen dazu auffordern, seine Verfahren in Einklang mit dem Datenschutzgesetz zu bringen. Bei formalen Verfahren kann die NAIH die Berichtigung von personenbezogenen Daten, die als inkorrekt erachtet werden, die Sperrung, Löschung oder Vernichtung unrechtmäßig erfasster personenbezogener Daten anordnen, die unrechtmäßige Prüfung oder Verarbeitung personenbezogener Daten oder deren Übermittlung an Drittländer verbieten oder die Daten der betroffenen Personen einfordern, falls der für die Datenverarbeitung Verantwortliche den Zugang auf unrechtmäßige Weise verweigert, und eine Geldbuße verhängen.
Geldbußen	Die Durchsetzung von Verwaltungsgeldbußen gehört zu den Verantwortlichkeiten der Datenschutzbehörde. Dies sind die wichtigsten Zahlen dieser Aktivität für die Jahre 2012 und 2013: Anzahl der Fälle: 47 Geldbußen: 20 677 478 HUF
Datenschutzbeauftragte (DPO)	Seit 2012 organisiert die NAIH gemäß ihren gesetzlichen Verpflichtungen mindestens einmal im Jahr die Konferenz der ungarischen Datenschutzbeauftragten.
Zahlenangaben zu DPO	Die Datenschutzbehörde führt ein DPO-Register. 2013 wurden über 400 DPOs in der Datenbank registriert, die dazu verwendet wird, alle interessierten DPOs zur Konferenz einzuladen.

B. Informationen zur Rechtsprechung

Relevante Fälle

A) Untersuchungen von Datenverarbeitungsaktivitäten durch Websites, Registrierungsverfahren und der Durchsetzung der Rechte betroffener Personen im Internet, vor allem die der Kinder

Die NAIH führte allgemeine Untersuchungen von Datenverarbeitungsaktivitäten durch bestimmte Websites durch, um deren Datenschutzrichtlinien, Registrierungsverfahren, den Umfang der verarbeiteten Daten und die Durchsetzung der Rechte betroffener Personen zu beurteilen. Im Rahmen dieses Verfahrens ließ die NAIH der Verarbeitung der Daten von Kindern besondere Aufmerksamkeit zukommen. Der Schwerpunkt auf Minderjährigen als betroffene Personen wurde dadurch gerechtfertigt, dass das neue Datenschutzgesetz im Gegensatz zum alten in Artikel 6 Absatz 3 vorsieht, dass Minderjährige über 16 Jahre das Recht haben, unabhängig von ihren Erziehungsberechtigten Datenverarbeitungsaktivitäten zuzustimmen.

Um die Gültigkeit rechtlicher Aussagen und der Einwilligung Minderjähriger zur Datenerfassung zu bestimmen, muss außerdem Gesetz IV von 1959 des Bürgerlichen Gesetzbuchs berücksichtigt werden. Laut Artikel 12/C Absatz 1 des Bürgerlichen Gesetzbuchs dürfen nur Erziehungsberechtigte als rechtliche Vertreter Minderjähriger rechtliche Aussagen in deren Namen treffen. Laut Artikel 12/A Absatz 2 des Bürgerlichen Gesetzbuchs „sind rechtliche Aussagen Minderjähriger mit beschränkter Rechtsfähigkeit nur dann gültig, wenn sie unter vorheriger oder nachträglicher Einwilligung ihrer Erziehungsberechtigten erfolgen, es sei denn, dies ist durch andere Gesetze anders geregelt". Artikel 6 Absatz 3 des Datenschutzgesetzes enthält eine solche Ausnahme. Damit hat der Gesetzgeber spezielle Bestimmungen für Minderjährige zwischen 16 und 18 Jahren geschaffen, doch für Minderjährige zwischen 14 und 16 Jahren ist sowohl die Einwilligung der betroffenen Personen als auch deren Erziehungsberechtigten erforderlich, wie es das Bürgerliche Gesetzbuch grundsätzlich vorsieht.

Die NAIH befasste sich mit dem Fall eines Unternehmens, das mehrere Websites betreibt, darunter eine Dating-Website, auf der man angemeldete Nutzer unter 16 Jahren antraf, die sich ohne die vorherige oder nachträgliche Einwilligung ihrer Erziehungsberechtigten registrieren konnten. Die NAIH untersuchte mehrere Dating-Websites und beobachtete, dass unter den registrierten Nutzern häufig Minderjährige unter 16 anzutreffen waren. Laut der NAIH ist es wichtig, bei der Untersuchung der Online-Aktivitäten und der Datenverarbeitung von Kindern deren übergeordneten Interessen zu berücksichtigen. Dies trifft insbesondere auf soziale Netzwerke zu. In dieser Kategorie stellen Dating-Websites die größte Bedrohung dar. Im Gegensatz zu regulären sozialen Netzwerken, in denen Nutzer hauptsächlich mit ihnen bekannten Freunden kommunizieren, liegt der Hauptzweck von Dating-Websites darin, neue Leute kennenzulernen. Angesichts der Tatsache, dass Dienste, die Minderjährigen Dating-Portale bereitstellen, sowie deren Datenverarbeitungsaktivitäten nicht in die Kategorie kleiner täglicher Handlungen fallen, die zur Erfüllung der Grundbedürfnisse des Kindes üblich und nötig sind, ist die NAIH der Ansicht, dass eine angemessene Einwilligung nur zusammen mit der Einwilligung eines Erziehungsberechtigten erteilt werden kann.

Man muss danach streben, diese Vorschriften auch dann einzuhalten, wenn ein Nachweis der elterlichen Einwilligung nur schwer zu erbringen ist. Andernfalls fördert der Eigentümer oder Betreiber der Website die Verfügbarkeit von Kindern für romantische oder sexuelle Beziehungen, was zu ihrer Viktimisierung beitragen kann.

Wir dürfen unsere Augen nicht vor der Tatsache verschließen, dass Kinder auf Dating-Websites erscheinen können und auf Websites verfügbar sind, die auf den Aufbau neuer Beziehungen ausgerichtet sind. Wir dürfen solche Praktiken nicht ignorieren und somit passiv erlauben. Dies muss trotz des Wissens, dass Registrierungsbestimmungen und -verfahren leicht umgangen werden können, geltend gemacht werden. In diesem Fall liegt das Problem nicht beim Verhalten des für die Datenverarbeitung Verantwortlichen, sondern im Bereich der Eltern-Kind-Beziehungen, und wird somit Teil eines breiteren sozialen Problems.

Aus diesem Grund überprüfte die NAIH die Registrierungsverfahren von mindestens 50 Dating-Websites. Die NAIH ging der Frage nach, ob es Minderjährigen möglich sei, sich ohne einer elterlichen Einwilligung zu registrieren. Im Laufe unserer Testregistrierungen sah sich die NAIH gezwungen, bei 18 Websites administrative Datenschutzverfahren in die Wege zu leiten. Insgesamt wurden 4 200 Profile von Minderjährigen unter 16 Jahren aufgespürt. Der jüngste Nutzer war gerade einmal zehn Jahre alt. Alle Profile waren online verfügbar und verfolgten die Absicht, Beziehungen aufzubauen. Demzufolge verhängte die NAIH Geldbußen in Höhe von insgesamt 2 900 000 HUF und zwang die für die Datenverarbeitung Verantwortlichen, die betreffenden Daten zu löschen und ihre Datenschutzrichtlinien zu ändern.

Die für die Datenverarbeitung Verantwortlichen zeigten sich während der Verfahren im Großen und Ganzen kooperativ und löschten die unrechtmäßig verarbeiteten personenbezogenen Daten, d. h. die Profile der Minderjährigen unter 16 Jahren. Sie passten ihre Verfahren an und erhöhten dementsprechend die Altersgrenze für die Registrierung.

B) Aufbau einer gemeinsamen Marketing-Datenbank

Die NAIH untersuchte im Rahmen eines administrativen Datenschutzverfahrens die Datenverarbeitung zweier Unternehmen mit Marketing-Datenbanken. Die Daten wurden durch die Registrierung auf den Websites der Unternehmen erfasst. Die beiden Unternehmen tauschten die Daten untereinander aus und schickten E-Mails und SMS-Nachrichten an die registrierten Nutzer. Über das Call-Center eines Subunternehmers wurden Telemarketing-Aktivitäten durchgeführt. Ziel war es, für verschiedene Bank- und Versicherungsprodukte zu werben. Ihr Partner rief im Namen des Unternehmens bei Leuten an, die in einer der Datenbanken der beiden Unternehmen registriert waren, um eigene Produkte oder die anderer zu bewerben. Die personenbezogenen Daten wurden demnach vom Call-Center empfangen und genutzt und nicht vom ursprünglichen für die Datenverarbeitung Verantwortlichen.

Die NAIH kam zu dem Schluss, dass die untersuchten Aktivitäten nicht ausreichend mit den Datenschutzanforderungen konform waren und dass der angegebene Zweck der Aktivitäten („Marketing") zu vage war. Die Rechtsgrundlage – wie z. B. die Einwilligung der betroffenen Personen – für die Übermittlung personenbezogener Daten durch beide Unternehmen an einen Partner, der in den allgemeinen Geschäftsbedingungen noch nicht einmal erwähnt wurde, fehlte völlig. Beide für die Verarbeitung Verantwortlichen stellten keine adäquaten und präzisen Informationen bereit und baten nicht um eine bewusste Einwilligung. Außerdem wurde in der Meldung an die NAIH zur Vorabregistrierung nicht alle Beteiligten erwähnt.

Angesichts dieser Verstöße beschloss die NAIH, eine Geldbuße aufzuerlegen, eine Änderung der Datenschutzrichtlinien und Datenschutzverfahren gemäß dem Datenschutzgesetz zu fordern und die Löschung aller unrechtmäßig erfassten Daten zu veranlassen.

C) Verstoß gegen das Datenschutzgesetz infolge eines Hackerangriffs

Ein Unternehmen erfasste personenbezogene Daten im Rahmen eines Lotteriespiels zu Direktmarketingzwecken, wofür die Einwilligung der betroffenen Personen eingeholt wurde. Auf der Website ermöglichte das Unternehmen registrierten Benutzern außerdem den Zugang zu einem 3D-Spiel. Als die Marketingkampagne zu Ende war, hinterließ der für die Datenverarbeitung Verantwortliche einen aktiven Link, der auf die Datenbank auf seiner Website verwies. Eine Hackergruppe verschaffte sich Zugang zum Datenbankserver. Sie lud die gestohlenen Daten auf mehrere Websites hoch, darunter Namen, E-Mail-Adressen, Telefonnummern, Geburtsdaten, Ortsnamen und in einigen Fällen die Passwörter. Dieser Verstoß gegen das Datenschutzgesetz betraf über 50 000 Personen.

Angesichts der wirtschaftlichen Größe des für die Datenverarbeitung Verantwortlichen sah die NAIH das Unternehmen in der Pflicht, die effizientesten Datensicherheitsmaßnahmen zu ergreifen. Dies wurde durch die Tatsache bekräftigt, dass nach internen Prüfungen bereits darauf hingewiesen worden war, dass die Daten, insbesondere hinsichtlich Fernzugriffen, nicht ausreichend geschützt waren.

D) Biometrische Systeme

Bei einigen der Fälle bezüglich biometrischen Systemen handelte es sich um Konsultationsanträge von Organisationen, welche die Einführung biometrischer Schlösser oder Eingangssysteme in Betracht zogen. Wie üblich betonte die NAIH, dass die Nutzung biometrischer Systeme gemäß Artikel 4 des Datenschutzgesetzes angemessen, relevant und verhältnismäßig sein muss. Daraus ergeben sich die Fragen nach Notwendigkeit der Nutzung solcher Daten, nach ihrer Verhältnismäßigkeit sowie der strengen Bewertung, ob es möglich wäre, dasselbe Ziel mit anderen, weniger in die Privatsphäre eindringenden Methoden zu erreichen. Des Weiteren berief sich die NAIH weiterhin auf die Schlussfolgerungen in Stellungnahme 3/2012 der Artikel-29-Datenschutzgruppe zur Entwicklung biometrischer Technologien und insbesondere die im Zusammenhang mit der Beurteilung der Verhältnismäßigkeit solcher Verarbeitungsmethoden. Laut dieser Grundsätze geben Vorhaben von Schulen, biometrische Eingangssysteme einzuführen, nach wie vor Anlass zur Sorge. Solche Systeme sind

nicht unverzichtbar für die Sicherheit der interessierten Parteien oder des Schuleigentums. Schlussendlich kann der gewünschte Zweck eines solchen Systems auch durch Methoden erreicht werden, die weniger in die Privatsphäre eindringen.

Die NAIH ging außerdem Fällen nach, in denen Unternehmen an Kassen eine relativ übliche Vorrichtung, ein Fingerabdrucklesegerät, anbringen wollten, um den Zugang auf befugte Mitarbeiter zu beschränken. Die NAIH erinnerte die Unternehmen daran, dass gemäß Artikel 10 Absatz 1 des Arbeitsgesetzbuches „von einem Arbeitnehmer nur Erklärungen oder Daten, die für die Etablierung, Durchführung oder Beendigung von Beschäftigungsverhältnissen relevant sind, angefordert werden dürfen und nur solange diese nicht gegen die Bürgerrechte der Person verstoßen".

Artikel 9 des Arbeitsgesetzbuches enthält die allgemeinen Bestimmungen und wichtigsten Grundsätze der Bürgerrechte von Arbeitnehmern bei Beschäftigungsverhältnissen sowie deren potenzielle Einschränkungen. Um diese Bürgerrechte zu schützen, sieht das Gesetzbuch zwei strenge prozedurale Verpflichtungen vor, die Arbeitgeber respektieren müssen. Dieses Verfahren muss exklusiv und direkt mit dem Kerngeschäft des Arbeitgebers in Zusammenhang stehen. Diese Grenzen dürfen nicht überschritten werden. Selbst der Begriff „einwandfreies Funktionieren" ist streng auszulegen. Der Arbeitgeber darf sich nur dann zu einem solchen Verfahren entschließen, wenn es offensichtlich und objektiv notwendig ist.

