EUROPÄISCHE
KOMMISSION

# 12. Jahresbericht

## der Artikel 29

# Datenschutzgruppe

1830-6462

# 12. Jahresbericht

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

Berichtsjahr 2008

---

Angenommen am 16. Juni 2009

Dieser Bericht wurde von der Artikel 29 Datenschutzgruppe erstellt. Er gibt nicht unbedingt die Überzeugungen und Ansichten der Europäischen Kommission wieder und ist nicht an ihre Weisungen gebunden.

Dieser Bericht ist ebenfalls in englischer und französischer Sprache erhältlich. Er kann auf der Internetseite der Generaldirektion für Justiz, Freiheit und Sicherheit der Europäischen Kommission in der Rubrik „Datenschutz" heruntergeladen werden:
http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

# INHALT

# VORWORT DES VORSITZENDEN DER ARTIKEL 29 DATENSCHUTZGRUPPE

**„Die Freiheit gehört denen, die sie sich erobert haben."** André Malraux

Der vorliegende zwölfte Tätigkeitsbericht zum Datenschutz zieht eine Bilanz der bedeutsamsten Fortschritte, die im Laufe eines überaus ereignis- und herausforderungsreichen Jahres realisiert werden konnten. Zugleich ist dies der erste Bericht, den ich als Vorsitzender der Artikel 29 Datenschutzgruppe und Nachfolger meines geschätzten Kollegen und Freundes Peter Schaar vorlegen darf.

Dieser Bericht ist umso bedeutsamer, da er die bemerkenswerte Arbeit wiedergibt, die von den verschiedenen nationalen Delegationen der Artikel 29 Datenschutzgruppe 2008 geleistet wurde. Er zeigt in der Tat die überaus wirkungsvolle Synergie auf, die die Annahme entscheidender Stellungnahmen zum Schutz der individuellen Freiheiten möglich gemacht hat.

Angesichts neuer, komplexer Problematiken, die mit der außerordentlichen Entwicklung der Informationssysteme einhergehen, ist es unserer Gruppe gelungen, eine eigene Rechtsdoktrin aufzustellen, durch die Synthese der Konzepte, die von verschiedenen nationalen, für den Datenschutz verantwortlichen Behörden geteilt wird. Sie hat gewisse interpretatorische Divergenzen überwinden können und sich auf die gemeinschaftliche Schaffung einer Grundlage von Werten und Grundprinzipien konzentrieren können, die in ihren Augen einen geeigneten Schutz verdienen.

Dabei richtete sich unsere Aufmerksamkeit im Laufe unserer Tätigkeiten 2008 vor allem auf vier strategische Aufgaben.

Eines der zentralen Themen unseres Arbeitsprogramms ist der Schutz personenbezogener Daten von Kindern. Die diesbezügliche Besorgnis resultiert vor allem aus der Entwicklung sozialer Netzwerke im Internet und aus den neuen Verhaltensweisen, zu denen sie verleiten. Die spezifische Situation des Kindes, seine Verletzlichkeit und die Tatsache, dass es sich noch in der Entwicklung befindet, machte eine Kräftebündelung unserer Gruppe in diesen Fragen erforderlich und brachte passende Lösungen hervor.

Das Ergebnis ist die Annahme der Stellungnahme WT147 vom Februar 2008. So hat unsere Gruppe eine strukturierte Synthese der Sorgen bezüglich des Schutzes personenbezogener Daten von Kindern präsentiert und auf der Definition von diesbezüglich anwendbaren Grundprinzipien beharrt. Die konkrete Umsetzung dieser Grundprinzipien im Schulkontext wurde präzise dargelegt. Dieses Thema ist damit jedoch noch nicht erschöpft und es werden notwendigerweise noch andere Entwicklungen folgen. Im Augenblick stellen die bereits realisierten Fortschritte unserer Gruppe eine gemeinschaftliche Errungenschaft dar, die für die zukünftige Arbeit wesentlich ist.

Ein weiteres zentrales Thema sind Suchmaschinen. In unserer heutigen Informationsgesellschaft sind Anbieter von Suchmaschinen aus dem Alltag der Internetnutzer nicht mehr wegzudenken. Darum spielen sie eine entscheidende Vermittlerrolle beim ungehinderten Zugriff auf Informationen.

Indessen haben die erheblichen Massen von Nutzerdaten, die diese jeden Tag sammeln, verarbeiten und speichern, einen Einfluss auf den Schutz personenbezogener Daten der Nutzer, der nicht vernachlässigt werden darf. Demzufolge drängten sich eine gemeinsame Reflexion sowie auch die Schaffung eines präzisen Rahmens für diese Praktiken auf.

So ist es unserer Gruppe gelungen, mit ihrer gemeinschaftlichen Stellungnahme WT 158 vom April 2008 Regeln zu definieren, die ein Gleichgewicht zwischen den vorhandenen rechtmäßigen Interessen schaffen. Diese Stellungnahme

bot die Gelegenheit, einen Aktionsrahmen für Anbieter von Suchmaschinen, deren Verpflichtungen künftig deutlich definiert sind, zu schaffen. Sie ermöglichte es außerdem, nochmals auf das Zugangs- oder Berichtigungsrecht von Benutzern hinzuweisen.

Die angenommene Stellungnahme stellt einen entscheidenden Fortschritt im Bezug auf die Achtung der Privatsphäre von Nutzern dar. Dies ist umso bedeutungsvoller, da Anbieter von Suchmaschinen wie Google die in der Stellungnahme enthaltenen Empfehlungen bereits umgesetzt haben.

Die Arbeiten bezüglich der Übermittlung von personenbezogenen Daten aus der Europäischen Union an Filialen in der ganzen Welt wurden ebenfalls von unserer Gruppe fortgesetzt. Sie hat sich mit der Aufgabe befasst, die Klarheit der vorhandenen Werkzeuge zu optimieren. Dazu wurde ein Rahmenwerk der verbindlichen unternehmensinternen Datenschutzregelungen (BCR) aufgestellt, mit dem Ziel, deren Einhaltung für multinationale Unternehmen zu vereinfachen.

Im Bereich Informationen über Fluggäste bzw. im Rahmen der Übermittlung von Fluggastdatensätzen (Personal Name Records – PNR) an amerikanische Behörden, haben wir uns dafür eingesetzt, Musterinformationsblätter auszuarbeiten, die der Realität des Lufttransportsektors entsprechen. Das Ziel, das wir damit verfolgten, war die Aktualisierung der vorhandenen Werkzeuge und die Vereinfachung der Aufgaben der Reisebüros, der Luftfahrtgesellschaften, oder allen Organisationen, die Reisedienstleistungen an Passagiere bei Flügen in die und aus den Vereinigten Staaten erbringen.

Diese verschiedenen Arbeitsschwerpunkte und die Antworten, die gefunden werden konnten, illustrieren in vielfältiger Weise unser resolutes Engagement im Dienst des personenbezogenen Datenschutzes. Die gegenwärtige Tendenz der Einmischung in die Privatsphäre der europäischen Bürger stellt eine reelle Bedrohung dar und erfordert eindeutige und stabile Antworten sowie die Definition von unantastbaren Grenzen.

**Alex Türk**

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

[1] Alle von der Artikel 29 Datenschutzgruppe angenommenen Dokumente können von folgender Website abgerufen werden: http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_de.htm

## 1.1. TRANSFER VON DATEN IN DRITTLÄNDER

### 1.1.1. Passagierdaten/PNR

**Stellungnahme 2/2007 (WP 151) zur Information von Fluggästen über die Übermittlung von PNR-Daten an amerikanische Behörden, angenommen am 15. Februar 2007 und überarbeitet am 24. Juni 2008**

Diese Stellungnahme und die Anhänge dazu (häufig gestellte Fragen und Musterinformationsblatt) sind für Reisebüros, Fluggesellschaften und sonstige Organisationen bestimmt, die Fluggästen Reisedienste für Flüge in die und aus den Vereinigten Staaten anbieten. Die Stellungnahme und die Anhänge ändern und ersetzen die Stellungnahme vom 30. September 2004 (WP97). Die Übermittlung von PNR-Daten an amerikanische Behörden ist durch das Abkommen vom Juli 2007 geregelt. Reisebüros, Fluggesellschaften und andere Organisationen müssen weiterhin die Fluggäste über die Verarbeitung ihrer personenbezogenen Daten informieren. Diese Stellungnahme soll beraten und darüber informieren, wer welche Informationen wie und wann vorzulegen hat. Die Informationen sind den Fluggästen beim Kauf eines Flugscheins und bei der Bestätigung des Flugs vorzulegen. Die Stellungnahme enthält Ratschläge dazu, wie die Informationen über Telefon, im persönlichen Gespräch und über das Internet zu erteilen sind.