Auf dieser Grundlage kam die NAIH zu dem Schluss, dass die Einführung von Fingerabdrucklesegeräten an Kassen nicht verhältnismäßig ist, da der Zweck auch durch weniger in die Bürgerrechte eingreifende Methoden erzielt werden kann, wie z. B. Kassen mit erhöhter Sicherheit, die nur durch Eingabe eines bestimmten Codes geöffnet werden können, die befugte Mitarbeiter vom Arbeitgeber erhalten.

C. Sonstige wichtige Informationen

Statistik

Die Datenschutzbehörde erhielt 2013 über 5 700 Anschreiben per Post und 11 222 E-Mails. Des Weiteren bearbeiteten wir 11 686 Meldungen von Verarbeitungen personenbezogener Daten, wovon 7 420 per Post und 4 266 per E-Mail eingingen. Im Jahr 2013 eröffneten wir 3 280 Fälle. Dies entspricht einer Steigerung von 9 % im Vergleich zu 2012. Hiervon leiteten wir 40 Verwaltungsverfahren und 2 481 Untersuchungen in die Wege. Die übrigen 759 Fälle bezogen sich auf andere Bereiche unserer Tätigkeit, wie z. B. internationale Angelegenheiten oder Beziehungen zu Datenschutzbeauftragten. Nur 370 Untersuchungen, die 2012 eingeleitet wurden, mussten 2013 fortgesetzt werden. Im Januar 2014 reduzierte sich die Zahl der noch vom Vorjahr laufenden Fälle auf 341. Wir konnten 2013 90 % unserer Verfahren abschließen. Dies stellt bei einer allgemeinen Steigerung der Fälle eine bedeutende Leistung dar. Wir bearbeiteten außerdem 106 internationale Fälle.

„Schlüssel zur Welt des Internets!": Das Kinderschutzprojekt der NAIH

Die NAIH startete 2013 ihr erstes langfristiges Projekt. Thema war eines unserer wichtigsten Prioritäten: der Schutz der Rechte von Kindern im Internet. Der erste Schritt dieses Projekts war die Durchführung einer umfassenden Studie zur Internetnutzung durch junge Menschen, den Gefahren, die ihnen im Internet begegnen, sowie den einschlägigen Vorschriften in Ungarn und im Ausland. Wir führten unsere Studie in Zusammenarbeit mit verschiedenen nationalen und internationalen Partnern durch. Unser Ziel war es, die Hilfe von Sachverständigen des Bildungswesens, der Psychiatrie, der Justiz, der Kriminologie und der Informationstechnologie in unsere Arbeit einzubeziehen und Informationen zu internationalen Best Practices zu sammeln. Ganze zwölf Sachverständige waren am Verfassen und Veröffentlichen einer 122 Seiten langen Studie beteiligt. Des Weiteren wurde eine Informationsbroschüre für Kinder erstellt und in zahlreichen ungarischen Schulen vorgestellt. Das Dokument wurde ins Englische übersetzt; eine kurze Zusammenfassung ist außerdem auf Französisch erhältlich. Beides kann kostenlos von unserer Website heruntergeladen werden: www.naih.hu. Es ist unser Ziel, dieses Projekt mit unseren

internationalen Partnern im Rahmen eines internationalen Workshops zu digitaler Bildung unter der Leitung der französischen Datenschutzbehörde (CNIL) fortzusetzen. Gleiches gilt auch für ein von der Europäischen Union gefördertes Projekt namens „Introducing data protection and privacy issues in the European Union“ (Einführung von Themen rund um den Datenschutz und die Privatsphäre in der Europäischen Union“), das unter der Leitung der polnischen Datenschutzbehörde (GIODO) steht.

VEREINIGTES KÖNIGREICH

A. Zusammenfassung der Aktivitäten und Neuerungen

Die ICO hat sich fünf Kernziele gesetzt. Es folgen ausgewählte Höhepunkte der Aktivitäten zum Erreichen dieser Ziele.

1. Organisationen sind sich ihrer Verpflichtungen hinsichtlich des Datenschutzes stärker bewusst.

Die ICO hat folgende Leitlinien veröffentlicht:

- Verfahren für den Zugang betroffener Personen zu ihren Daten;
- Direktmarketing sowie
- Datenschutz-Folgenabschätzungen.

U. a. wurde Care.data untersucht. Hierbei handelt es sich um ein System für Allgemeinärzte in England, mit dem medizinische Informationen zu medizinischen Forschungszwecken freigegeben werden können. Dieses System war unlängst in die Kritik geraten. Unsere Intervention führte zu verbesserten Patienteninformationen und überarbeiteten Zeitrahmen, doch trotz gegenteiliger Versicherungen wurde ersichtlich, dass diese Mechanismen keine Wirkung zeigten. Wir werden weiterhin versuchen, für effektive Mechanismen zu sorgen, um Patientenentscheidungen zu respektieren.

2. Durchsetzungsbefugnisse werden angemessen genutzt, um eine bessere Einhaltung der Datenschutzrechte zu gewährleisten.

In Strafverfolgungssachen bezüglich der unrechtmäßigen Erfassung oder Offenlegung personenbezogener Daten erreichten wir 12 strafrechtliche Verurteilungen und erteilten zwei Verwarnungen.

3. Kunden erhalten eine angemessene, faire und effiziente Antwort auf ihre Datenschutzanliegen.

Dieses Jahr haben wir eine Rekordzahl an Fällen erhalten und abgeschlossen. Die ICO wird auch weiterhin die individuellen Belange der Bürger berücksichtigen, um die Datenschutzpraktiken allgemein weiter zu verbessern. Bei einer Bankenaufsicht beantragten wir zum Beispiel einen Aktionsplan, da die Bearbeitung eines Antrags auf Zugang zu den eigenen personenbezogenen Daten einer betroffenen Person über neun Monate dauerte. Des Weiteren haben wir dafür gesorgt, dass AXA PPP Healthcare bei der Verarbeitung medizinischer Daten seine Abläufe für die Einholung einer angemessenen Einwilligung überarbeitet.

4. Menschen werden dazu ermutigt, ihre Datenschutzrechte in Anspruch zu nehmen.

Das Recht auf Zugang ist ein Grundstein des Datenschutzgesetzes. Seit einiger Zeit wird dieses Recht jedoch von Organisationen missbraucht, indem Einzelpersonen gezwungen werden, Zugang zu personenbezogenen Daten zu beantragen und diese dann der Organisation offenzulegen. Dieser erzwungene Zugang ist eine Verdrehung der Rechte des Einzelnen, und obwohl das Datenschutzgesetz von 1998 in solchen Fällen strafrechtliche Sanktionen vorsieht, wurden diese bislang nicht verhängt.

Wir sind diesbezüglich seit geraumer Zeit um Änderungen bemüht, und der neue Justizminister Simon Hughes hat nun bestätigt, dass weitere, kürzlich in Kraft getretene Gesetzesänderungen Hindernisse beseitigt haben und der Weg nun frei ist, um aus erzwungenem Zugang eine Straftat zu machen. Wir

arbeiten mit dem Justizministerium und anderen Stellen zusammen, um dies ohne weitere Verzögerungen umzusetzen.

5. Die ICO reagiert aufmerksam und schnell auf Änderungen, die Auswirkungen auf den Datenschutz haben.

Wir haben das Justizministerium und Parlamentsabgeordnete im Hinblick auf die vorgeschlagene Reform des EU-Datenschutzgesetzes beraten und waren im Rahmen der Artikel-29-Datenschutzgruppe aktiv. Eine gründliche Analyse der neuesten Vorschläge ist auf unserer Website zu finden.

Des Weiteren veröffentlichten wir Forschungsergebnisse zu den Auswirkungen der vorgeschlagenen Revisionen auf Unternehmen, welche die Unsicherheit vieler Kostenschätzungen, die in dieser Debatte kursieren, deutlich werden lassen:

- 40 % der Unternehmen haben nicht alle der zehn wichtigsten vorgeschlagenen Vorkehrungen verstanden, und
- 87 % waren nicht in der Lage, die Kosten der Vorschläge für ihr Unternehmen abzuschätzen.

Im Laufe des Jahres führten wir Konsultationen zur Machbarkeit einer ICO-Akkreditierung Dritter durch Datenschutzsiegel oder Zertifizierungen durch. Hierfür arbeiteten wir mit der britischen Akkreditierungsstelle zusammen. Eine Ankündigung des von der ICO vorgeschlagenen Programms wird es 2014/15 geben.

6. Eine effiziente, zukunftstaugliche ICO.

Bedeutende neue Initiativen, die in diesem Jahr eingeführt wurden, gestalteten unsere Arbeit effektiver und verbesserten die Dienstleistungen für die Öffentlichkeit:

Unser neues Registrierungssystem und der damit zusammenhängende Dienst sorgten dafür, dass das öffentliche Register der für die Datenverarbeitung Verantwortlichen für Besucher aussagekräftiger ist. Außerdem wurde die Registrierung benutzerfreundlicher gestaltet. Wir schlossen das Jahr mit einem komplett online verfügbaren Registierungsdienst ab.

Wir verbesserten unser Telefonsystem, um der steigenden Nachfrage gerecht zu werden. Wir sind jetzt in der Lage, Anrufe besser an die zuständigen Mitarbeiter umzuleiten, und haben einen besseren automatischen Service für Anrufe außerhalb der Öffnungszeiten.

Im Laufe des Jahres arbeiteten wir immer proaktiver an der Transparenz unserer Behörde.

Organisation	Amt des Datenschutzbeauftragten (Information Commissioner's Office)
Vorsitz und/oder Gremium	Christopher Graham (Datenschutzbeauftragter)
Budget	Rund 21 Millionen GBP (Meldegebühren 16,5 Mio. GBP und Zuschüsse bezüglich Informationsfreiheit in Höhe von 4,25 Mio. GBP)
Personal	370 Vollzeitbeschäftigte
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Verfahren für den Zugang betroffener Personen zu ihren Daten Direktmarketing

	Datenschutz-Folgenabschätzungen
Meldungen	Gesamtzahl der Meldungen von für die Datenverarbeitung Verantwortlichen 389 036
Vorabprüfungen	k. A.
Anträge betroffener Personen	Anrufe bei der Hotline: 259 903
Beschwerden betroffener Personen	Zum Thema Datenschutz eingegangene Beschwerden: 13 760 Zum Thema Informationsfreiheit eingegangene Beschwerden: 4 688 Zum Gesetz über den Schutz der Privatsphäre in der elektronischen Kommunikation eingegangene Beschwerden: 161 720
Vom Parlament bzw. der Regierung angeforderte Beratung	44 Konsultationen
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Keine
Prüfmaßnahmen	
Prüfungen, Untersuchungen	63 Prüfungen (und 117 Beratungen)
Sanktionsmaßnahmen	
Sanktionen	Untersuchung von 1 755 Datenschutzfällen 7 Vollzugsmitteilungen und 20 Vereinbarungen. 15 Verfahren (1 Fall führte zu konfiszierten Mitteln in Höhe von insgesamt 73 000 GBP, die zurückgezahlt werden müssen)
Geldbußen	Zivile Geldbußen in Höhe von 1,97 Mio. GBP
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

k. A.

C. Sonstige wichtige Informationen

Weitere Höhepunkte:

Darlehen für Studierende

Die Veräußerung der Studierendenkredite an den privaten Sektor hätte dazu führen können, dass Kreditauskunfteien eine Menge unnötiger Kreditdaten zugänglich gemacht werden. Wir arbeiteten daran, dass Kontodaten, die auf dem neuesten Stand waren, nicht an Kreditauskunfteien übermittelt werden, und sorgen für effektive Schutzmechanismen, welche die Richtigkeit der übermittelten Informationen gewährleisteten.

Online-Datingdienste

Die Nutzung von Online-Datingdiensten hat zugenommen und Bedenken hinsichtlich der Nutzung und des Austauschs personenbezogener Daten aufkommen lassen. Wir haben die Zusammenarbeit mit der Online Dating Association begonnen, um dem Sektor Leitlinien bereitzustellen.

Mit dem Internet verbundene Fernseher

Wir stehen mit einem Hersteller von Fernsehern in Kontakt, um Bedenken im Hinblick auf die Erfassung von Daten zu Fernsehgewohnheiten durch mit dem Internet verbundene Fernseher selbst bei Aktivierung der Datenschutzfunktionen auszuräumen.

Wohltätigkeitsorganisationen und Gemeindegruppen

Wir arbeiteten mit Wohltätigkeitsorganisationen und Gemeindegruppen zusammen, die sich für die hilfsbedürftigsten Menschen der Gesellschaft einsetzen, und hielten Präsentationen, Beratungssitzungen und Workshops ab.

Consulting Association

Eine wichtige Initiative der ICO bezog sich auf einen Fall aus dem Jahr 2009. Nach der Beschlagnahmung von Datensätzen bei The Consulting Association war die ICO in Besitz von Daten, die als „schwarze Liste“ der Bauindustrie genutzt worden waren.

Neben der Behandlung der sich daraus ergebenden Datenschutzbelange wollten wir diejenigen kontaktieren, die möglicherweise auf die schwarze Liste gesetzt worden waren. In vielen Fällen schien es aufgrund der verstrichenen Zeit unwahrscheinlich, dass Personen anhand der Daten identifiziert werden könnten. Durch die Zusammenarbeit mit Equifax und dem Arbeits- und Rentenministerium waren wir jedoch in der Lage, die Kontaktdaten einiger aufgeführter Personen zu ermitteln.

Wir wurden von vielen weiteren derzeitigen und ehemaligen Mitarbeitern des Baugewerbes und deren Vertreter kontaktiert, die herausfinden wollten, ob auch sie auf der beschlagnahmten Liste standen. Zwischen 2009 und Ende März 2014 stellten wir 776 Personen die einschlägigen Informationen bereit. Davon wurden 461 Auskünfte im Berichtsjahr 2013/14 erteilt.