Die Artikel 29 Datenschutzgruppe hat Musterinformationsblätter ausgearbeitet (Anhänge zu dieser Stellungnahme), um es den Organisationen und Agenturen zu erleichtern, ihrer Informationspflicht nachzukommen, und um sicherzustellen, dass in der gesamten Europäischen Union einheitlich informiert wird. Das kurze und das noch kürzere Informationsblatt enthalten Hinweise für Fluggäste auf die Übermittlung von Daten an die US-Behörden und dazu, wie sie weitere Informationen erhalten können. Das längere Informationsblatt enthält häufig gestellte Fragen und ausführlichere Informationen über die Datenverarbeitung. Zunächst werden Fluggastdaten allgemein, dann speziell die PNR-Daten erklärt. Auch sind Links zum derzeit gültigen Abkommen und anderen einschlägigen Dokumenten enthalten.

### 1.1.2. Welt-Anti-Doping-Agentur (WADA)

**Stellungnahme 3/2008 (WP 156) zum Entwurf eines Internationalen Datenschutzstandards zum Welt-Anti-Doping-Code**

Die Generaldirektion Bildung und Kultur (GD EAC) der Europäischen Kommission hat die Artikel 29 Datenschutzgruppe um eine Stellungnahme zum Entwurf eines von der Welt-Anti-Doping-Agentur (WADA) erarbeiteten Internationalen Datenschutzstandards ersucht. Der Entwurf des Standards ist in Verbindung mit dem Welt-Anti-Doping-Code der WADA, im Besonderen mit Artikel 14, zu sehen. Nach dem Code sind die Athleten verpflichtet, den Anti-Doping-Organisationen regelmäßig bestimmte Daten zu übermitteln. Diese Daten werden anschließend zusammen mit anderen Daten (darunter auch sensible Daten) in der in Kanada geführten Datenbank ADAMS gespeichert. Entsprechend den im Code festgelegten Verpflichtungen werden auch Daten verarbeitet, die ihre Betreuer sowie andere Personenkategorien betreffen. In ihrer Stellungnahme führte die Artikel 29 Datenschutzgruppe aus, dass die Bestimmungen des Codes Fragen der Vereinbarkeit mit europäischen Datenschutzstandards aufwerfen. Bezüglich der Internationalen Standards der WADA befasste sich die Artikel 29 Datenschutzgruppe mit mehreren Problemen hinsichtlich der Qualität der Verarbeitung der einschlägigen Daten, der Zustimmung der betroffenen Personen, der bei ihnen erhobenen Daten, der Offenlegung personenbezogener Daten an Dritte, der Gewährleistung der Sicherheit und der Rechte der betroffenen Personen.

### 1.1.3. Verbindliche unternehmensinterne Vorschriften (BCR)

**Arbeitsdokument (WP153) mit einer Übersicht über die Bestandteile und Grundsätze verbindlicher unternehmensinterner Datenschutzregelungen (BCR)**

Von der Artikel 29 Datenschutzgruppe wurde eine Übersicht erstellt, um Unternehmensgruppen, die Daten an ihre Mitglieder außerhalb der EU übermitteln, die

Anwendung ihrer verbindlichen unternehmensinternen Datenschutzregelungen (Binding Corporate Rules – BCR) zu erleichtern:

- In der Übersicht ist aufgeführt, was in den BCR nach Maßgabe der Arbeitsdokumente WP 74[2] und WP 108[3] geregelt werden muss.
- Es wird genau angegeben, welche Bestimmungen in die BCR aufzunehmen sind und welche Angaben das Antragsformular für die Genehmigung der BCR enthalten muss (Arbeitsdokument WP 133[4]).
- Zum besseren Verständnis wird grundsätzlich auf die entsprechenden Textstellen in den Arbeitsdokumenten WP 74[5] und WP 108[6] verwiesen.
- Jeder Grundsatz wird gesondert erläutert bzw. kommentiert.

### Arbeitsdokument (WP 154) „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (BCR)"

Innerhalb einer Unternehmensgruppe dürfen personenbezogene Daten auf der Grundlage verbindlicher unternehmensinterner Datenschutzregelungen (Binding Corporate Rules – BCR) aus der EU in Drittländer übermittelt werden. Die Datenschutzgruppe hat in ihren Arbeitsdokumenten WP 74[7] und WP 108[8] Überlegungen zu den wesentlichen Bestandteilen solcher Regelungen angestellt.

Um Unternehmen bei der Ausarbeitung eigener BCR Hilfestellung zu leisten, hat die Gruppe einen Rahmen ausgearbeitet, der zeigen soll, wie eine verbindliche unternehmensinterne Datenschutzregelung mit allen notwendigen Bestandteilen, die in den Arbeitsdokumenten WP 74[9] und WP 108[10] vorgestellt wurden, aussehen könnte.

### Arbeitsdokument (WP 155) zu „Häufig gestellten Fragen" über verbindliche unternehmensinterne Datenschutzregelungen (BCR)

Verbindliche unternehmensinterne Datenschutzregelungen (BCR) stellen nach Auffassung der Artikel 29 -Datenschutzgruppe, wie in Arbeitsdokument WP 74[11] erläutert, eine geeignete Lösung für multinationale Konzerne und ähnliche Unternehmensgruppen dar, um ihren rechtlichen Verpflichtungen nachzukommen und bei der Übermittlung personenbezogener Daten in Länder außerhalb der Europäischen Union ein angemessenes Datenschutzniveau zu gewährleisten.

Die Gruppe/Datenschutzbehörden haben anhand ihrer Erfahrungen mit den Anträgen auf Genehmigung unternehmensinterner Datenschutzregelungen und den Anfragen zur Auslegung der Arbeitsdokumente WP 74[12] und WP 108[13] eine Liste häufig gestellter Fragen zusammengestellt. Anhand dieser Fragen sollen sich die Antragsteller ein klareres Bild von den Anforderungen machen können, so dass sie die Genehmigungsvoraussetzungen für ihre BCR leichter erfüllen können. Die Liste der häufig gestellten Fragen wird bei Bedarf aktualisiert.

[2] Arbeitsdokument WP 74: „Übermittlung personenbezogener Daten in Drittländer: Anwendung von Artikel 26 Absatz 2 der EU-Datenschutzrichtlinie auf verbindliche unternehmensinterne Vorschriften für den internationalen Datentransfer", angenommen am 3. Juni 2003. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_de.htm

[3] Arbeitsdokument WP 108: „Einführung eines Prüfungskatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften", angenommen am 14. April 2005. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_de.htm

[4] Arbeitsdokument WP 133: Empfehlung 1/2007 über das Antragsformular für die Genehmigung von verbindlichen unternehmensinternen Datenschutzregelungen zur Übermittlung personenbezogener Daten. http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_de.htm (nur EN)

[5] Vgl. Fußnote 2.

[6] Vgl. Fußnote 3.

[7] Vgl. Fußnote 2.

[8] Vgl. Fußnote 3.

[9] Vgl. Fußnote 2.

[10] Vgl. Fußnote 3.

[11] Vgl. Fußnote 2.

[12] Vgl. Fußnote 2.

[13] Vgl. Fußnote 3.

## 1.2. ELEKTRONISCHE KOMMUNIKATION, INTERNET UND NEUE TECHNOLOGIEN

### Stellungnahme 1/2008 (WP 148) zu Datenschutzfragen im Zusammenhang mit Suchmaschinen

Suchmaschinen sind zu einem festen Bestandteil des Alltags der Menschen geworden, die das Internet und Technologien zur Informationsgewinnung nutzen. In der vorliegenden Stellungnahme ist sich die Arbeitsgruppe der Nützlichkeit der Suchmaschinen bewusst und erkennt ihre Bedeutung an. Sie benennt klare Verantwortlichkeiten im Rahmen der Datenschutzrichtlinie (95/46/EG) für Suchmaschinenbetreiber in ihrer Rolle als Verantwortliche für die Verarbeitung von Benutzerdaten. In bestimmten Situationen ist das europäische Datenschutzrecht auch auf Suchmaschinen anwendbar, wenn sie als Anbieter von Inhaltsdaten (d. h. Index der Suchergebnisse) fungieren, z. B. wenn sie einen Caching-Dienst anbieten oder sich auf die Erstellung von Personenprofilen spezialisieren. Vorrangiges Ziel dieser Stellungnahme ist es, ein Gleichgewicht zwischen den berechtigten geschäftlichen Erfordernissen der Suchmaschinenbetreiber und dem Schutz der personenbezogenen Daten von Internet-Benutzern herzustellen. Diese Stellungnahme befasst sich mit der Definition von Suchmaschinen, den Arten der bei der Bereitstellung von Suchdiensten verarbeiteten Daten, dem Rechtsrahmen, den Zwecken/Gründen für eine zulässige Verarbeitung, der Verpflichtung zur Information der betroffenen Personen und den Rechten der betroffenen Personen.

Eine wichtige Schlussfolgerung dieser Stellungnahme besteht darin, dass die Datenschutzrichtlinie grundsätzlich auf die Verarbeitung personenbezogener Daten durch Suchmaschinen anwendbar ist, auch wenn sich deren Hauptsitz außerhalb des EWR befindet, und dass es unter diesen Umständen Sache der Suchmaschinenbetreiber ist, ihre Rolle im EWR und den Umfang ihrer Verantwortlichkeiten im Rahmen der Richtlinie zu klären. Des Weiteren wird klargestellt, dass die Richtlinie über die Vorratsspeicherung von Daten (2006/24/EG) eindeutig nicht auf Suchmaschinenbetreiber anwendbar ist. Die vorliegende Stellungnahme kommt zu dem Ergebnis, dass personenbezogene Daten nur für rechtmäßige Zwecke verarbeitet werden dürfen. Die Suchmaschinenbetreiber müssen personenbezogene Daten löschen oder irreversibel anonymisieren, sobald sie der angegebenen rechtmäßigen Zweckbestimmung nicht mehr dienen, und sie müssen in der Lage sein, die Speicherung und die Lebensdauer der gesetzten Cookies jederzeit zu begründen. Bei allen geplanten Querverbindungen von Benutzerdaten und bei der Anreicherung von Benutzerprofilen muss die Einwilligung des Benutzers eingeholt werden. Die Suchmaschinenbetreiber müssen Nichtbeteiligungsklauseln („Opt-outs") von Website-Herausgebern beachten und den Aufforderungen von Benutzern zur Aktualisierung oder Auffrischung ihrer Cache-Speicher unverzüglich nachkommen. Die Arbeitsgruppe erinnert in diesem Zusammenhang an die Verpflichtung der Suchmaschinenbetreiber, die Benutzer im Vorhinein über alle beabsichtigten Verwendungszwecke ihrer Daten zu informieren und ihre Rechte auf Auskunft, Einsichtnahme oder Berichtigung ihrer personenbezogenen Daten gemäß Artikel 12 der Datenschutzrichtlinie (95/46/EG) zu respektieren.

### Stellungnahme 2/2008 (WP 150) zur Überprüfung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

Am 13. November 2007 nahm die Kommission den Vorschlag für eine Richtlinie zur Änderung u. a. der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation an. Hauptanliegen des Vorschlags ist ein verbesserter Schutz personenbezogener Daten und der Privatsphäre natürlicher Personen in der elektronischen Kommunikation, insbesondere durch strengere Sicherheitsbestimmungen und bessere Durchsetzungsmechanismen. Die Artikel 29 Datenschutzgruppe gibt eine Stellungnahme zum Vorschlag ab und weist auf einige zusätzliche Aspekte hin.

Diese betreffen hauptsächlich die Meldung von Sicherheitsverletzungen, das Konzept der „personenbezogenen Daten", das Konzept des

„öffentlichen Kommunikationsnetzes" und der „elektronischen Kommunikationsdienste", die nationalen Regulierungsbehörden und unerbetene Werbung.

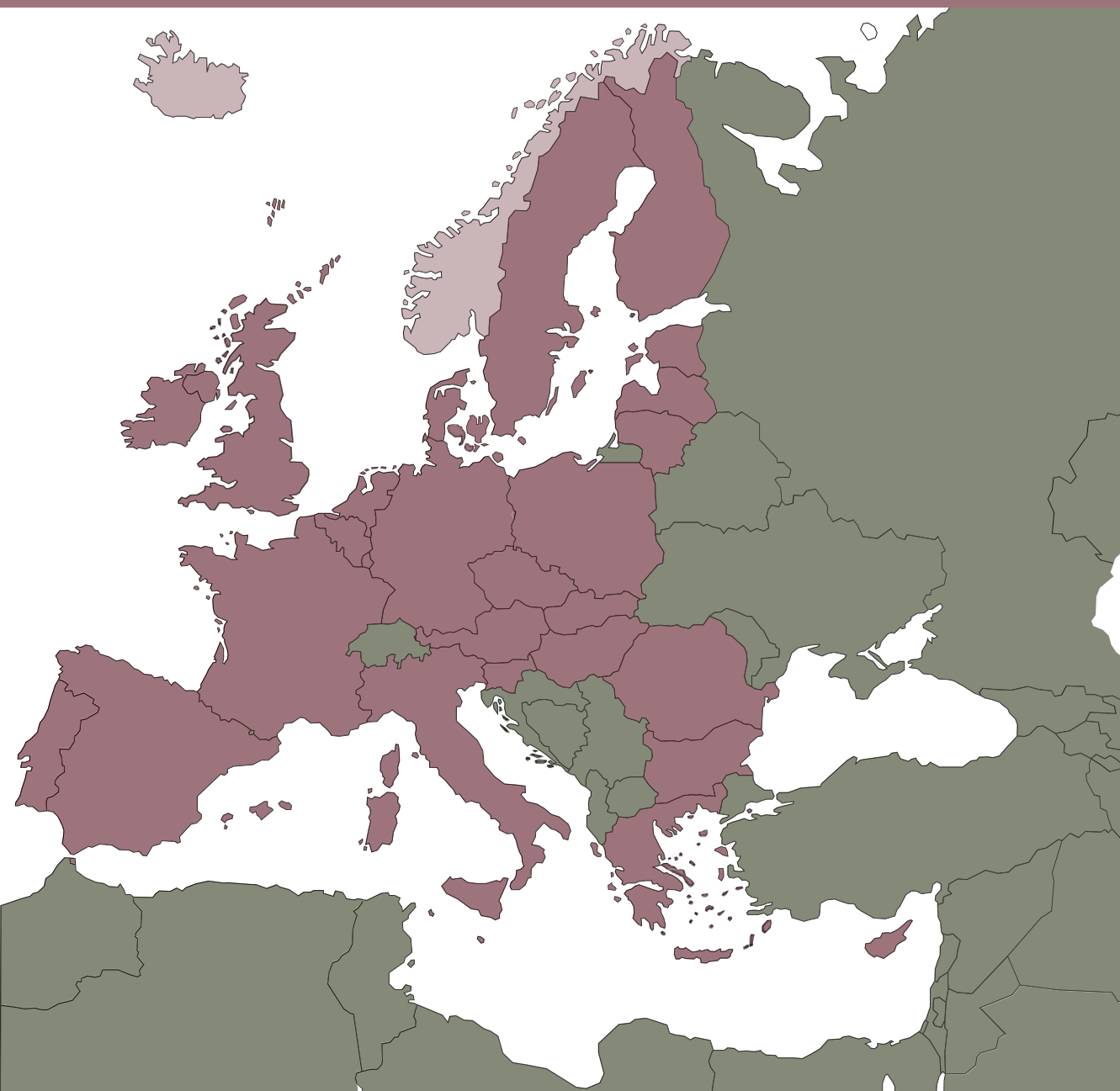
## 1.3. PERSONENBEZOGENE DATEN

### Arbeitspapier 1/2008 (WP147) zum Schutz der personenbezogenen Daten von Kindern (Allgemeine Leitlinien und Anwendungsfall Schulen)

Gegenstand der vorliegenden Stellungnahme ist der Schutz der Daten von Kindern. Die Stellungnahme richtet sich hauptsächlich an Zielgruppen, die personenbezogene Daten von Kindern verarbeiten. Im schulischen Kontext sind dies vor allem Lehrer und Schulbehörden. Außerdem wendet sich die Stellungnahme an die nationalen Kontrollstellen für den Datenschutz, die für die Überwachung der Verarbeitung derartiger Daten zuständig sind.

Die Artikel 29 Datenschutzgruppe hat bereits mehrere Stellungnahmen zu diesem Thema angenommen, und insofern ist das Thema für sie nicht neu. Einige Grundsätze oder Empfehlungen in Bezug auf den Schutz der personenbezogenen Daten von Kindern finden sich in ihren Stellungnahmen zum Verhaltenskodex von FEDMA (Stellungnahme 3/2003), zur Nutzung von Standortdaten (Stellungnahme 5/2005) sowie zu Visumanträgen und biometrischen Identifikatoren (Stellungnahme 3/2007). Ziel des Arbeitspapiers ist es, das Thema in strukturierter Form zusammenzufassen, die maßgeblichen Grundsätze zu definieren und sie am Beispiel von Schuldaten zu veranschaulichen. Der Bereich der Schuldaten wurde gewählt, weil er zu den wichtigen Bereichen im Leben eines Kindes gehört und in seinem Alltag einen breiten Raum einnimmt. Auch der sensible Charakter vieler Daten, die in Bildungseinrichtungen verarbeitet werden, trägt zur Bedeutung dieses Bereichs bei.