Für bessere Kontinuität und Koordinierung der Untersuchung und Durchsetzung globaler Datenschutzfragen

Die ICO spielte außerdem bei der Verbesserung der Durchsetzungskoordinierung mit anderen Datenschutzbehörden eine führende Rolle:

Wir hatten den gemeinsamen Vorsitz der Arbeitsgruppe für die internationale Durchsetzungskoordinierung inne, die auf der internationalen Konferenz der Datenschutzbeauftragten zur Verabschiedung einer Verordnung führte, die diese Arbeit voranbringt. Wir leiten derzeit die Entwicklung eines Regelwerks für den Austausch von Daten zu Durchsetzungsmaßnahmen.

Wir sitzen im Vorsitz des globalen Netzwerks für die Durchsetzung des Rechts auf Datenschutz.

Wir sind in der OECD-Arbeitsgruppe für Datenschutz und Privatsphäre in der digitalen Wirtschaft vertreten und beteiligen uns dort an der Aktualisierung der Datenschutzleitlinien der OECD, die mittlerweile vom OECD-Rat verabschiedet worden sind.

Wir unterzeichneten eine Absichtserklärung mit der US-Kartellbehörde und mit der Finanzaufsichtsbehörde Dubai International Financial Centre.

Änderungen im Umgang mit Beschwerden

Im Berichtszeitraum führten wir umfassende Vorbereitungsarbeiten einschließlich Konsultationen durch, bevor wir im April 2014 schließlich unseren Umgang mit Beschwerden und Bedenken der Öffentlichkeit änderten. Dank dieser Änderungen sind wir nun in der Lage, diesen wichtigen Bereich unserer Arbeit als Aufsichtsbehörde auf kooperativere und angemessenere Art und Weise auszuführen.

ZYPERN

A. Zusammenfassung der Aktivitäten und Neuerungen

Das Amt des Datenschutzbeauftragten wurde zu einer Reihe von EU-Gesetzesvorlagen konsultiert, wie z. B. zum Vorschlagspaket für den Datenschutz, das die Kommission im Januar 2012 vorgestellt hat, sowie zu den Vorschlägen zur Regulierung von Europol und Eurojust im Zusammenhang mit dem Schutz personenbezogener Daten.

Das Amt des Datenschutzbeauftragten beteiligte sich am Beratenden Ausschuss des Europarates (T-PD) und dem CAHDATA-Ausschuss zur Modernisierung der Konvention 108 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.

Im Rahmen der Aktivitäten zur Feier des Europäischen Datenschutztages nutzte das Amt des Datenschutzbeauftragten ein Budget in Höhe von 4 300 **EUR** 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.

Infolge der Überprüfung einer Beschwerde, die Mitarbeiter durch ihre Gewerkschaften gegen ein privates Krankenhaus vorgebracht hatten, das ein biometrisches System zur Überwachung der Anwesenheit installiert hatte und biometrische Daten (Fingerabdrücke) nutzte, die 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. Das Krankenhaus wurde aufgefordert, die Verarbeitung einzustellen und das System zu deinstallieren. Das Krankenhaus leistete dem Beschluss nicht Folge und focht den Beschluss vor Gericht an. Das Urteil steht noch aus.

Organisation	Amt des Datenschutzbeauftragten
Vorsitz und/oder Gremium	Herr Yiannos Danielides
Budget	Zugewiesenes Budget: 257 352 **EUR** Ausgegebenes Budget: 225 120 **EUR**
Personal	Verwaltungsbedienstete: 7 Fachkräfte für Informationstechnologie: 2 Bürofachkräfte: 6 Hilfskräfte: 2
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Stellungnahmen: 61 Beschlüsse: 5 Empfehlungen: 2
Meldungen	278
Vorabprüfungen	k. A.
Anträge betroffener Personen	Schriftlich oder telefonisch: k. A.
Beschwerden betroffener Personen	Spam: 308 Sonstige: 77

Vom Parlament bzw. der Regierung angeforderte Beratung	In 21 Fällen wurde unser Amt von parlamentarischen Ausschüssen des zypriotischen Parlaments um Beratungsdienste/Konsultationen gebeten.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	Genehmigungen für die Verknüpfung von Speichersystemen: 16 Genehmigungen für Übermittlungen an Drittländer: 50
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Anzahl der Prüfungen: 1
Sanktionsmaßnahmen	
Sanktionen	Für drei der fünf Beschlüsse wurden Verwaltungssanktionen verhängt. In den zwei anderen Beschlüssen gab der Datenschutzbeauftragte Empfehlungen an die für die Datenverarbeitung Verantwortlichen ab.
Geldbußen	In zwei der drei Beschlüsse, die Verwaltungssanktionen zur Folge hatten, wurden den für die Datenverarbeitung Verantwortlichen Bußgeldern in Höhe von 3 000 EUR bzw. 300 EUR auferlegt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Das Amt des Datenschutzbeauftragten war 2012 einer Beschwerde gegen ein Versicherungsunternehmen nachgegangen, 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 allgemeinen Bedingungen der Versicherungspolice und der Anzahl der (zusätzlichen) Dokumente, die die Beschwerdeführerin zuweilen einreichen musste, erließ der Datenschutzbeauftragte 2013 einen Beschluss, in dem er zu dem Schluss kam, dass der Versicherer aufgrund der Tatsache, dass er die Forderung nicht in einem zumutbaren Zeitrahmen unter Berücksichtigung einer angemessenen, von der Beschwerdeführerin eingereichten Anzahl von Dokumenten akzeptiert bzw. abgelehnt, sondern stattdessen um zusätzliche Tests und Dokumente gebeten und dadurch die Untersuchung des Anspruchs verlängert hat, gegen den Grundsatz der Verhältnismäßigkeit verstoßen hat. Aus diesem Grund wurde dem Versicherer eine Verwaltungssanktion in Höhe von 3 000 EUR auferlegt. Der Beschluss der Datenschutzbehörde wurde vor einem Gericht angefochten; das Urteil steht noch aus.

C. Sonstige wichtige Informationen

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, wurde am 20. Dezember 2013 per Beschluss des Ministerrats in nationales Recht umgesetzt. Dem Beschluss nach sieht das Gesetz die Datenschutzbehörde als zuständige Aufsichtsbehörde vor.

Kapitel Drei

Aktivitäten der Europäischen Union und der Gemeinschaft

3.1. Europäisches Parlament

3.1.1 Berichtsentwürfe des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) – 10. Januar 2013

Der LIBE-Ausschuss legte zwei Berichtsentwürfe zur von der Europäischen Kommission vorgeschlagenen Reform des EU-Datenschutzgesetzes vor. Jan-Philipp Albrecht, Berichterstatter des Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments für die geplante Datenschutzverordnung, und Dimitrios Droutsas, Berichterstatter des Strafverfolgungssektors für die geplante Datenschutzrichtlinie, brachten ihre volle Unterstützung eines kohärenten, robusten Datenschutzrahmens mit starken, durchsetzbaren Rechten für Einzelpersonen zum Ausdruck und wiesen nachdrücklich auf die Notwendigkeit eines hohen Schutzniveaus bei allen Datenverarbeitungsaktivitäten in der Europäischen Union hin, um für mehr Rechtssicherheit, Klarheit und Einheitlichkeit zu sorgen.

Zu den wichtigsten Themen gehören das Ersetzen der Richtlinie 95/46/EG durch eine unmittelbar geltende Verordnung, welche die Verarbeitung personenbezogener Daten im privaten und öffentlichen Sektor mit einem einzigen, in der ganzen EU geltenden Regelsatz, die Unterstützung einer einzigen Anlaufstelle für Unternehmen, die in mehreren EU-Ländern tätig sind, sowie für Verbraucher, die sich über ein im Ausland ansässiges Unternehmen beschweren möchten, und eine starke, unabhängige EU-Datenschutzbehörde, die rechtsverbindliche Entscheidungen gegenüber nationalen Datenschutzbehörden trifft; die Unterstützung für die Stärkung von Nutzungsrechten sowie die Anwendbarkeit von EU-Vorschriften abdeckt, bei denen personenbezogene Daten von EU-Bürgern im Ausland von Unternehmen verarbeitet werden, die keinen Sitz in der EU haben.

3.1.2 Bericht des Ausschusses für Industrie, Forschung und Energie (ITRE) – 20. Februar 2013

Der ITRE-Ausschuss verabschiedete seine Stellungnahme zu den Vorschlägen der Kommission zur Reformierung des EU-Datenschutzgesetzes. Diese wird nun an den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) geleitet, der sämtliche bislang übermittelte Änderungen konsolidiert und Ende April über seinen eigenen Bericht abstimmt.

Der ITRE-Ausschuss unterstützte die wichtigsten Neuerungen der Datenschutzreform der Kommission. Die Stellungnahme des ITRE-Ausschusses folgte auf die Veröffentlichung der Berichtsentwürfe des LIBE-Ausschusses zur Reform des EU-Datenschutzgesetzes am 10. Januar 2013.

3.1.3 Stellungnahme des Rechtsausschusses (JURI) – 19. März 2013

Der JURI-Ausschuss verabschiedete seine Stellungnahmen zu den Vorschlägen der Kommission zur Reformierung des EU-Datenschutzgesetzes. Die Stellungnahmen werden an den Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) geleitet.

Der JURI-Ausschuss unterstützte die Architektur und die wichtigsten Grundlagen der Datenschutzreform der Kommission:

Die Stellungnahme des JURI-Ausschusses folgte auf die Veröffentlichung der Berichtsentwürfe des LIBE-Ausschusses zur Reform des EU-Datenschutzgesetzes am 10. Januar 2013 und auf die Abstimmungen der ITRE-, EMPL- und IMCO-Ausschüsse.

3.1.4 Berichte des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE) – 22. Oktober 2013

Der LIBE-Ausschuss verabschiedete zwei Berichte zur von der Europäischen Kommission vorgeschlagenen Reform des EU-Datenschutzgesetzes und unterstützte darin nachdrücklich die

Architektur und die wichtigsten Grundsätze der Kommissionsvorschläge zur Datenschutzreform (sowohl die Datenschutz-Grundverordnung als auch die Datenschutzrichtlinie für Strafverfolgungssituationen).

Die LIBE-Abstimmung erteilt den Berichterstattern, den MdEP Albrecht und Droutsas, das Mandat zur Verhandlung mit dem Rat der EU.

3.2. Europäische Kommission

Am 27. November 2013 stellte die Europäische Kommission ein Maßnahmenpaket zur Wiederherstellung des Vertrauens in die Datenströme zwischen der EU und den Vereinigten Staaten vor, nachdem die Enthüllungen über die umfangreichen Programme der US-Nachrichtendienste zur Sammlung von Informationen Besorgnis ausgelöst und sich negativ auf die transatlantischen Beziehungen ausgewirkt hatten.

Das Paket bestand aus einem Strategiepapier in Form einer Mitteilung über die transatlantischen Datenströme, in dem die sich aus diesen Enthüllungen ergebenden Herausforderungen und Risiken beschrieben und die erforderlichen Maßnahmen zur Ausräumung der genannten Bedenken dargelegt werden; einer Analyse des Funktionierens des Safe-Harbor-Abkommens, das die zu gewerblichen Zwecken erfolgende Datenübermittlung zwischen der EU und den USA regelt; eines Berichts über die Feststellungen der gemeinsamen Arbeitsgruppe EU-USA zu Fragen des Datenschutzes, die im Juli 2013 eingerichtet wurde; einer Überprüfung der bestehenden Abkommen zu Fluggastdaten sowie einer Überprüfung des Programms zum Aufspüren der Finanzierung des Terrorismus (TFTP), das die zu Strafverfolgungszwecken erfolgende Datenübermittlung in diesen Bereichen regelt.

Die Kommission schlug eine rasche Annahme der Datenschutzreform der EU; eine Verbesserung des durch die Safe-Harbor-Regelung gebotenen Schutzes; eine Verstärkung der Datenschutzgarantien im Strafverfolgungsbereich; einen Rückgriff auf die geltenden einvernehmlichen Rechtshilfeabkommen und sektorspezifischen Abkommen zum Zwecke der Datenerfassung; die Berücksichtigung der von der EU geäußerten Bedenken im Rahmen des laufenden Reformprozesses in den Vereinigten Staaten sowie die Förderung von Datenschutzstandards auf internationaler Ebene vor.

3.2.1 Wiederherstellung des Vertrauens in die Datenströme zwischen der EU und den USA

Die Kommission schlägt Maßnahmen in sechs Bereichen vor:

Rasche Annahme der Datenschutzreform der EU: Der von der Europäischen Kommission im Januar 2012 vorgeschlagene robuste legislative Rahmen mit klaren Regeln, die auch in Situationen durchsetzbar sind, wenn Daten ins Ausland übermittelt und dort verarbeitet werden, ist jetzt dringender notwendig denn je. Die EU-Organe sollten daher weiterhin darauf hinwirken, dass die Datenschutzreform der EU spätestens im Frühjahr 2014 angenommen wird, damit personenbezogene Daten wirksam und umfassend geschützt sind.

Verbesserung des durch die Safe-Harbor-Regelung gebotenen Schutzes: Die Kommission hat heute 13 Empfehlungen ausgesprochen, durch die das Funktionieren der Safe-Harbor-Regelung verbessert werden soll und die auf eine ebenfalls heute veröffentlichte Analyse zurückgehen, derzufolge die Regelung in mehrerlei Hinsicht mangelhaft funktioniert. Bis Sommer 2014 sollen entsprechende Lösungen gefunden werden. Anschließend wird die Kommission das Funktionieren der Regelung auf Grundlage der umgesetzten 13 Empfehlungen überprüfen.

Verstärkung der Datenschutzgarantien im Strafverfolgungsbereich: Die laufenden Verhandlungen über ein Rahmenabkommen, das die Datenübermittlung und -verarbeitung im Zusammenhang mit der polizeilichen und justiziellen Zusammenarbeit regelt, sollten rasch zum Abschluss gebracht werden. Das Abkommen muss ein hohes Datenschutzniveau für die Bürger gewährleisten und gleiche Rechte für die Bürger auf beiden Seiten des Atlantiks vorsehen. Insbesondere sollten allen nicht in den Vereinigten Staaten ansässigen EU-Bürgern geeignete Rechtsmittel offenstehen.