# Kapitel 2
# Die wichtigsten Entwicklungen in den Mitgliedstaaten



# Österreich

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

Für 2008 war ein Projekt zu den Änderungen des **österreichischen Datenschutzgesetzes** 2000 geplant. Anfang 2008 wurde ein Entwurf verbreitet und es wurden Stellungnahmen eingeholt[14]. Die Wahlen im Herbst 2008 beendeten das Projekt jedoch, das noch nicht wieder in den Gesetzgebungsprozess eingebracht wurde. Der Entwurf befasste sich unter anderem mit folgenden Themen:

- Das aktuelle Datenschutzgesetz 2000 im Hinblick auf **juristische Personen oder Gruppen natürlicher Personen als Datensubjekte**. Der Entwurf würde den Schutz natürlicher Personen beschränken. Dieser Vorschlag erzeugt gemischte Reaktionen. Die österreichische Anwaltskammer bemerkte, dass viele Unternehmen zum Schutz ihrer Interessen das Recht auf Zugang sowie das Recht auf Berichtigung und Löschung von Daten ebenso benötigten wie natürliche Personen und dass sie keine anderen rechtlichen Alternativen hätten.
- Der Entwurf sieht die Einsetzung eines **Datenschutzbeauftragten** für (größere) Unternehmen vor.
- Der Entwurf umfasst wesentliche Änderungen im Hinblick auf die **Meldungen**. Es war geplant, dass alle Meldungen online über ein neues, ausschließlich elektronisches Meldesystem erfolgen sollten. Um die Meldeverfahren zu beschleunigen, würden Prüfungen von Meldungen auf Vorabkontrollen beschränkt.
- Eine komplett neue Verordnung sollte sich mit dem Thema **Videoüberwachung** befassen. Die Datenschutzkommission hat so viele Beschwerden und Meldungen erhalten, dass eine gesetzliche Regelung durch eine detailliertere Verordnung zum Thema Videoüberwachung (insbesondere Videoüberwachung durch Privatpersonen) notwendig erscheint.

Die **Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten** wurde 2008 nicht umgesetzt. Nach der Verkündung des Urteils zur rechtlichen Grundlage für die Richtlinie über die Vorratsspeicherung von Daten durch die Europäische Kommission wurden neue Bemühungen zur Umsetzung unternommen.

[14] Der Entwurf sowie alle Stellungnahmen sind auf der Website des österreichischen Parlaments abrufbar.
http://www.parlament.gv.at/PG/DE/XXIII/ME/ME_00182/pmh.shtml

## B. Bedeutende Rechtsprechung

Das Urteil im ersten „**Informanten**"-Fall wurde Ende 2008 gesprochen. Die Datenschutzkommission entschied – nach langen Diskussionen –, dass die österreichische Niederlassung die von einer US-amerikanischen Muttergesellschaft übertragenen Daten über ein Informanten-System kontrollieren sollte. Diese rechtliche Ansicht wurde aus folgenden Gründen angenommen:

Die Angestellten der österreichischen Niederlassung wurden von ihrem Arbeitgeber in ihrem Arbeitsvertrag verpflichtet, einen bestimmten Verhaltenskodex einzuhalten (dieser Kodex war für alle Angestellten aller Unternehmen innerhalb des Konzerns bindend). Der Kodex umfasst – neben zahlreichen anderen Pflichten – die Verpflichtung, dass Angestellte Bericht über bestimmte unethische oder gar illegale Situationen erstatten müssen, wenn sie von solchen Situationen Kenntnis erhalten. Als eine Möglichkeit zur Berichterstattung über solche Situationen wurde die Nutzung der Informanten-Hotline genannt. Ein Angestellter, der über diese Informanten-Hotline Bericht erstattet, befolgt somit allgemeine Anweisungen seines Arbeitgebers – er handelt als Angestellter der österreichischen Niederlassung und nicht als Privatperson. Datenübertragungen durch Angestellte sind dem Arbeitgeber als Kontrolleur zuzuschreiben, insbesondere dann, wenn sie vom Arbeitgeber in Auftrag gegeben wurden (Fallnummer K178.274/0010-DSK/2008).

Mehr zur Rechtsprechung zum Thema **Videoüberwachung** siehe „Wichtige spezifische Themen".

## C. Wichtige spezifische Themen

### Videoüberwachung

Der Bereich Videoüberwachung war sowohl in Form von Beschwerden gegen Videoüberwachung als auch in Form von Meldungen ein wichtiges Thema.

Ein Beschluss über das Recht auf Zugang zu einer nicht verwerteten Videoüberwachungsdatei könnte von allgemeinem Interesse sein:

Ein Bürger beantragte den Zugang zur Videodatei einer öffentlichen Verkehrsbehörde. Die Videodaten werden in diesem System nach 48 Stunden gelöscht, sofern keine Überfälle oder Fälle von Vandalismus aufgezeichnet wurden. Dem Bürger wurde der Zugang vom Kontrolleur (Verkehrsbehörde) verweigert.

Die Beschwerde des Bürgers bei der Datenschutzkommission wurde aus folgenden Gründen abgewiesen: Um Zugang zu Videoüberwachungsdaten zu gewähren, wäre eine Untersuchung der Datenaufzeichnungen erforderlich gewesen, die andernfalls nach 48 Stunden ohne Untersuchung gelöscht worden wären. Darüber hinaus hätte die zur Beantwortung der Frage, ob das Bild des Beschwerdeführers auf der Aufzeichnung zu sehen ist, erforderliche Untersuchung Daten über alle anderen Personen auf der Aufzeichnung offen gelegt, die andernfalls geheim gehalten und nach 48 Stunden gelöscht worden wären.

In Anbetracht der Tatsache, dass Videoüberwachungsdateien in Österreich nur dann verwertet werden dürfen, wenn sie einen Tatbestand zeigen, für den die Überwachung genehmigt wurde (z. B. Vandalismus), wurde entschieden, dass der Zugang zu nicht verwerteten Dateien nicht gewährt werden soll, wenn die Daten der entsprechenden Datei nach einer sehr kurzen Aufbewahrungszeit (z. B. 48 Stunden) gelöscht werden und wenn es sehr wahrscheinlich ist, dass andere Personen auf der Aufzeichnung zu sehen sind und die Gewährung des Zugangs für eine Person somit die Datenschutzrechte zahlreicher anderer Personen verletzen würde (Fallnummer K121.385/0007-DSK).

Zwei Meldungen betrafen die Videoüberwachung in Schulen. Die Datenschutzkommission ließ Videoüberwachung als Mittel zur Sicherung der Ordnung in den Schulgebäuden nicht zu (da diese erzieherische Aufgabe vom Lehrpersonal zu erledigen sei), gestattete jedoch Videokameras in einigen Bereichen außerhalb des Schulgebäudes als Mittel zur Sicherung von Eigentum, z. B. zur Verhinderung von Fahrraddiebstählen (Fallnummern K600.054-001/0002-DVR/2008 und K600.055-001/0002-DVR/2008).

**Kreditmeldungen**

Bei der Datenschutzkommission gehen noch immer zahlreiche Beschwerden über Evidenzzentralen ein.

**Private Krankenversicherung**

Die österreichische Datenschutzkommission startete 2008 eine Prüfung des privaten Krankenversicherungssektors. Die erforderlichen Empfehlungen werden in Kürze veröffentlicht.

# Belgien

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

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

## B. Bedeutende Rechtsprechung

Es gibt unserer Meinung nach keine besonders relevanten gerichtlichen Entscheidungen, die hier zu erwähnen wären, mit Ausnahme des vom obersten Verwaltungsgericht geäußerten Standpunktes, gemäß welchem: in Anwendung des Artikels 7 § 3 des *Privatsphäre-Gesetzes* (Gesetz vom 8. Dezember 1992 zum Schutz der Privatsphäre bei der Verarbeitung personenbezogener Daten)[15] jeglicher Entwurf eines königlichen Erlasses im Bezug auf die Verarbeitung von gesundheitsbezogenen Daten im Ministerrat erörtert und der Stellungnahme der Kommission zum Schutz der Privatsphäre (hiernach genannt die „belgische Kommission" oder die CPVP) unterbreitet werden muss (sektoraler Ausschuss Sozialversicherung und Gesundheit – Stellungnahme 09/2008 vom 27. Februar 2008).