Rückgriff auf die geltenden einvernehmlichen Rechtshilfeabkommen und sektorspezifischen Abkommen zum Zwecke der Datenerfassung: Die US-Behörden sollten sich dazu verpflichten, grundsätzlich auf Rechtsrahmen wie die geltenden einvernehmlichen Rechtshilfeabkommen und die sektorspezifischen Abkommen zwischen der EU und den Vereinigten Staaten (wie das Fluggastdaten-Abkommen und das

Programm zum Aufspüren der Finanzierung des Terrorismus, TFTP) zurückzugreifen, wenn Datenübermittlungen für Strafverfolgungszwecke benötigt werden. Direkte Datenanfragen bei Unternehmen sollten nur in Ausnahmefällen und unter klar festgelegten, der gerichtlichen Kontrolle unterliegenden Bedingungen zulässig sein.

Berücksichtigung der von der EU geäußerten Bedenken im Rahmen des laufenden Reformprozesses in den Vereinigten Staaten: US-Präsident Obama hat eine Überprüfung der Tätigkeit von nationalen Sicherheitsbehörden der USA angekündigt. Dieser Prozess müsste auch Positives für die EU-Bürger bewirken. Am wichtigsten wäre es, die für US-Bürger geltenden Garantien auf nicht in den Vereinigten Staaten ansässige EU-Bürger auszuweiten, mehr Transparenz zu schaffen und die Kontrolle zu verbessern.

Förderung von Datenschutzstandards auf internationaler Ebene: Die Vereinigten Staaten sollten, nachdem sie bereits dem Übereinkommen des Europarats über die Cyber-Kriminalität von 2001 beigetreten sind, nun auch dem Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten („Übereinkommen Nr. 108“) beitreten.

Die Kommission hat außerdem klargestellt, dass die Datenschutzstandards nicht Teil der laufenden Verhandlungen über ein transatlantisches Handels- und Investitionsabkommen sein werden.

3.2.2 Bericht zu den Ergebnissen der gemeinsamen Arbeitsgruppe EU-USA zu Fragen des Datenschutzes

Dieser Bericht folgte auf die Enthüllungen der Existenz einer Reihe von US-Überwachungsprogrammen zur umfangreichen Erfassung und Verarbeitung personenbezogener Daten, welche die Erfassung personenbezogener Daten von US-Internet- und Telekommunikationsdienstleistern und die Überwachung der Datenströme innerhalb und außerhalb der Vereinigten Staaten betreffen und das Potenzial haben, erheblichen Auswirkungen für EU-Bürgern zu haben.

Die US-Behörden wurden um Klarstellungen bezüglich einer Reihe von Punkten gebeten, wie z. B. dem Umfang der Programme, der Menge der erfassten Daten, der Existenz rechtlicher und administrativer Überwachungsmechanismen und deren Verfügbarkeit für EU-Bürger sowie der verschiedenen, für US- und EU-Bürger geltenden Schutzniveaus und Schutzmechanismen. In der Folge wurde eine gemeinsame Arbeitsgruppe EU-US ins Leben gerufen, um die Fakten zu den US-Überwachungsprogrammen zusammenzutragen und deren Auswirkungen auf die Grundrechte in der EU und auf die personenbezogenen Daten von EU-Bürgern zu beurteilen.

Die Vereinigten Staaten stellten Informationen zur Rechtsgrundlage bereit, auf der Überwachungsprogramme beruhen und durchgeführt werden, und stellten klar, dass die Befugnis des Präsidenten zur Erfassung von ausländischen Nachrichtendienstdaten außerhalb der USA direkt auf seine Funktion als Oberbefehlshaber sowie auf seine in der US-Verfassung vorgesehene Kompetenz in Bereich der Außenpolitik zurückgeht.

Der Bericht endet mit der Schlussfolgerung, dass nach US-Recht eine Reihe von Rechtsgrundlagen die umfangreiche Erfassung und Verarbeitung personenbezogener Daten, die in die USA übermittelt wurden oder von US-Unternehmen verarbeitet werden, zu Nachrichtendienstzwecken, einschließlich der Bekämpfung von Terrorismus, ermöglichen. Die USA haben die Existenz und die wichtigsten Bestandteile bestimmter Aspekte dieser Programme bestätigt, mit denen die Datenerfassung und -verarbeitung auf der Grundlage des US-Rechts, das spezifische Bedingungen und Schutzmechanismen vorsieht, erfolgt. Wie viele EU-Bürger von diesen Überwachungsprogrammen betroffen sind und das geografische Ausmaß der Programme sind unklar.

Zwischen den Schutzmechanismen, die für betroffene Personen in der EU gelten, und denen, die für betroffene Personen in den USA gelten, gibt es Unterschiede – die Erfassung der Daten von US-Bürgern ist grundsätzlich nicht erlaubt. Bei vorhandener Erlaubnis gelten sie nur dann als „ausländische Nachrichtendienstdaten“, wenn die Erfassung für diesen bestimmten Zweck erforderlich ist. Diese

Notwendigkeitsanforderung gilt nicht für Daten von EU-Bürgern, die als „ausländische Nachrichtendienstdaten“ gelten, wenn sie sich auf den verfolgten Zweck beziehen. Dies führt zu niedrigeren Hemmnissen bei der Erfassung personenbezogener Daten von EU-Bürgern.

Die Zweckbindungs- und Minimierungsverfahren sollen die Erfassung, Aufbewahrung und Verbreitung personenbezogener Daten von bzw. bezüglich US-Bürgern reduzieren und erfordern keine spezifischen Anforderungen oder Einschränkungen in Bezug auf die Erfassung, Verarbeitung oder Aufbewahrung personenbezogener Daten von EU-Bürgern. Die Beaufsichtigung der Überwachungsprogramme zielt vorwiegend auf den Schutz von US-Bürgern ab. US-Bürger profitieren von in der US-Verfassung (erste und vierte Änderung) verankerten Schutzmechanismen, die für nicht in den USA ansässige EU-Bürger nicht gelten.

Verschiedene Niveaus von Datenschutzmechanismen gelten für verschiedene Arten von Daten (Metadaten im Vergleich zu Inhaltsdaten) und verschiedene Phasen der Datenverarbeitung (erste Erfassung im Vergleich zu Weiterverarbeitung/Analyse). Es ist unklar, ob weitere verfügbare Rechtsgrundlagen angewendet werden oder weitere Überwachungsprogramme bestehen.

Da die einschlägigen Anordnungen des FISC nicht öffentlich zugänglich und Unternehmen im Hinblick auf deren verpflichtende Unterstützung zur Verschwiegenheit verpflichtet sind, gibt es für EU- oder US-Bürger weder rechtliche noch administrative Wege, um zu erfahren, ob ihre personenbezogenen Daten erfasst oder weiterverarbeitet werden. Natürliche Personen haben nicht die Möglichkeit, auf Daten zuzugreifen oder diese zu berichtigen oder zu löschen, und es gibt diesbezüglich auch keine Widerspruchsverfahren oder Rechtsmittel.

Aktivitäten, die eine zwingende Erfassung von Informationen erfordern, stehen unter gerichtlicher Aufsicht. Es gibt keine gerichtliche Genehmigung individueller Auswahlkriterien zur Erfassung von Daten oder zur Abfrage der erfassten Daten. Es gibt keine gerichtliche Aufsicht der Erfassung ausländischer Nachrichtendienstdaten außerhalb der USA. Dies wird ausschließlich von der Exekutive durchgeführt.

3.2.3 Kommunikation über die Funktionsweise der Safe-Harbor-Regelung aus Sicht der EU-Bürger und der in der EU niedergelassenen Unternehmen

Im Jahr 2000 erließ die Kommission den Beschluss 2000/520/EG, mit dem anerkannt wurde, dass die vom US-Handelsministerium herausgegebenen „Grundsätze des ‚sicheren Hafens‘ zum Datenschutz“ und „Häufig gestellten Fragen“ ein angemessenes Schutzniveau für die Übermittlung personenbezogener Daten aus der EU in die USA gewährleisten.

Die Safe-Harbor-Regelung erlaubt somit die Übermittlung personenbezogener Daten aus der EU an Unternehmen in den USA, die diese Grundsätzen unterzeichnet haben, auch dann, wenn die Übermittlung ansonsten nicht den EU-Normen zur Gewährleistung eines angemessenen Datenschutzniveaus genügen würde. Die Funktionsweise der Safe-Harbor-Vereinbarung basiert auf den Verpflichtungserklärungen und Selbstzertifizierungen der beteiligten Unternehmen. Die Beteiligung ist zwar freiwillig, jedoch sind die Regelungen für die unterzeichnenden Unternehmen bindend. Die wichtigsten Grundsätze einer solchen Regelung sind Transparenz der Datenschutzbestimmungen der beteiligten Unternehmen, die Übernahme der Safe-Harbor-Grundsätze in die Datenschutzbestimmungen der Unternehmen sowie die Durchsetzung der Grundsätze, einschließlich durch staatliche Instanzen.

Safe Harbor muss angesichts der exponentiellen Zunahme der Datenströme, des raschen Wachstums der digitalen Wirtschaft und der signifikanten Entwicklungen bei der Datenerhebung, -verarbeitung und -nutzung; der Bedeutung von Datenströmen für die transatlantische Wirtschaft; der Zunahme der Anzahl von Unternehmen, die sich an der Safe-Harbor-Regelung beteiligen (die sich seit 2004 verachtfacht hat); sowie die kürzlich bekannt gewordenen Informationen zu den Überwachungsprogrammen der USA, die neue Fragen über das Schutzniveau aufwerfen, das mit der Safe-Harbor-Vereinbarung gewährleistet werden soll, überprüft werden.

Die Mitteilung basiert auf von der Kommission zusammengetragenen Fakten, der Arbeit der „EU–US Privacy Contact Group“ aus dem Jahr 2009, der Studie eines unabhängigen Auftragnehmers aus dem Jahr 2008 sowie den Informationen der Ad-hoc-Arbeitsgruppe EU-USA, die infolge der Enthüllungen über die US-Überwachungsprogramme eingerichtet wurde. Sie folgt auf zwei Bewertungsberichte der Kommission von 2002 und 2004.

In der Mitteilung wird der Tatsache Rechnung getragen, dass die Safe-Harbour-Regelung ein Instrument für die Übermittlung personenbezogener Daten zwischen der EU und den USA ist, dass US-Unternehmen mehrere Hundert Millionen Kunden in der EU haben und dass das aktuelle Volumen der Datenübermittlungen zum Zeitpunkt der Einführung der Regelung unvorstellbar war.

Besondere Aufmerksamkeit gilt der Transparenz der Datenschutzpraktiken der Safe-Harbor-Teilnehmer, der effektiven Anwendung der Datenschutzgrundsätze durch Unternehmen in den USA und der Wirksamkeit der Durchsetzung. Es stellt sich auch die Frage, ob die Datenschutzrechte europäischer Bürger, deren Daten in die USA übermittelt werden, angesichts des umfassenden Zugriffs der Nachrichtendienste auf Daten, die von Safe-Harbor-Unternehmen in die USA übermittelt werden, kontinuierlich geschützt sind.

Die Kommission empfiehlt zum Thema Transparenz daher Folgendes:

- Selbstzertifizierte Unternehmen sollten ihre Datenschutzbestimmungen offenlegen;

- die Datenschutzbestimmungen auf der Website selbstzertifizierter Unternehmen sollten stets mit der Safe-Harbor-Website des US-Handelsministeriums verlinkt sein, auf der alle aktuellen Teilnehmer der Safe-Harbor-Regelung aufgeführt sind;

- Selbstzertifizierte Unternehmen sollten Datenschutzbestimmungen in Verträgen, die sie mit Unterauftragnehmern, z. B. mit Cloud-Computing-Diensten, abschließen, veröffentlichen;

- auf der Website des US-Handelsministeriums sollten alle Unternehmen aufgeführt werden, die nicht mehr an der Safe-Harbor-Regelung teilnehmen.

In Bezug auf Rechtsschutz empfiehlt die Kommission Folgendes:

- die Datenschutzbestimmungen auf Unternehmenswebsites sollten einen Link zu der zuständigen Stelle für alternative Streitbeilegung (ADR) bzw. zu dem EU-Datenschutzgremium enthalten;

- ADR sollte leicht verfügbar und erschwinglich sein;

- das US-Handelsministerium sollte die ADR-Anbieter hinsichtlich der Transparenz der Informationen, die sie über ihre Verfahren und das Follow-up bei Beschwerden bereitstellen, sowie des Zugangs zu diesen Informationen systematischer überprüfen.

Zum Thema Durchsetzung empfiehlt die Kommission Folgendes:

- nach einer Safe-Harbor-Zertifizierung oder Rezertifizierung sollte bei einem bestimmten Anteil der Unternehmen von Amts wegen überprüft werden, ob sie ihre Datenschutzbestimmungen einhalten (diese Kontrolle sollte über formale Erfordernisse hinausgehen);

- wurde im Zuge einer Beschwerde oder Untersuchung ein Verstoß gegen die Datenschutzbestimmungen festgestellt, sollte das Unternehmen ein Jahr später erneut überprüft werden;

- bestehen Zweifel an der Einhaltung der Safe-Harbor-Grundsätze oder liegen Beschwerden gegen ein Unternehmen vor, sollte das US-Handelsministerium die zuständige Datenschutzbehörde in der EU davon in Kenntnis setzen;

- Falschbehauptungen in Bezug auf die Einhaltung der Safe-Harbor-Regelung sollten weiter untersucht werden.

Was das Zugriffsrecht der US-Behörden betrifft, empfiehlt die Kommission Folgendes:

- die Datenschutzbestimmungen selbstzertifizierter Unternehmen sollten Auskunft darüber geben, in welchem Umfang die Behörden nach Maßgabe des US-Rechts Daten erheben und verarbeiten dürfen, die auf der Grundlage der Safe-Harbor-Regelung übermittelt worden sind; und

- von der in der Safe-Harbor-Entscheidung vorgesehenen Ausnahme der nationalen Sicherheit soll nur so weit Gebrauch gemacht werden, wie dies unbedingt notwendig oder angemessen ist.