## C Wichtige spezifische Themen[16]

**Verarbeitung sensibler Daten**

***Gesundheitsbezogene Daten – E-Health-Plattform (sektoraler Ausschuss Sozialversicherung und Gesundheit – Stellungnahme 14/2008)***

Innerhalb der Bank Carrefour de la sécurité sociale wurde eine neue öffentliche Institution mit der Rechtsperson namens „Plate–forme e-health" ins Leben gerufen. Vornehmliches Ziel dieses Forums ist es, eine Infrastruktur sowie Basisdienste zum Austausch gesundheitsbezogener Daten zwischen den verschiedenen Beteiligten des Gesundheitssektors zu bieten und als Vermittlerorganisation aufzutreten, die mit der Erfassung und Verschlüsselung von Daten zu geschichtlichen, statistischen und wissenschaftlichen Zwecken beauftragt ist. Die nationale Registernummer (eindeutiges Kennzeichen) und die Sozialversicherungsnummer (aus Ersterer abgeleitet) dienen als Identifikatoren innerhalb der Plattform. Diese speichert im Übrigen ein Verzeichnis der Referenzen, das festhält, sofern der Patient einwilligt, welche personenbezogenen Daten bei welchen Gesundheitsdienststellen über ihn aufgenommen werden. Das Verzeichnis soll Datenanfragen an die Stellen weiterleiten, an denen diese Daten verfügbar sind, und eine wirksame, präventive Kontrolle bieten.

Die Kommission urteilte, dass eine derartige dezentralisierte Plattform, die sich auf die Weitergabe personenbezogener Daten beschränkt, diese jedoch nicht aufbewahrt (mit Ausnahme solcher Daten, die im Referenzverzeichnis enthalten sind), eine zufriedenstellende Wahrung der Privatsphäre der Patienten darstellt und den Empfehlungen der Artikel 29 Datenschutzgruppe entspricht (*Arbeitsdokument 131 über die Verarbeitung personenbezogener Gesundheitsdaten in elektronischen Krankenakten*).

In Bezug auf die Nutzung der nationalen Registernummer als Identifikator innerhalb der Plattform hat die belgische Kommission auf ihre allgemeine Rechtsprechung, die den Gebrauch von sektoralen Kennnummern befürwortet, hingewiesen. Sie hat sich jedoch nicht dem Gebrauch im vorliegenden Fall entgegengestellt. Auf weitere Fragen bezüglich des Gebrauches der nationalen Registernummer, die, wenngleich nicht als sensible Information eingestuft, dennoch nicht weniger Garantien bei ihrer Nutzung erfordert, gehen wir später ein. (Artikel 8 § 7 der Richtlinie 95/46/EG).

***Personenbezogene Daten von verurteilten Personen (Stellungnahme 28/2008)***

Angesichts der steigenden Anzahl von Fragen in Bezug auf verurteilte Personen im Rahmen der parlamentarischen Kontrolle und vonseiten der Presse hat der Justizminister die belgische Kommission zu der heiklen Frage des Bezuges zwischen der Wahrung der Privatsphäre und des Informationsrechtes befragt. Das Auskunftsrecht impliziert für jeden Parlamentarier das Recht, dem Minister mündliche oder schriftliche Fragen zu stellen. In Übereinstimmung mit den Vorschriften des

[15] Der König bestimmt mittels eines im Ministerrat ausgearbeiteten Erlasses und gemäß der Stellungnahme der belgischen Kommission die besonderen Bedingungen, denen die Verarbeitung personenbezogener Daten entsprechen muss.

[16] Alle Stellungnahmen, Genehmigungen und andere in diesem Beitrag genannten Dokumente können auf der Website der belgischen Kommission unter folgender Adresse eingesehen werden: http://www.privacycommission.be

Parlamentes sind alle Fragen, die einen persönlichen Fall betreffen, prinzipiell unzulässig. Ausgehend von der Stellungnahme der belgischen Kommission könnte sich der Minister folglich auf diese Anordnungen berufen und die Antwort auf eine Frage bezüglich der Daten einer verurteilten Person verweigern. Er könnte sich jedoch auch auf das in der Verfassung verankerte Auskunftsrecht berufen, um dem Fragesteller zu antworten. Gemäß dem Privatsphäre-Gesetz ist die Verarbeitung juristischer Daten prinzipiell verboten. Es wird jedoch eine Ausnahme vorgesehen für Verarbeitungen, die unter der Aufsicht einer öffentlichen Behörde stattfinden, wenn diese Verarbeitung für die Ausführung ihrer Aufgaben als *nötig* erachtet wird. Die belgische Kommission vertritt die Ansicht, dass diese Ausnahme sich auf die Verarbeitung gerichtlicher Daten durch den Minister bezieht. Die Beurteilung der Notwendigkeit dieser Verarbeitung geschieht abhängig von den Umständen und die belgische Kommission gibt an, zu diesem Punkt keine allgemeinen Aussagen machen zu können. Das Verbot der Verarbeitung gerichtlicher Daten gilt ebenfalls nicht für die Verarbeitung personenbezogener Daten zu ausschließlich journalistischen Zwecken, wenn diese Verarbeitung Daten betrifft, die bekanntermaßen von der betroffenen Person veröffentlicht werden oder in direktem Zusammenhang mit dem offiziellen Charakter der Person oder den Umständen, in die diese verwickelt ist, stehen. Auch hier schließt die Kommission, dass alles von den Umständen abhängig ist und beschränkt sich auf die Formulierung einiger Richtlinien. Sie weist ebenfalls auf die verfassungsrechtliche Anordnung, die besagt, dass ein Urteil öffentlich ausgesprochen wird. Ist die Presse bei der Urteilssprechung zugegen, hat sie die Möglichkeit, davon Kenntnis zu nehmen. Hinsichtlich dessen urteilt die belgische Kommission, dass es erst der Magistratur zukommt, den Gehalt eines Urteils mitzuteilen und dieses durch den Pressemagistrat. Schließlich verdeutlicht die belgische Kommission, dass der Minister, wenn ein persönlicher Fall gesetzgebungstechnische, strategische oder strukturelle Fragen aufwirft, Daten zum besseren Verständnis des Problems bekannt geben kann. Er muss jedoch von Fall zu Fall entscheiden, ob eine Frage aus dem individuellen Rahmen fällt. Ist dies nicht der Fall, ist die belgische Kommission der Ansicht, dass eine gewisse Zurückhaltung unerlässlich ist.

***Verarbeitung sensibler Daten und Umsetzung einer Antidiskriminierungspolitik (Stellungnahme 05/2008)***

Das flämische Amt für Arbeitsvermittlung und Berufsbildung wollte sich im Rahmen seiner Gleichstellungs- und Diversitätspolitik ein Bild über die Anzahl sowohl von ausländischen als auch von behinderten Personen in seiner Personaldatenbank machen. Unter welchen Bedingungen konnten solcherlei Nachforschungen in Übereinstimmung mit dem belgischen Privatsphäre-Gesetz angestellt werden? Die belgische Kommission beschloss, dass die auf die Diversität Bezug nehmenden Daten ausreichend transparent und verhältnismäßig waren und auf freiwilliger Basis verarbeitet wurden. Der Zweck der Verarbeitung ist legitim und beruht unter anderem auf den in einem Gesetzestext über die verhältnismäßige Beschäftigung auf dem Arbeitsmarkt festgelegten Rechten und Verpflichtungen. Die belgische Kommission hat dennoch eine Reihe von Mängeln feststellen können und deren Behebung spätestens bis zur Umsetzung des Monitoring-Systems gefordert:

- die Mitarbeiter müssen ihr Einverständnis oder ihre Weigerung wieder zurückziehen können; diese Veränderung darf nicht dauerhaft im System gespeichert werden;
- die Umsetzungsphase der Selbstregistrierung ist schlecht gewählt, da sie zusammenfällt mit der Phase der Mitarbeiterbewertung. Das könnte bei den Mitarbeitern der betroffenen Gruppen den Eindruck erwecken, dass sie unter Druck gesetzt werden, um ihre Daten zu vermitteln;
- angesichts der Tatsache, dass die Gleichstellungs- und Diversitätspolitik sich nicht auf gewisse Nationalitäten bezieht, beurteilt die belgische Kommission die Frage nach der Nationalität der Großeltern/des Großelternteils des Mitarbeiters als übertrieben;
- es kann keinerlei Monitoring der Mitarbeiter auf der Grundlage ihrer Nationalität durchgeführt werden, wenn diese Personen ihre Nationalität nicht vorher freiwillig zum Zweck dieses Monitoring registriert haben.

Schließlich hebt die belgische Kommission hervor, dass es sich bei der Verarbeitung dieser Daten um sensible Daten handelt. Sie empfiehlt, das gesamte Projekt von einem Sicherheitsberater überwachen zu lassen, der eine Aufsichtsfunktion übernimmt (mit dem Datenschutz im Sinne der Richtlinie betraut wird).

*Verarbeitung sensibler Daten und Antidiskriminierungsstudie*

Anlässlich einer Empfehlung (02/2008) an eine öffentliche Wohnungsbaugesellschaft, die eine soziologische Studie über Mieter und Wohnungsbewerber durchzuführen wünschte, wies die belgische Kommission darauf hin, dass der sensible Charakter der Angaben „Geburtsort" und „Nationalität" nicht deutlich genug hervorgehoben wird. Ihre Erfassung sollte unerheblich bleiben. Der Autor der Studie berief sich darauf, die *soziale Vermischung und den Kampf gegen die Diskriminierung im Wohnungssektor* zum Ziel zu haben. In Antwort auf dieses Argument hob die belgische Kommission hervor, dass die Unterscheidung aufgrund eines der diskriminierenden Motive gemäß der Gesetzgebung bezüglich der Antidiskriminierung an sich keine Diskriminierung darstellt, wenn sie durch ein legitimes Ziel gerechtfertigt wird und wenn die Mittel zur Realisation dieses Zieles geeignet und erforderlich sind. Überdies wird die präzise Bestimmung des Zweckes oder der Zwecke und der Zuweisungskriterien umso bedeutsamer, wenn potenziell sensible oder diskriminierende Daten verarbeitet werden. Die belgische Kommission hat empfohlen, dass in den Texten eine bessere Bestimmung der Zwecke (Kampf gegen die Diskriminierung) und der zu verarbeitenden Daten vorgesehen werden sollte. Es genügt nicht, sich generell auf die Verpflichtung zur Nicht-Diskriminierung zu berufen.

In derselben Stellungnahme hebt die belgische Kommission hervor, dass die Prüfung der Kompatibilität einer Weiterverarbeitung von Daten durch einen für die Datenverarbeitung Verantwortlichen aus dem öffentlichen Sektor auf ordnungsgemäße Rechtsverordnungen gestützt sein muss, die die weitere Verarbeitung, die Art der zu verarbeitenden Daten, ihre Herkunft und den Zweck der Verarbeitung in ausreichender Weise beschreiben. Die *Ad-hoc*-Annahme einer Anordnung oder eines Dekretes könnte so zur Wahrung der Kompatibilität einer solchen Weiterverarbeitung mit der ursprünglichen Verarbeitung beitragen. Im gegenteiligen Fall gelten sämtliche mittels Königlichen Erlasses festgelegte Bestimmungen (13. Februar 2001) des *Privatsphäre-Gesetzes*.

2008 ergriff die belgische Kommission im Übrigen mehrere Initiativen hinsichtlich der Verarbeitung von Daten im Forschungskontext. Einige von diesen werden im Folgenden beschrieben.

**Historische, statistische und wissenschaftliche Untersuchung**

*Leitfaden für den Forscher*

2008 hat die belgische Kommission z. B. einen Leitfaden für den Forscher veröffentlicht. In dieser Veröffentlichung informiert sie den wissenschaftlichen Sektor über die Regeln und die zu befolgenden Prozeduren bei der Erfassung von personenbezogenen Daten im Rahmen einer Untersuchung. Die belgische Kommission unterscheidet vier Etappen, für die sie einige Fragen festlegt und Empfehlungen formuliert: vor dem Beginn der Untersuchung (Prinzipien bezüglich der Nutzung von Sekundärdaten, die Erfassung von sensiblen Daten), während der Datenerfassung (Informationen bei der ersten Kontaktnahme, Verweigerung der Teilnahme und die Löschung der Identifikationsdaten der Personen, die sich entscheiden die Teilnahme zu verweigern, die Erfassung im engeren Sinn und Recht auf Zugang, Änderung und Löschung), während der Analyse und der Veröffentlichung (umfassendste und schnellstmögliche Anonymisierung, Sensibilisierung der Mitarbeiter, Veröffentlichungen) und nach der Untersuchung. Schließlich enthält der Leitfaden auch einen Verhaltenskodex (siehe unten), zu dessen Einhaltung Empfänger von Daten aus dem nationalen Personenstandsregister sich bei der Ausführung ihrer Untersuchungsaufgaben verpflichten.

*Verhaltenskodex für Wissenschaftler mit Zugriff auf das nationale Personenstandsregister (Stellungnahme 27/2008)*

Die strikten Prozeduren der belgischen Kommission zum Schutz der Privatsphäre beunruhigten die Forscher. Die erschwerten Zugriffsbedingungen auf das nationale Personenstandsregister ließ sie befürchten, dass keine verantwortungsvolle Untersuchung mehr durchgeführt werden könne. Die belgische Kommission hat sich diese Befürchtung zu Herzen genommen und sowohl intern als auch zusammen mit dem wissenschaftlichen Sektor Überlegungen zu dieser Frage angestellt.

Im Rahmen einer wissenschaftlichen Untersuchung, die auf einer Stichprobe aus der Bevölkerung aufbaut und eine Zweckbestimmung von allgemeinem Interesse verfolgt, ist jede belgische Institution nach der Zustimmung des jeweiligen sektoralen Komitees, berechtigt, Identifikationsdaten aus dem nationalen Personenstandsregister zu empfangen. Die schriftliche Erhebung ist hierbei die Regel, die

mündliche Erhebung (also im Beisein der Person) bildet die Ausnahme. Wenn der Untersucher nicht mit einem schriftlichen Fragebogen arbeiten will oder kann, muss er dies beim sektoralen Komitee des nationalen Personenstandregisters beantragen und seine Entscheidung begründen. Handelt es sich um eine einmalige schriftliche Erhebung, übernimmt das nationale Personenstandsregister selbst die Versendung der Fragebögen sowie des beigefügten Begleitschreibens und der von der Institution gelieferten Dokumente. Weitere Sendungen sind ebenfalls unter Einhaltung derselben Prozedur möglich. In diesem Fall übermittelt das nationale Personenstandsregister der Forschungseinrichtung lediglich die Informationen, die für eine Analyse der Verweigerungen erforderlich sind, und dieses ausschließlich in verschlüsselter Form. Bei mündlichen Erhebungen, in deren Rahmen Identifikationsdaten erforderlich sind, übermittelt das nationale Personenstandsregister der Forschungseinrichtung die relevanten Daten mit der Bedingung, dass Folgendes eingehalten wird:

- die betreffende Person darf nicht öfter als sie es wünscht beansprucht werden;
- die untersuchende Institution hat sich korrekt und professionell zu verhalten;
- Identifikationsdaten müssen einem besonderen Schutz unterliegen, eventuell durch beauftragte, vertrauenswürdige Dritte;
- Berichte und Veröffentlichungen auf der Grundlage von Daten, die vom nationalen Personenstandsregister zur Verfügung gestellt wurden, dürfen lediglich anonyme Daten enthalten.

*Wiederverwendung administrativer Daten zu Forschungszwecken – vertrauenswürdige Dritte (Stellungnahme 20/2008)*

Anlässlich eines Antrages auf eine Stellungnahme zur Wiederverwendung von Daten aus Hochschul-Verwaltungsdatenbanken mit dem Ziel, die sektorale und internationale Mobilität von Forschern zu verfolgen sowie den Einfluss eines Doktorats auf den Arbeitsmarkt zu untersuchen, hat die belgische Kommission die Einstellung eines *vertrauenswürdigen Dritten* gefordert, der mit der Verknüpfung der Daten betraut wird. Diese Forderung hat zum Ziel, eine gewisse Sicherheit zu gewährleisten zwischen der Einheit, bei der die administrativen Daten erfasst und verknüpft werden und der Institution, die lediglich anonymisierte Daten zu wissenschaftlichen und statistischen Studienzwecken erhält. Inzwischen sollte die interne Abteilung, die mit der Datenverknüpfung betraut ist, den folgenden Anforderungen entsprechen:

- die interne Datenverknüpfung muss von einer externen Stelle kontrolliert werden;
- die Leitung der internen Abteilung sollte von einem Organ gewährleistet werden, in dem die verschiedenen Kategorien von Personen, deren Daten verarbeitet werden, vertreten sind;
- die Abteilung zur Datenverknüpfung muss, gemäß dem Privatsphäre-Gesetz und dem königlichen Erlass zur Ausführung, als autonom verantwortlich (und nicht als beauftragter Datenverarbeiter) angesehen werden; sie trägt daher die sich daraus ergebende Verantwortlichkeit;
- die Abteilung zur Datenverknüpfung muss die Daten anonymisieren, sodass die Untersuchungseinrichtung nicht selbst eine Beziehung zwischen den erhaltenen Informationen und identifizierten oder identifizierbaren physischen Personen herstellen kann.

In der bereits erwähnten Akte zur E-Health-Plattform hatte die belgische Kommission in demselben Sinne ebenfalls darauf hingewiesen, dass die Rolle der E-Health-Plattform als Vermittlerorganisation ihren Wünschen entspreche, die Datenverschlüsselung zu historischen, statistischen oder wissenschaftlichen Zwecken von einem unabhängigen und neutralen Dritten gewährleisten zu lassen. Die belgische Kommission betont die Notwendigkeit, dass diese Vermittlerorganisation selbst keinerlei Untersuchungen ausführt.