3.2.4 Evaluierungsbericht zum Programm zum Aufspüren der Finanzierung des Terrorismus (TFTP)

Die Kommission gelangt in dem Bericht über die Bedeutung der im Rahmen des TFTP gesammelten Daten für Ermittlungen zur Bekämpfung terroristischer Handlungen zu dem Schluss, dass das TFTP umfangreiche sachdienliche Erkenntnisse ermöglicht hat, welche zur Aufdeckung geplanter terroristischer Handlungen und zur Verfolgung der dafür verantwortlichen Personen beigetragen haben. So wurden beispielsweise die aus den Daten gewonnene Erkenntniss für die Ermittlungen im Zusammenhang mit dem Bombenanschlag beim Boston-Marathon im April 2013, mit den Anschlagsdrohungen bei den Olympischen Spielen in London und den Ausbildungslagern für aus der EU stammende Terroristen in Syrien genutzt.

Die TFTP-Daten ermöglichen wichtige Erkenntnisse über finanzielle Netze zur Unterstützung von Terrororganisationen und tragen zur Aufdeckung neuer Formen der Terrorismusfinanzierung und der daran beteiligten Personen in den Vereinigten Staaten, in der EU und in anderen Ländern bei. Sie sind sowohl für die Mitgliedstaaten der EU als auch für Europol von Nutzen und ermöglichen wichtige konkrete Erkenntnisse für die Ermittlungsarbeit. In den vergangenen drei Jahren haben die insgesamt 158 Informationsanfragen, die von den Mitgliedstaaten und der EU gestellt wurden, zu insgesamt 924 konkreten Ermittlungsansätzen geführt.

Was die unlängst erhobenen Vorwürfe bezüglich eines gegen das TFTP-Abkommen verstoßenden Zugriffs auf Zahlungsverkehrsdaten in der EU anbelangt, so hat die US-Regierung schriftlich versichert, dass sie nicht gegen das Abkommen verstoßen hat und es auch weiterhin in vollem Umfang einhalten wird. Im Jahr 2013 war man der Auffassung, dass keine weiteren Gespräche mit den Vereinigten Staaten über die Umsetzung des TFTP-Abkommens erforderlich sind.

Die Kommission hat auf Anfragen des Europäischen Parlaments und des Rates die Optionen für die Einrichtung eines europäischen Systems zum Aufspüren der Terrorismusfinanzierung (TFTS) geprüft und dabei bei jeder Option die Wahrung der Grundrechte, die Notwendigkeit, die Verhältnismäßigkeit und die Kostenwirksamkeit im Vergleich zur jetzigen Situation bewertet.

Die Kommission ist zu dem Schluss gelangt, dass für die Einrichtung eines solchen Systems in der Europäischen Union keine eindeutige Notwendigkeit besteht, da es u. a. erforderlich wäre, eine neue Datenbank mit Informationen über die finanziellen Transaktionen aller EU-Bürger einzurichten und zu verwalten. Die Schaffung einer solchen Datenbank würde schwer wiegende Fragen in punkto Datenspeicherung, Datenzugriff und Datenschutz aufwerfen und einen enormen technischen und finanziellen Aufwand erfordern.

3.2.5 Bericht über die gemeinsame Überprüfung des Fluggastdaten-Abkommens zwischen der EU und den USA

Das Abkommen zwischen der EU und den Vereinigten Staaten über die Übermittlung von Fluggastdaten bei Flügen aus der EU in die USA ist am 1. Juli 2012 in Kraft getreten. Im Anschluss an eine Überprüfung

des Abkommens durch Sachverständige aus der EU und den Vereinigten Staaten hat die Kommission befunden, dass die US-Behörden das Abkommen in Übereinstimmung mit den im Abkommen festgelegten Standards und Bedingungen umgesetzt haben.

Das Abkommen ist ein effizientes Instrument zur Bekämpfung von schwerer grenzüberschreitender Kriminalität und Terrorismus. Gleichzeitig enthält es eindeutige Bestimmungen darüber, innerhalb welcher Grenzen und zu welchen Zwecken Fluggastdaten verwendet werden dürfen, sowie verschiedene robuste Datenschutzgarantien.

In dem gemeinsamen Bericht wird insbesondere festgestellt, dass die US-Behörden ihre Pflichten bezüglich der Datenzugangsrechte der Fluggäste einhalten und über einen ordnungsgemäßen Überwachungsmechanismus verfügen, um eine widerrechtliche Diskriminierung zu verhindern. Die Bestimmungen bezüglich der Schwärzung und der Löschung von sensiblen Daten werden eingehalten. Die Datenweitergabe an inländische US-Stellen wie auch an Drittländer erfolgt in Übereinstimmung mit dem Abkommen.

3.3. Europäischer Gerichtshof

3.3.1 Gericht: T-214/11 – ClientEarth und PAN Europe gegen EBLS (anhängig)

Urteil des Gerichts (Sechste Kammer) vom 13. September 2013 – ClientEarth und Pesticide Action Network Europe (PAN Europe) gegen Europäische Behörde für Lebensmittelsicherheit (EBLS).

Bei dieser Rechtssache begehrte der Kläger gemäß Verordnung 1049/2001 Zugang zu Dokumenten, die von EU-Sachverständigen angefertigt wurden. Dem Kläger waren die Namen der Sachverständigen sowie der Inhalt der Dokumente bekannt. Er wollte jedoch wissen, welche Äußerungen von welchen Sachverständigen stammten. Die Offenlegung solcher Informationen wurde auf der Grundlage der Verordnung 45/2001 abgelehnt, die vorsieht, dass der Zugang zu Dokumenten verweigert werden könne, wenn eine Offenlegung gegen den Datenschutz und die Integrität der betroffenen Person verstoßen würde.

Die Kläger behaupteten, dass die Institution auf ihrer Website die Namen, Lebensläufe und Interessensbekundungen der Sachverständigen offengelegt habe und es sich daher nicht um personenbezogene Daten handele.

Das Gericht urteilte, dass die Tatsache, dass Einzelpersonen auf einer öffentlich zugänglichen Website genannt werden, nicht unbedingt heißt, dass ihre Namen nicht mehr als personenbezogene Daten gelten können.

Die Kläger behaupteten außerdem, dass die Meinungen von Sachverständigen öffentlich gemacht werden müssten, selbst wenn dies zu Kontroversen führen oder die Sachverständigen davon abhalten könnte, einen Beitrag zum Entscheidungsfindungsprozess einer Institution zu leisten.

Das Gericht urteilte, dass sich daraus nicht ergibt, dass der Name eines Sachverständigen, der zu einer Maßnahme der EU Stellung genommen hat, nicht als personenbezogene Daten gelten kann.

3.3.2 Europäischer Gerichtshof C-486/12 – X

Urteil des Gerichtshofs (Achte Kammer) vom 12. Dezember 2013 – Auf Antrag von X.

Das Gericht kam zu dem Schluss, dass Art. 12 lit a der Richtlinie 95/46 der Erhebung von Gebühren für die Mitteilung personenbezogener Daten durch eine Behörde nicht entgegensteht, sofern diese Gebühren nicht überhöht sind. Es ist Sache der Mitgliedstaaten, die Höhe dieser Gebühren so festzusetzen, dass ein gerechter Ausgleich geschaffen wird zwischen dem Interesse der betroffenen Person am Schutz ihrer Privatsphäre, insbesondere mittels ihres Anspruchs, dass ihr die Daten in verständlicher Form übermittelt werden, damit sie gegebenenfalls Ansprüche auf Berichtigung, Löschung oder Sperrung der Daten – falls deren Verarbeitung nicht der Richtlinie entspricht – sowie die Rechte auf Widerspruch und gerichtlichen Rechtsschutz geltend machen kann, sowie der Belastung, die die Pflicht zur Mitteilung dieser Informationen für den für die Verarbeitung Verantwortlichen darstellt.

Wenn im Rahmen der Anwendung von Art. 12 lit a eine nationale Behörde Gebühren dafür erhebt, dass eine natürliche Person ihr Recht auf Auskunft über die sie betreffenden personenbezogenen Daten ausübt, dürfen diese Gebühren die Kosten der Mitteilung dieser Daten nicht übersteigen. Eine solche Obergrenze lässt jedoch die Befugnis der Mitgliedstaaten unberührt, diese Gebühren niedriger anzusetzen, um für jede natürliche Person zu gewährleisten, dass das Auskunftsrecht seine Wirksamkeit behält.

3.3.3 Europäischer Gerichtshof C-473/12 – IPI

Urteil des Gerichtshofs (Dritte Kammer) vom 7. November 2013 – Institut professionnel des agents immobiliers (IPI) gegen Geoffrey Englebert u. a.

In diesem Urteil befand das Gericht, dass Artikel 13 Absatz 1 der Richtlinie 95/46 dahin auszulegen ist, dass die Mitgliedstaaten nicht die Pflicht, wohl aber die Möglichkeit haben, eine oder mehrere der in dieser Bestimmung vorgesehenen Ausnahmen von der Pflicht, die betroffene Person über die Verarbeitung ihrer personenbezogenen Daten zu informieren, in ihr nationales Recht umzusetzen, und dass die Bestimmungen in dieser Hinsicht allgemein und flexibel sind und die Entscheidung den Mitgliedstaaten überlassen bleibt.

Mitgliedstaaten können frei entscheiden, ob und gegebenenfalls zu welchen Zwecken sie Ausnahmen zu den in Art. 13 Abs. 1 lit a bis g aufgezählten Zwecken verfügen, einschließlich der Beschränkung der Pflichten zur Unterrichtung der betroffenen Person. Solche Maßnahmen können nur vorgesehen werden, wenn sie notwendig sind.

Die Situation eines Privatdetektivs, der von einem Berufsverband engagiert wurde, zu Verstößen gegen die berufsständischen Regeln eines reglementierten Berufs zu ermitteln, wird durch Artikel 13 Absatz 1 lit d abgedeckt. Da die Richtlinie nicht angibt, auf welche Weise die Verstöße gegen die Vorschriften aufzuspüren und aufzudecken sind, hindert diese Richtlinie einen solchen Berufsverband nicht daran, seinen Pflichten nachzukommen.

Falls dies im nationalen Recht vorgesehen ist, sind weder der Berufsverband noch die Privatdetektive dazu verpflichtet, die betroffene Person gemäß Artikel 10 und 11 zu unterrichten. Falls dies nicht vorgesehen ist, müssen die betroffenen Personen unterrichtet werden.

Mitgliedstaaten können auch zu dem Schluss kommen, dass Berufsverbände und die für sie tätigen Privatdetektive dazu in der Lage sind, ihren Pflichten nachzugehen, ohne sich dabei auf die Ausnahmen von Artikel 13 Absatz 1 zu stützen.

3.3.4Europäischer Gerichtshof C-342/12 – Worten

Urteil des Gerichtshofs (Dritte Kammer) vom 30. Mai 2013 – Worten – Equipamentos para o Lar SA gegen Autoridade para as Condições de Trabalho (ACT).

In diesem Urteil kam der Gerichtshof zu dem Schluss, dass Art. 6 Abs. 1 lit b und c und Art. 7 lit c und e der Richtlinie 95/46 in dem Sinne auszulegen sind, dass sie einer nationalen Regelung nicht entgegenstehen, nach der Arbeitgeber dazu verpflichtet sind, der für die Überwachung der Arbeitsbedingungen zuständigen nationalen Behörde die Aufzeichnungen über die Arbeitszeiten so zur Verfügung zu stellen, dass sie unverzüglich eingesehen werden können, vorausgesetzt, diese Verpflichtung ist notwendig, damit diese Behörde ihre Überwachungsaufgaben hinsichtlich der Anwendung der Regelungen über Arbeitsbedingungen, insbesondere in Bezug auf Arbeitszeit, wahrnehmen kann.

3.3.5 Europäischer Gerichtshof C-291/12 – Schwarz

Urteil des Gerichtshofs (Vierte Kammer) vom 17. Oktober 2013 – Michael Schwarz gegen Stadt Bochum.

Der Gerichtshof urteilte, dass Art. 62 Abs. 2 lit a EG, der zu Titel IV des EG-Vertrages gehörte, den Rat dazu ermächtigt, die Durchführung von Kontrollen an den Außengrenzen der Europäischen Union zu regeln, die der Überprüfung der Identitäten von die Grenze überschreitenden Personen dienen. Da eine solche Überprüfung notwendigerweise die Vorlage von Dokumenten erfordert, anhand derer diese

Identität festgestellt werden kann, ermächtigte Art. 62 Abs. 2 lit a EG demgemäß den Rat, gesetzliche Bestimmungen für solche Dokumente, insbesondere Reisepässe, zu erlassen.

In Bezug auf die EU-Gesetzgebung in diesem Bereich war die Bestimmung – die sich ohne weitere Präzisierung auf die Kontrollen von „Personen" bezog – nicht nur für Angehörige von Drittländern, sondern auch für Unionsbürger und damit auch für deren Reisepass vorgesehen.

Zum anderen kann eine Harmonisierung der Sicherheitsnormen für Pässe von EU-Bürgern geboten sein, um zu vermeiden, dass diese Pässe Sicherheitsmerkmale aufweisen, die hinter denen zurückbleiben, die für die einheitliche Visagestaltung und die einheitlichen Aufenthaltstitel für Drittstaatsangehörige vorgesehen sind. Daher ist der Unionsgesetzgeber befugt, gleichwertige Sicherheitsmerkmale für die Pässe der Unionsbürger vorzusehen, da eine solche Befugnis es ermöglicht zu verhindern, dass diese Reisepässe zum Ziel von Fälschungen und betrügerischen Verwendungen werden.

3.4. EUROPÄISCHER DATENSCHUTZBEAUFTRAGTER

A. Zusammenfassung der Aktivitäten und Neuerungen

Der Europäische Datenschutzbeauftragte (EDSB) ist eine unabhängige Aufsichtsbehörde mit der Aufgabe, den Schutz personenbezogener Daten und die Achtung der Privatsphäre zu gewährleisten und den Einsatz bewährter Verfahren in den Organen und Einrichtungen der EU zu fördern. Dies wird durch Folgendes erreicht:

- Überwachung der Verarbeitung personenbezogener Daten durch die EU-Verwaltung;
- Beratung im Hinblick auf politische Strategien und Gesetze, die Auswirkungen auf den Datenschutz haben;
- Zusammenarbeit mit ähnlichen Behörden zur Gewährleistung eines konsequenten Datenschutzes.

Zehn Jahre nach ihrer Gründung ist die Behörde des EDSB ausgereift und ist in der Lage, sich mit den vielfältigen Herausforderungen, die in einem hoch dynamischen Umfeld an eine Datenschutzbehörde gestellt werden, wirkungsvoll auseinanderzusetzen. Im operativen Bereich bestand 2013 die wichtigste Herausforderung darin, dass sowohl der Umfang als auch die Reichweite der Tätigkeit des EDSB weiter zunahmen, während zugleich die Haushaltsbeschränkungen und die personellen Maßnahmen aufgrund der Finanzkrise weiterhin Bestand hatten.

Die Strategie 2013-2014 des EDSB sowie die Geschäftsordnung und der jährliche Managementplan bieten wertvolle Orientierungshilfe, da in diesen Dokumenten die nötige Vision und Methodik formuliert sind, um die Fähigkeit des EDSB zu effizienter und wirkungsvoller Arbeit trotz der gegenwärtig verfolgten Sparpolitik zu verbessern.

A.1. Aufsicht und Durchsetzung

Im Rahmen des Tätigkeitsbereichs Aufsicht und Durchsetzung stieg die Zahl der Meldungen für Vorabprüfungen. Dieser Anstieg ist hauptsächlich darauf zurückzuführen, dass die Frist für Meldungen zur nachträglichen oder Ex-post-Vorabprüfung für bereits laufende Verarbeitungen im Juni 2013 endete. Auch der Anstieg bei den in diesem Jahr abgegebenen Stellungnahmen des EDSB ist durch die große Zahl der eingegangenen Meldungen begründet. Die Weiterverfolgung der Empfehlungen, die in bereits abgegebenen Stellungnahmen des EDSB im Rahmen von Vorabprüfungen ausgesprochen wurden, wurde fortgeführt, und eine beträchtliche Anzahl von Fällen konnte abgeschlossen werden.

Die Zahl der eingegangenen Beschwerden entwickelte sich rückläufig, was zum Teil auf die bessere Information und Aufklärung über die Zuständigkeiten des EDSB, zum Teil aber auch auf die Wirksamkeit des Beschwerdeformulars zurückzuführen ist.

Der in der Strategie 2013-2014 des EDSB festgelegte Aktionsplan sieht unter anderem vor, eine „Kultur des Datenschutzes“ bei den Organen und Einrichtungen der EU zu fördern, so dass diese sich ihrer Verpflichtungen bewusst und hinsichtlich der Einhaltung der Datenschutzanforderungen rechenschaftspflichtig sind.

Daher wurden vom EDSB weiterhin Handlungsempfehlungen und Weiterbildungsmaßnahmen für die für die Datenverarbeitung Verantwortlichen, behördliche Datenschutzbeauftragte (DPO, Data Protection Officers) und Datenschutzkoordinatoren (DSK) angeboten. Dies geschah 2013 hauptsächlich in Form von Leitlinien für die Verarbeitung personenbezogener Daten bei der Vergabe öffentlicher Aufträge, der Gewährung von Finanzmitteln und der Auswahl und dem Einsatz externer Sachverständiger, durch Grundlagenschulungen für neue Datenschutzbeauftragte zum Verfahren der Vorabprüfung sowie durch spezielle Weiterbildungsmaßnahmen für die Datenschutzbeauftragten von fünf Gemeinsamen

Unternehmen der EU. Im Rahmen der vom EDSB durchgeführten Sensibilisierungsmaßnahmen bei den Organen und Einrichtungen der EU wurden fachlich ausgerichtete und allgemeine Workshops angeboten.

Eine wichtige Rolle kam auch dem anhaltenden Dialog mit den für die Datenverarbeitung Verantwortlichen, den DPO und den DSK zu. Durch diese Gespräche erhält der EDSB einen besseren Einblick in die Sachzwänge, denen die Organe und Einrichtungen unterliegen, und kann so seine Ratschläge an der Praxis ausrichten. Im Zuge von Vorabprüfungen bzw. im Rahmen der Weiterverfolgung von Stellungnahmen und Entscheidungen fanden zahlreiche Treffen mit für die Verarbeitung Verantwortlichen statt. Als nützliche Kommunikationskanäle für die Zusammenarbeit mit den DPO und DSK erwiesen sich auch die Sitzungen des Netzes der behördlichen Datenschutzbeauftragten, bilaterale Treffen und die telefonische Hotline für behördliche Datenschutzbeauftragte.

A.2. Strategie und Beratung

Während des gesamten Jahres 2013 war der EDSB weiter eng in die laufende Arbeit zur Reform des EU-Datenschutzrahmens eingebunden. Am 15. März 2013 übermittelte er zusätzliche Bemerkungen zu der Reform an das Europäische Parlament, die Kommission und den Rat. Auch an den darauf folgenden Beratungen im Parlament und im Rat war der EDSB weiterhin beteiligt.

Darüber hinaus veröffentlichte die Kommission zahlreiche Rechtsetzungsvorschläge, die Auswirkungen auf das Grundrecht auf den Schutz personenbezogener Daten haben.

Auf den Themenbereich „Digitale Agenda und Internet“ ging der EDSB bei verschiedenen Gelegenheiten ein, u. a. in der Stellungnahme zur Mitteilung der Kommission „Die Digitale Agenda für Europa – digitale Impulse für das Wachstum in Europa“, der Stellungnahme zum europäischen Binnenmarkt der elektronischen Kommunikation und der Stellungnahme zum Grünbuch über die „Vorbereitung auf die vollständige Konvergenz der audiovisuellen Welt: Wachstum, Schöpfung und Werte“.

In Bezug auf den Raum der Freiheit, der Sicherheit und des Rechts gab der EDSB Stellungnahmen zu Europol, zur Cybersicherheitsstrategie der EU und zur Initiative „Intelligente Grenzen“ sowie zum Abkommen zwischen der EU und Kanada über die Übermittlung von Fluggastdatensätzen und zum Europäischen Modell für den Informationsaustausch ab

Mit Blick auf den Binnenmarkt waren die Stellungnahmen des EDSB zu den Anti-Geldwäsche-Vorschlägen, zur Terrorismusfinanzierung, zu Zahlungsdiensten im Binnenmarkt, zum Europäischen Gesellschaftsrecht und Corporate Governance sowie zur elektronischen Rechnungsstellung bei öffentlichen Aufträgen erwähnenswert.

Auf dem Gebiet der elektronischen Gesundheitsdienste sind vor allem die Stellungnahmen des EDSB zu Medizinprodukten, Drogenausgangsstoffen und dem Aktionsplan für elektronische Gesundheitsdienste zu nennen.

A.3. Zusammenarbeit

Der EDSB arbeitet mit anderen Datenschutzbehörden zusammen, um in ganz Europa einen einheitlichen Datenschutz zu fördern. Diese kooperative Funktion erstreckt sich auch auf die Zusammenarbeit mit Aufsichtsbehörden, die im Rahmen der ehemals „dritten Säule“ der EU im Kontext von IT-Großsystemen eingerichtet worden waren.

Im Jahr 2013 leistete der EDSB weiterhin einen aktiven Beitrag zur Tätigkeit der Artikel-29-Datenschutzgruppe. Insbesondere war der EDSB als Berichterstatter und Mitberichterstatter stark in die Erarbeitung der Stellungnahmen zu Zweckbindung und berechtigtem Interesse (Untergruppe „Zentrale Bestimmungen“), der Stellungnahme zur Vorlage für die Datenschutz-Folgenabschätzung für intelligente Netze (Untergruppe „Technologie“) und der Stellungnahme zu offenen Daten (Untergruppe „E-Government“) eingebunden.

Die direkte Zusammenarbeit mit den nationalen Behörden spielt auch im Hinblick auf große internationale Datenbanken wie Eurodac, das Visa-Informationssystem (VIS), das Schengener Informationssystem II (SIS II) und das Zollinformationssystem (ZIS) eine wichtige Rolle, da die Aufsicht über diese Systeme eine koordinierte Vorgehensweise erfordert. Der EDSB übernahm 2013 die Sekretariatsaufgaben für die neu eingerichtete Koordinierungsgruppe für die Aufsicht über SIS II und führte weiterhin den Vorsitz der Koordinierungsgruppen für die Aufsicht über Eurodac, VIS und ZIS. Der EDSB organisierte 2013 für alle Koordinierungsgruppen zwei Treffen in Brüssel.

Außerdem wurde SIS II in Betrieb genommen. Um den finanziellen und bürokratischen Aufwand sowie den Aufwand für Dienstreisen zu verringern, wurden die Sitzungstermine der Koordinierungsgruppen so gelegt, dass sie unmittelbar aneinander anschließen; ferner wird angestrebt, die Aufsichtsmaßnahmen für IT-Großsysteme durchgängig möglichst einheitlich zu gestalten.

Das Modell der Koordinierungsgruppen wird 2014 um eine neue Koordinierungsgruppe für die Aufsicht über das Binnenmarktinformationssystem (IMI) erweitert. Im Zuge der Vorbereitung auf die für 2014 vorgesehene erste Sitzung dieser Gruppe wurden 2013 die nationalen Datenschutzbehörden und die Kommission zum aktuellen Sachstand und den weiteren Entwicklungen bei der IMI-Verordnung konsultiert.

Im Rahmen des Europarates nahm der EDSB an drei Sitzungen des Beratenden Ausschusses zum Übereinkommen 108 des Europarates teil. Damit bot sich für ihn eine wichtige Gelegenheit, die laufende Überarbeitung des Übereinkommens zu verfolgen und darauf Einfluss zu nehmen.

Der EDSB war auch Mitglied der Expertengruppe, die mit der Aktualisierung der Leitlinien zum Schutz der Privatsphäre der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) beauftragt war.

Darüber hinaus beteiligte sich der EDSB mit wichtigen Beiträgen zu Datenschutzfragen an zahlreichen weiteren bedeutenden Gremien, darunter die Asiatisch-Pazifische Wirtschaftskooperation (APEC), die Vereinigung der französischsprachigen Datenschutzbehörden (AFAPDP) und die Internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation („Berliner Gruppe“).

Organisation	Europäischer Datenschutzbeauftragter (EDSB)
Vorsitz und/oder Gremium	Peter Hustinx, Europäischer Datenschutzbeauftragter Giovanni Buttarelli, Stellvertretender Europäischer Datenschutzbeauftragter
Budget	7 661 409 EUR
Personal	62 (alle Kategorien zusammengefasst)
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Es wurden 20 legislative Stellungnahmen u. a. zu Initiativen bezüglich des Raums der Freiheit, der Sicherheit und des Rechts sowie in den Bereichen digitale Agenda, elektronischer Gesundheitsdienst, internationale Zusammenarbeit und Binnenmärkte abgegeben. Es wurden 13 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.

	33 informelle Kommentare
Meldungen	Die Datenschutzbeauftragten der Institutionen und Organe der EU reichten 272 Meldungen von Datenverarbeitungsvorgängen zur Vorabprüfung ein.
Vorabprüfungen	Es wurden 91 Stellungnahmen im Rahmen einer Vorabprüfung abgegeben, insbesondere zur Urlaubsplanung, zu Beurteilungen und zur Einstellung von Personal, zum Verdacht auf Verstöße und zur Vergabe öffentlicher Aufträge. 21 Stellungnahmen zu Verarbeitungen, die nicht einer Vorabprüfung unterliegen.
Anträge betroffener Personen	176 Anträge auf Informationen und Beratung aus der Öffentlichkeit oder interessierten Parteien; ein Großteil davon bezog sich auf ausführlichere Informationen über Fragen der Privatsphäre informieren oder Unterstützung bei Problemen wie Sicherheit ihrer personenbezogenen Daten oder deren Missbrauch.
Beschwerden betroffener Personen	78 eingegangene Beschwerden, 30 davon zulässig
Vom Parlament bzw. der Regierung angeforderte Beratung	Der Großteil der 20 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	37 Konsultationen zu verwaltungsrechtlichen Maßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten in der EU-Verwaltung. Es wurde im Hinblick auf eine breite Vielfalt von rechtlichen Aspekten beraten, wie z. B. die Übermittlung von Personaldaten, die Änderung der Zweckbestimmung von Daten, die für einen konkreten Zweck erhoben wurden, sowie Anträge auf Zugang der Öffentlichkeit. Des Weiteren wurden Leitlinien zur Verarbeitung personenbezogener Daten im Bereich der Vergabe öffentlicher Aufträge bereitgestellt. Zu bestimmten Themen wurde eine Reihe von Schulungen und Workshops organisiert, wie z. B. zur Rolle der Datenschutzbeauftragten, zu Bereichen wie Personal, IT und die Vergabe öffentlicher Aufträge sowie zum Meldeverfahren und zu Vorabprüfungen. Die Workshops befassten sich mit Themen wie der Nutzung elektronischer Kommunikation am Arbeitsplatz, der Nutzung mobiler Geräte am Arbeitsplatz, den von den Organen und Einrichtungen der EU verwalteten Websites sowie der grenzüberschreitenden Übermittlung personenbezogener Daten.
Prüfmaßnahmen	
Prüfungen, Untersuchungen	5 Prüfungen vor Ort und 2 Besuche.
Sanktionsmaßnahmen	k. A.

Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	62 DPOs in Einrichtungen, Organen und Agenturen der EU

B. Rechtsprechung

Rechtssachen

Im Jahr 2013 trat der EDSB mehreren Verfahren vor dem Gerichtshof der Europäischen Union und dem Gericht für den öffentlichen Dienst als Streithelfer bei.

Der EDSB äußerte sich in einer Verhandlung vor der Großen Kammer des Gerichtshofs in einem Vorabentscheidungsverfahren. Die Verhandlung betraf die verbundenen Rechtssachen Digital Rights Ireland (C-293/12) und Seitlinger u. a. (C-293/12). Beide bezogen sich auf die Gültigkeit der Richtlinie zur Vorratsdatenspeicherung (Richtlinie 2006/24/EG).