**Privatsektor – wirtschaftliche und finanzielle Aktivitäten**

*SWIFT*

Mit einem Beschluss vom 8. Dezember 2008 hat die belgische Kommission das Empfehlungsverfahren, das gegenüber der Gesellschaft SWIFT eingeleitet worden war, eingestellt (siehe auch Jahresberichte 2007 und 2006). Einige Merkmale des Verfahrensablaufs und der Entscheidung der belgischen Kommission verdienen eine Hervorhebung:

SWIFT hat loyal und vorbehaltlos an der Aufstellung der Tatsachen mitgearbeitet und der belgischen Kommission Zugang zu allen Informationen und nützlichen Dokumenten gewährt. Die belgische Kommission hat

demzufolge präzise die betreffenden Verantwortlichen verschiedener bekannter Operationen bestimmen können (die bis dato herrschende Unbestimmtheit war vornehmlich der Komplexität und Unkenntnis des Systems zuzuschreiben). Die Banken, die finanzielle Gemeinschaft, SWIFT, alle haben sie ab jetzt genaue Verpflichtungen einzuhalten – als Verantwortliche für die Datenverarbeitung – zum Schutz personenbezogener Daten, die beim Abschluss finanzieller Transaktionen gebraucht werden.

SWIFT hat sich mit der Anerkennung und der Einhaltung der wohlumschriebenen Verantwortlichkeiten einverstanden erklärt. Sie hat diese im öffentlichen Register der belgischen Kommission eintragen lassen und sich auf diese Weise dazu bereit erklärt, den gesetzlichen Verpflichtungen bezüglich der Transparenz im Bereich der Datenverarbeitung nachzukommen.

Des Weiteren hat die belgische Kommission festgestellt, dass SWIFT in Beantwortung der gegen sie erhobenen Anklagen eine Reihe von Maßnahmen zur Vorbeugung gewisser Risiken und zum Schutz personenbezogener Daten, die sie verarbeitet, ergriffen hat: Errichtung einer neuen Architektur des internationalen Netzes und Errichtung eines Verarbeitungszentrums in der Schweiz zur Verwaltung der innereuropäischen Mitteilungen (die nicht mehr an die USA übermittelt werden); Ernennung eines „Vollzeit-Privacy-Officers" mit deutlich umrissenen Zuständigkeiten und Aufgaben; Formalisierung der Rahmen- und Orientierungsprozeduren und der Bearbeitung von Anfragen der Personen, deren Daten verarbeitet werden; Einrichtung einer permanenten „Data-Protection"-Arbeitsgruppe, die mit der Beurteilung und Anpassung der vorhandenen Sicherheitsmaßnahmen betraut ist; Entwicklung einer zugänglichen Informationspolitik, usw.

*Direktmarketing*
Im Juni 2008 hat die belgische Kommission die Initiative zur Veröffentlichung einer rechtlichen Mitteilung zur Problematik des Direktmarketing ergriffen. Zum besseren Schutz der Privatsphäre im Rahmen der Datenverarbeitung zu Direktmarketing-Zwecken bringt die belgische Kommission die folgenden Punkte verstärkt ins Bewusstsein:

- es ist unerlässlich, einen deutlicheren Unterschied zu machen zwischen dem Direktmarketing auf (vor-) vertraglicher Basis – Direktmarketing im Rahmen einer normalen Kundenbetreuung – und anderen Formen von Direktmarketing, zu denen die belgische Kommission zahlreiche Klagen empfängt;
- das rechtmäßige Interesse des für die Datenverarbeitung Verantwortlichen (Artikel 5f des Privatsphäre-Gesetzes – Artikel 7 f der Richtlinie 95/46/EG – mit Verdeutlichung der Umstände, unter denen diese angewendet werden kann) – darf als nichts anderes angesehen werden als eine Restgrundlage gemäß den Artikeln 5a und 5b des Privatsphäre-Gesetzes (Artikel 7a und b der Richtlinie 95/46/EG);
- im Rahmen des Handels mit Adressen und der Profilierung zu Marketingzwecken wird die Zustimmung bei den Verarbeitungen, die nicht *von vornherein* durch einen direkten Kontakt mit der Person legitimiert werden, als Bedingung vorausgesetzt;
- die Bedeutung der Nichtbeachtung des Loyalitätsprinzips wurde anhand von konkreten Beispielen erklärt;
- der Begriff „inkompatible Nutzung" wurde verdeutlicht, wie auch die Notwendigkeit einer Aufbewahrungsfrist;
- auf der Grundlage des Loyalitätsprinzips befürwortet die belgische Kommission die Verpflichtung zur proaktiven Meldung von Marketingaktionen, wenn kein direkter Kontakt mit der betreffenden Person vorliegt (z. B. im Falle von Datenhandel). Die belgische Kommission ruft zur Vorsicht auf bei der Benutzung von Standardklauseln und betont, dass diese Informationen so deutlich und verständlich wie möglich sein müssen.

Diese Mitteilung ist gegenwärtig Gegenstand einer Beratung mit dem Sektor und könnte, abhängig von den im Rahmen dieser Beratung empfangenen Bemerkungen, künftig abgeändert werden.

*Negativlisten*
Wie in den vorangegangenen Jahren stand die Frage der schwarzen Listen bei der belgischen Kommission im Mittelpunkt der Aufmerksamkeit. Stellungnahme 34/2008 zu einem Gesetzesvorschlag zur Kontrolle von Negativlisten ist eine Zusammenfassung der

Ansichten der belgischen Kommission im Verlauf von 9 Stellungnahmen seit 1998:

- Die Negativlisten stellen eine Einmischung in die Privatsphäre dar und stehen im Widerspruch zu Artikel 8 der europäischen Menschenrechtskonvention;
- einzig der Gesetzgeber ist zur Genehmigung solcher Listen befugt; die belgische Kommission drängt den Gesetzgeber, für bestehende, nicht reglementierte Negativlisten entsprechende Vorkehrungen zu treffen;
- Hauptelemente eventueller Negativlisten sollten gesetzlich festgelegt werden. Es geht vor allem um die Definition des Zweckes, der Speicherungsbedingungen, der Situationen und der Umstände, in denen der für die Datenverarbeitung Verantwortliche seine Verarbeitung legitimieren kann gemäß Artikel 5 f des Privatsphäre-Gesetzes (Artikel 7 f der Richtlinie 95/46/EG), der Art der Daten, der Speicherungsfrist, der Verbreitung und des Zuganges zu den Daten;
- die Zweckbestimmungen der Negativlisten sollten deutlich formuliert werden; Zweckbestimmungen wie „Kampf gegen Betrug" oder „Wahrung der Sicherheit" sind unzureichend;
- die Verpflichtung, Negativlisten zu melden, um Diskriminierung zu bekämpfen;
- ein einmaliges System zur Genehmigung und zur Konformitätserklärung auf einer gesetzlichen Basis, wie es in Frankreich bereits weitgehend der Fall;
- die Einführung einer Garantie der Gegenseitigkeit hinsichtlich des Austausches von personenbezogenen Daten mit anderen Ländern der Europäischen Union, die striktere Maßnahmen anwenden, vor allem multisektorale Negativlisten oder sektorale „Null-Toleranz-Listen".

*Privatsphäre und Besitzrecht*

2008 wurde die belgische Kommission regelmäßig zur Anwendung des *Privatsphäre-Gesetzes* im Bereich Zwangs-Gemeinschaftseigentums von Gebäuden (copropriété forcée d'immeubles) befragt. Diese Fragen gingen mal von Gebäudeverwaltungen (beruflich oder nicht) aus, mal von den Miteigentümern selbst. In einer Stellungnahme 22/2008 urteilte die Kommission, dass der Verband der Gemeinschaftseigentümer für die diversen Datenverarbeitungsvorgänge der Gebäudeverwaltung, seines Bevollmächtigten, im Rahmen oder im Zusammenhang mit der Verwaltung des Gemeinschaftseigentums als verantwortlich angesehen werden muss. Die Stellungnahme stellt außerdem die Rechtmäßigkeit bestimmter Datenverarbeitungen fest, etwa die Übermittlung von Namen und Adressen anderer Miteigentümer durch die Gebäudeverwaltung sowie auch die Übermittlung finanzieller Daten (Aufteilung der Ausgaben und Lasten) jedes einzelnen Miteigentümers an alle Miteigentümer. Die belgische Kommission hat auf die Annahme eventueller beruflicher oder sektoraler Verhaltenskodizes gedrängt.

**Fragen zur Identifikation**

Belgien hat sehr lang schon für eine eindeutige Identifikation plädiert – die nationale Registernummer. Zugang und Nutzung derselben unterliegen strikten Regeln. Ein Ausschuss (Ausschuss für den sektoralen Dialog – nationales Personenstandsregister), der sich zum Teil aus Mitgliedern der Kommission zusammensetzt, genehmigt Zugang und Nutzung unter Einhaltung strikter Garantien.