Der EDSB war vom Gerichtshof erstmals zu einer Verhandlung im Vorabentscheidungsverfahren geladen worden. Für den EDSB war dies als ein bedeutender Schritt zu werten, der zu einer wegweisenden Entscheidung in einer Frage führen könnte, die von der Behörde bereits seit Jahren mit großem Interesse verfolgt wird.

Ferner gab der EDSB in der Verhandlung in der Rechtssache *Kommission/Ungarn* (C-288/12) eine Stellungnahme ab. Dies ist die dritte Rechtssache, die Vertragsverletzungen hinsichtlich der Unabhängigkeit von Datenschutzbehörden betrifft. Die beiden anderen Rechtssachen – Kommission/Österreich (C-614/10) und Kommission/Deutschland (C-518/07) – wurden bereits 2012 bzw. 2010 entschieden.

Weitere Rechtssachen, denen der EDSB beitrat, sind noch anhängig, so z. B. Pachtitis/Kommission und EPSO (T-374/07), Pachtitis/Kommission (F-35/08), ZZ/EIB (F-103/11) sowie Dennekamp/Europäisches Parlament (T-115/13).

Im Oktober 2013 beantragte der EDSB, als Streithelfer in zwei weiteren Rechtssachen zugelassen zu werden: Elmaghraby und El Gazaerly/Rat der Europäischen Union (T-319/13) und CN/Europäisches Parlament (T-343/13).

C. Sonstige wichtige Informationen

Überprüfung des Rechtsrahmens der EU für den Datenschutz

Nach zahlreichen Aktivitäten zur EU-Datenschutzreform im Jahr 2012, einschließlich der Stellungnahme vom 7. März 2012, übermittelte der EDSB am 15. März 2013 zusätzliche Anmerkungen an das Europäische Parlament, die Kommission und den Rat. Diese Anmerkungen bezogen sich auf bestimmte Bereiche, in denen Klarstellungsbedarf bestand. Außerdem ging der EDSB auf die von den Mitgliedern des Europäischen Parlaments vorgeschlagenen Abänderungen ein.

In den Anmerkungen sprach sich der EDSB dagegen aus, bestimmte Sektoren vom Anwendungsbereich des Rechtsrahmens der EU für den Datenschutz auszunehmen und den räumlichen Anwendungsbereich der vorgeschlagenen allgemeinen Datenschutzverordnung zu beschränken. Des Weiteren wies der EDSB erneut darauf hin, dass pseudonymisierte Daten weiterhin personenbezogene Daten (oder personenbezogene Informationen) bleiben und als solche geschützt werden sollten. Jegliche Definition anonymer oder pseudonymer Daten sollte daher der Begriffsbestimmung der personenbezogenen Daten voll und ganz gerecht werden und nicht unzulässigerweise zu einer Herausnahme bestimmter Kategorien von personenbezogenen Daten aus dem Anwendungsbereich des Rechtsrahmens für den Datenschutz

führen. Die Streichung der Möglichkeit zur Weiterverarbeitung von Daten für unvereinbare Zwecke wurde vom EDSB unterstützt, der zugleich hervorhob, dass die Definition der expliziten Einwilligung beibehalten werden sollte. Befürwortet wurden auch die von der Kommission vorgeschlagene Definition und die Zuständigkeiten der für die Datenverarbeitung Verantwortlichen und der Auftragsverarbeiter ebenso wie der Grundsatz der Rechenschaftspflicht, der für das gesamte Paket gelten sollte. Der EDSB begrüßte einige Elemente des so genannten *risikoorientierten Ansatzes*, er verwies jedoch darauf, dass – wie in der Verordnung vorgesehen – für alle Verarbeitungsvorgänge der volle Schutz gelten sollte. Hinsichtlich des internationalen Datenaustauschs empfahl der EDSB eine Klarstellung der Vorschriften und befürwortete die Änderungen, die die Aufnahme eines neuen Artikels zu Datenübermittlungen, die nach EU-Recht nicht zulässig sind, vorsehen.

Was den Vorschlag für eine Richtlinie zum Datenschutz für Zwecke der Strafverfolgung angeht, sprach sich der EDSB im Interesse der Kohärenz für eine stärkere Angleichung der vorgeschlagenen Richtlinie an die vorgeschlagene Verordnung aus. Der EDSB begrüßte auch die Änderungen, mit denen spezielle Bedingungen und Schutzklauseln für den Zugang der Strafverfolgungsbehörden zu Daten eingeführt werden, die ursprünglich für andere Zwecke verarbeitet wurden, und betonte, dass jede Datenübermittlung an nicht mit der Strafverfolgung befasste Behörden oder Privatpersonen streng begrenzt werden sollte.

Nach schwierigen Verhandlungen und zahlreichen politischen Kompromissen nahm der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres (LIBE) des Europäischen Parlaments am 21. Oktober 2013 seinen Bericht an. Das Europäische Parlament stimmte dem Bericht in erster Lesung in der Plenarabstimmung am 12. März 2014 zu. Im Rat geht die Arbeit langsamer voran. Die Verhandlungen zwischen den Mitgliedstaaten über wichtige Teile des Rechtsrahmens dauern an – neben anderen politisch sensiblen und rechtlich komplizierten Fragestellungen wird z. B. weiter über eine zentrale Anlaufstelle und den Umfang von Verordnung und Richtlinie verhandelt.

Im Verlauf des Jahres 2013 setzte der EDSB seine Beratungstätigkeit für das Europäische Parlament und den Rat fort und beteiligte sich an der Diskussion. Auch an der Einleitung des Prozesses zur Überarbeitung der Verordnung (EG) Nr. 45/2001, die die Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft regelt, war der EDSB mit einem Schreiben an die Kommission, in dem er seine ersten Überlegungen zum Ausdruck brachte, beteiligt.

Kapitel Vier

Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum

ISLAND

A. Zusammenfassung der Aktivitäten und Neuerungen

Die bevorstehende Änderung des isländischen Datenschutzgesetzes, die sich am stärksten auf die aktuelle Arbeit der Datenschutzbehörde auswirken würde, war ein Gesetzentwurf zur wissenschaftlichen Forschung im Gesundheitswesen. Das Gesetz sah vor, dass lediglich die nationale Ethik-Kommission die Genehmigung für den Zugang zu Gesundheitsdaten zum Zwecke solcher Forschungen erteilen und die Datenschutzbehörde hierfür nicht mehr zuständig sein solle. Die nationale Ethik-Kommission solle jedoch der Datenschutzbehörde eine Zusammenfassung der erteilten Genehmigungen zukommen lassen, damit diese beschließe, welche Forschungsprojekte sie genauer untersuchen wolle. Die nationale Ethik-Kommission könne erst zehn Tage nach Zusendung besagter Zusammenfassung an die Datenschutzbehörde eine Genehmigung erteilen. Sollte die Datenschutzbehörde die Ethik-Kommission über eine genauere Untersuchung eines spezifischen Forschungsprojekts informieren, dürfe die Kommission erst dann eine Genehmigung erteilen, wenn die Datenschutzbehörde zu einem Entschluss gekommen ist. Laut dem Gesetz könnte die Datenschutzbehörde Sicherheitsmaßnahmen für den Umgang mit personenbezogenen Daten anordnen. Schließlich dürfe die Ethik-Kommission das Forschungsprojekt nicht genehmigen, wenn die Datenschutzbehörde der Meinung ist, dass die Verarbeitung der personenbezogenen Daten zum Zweck der wissenschaftlichen Forschung gegen Gesetz Nr. 77/2000 zum Schutz der Privatsphäre im Zusammenhang mit der Verarbeitung personenbezogener Daten verstößt.

Eine weitere Änderung des isländischen Datenschutzrechts war die Änderung des Gesetzes Nr. 163/2007 zum isländischen Statistikamt. Der Entwurf dieser Änderung sollte das isländische Statistikamt in die Lage versetzen, für statistische Berichte in sehr großem Umfang Daten zu Krediten betroffener Personen zu erfassen, um daraus Maßnahmen abzuleiten, die den verschuldeten Haushalten zugute kommen. Die Datenschutzbehörde lehnte eine derart weitreichende Datenverarbeitung ab und wies darauf hin, dass der Gesetzesänderungsentwurf nicht die Notwendigkeit solch umfassender Verarbeitungen/Eingriffe in die Privatsphäre betroffener Personen erläuterte, um das Ziel des Gesetzes zu erreichen – nämlich die Ableitung von Maßnahmen, die den verschuldeten Haushalten zugute kommen. Das Parlament berücksichtigte die Beobachtungen der Datenschutzbehörde und änderte den Entwurf u. a. im Hinblick auf den Schutz der erfassten Daten, die Aufbewahrungsfrist und die Löschung der Daten.

Schließlich wurde eine Änderung am Sozialversicherungsgesetz Nr. 805/2013 vorgenommen. Die Arbeit der Datenschutzbehörde war dabei am stärksten von einer Bestimmung betroffen, welche die Befugnisse der Sozialversicherungsanstalt zur Überwachung und Erfassung von Daten anderer Regierungsbehörden wie z. B. der Steuerbehörden, des Arbeitsministeriums, des Nationalregisters, bestimmter Rentenfonds, Seniorenheime, Gemeinden, des isländischen Fonds für Studentenkredite und anderer Stellen und Unternehmen ausweitete. Das Gesetz sah eine derartige Datenerfassung ohne die bislang erforderliche Einwilligung der betroffenen Personen vor. Die Datenschutzbehörde stellte fest, dass die Bestimmung über die Datenerfassung ohne Einwilligung zu weitreichend und offen sei, da weder genau angegeben wurde, welche Parteien die Informationen bereitstellen sollen, noch welche Informationen gemäß der Bestimmung erfasst werden könnten. Außerdem würde das Recht auf Selbstbestimmung der betroffenen Personen grundlos eingeschränkt werden. Die Beobachtungen der Datenschutzbehörde wurden berücksichtigt und die Bestimmung der Datenerfassung ohne Einwilligung gestrichen.

Organisation	Isländische Datenschutzbehörde
Vorsitz und/oder Gremium	Sigrún Jóhannesdóttir, Kommissarin (bis April 2013, als Hörður Helgi Helgason den Posten übernahm); Björg Thorarensen, Vorsitzender.

Budget	66 Millionen ISK (ca. 415 800 EUR zum 31. Dezember 2013)
Personal	Drei Rechtsberater, eine Sekretärin.
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	Ca. 120
Meldungen	485
Vorabprüfungen	118
Anträge betroffener Personen	510
Beschwerden betroffener Personen	90
Vom Parlament bzw. der Regierung angeforderte Beratung	Ca. 50
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	2013 wurden insgesamt 1 638 neue Fälle registriert
Prüfmaßnahmen	
Prüfungen, Untersuchungen	0 (aufgrund äußerst eingeschränkter Ressourcen durch finanzielle Kürzungen)
Sanktionsmaßnahmen	
Sanktionen	Mit Ausnahme der verhängten Geldbußen in Form von Tagessätzen für jeden Tag, an dem die Forderungen der Datenschutzbehörde nicht erfüllt werden, hat die Datenschutzbehörde keine Sanktionsbefugnisse.
Geldbußen	2013 wurden keine Geldbußen in Form von Tagessätzen verhängt.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	k. A.

B. Rechtsprechung

Im Mai 2013 bearbeitete die isländische Datenschutzbehörde einen Antrag auf Genehmigung einer Datenverarbeitung, der von DeCode Genetics (*Íslensk erfðagreining*), einem Unternehmen, welches das menschliche Erbgut analysiert und erforscht, und dem nationalen Krankenhaus (*Landspítali*) gestellt wurde. Laut dem Antrag sollte das nationale Krankenhaus große Datenmengen von allen Patienten, die während eines fünfjährigen Zeitraums im Krankenhaus behandelt worden waren, an DeCode Genetics übermitteln. Im Anschluss daran wollte DeCode Genetics die Informationen mit zuvor erfassten Daten (einschließlich Erbgutdaten) von insgesamt 95 085 betroffenen Personen, die an anderen

Forschungsprojekten des Unternehmens teilgenommen hatten, ohne deren Einwilligung verknüpfen. Darüber hinaus sollten die Daten mit Schätzungen, die DeCode anhand des Erbguts von 280 000 Personen, die sich nicht an den Forschungsprojekten des Unternehmens beteiligt hatten, ermittelt hat, ebenfalls ohne deren Einwilligung verknüpft werden. Die Datenschutzbehörde erachtete diese Verarbeitung als derart umfangreich, dass diese nur mit der Einwilligung der betroffenen Personen oder einem verfassungstreuen Gesetz als Rechtsgrundlage durchführbar wäre. Da keine dieser Anforderungen erfüllt wurde, verweigerte die Datenschutzbehörde die Genehmigung. Außerdem ordnete die Datenschutzbehörde die Löschung des geschätzten Erbguts der Nichtteilnehmer der Forschungsprojekte von DeCode Genetics an.

Im August 2013 fasste die isländische Datenschutzbehörde einen Beschluss zu einem Unternehmen namens Já, das 2005 zur Verwaltung des nationalen Telefonregisters und weiterer Informationssysteme und -lösungen gegründet worden war. Já hatte auf seiner Website ein System zum Hochladen von Fotos städtischer Gegenden mit 360-Grad-Ansicht ähnlich dem Dienst Google Street View eingerichtet. Bei der Projektvorstellung betonte Já, dass bei der Verarbeitung niemand persönlich identifizierbar sei. Jàs Version von Street View enthielt jedoch sehr wohl Fotos, auf denen die Gesichter von Personen und die Nummernschilder von Autos deutlich erkennbar waren. Die Datenschutzbehörde erachtete dies als Verstoß gegen das Datenschutzgesetz Nr. 77/2000 und verfügte, dass Já die Fotos anonymisieren solle. Já ließ der Datenschutzbehörde später die Bestätigung zukommen, dass alle Fotos mit identifizierbaren Daten unkenntlich gemacht worden seien.

LIECHTENSTEIN

A. Zusammenfassung der Aktivitäten und Neuerungen

2012 hatte die Datenschutzstelle (DSS) die Bereiche Gesundheit und Soziales, Finanzplatz und Datensicherheit als Schwerpunkte für die kommenden Jahre definiert. Diese Bereiche sind zu einem großen Teil komplex. Dabei gilt es, auch internationale oder europäische Entwicklungen zu verfolgen, damit die Privatsphäre beachtet wird. Insgesamt ist und bleibt das Aufgabengebiet dynamisch und anspruchsvoll. Erste Schritte zur Umsetzung dieser Schwerpunkte konnten 2013 getroffen werden. Die Notwendigkeit der Definition solcher Schwerpunkte ergibt sich aus der Breite der zu bearbeitenden Themen einerseits und der beschränkten Ressourcen der Datenschutzstelle anderseits.

Die Sensibilisierung stellt für die DSS weiterhin die wichtigste Aufgabe dar. Dies stützt sich insbesondere auf eine repräsentative Umfrage der DSS, welche ergeben hatte, dass die Bevölkerung noch wenig über Datenschutz weiß. Infolge des NSA-Skandals hat die DSS spezielle Tipps erstellt und veröffentlicht, wie sich jeder selbst schützen kann. Neben dem schon traditionellen Datenschutztag wurde mit dem Verein Sicheres Liechtenstein eine Podiumsdiskussion zum NSA-Skandal und den möglichen Auswirkungen auf Liechtenstein organisiert. Daneben führte die DSS verschiedene Schulungen durch, bei denen das Thema Datensicherheit und sichere Kommunikation einerseits sowie die Sensibilisierung von Jugendlichen und Lernenden im Umgang mit neuen Medien anderseits im Vordergrund stand.

Das Angebot an Hilfsmitteln für die Bevölkerung und für einzelne Zielgruppen wurde ebenfalls ausgebaut, z. B. mit einer Richtlinie für die Bearbeitung von Personendaten im Arbeitsbereich. Diese Richtlinie erörtert die Rechtslage und deckt den gesamten Bereich von der Bewerbung bis zum Zeugnis ab. Sie geht auf verschiedene Einzelfälle der Praxis ein, zum Beispiel die Nutzung von sozialen Netzwerken oder „Bring your own device“ am Arbeitsplatz. Ebenso wurde zum Beispiel eine Muster-Datenschutzerklärung für Betreiber von Internetseiten oder eine Empfehlung zur Protokollierung erstellt. Diese Hilfsmittel sind auf der Internetseite der DSS verfügbar.[7]

Organisation	Datenschutzstelle
Vorsitz und/oder Gremium	Philipp Mittelberger
Budget	596 000 EUR
Personal	2,3 Recht, 1,0 Technik, 0,8 Administration
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	10 Bewilligungen von Videoüberwachungsanlagen
Meldungen	Insgesamt per Jahresende 308 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	98 Anfragen von Privatpersonen

[7] http://www.llv.li/#/1758/datenschutzstelle

Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	10 Stellungnahmen zu Gesetzesvorhaben
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	669 Anfragen (inkl. Privatpersonen, siehe oben)
Prüfmaßnahmen	
Prüfungen, Untersuchungen	6 Kontrollverfahren abgeschlossen
Sanktionsmaßnahmen	
Sanktionen	k. A.
Geldbußen	k. A.
Datenschutzbeauftragte (DPO)	111 Datenschutzverantwortliche
Zahlenangaben zu DPO	

B. Rechtsprechung

2013 wurde keine Entscheidung der Datenschutzkommission veröffentlicht.

NORWEGEN

A. Zusammenfassung der Aktivitäten und Neuerungen

Strategische Beratung

Für die Datenschutzbehörde ist es strategisch wichtig, in jedem Prozess frühzeitig eine wichtige Rolle zu spielen. Wir freuen uns darüber, dass Regierungsbehörden, Organisationen und Unternehmen uns als wichtigen Ansprechpartner erachten.

Eingebauter Datenschutz

In den vergangenen Jahren haben wir versucht, die Grundsätze des eingebauten Datenschutzes zu fördern. Hierunter können die automatische Löschung von Daten oder automatisierte Prüflösungen fallen. Aus dem Weißbuch „Datenschutz – Ausblicke und Herausforderungen“ des norwegischen Parlaments geht hervor, dass die Grundsätze des eingebauten Datenschutzes bei der Entwicklung von staatlichen IT-Lösungen zur Anwendung kommen sollen. Wir freuen uns über diese Ansicht und beabsichtigen, diese Arbeit auch in Zukunft fortzuführen.

Das Snowden-Jahr

2013 war das Jahr, in dem wir von Edward Snowden erfuhren. Die Datenschutzbehörde hat sich infolge seiner Enthüllungen aktiv an der Debatte beteiligt. Dabei, wie weit Staaten bei der Überwachung ihrer Bürger gehen können, scheinen fast keine Grenzen gesetzt zu sein. Das technische Potenzial ist grenzenlos, und von unserem Standpunkt aus gesehen, war es wichtig darauf hinzuweisen, dass eine Überwachung dieser Art nicht hinnehmbar ist.

Wohlfahrtstechnologie

Wohlfahrtstechnologie war 2013 einer der Schwerpunkte der Datenschutzbehörde und wird dies auch in Zukunft sein. Die neue Gesetzgebung erlaubt den Einsatz von Ortungstechnologie für Demenzkranke und stellt damit eine Schwerpunktverlagerung von Befugnis zur Nutzung von Wohlfahrtstechnologie dar, um zu untersuchen, wie diese Technologien auf bestmögliche Weise genutzt werden können. Einmal mehr können sich die Grundsätze des eingebauten Datenschutzes als nützlich erweisen.

Wohlfahrtstechnologie kann jedoch im Hinblick auf den Schutz der Privatsphäre problematisch sein. Viele der Lösungen von heute ziehen eine Form der Überwachung nach sich. Demnach empfehlen wir den Ausgleich von technologischem Nutzen und Auswirkungen auf den Schutz der Privatsphäre. Wenn die Konsequenzen durch Einwilligung, Informationen, angemessene Sicherheitsmaßnahmen usw. so weit wie möglich reduziert werden, können wir das richtige Gleichgewicht finden.

Veröffentlichung des Berichts „Big Data – Grundsätze der Privatsphäre in Gefahr“

Die Datenschutzbehörde erstellte einen umfangreichen Bericht zu den Herausforderungen von Big Data für den Schutz der Privatsphäre. Der Bericht enthält außerdem Ratschläge zur Nutzung von Big Data und dem gleichzeitigen Schutz der Privatsphäre des Einzelnen. In dem Bericht weist die Datenschutzbehörde auf die folgenden Probleme hin:

- Datennutzung für neue Zwecke
- Datenmaximierung
- Mangel an Transparenz
- Zusammenführung kann sensible Daten bereitstellen
- Das Ende der Anonymität?

- Daten – Determinismus
- Abschreckende Wirkung

Auf Initiative der Datenschutzbehörde erstellte die Berlin Group ein Arbeitspapier zum Thema Big Data. Der Entwurf wurde den Mitgliedern der Berlin Group im September 2013 vorgelegt und sehr gut aufgenommen. Er soll beim nächsten Treffen der Gruppe im Mai 2014 verabschiedet werden.

Organisation	Norwegische Datenschutzbehörde
Vorsitz und/oder Gremium	Bjørn Erik Thon, Vorsitzender
Budget	37 Mio. NOK
Personal	41
Allgemeine Aktivitäten	
Beschlüsse, Stellungnahmen, Empfehlungen	k. A.
Meldungen	8 912 neue Meldungen, insgesamt 15 979 aktive Meldungen
Vorabprüfungen	155
Anträge betroffener Personen	Insgesamt erhielt der Beratungsdienst der norwegischen Datenschutzbehörde 5 032 telefonische Anträge und 2 546 Anträge per E-Mail.
Beschwerden betroffener Personen	k. A.
Vom Parlament bzw. der Regierung angeforderte Beratung	Wir erhielten 134 Aufforderungen zur Kommentierung neuer Gesetzesentwürfe und reichten 52 Kommentare ein.
Sonstige Informationen zu einschlägigen allgemeinen Aktivitäten	
Prüfmaßnahmen	
Prüfungen, Untersuchungen	Arbeitsplatz: 15 Gesundheitswesen: 28 Justiz und Polizei: 5 Öffentlicher Sektor: 15 Schule und Ausbildung: 10 Sonstige: 3 Insgesamt: 76

Sanktionsmaßnahmen	
Sanktionen	7 Geldbußen und kein Zwangsgeld, alle von der Datenschutzbehörde verhängt
Geldbußen	Geldbußen von insgesamt 1 925 000 NOK.
Datenschutzbeauftragte (DPO)	
Zahlenangaben zu DPO	210 DPO, die insgesamt 420 Unternehmen und öffentliche Stellen repräsentieren.

B. Rechtsprechung

Unrechtmäßige Bewertungsaktivitäten durch die Versicherungsgesellschaft Gjensidige

Im Mai 2013 führte die Datenschutzbehörde eine Prüfung der Versicherungsgesellschaft Gjensidige durch. Es sollte überprüft werden, wie die Gesellschaft vor allem bei Ermittlungen zur Aufdeckung von Betrug oder versuchtem Betrug personenbezogene Daten verarbeitet. Die Prüfung brachte stark in die Privatsphäre eingreifende Methoden in Verbindung mit den Ermittlungen ans Licht. Man nutzte verdeckte Beobachtungsmethoden sowie versteckte Audio- und Videoüberwachung, um den Gesundheitszustand betroffener Personen zu überprüfen. Im Rahmen der Prüfung wurden außerdem gravierende Missstände der internen Abläufe des Unternehmens im Umgang mit personenbezogenen Daten im Allgemeinen aufgedeckt. Wir erachteten die Missstände als derart gravierend, dass ein nicht hinzunehmendes Risiko bestand, dass das Unternehmen auch weitere Bestimmungen des Datenschutzgesetzes verletzt. Wir erlegten dem Unternehmen eine Geldbuße in Höhe von 600 000 NRK auf – der höchste Betrag, den die Datenschutzbehörde bislang verhängt hat. Das Unternehmen wurde außerdem dazu verpflichtet, interne Abläufe einzuführen, die mit dem Datenschutzgesetz in Einklang stehen.

C. Sonstige wichtige Informationen

Vorschlag eines neuen Gesetzes über Gesundheitsregister (zur medizinischen Behandlung) und Ärzteblätter (Nebenzweck)

Im Jahr 2013 legten das Gesundheitsministerium und Gesundheitsdienste den Entwurf eines neuen Gesetzes über Gesundheitsdaten sowie eines neuen Gesetzes zu Ärzteblättern vor. Die Datenschutzbehörde unterstützt das Vorhaben, das Gesetz aufzuspalten – eines für behandlungsorientierte Gesundheitsdaten und eines für Gesundheitsdaten zu Verwaltungs- und Forschungszwecken.

Andererseits brachte die Datenschutzbehörde in Bezug auf den Gesetzentwurf schwerwiegende Bedenken im Hinblick auf die Abschwächung des Rechts auf Selbstbestimmung der Patienten zum Ausdruck.

Kapitel Fünf

Mitglieder und Beobachter der Artikel-29-Datenschutzgruppe

MITGLIEDER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2013

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 2 274 48 00 Fax: +32 2 274 48 35 E-Mail: commission@privacycommission.be Website: http://www.privacycommission.be/	Herr Ventsislav Karadjov Kommission für den Schutz personenbezogener Daten (CPDP) (Комисия за защита на личните данни) 2 Prof. Tsvetan Lazarov Blvd. Sofia 1592 Tel.: + 359 2 915 35 31 Fax: + 359 2 915 35 25 E-Mail: kzld@cpdp.bg Website: http://www.cdpd.bg
Dänemark	**Deutschland**
(Temp.) Frau Birgit Kleis 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 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 – FIN – 00521 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 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 Tel.: +356 2328 7100 Fax: +356 2328 7198 E-Mail: joseph.ebejer@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: www.cbpweb.nl 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.dsk.gv.at/

Polen	Portugal
Herr Wojciech Rafał Wiewiórowski Generalinspektor für den Schutz personenbezogener Daten (Generalny Inspektor Ochrony Danych Osobowych) ul. Stawki 2 – PL – 00193 Warschau Tel: +48 22 860 73 12; +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 Ancuța Gianina Opre Nationale Aufsichtsbehörde für den Schutz personenbezogener Daten (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) Gen. Gheorghe Magheru Bld. 28-30, 1st District, RO – Bukarest Tel.: +40 31 805 9211 Fax: +40 31 805 9602 E-Mail: anca.opre@dataprotection.ro international@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 3231 3211 Fax: +421 2 3231 3234 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 Attila Péterfalvi Präsident der Nationalen Behörde für Datenschutz und Informationsfreiheit Szilágyi Erzsébet fasor 22/C H-1125 Budapest Tel.: +36 1 3911 400 E-Mail: ugyfelszolgalat@naih.hu Website: http://www.naih.hu	Herr Christopher Graham Amt des Datenschutzbeauftragten (Information Commissioner's Office) Wycliffe House Water Lane, Wilmslow SK9 5AF GB Tel.: 0303 123 1113 (Lokaltarif) Tel.: +44 1625 545745 (Landestarif) Fax: +44 1625 524510 E-Mail: Nutzen Sie bitte das Kontaktformular auf der Website Website: http://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: Rue Wiertz, 60, BE – 1047 Brüssel Amt: Rue Montoyer, 30, BE – 1000 Brüssel Tel: +32 2 283 1900 Fax: +32 2 283 1950 E-Mail: edps@edps.europa.eu Website: http://www.edps.europa.eu

BEOBACHTER DER ARTIKEL-29-DATENSCHUTZGRUPPE 2013

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	Herr Hörður Helgi Helgason Direktor 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**
Frau Dubravka Dolenc Stellvertretende Direktorin Frau Sanja Silaj Zeman Leiterin der Abteilung für Internationale Zusammenarbeit, 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 sanja.silaj-zeman@azop.hr Website: http://www.azop.hr	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	
Frau Kim Ellertsen Direktorin 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

WO ERHALTE ICH EU-VERÖFFENTLICHUNGEN?

Kostenlose Veröffentlichungen:

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

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

Kostenpflichtige Veröffentlichungen:

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

DS-AA-15-002-DE-N

Amt für Veröffentlichungen

ISBN 978-92-79-52064-8
doi:10.2838/646887