*Zugangs- und Nutzerverwaltung (Empfehlung vom 01/2008)*

2008 hat der Ausschuss des nationalen Personenstandsregisters mehrere Anträge auf Nutzungsgenehmigung der nationalen Registernummer zum Zweck der Zugangsverwaltung von Nutzern erhalten. Angesichts der Tatsache, dass es sich hierbei um eine allgemeine Problematik handelt, wurde die Akte der belgischen Kommission vorgelegt. Diese hat eine allgemeine Empfehlung formuliert, die mehrere praktische Regeln für diese Zugänge im öffentlichen Sektor beinhaltet:

- es ist wünschenswert, ein System auf Basis des Vertrauenskreis-Prinzips zu entwickeln;
- es ist eine qualitätsgesicherte Speicherung vorzusehen, mit einer Identitätskontrolle des Nutzers, der sich einloggt, sowie seiner Kennzeichen und seiner Aufgaben, anhand von Quellen mit bestätigter Authentizität (die Garantien für die Richtigkeit der Daten liefern);
- die elektronische Benutzererkennung muss vorzugsweise mithilfe des elektronischen Personalausweises erfolgen;
- die Zugriffsverwaltung schließt die Registrierung und die Überprüfung der Befugnisse mit ein.

*Zugangsmodalitäten zum nationalen Personenstandsregister*
Ein Gesetz aus dem Jahre 2008 betraut Bankinstitute und Versicherungsgesellschaften mit der Aufgabe, Inhaber von schlafenden Konten und Wertschließfächern sowie Inhaber schlafender Versicherungsverträge ausfindig zu machen. Die Einsichtnahme in Register wie das nationale Personenstandsregister, mit dem Ziel, solche Inhaber zu suchen und Verbindung mit ihnen aufzunehmen, ist genehmigt. In einer Stellungnahme 31/2008 teilt die belgische Kommission ihre Zufriedenheit hinsichtlich der vorgesehenen Konfiguration der Registerzugänge mit, sofern diese den Banken nicht unmittelbar zur Verfügung stehen. Eine *Zentralstelle hat die Aufgabe, die begründeten Zugriffsanträge* von Banken und Versicherungsanstalten zu sammeln und zu beantworten. Diese Art der Strukturierung (Zugriff auf das nationale Personenstandsregister für einen bestimmten Sektor über eine Zentralstelle, die auf diese Weise eine Zugangskontrolle bei diesem Sektor gewährleistet) verhindert jeglichen unbefugten Zugriff auf die Daten der betreffenden Register und jegliche Zweckentfremdung seitens Banken und Versicherungen.

*Nutzung des elektronischen Personalausweises (Empfehlung des Ausschusses für den sektoralen Dialog - nationales Personenstandsregister 02/2008)*
Der Ausschuss des nationalen Personenstandsregisters beantwortete einer Reihe Fragen über die Nutzung des elektronischen Personalausweises (eID). Wenngleich die belgische Kommission den eID als ideales Identifikationsinstrument hervorhebt, so weist sie auch auf die gesetzlichen Bedingungen hin, unter denen die Vorlage des eID verlangt werden kann. Diese Bedingungen schließen eine obligatorische Benutzung des eID als Bibliothekskarte aus. Es bleibt dem Bürger folglich frei, seinen eID als Bibliothekskarte zu benutzen. Er kann jedoch nicht dazu verpflichtet werden. Keiner der Vorteile für Inhaber einer bestimmten Bibliothekskarte darf an den als Bibliothekskarte genutzten eID gekoppelt werden.

**Öffentlicher Sektor**
*Kraftfahrzeug-Zentralregister*
Seit 2006 hat die belgische Kommission mehrere (negative) Stellungnahmen zur Schaffung einer authentischen Quelle von Kraftfahrzeugdaten herausgegeben. In einer Stellungnahme 23/2008 weist sie darauf hin, dass eine eindeutige Identifizierung des für die Datenverarbeitung Verantwortlichen erforderlich ist. Des Weiteren bieten eine zentrale Speicherung und die einer föderalen externen Kontrolle unterliegende Journalisierung der Daten die sichersten Garantien hinsichtlich des Schutzes personenbezogener Daten. Die belgische Kommission weist außerdem darauf hin, dass der Ausschuss für den sektoralen Dialog „Föderalbehörden"[17] den Fluss elektronischer Daten von der föderalen Institution, die diese Daten aufbewahren wird (DIV - belgische Kraftfahrzeugzulassungsstelle), genehmigen muss. Die belgische Kommission spricht sich gegen die Errichtung eines neuen Ausschusses für den sektoralen Dialog „Mobilität und Transport" aus und hat empfohlen, eher die größtmögliche Kohärenz mit den bestehenden Ausschüssen zu suchen.

In Ermangelung einer hinreichenden gesetzlichen Grundlage muss inzwischen die Übermittlung personenbezogener Daten aus dem Register der Kraftfahrzeugzulassungsstelle genehmigt werden, und um dem *Privatsphäre-Gesetz* zu entsprechen, müssen die Bedingungen dieser Bekanntgabe in den öffentlichen Aufträgen und in den mit den Konzessionären abgeschlossenen Vereinbarungen festgelegt werden.

*Föderale Abteilung zur Integration von Diensten (Stellungnahme 41/2008)*
Im Laufe des Jahres 2008 hat die belgische Kommission auch eine Stellungnahme zum Vorentwurf eines Gesetzes zur Einrichtung und Organisation einer *föderalen Abteilung zur Integration von Diensten* verabschiedet. Die Beurteilung dieser Initiative, für die die belgische Kommission schon in der Vergangenheit plädiert hat, war positiv, insbesondere unter Berücksichtigung der in Bezug auf den Datenschutz weniger bedrohlichen Wahl einer föderalen Abteilung zur *Integration von Diensten*, als es die Integration von Daten wäre. Die belgische Kommission wies erneut darauf hin, wie wichtig Konzepte wie authentische Quellen und Daten sind, aufgrund des Prinzips der einmaligen Erfassung und

[17] Dieser sektorale Ausschuss ist zur Genehmigung der von einer föderalen Behörde ausgehenden Datenübermittlung befugt.

der notwendigen Transparenz gegenüber dem Bürger (verfolgen können, wer die Daten eingesehen hat).

*Flämische Durchführungsverordnung zum elektronischen Austausch administrativer Daten (Stellungnahme 01/2008)*

Die Durchführungsverordnung wurde erlassen, um eine Lücke in der bisherigen Gesetzgebung zu füllen. Diese Lücke hatte Auswirkungen auf den Schutz der Privatssphäre, insbesondere durch das Fehlen einer Kontrolle des elektronischen Datenaustausches zwischen den Diensten der föderierten Institutionen. Das Schließen dieser Lücke wurde von der Kommission positiv aufgenommen. Jedoch bedauert die belgische Kommission, dass diese Kontrolle nicht einem innerhalb der Kommission eingerichteten oder einzurichtenden sektoralen Ausschuss übertragen wurde, sondern einer autonomen flämischen Kommission außerhalb der belgischen Kommission, deren Unabhängigkeit darüber hinaus nicht garantiert ist. Hinsichtlich dessen unterstrich sie, dass diese Option den Datenaustausch zwischen Behörden unterschiedlicher Niveaus verkomplizieren würde und das Risiko einer divergierenden Rechtsprechung beinhaltet. Die letztendlich angenommene Durchführungsverordnung berücksichtigt deutlich die Bemerkungen der belgischen Kommission. Die flämische Kommission wurde vom flämischen Parlament ins Leben gerufen, um ihre Unabhängigkeit zu garantieren. Es wurde auch eine direkte Verbindung mit der belgischen Kommission geschaffen, von der ebenfalls drei Mitglieder zu dieser neuen, föderierten Kommission gehören.

**Neue Technologien**

*Datenspeicherung (Stellungnahme 24/2008)*

2008 hat die belgische Kommission eine Stellungnahme abgegeben mit dem Ziel, die europäische Richtlinie 2006/24/EG über die Speicherung erzeugter oder verarbeiteter Daten im Rahmen der Lieferung von der Öffentlichkeit zugänglichen elektronischen Kommunikationsdiensten oder von öffentlichen Kommunikationsnetzwerken in belgisches Recht umzusetzen. Diese Richtlinie hat die Harmonisierung der den Dienstanbietern auferlegten Verpflichtungen im Bezug auf Datenspeicherung zum Ziel und sollte die Verfügbarkeit dieser Daten zu Untersuchungszwecken sowie die Erkennung und Verfolgung von schweren Vergehen, wie sie im innerstaatlichen Recht jedes Mitgliedstaates definiert sind, garantieren. Aus diversen Gründen hat die belgische Kommission eine negative Stellungnahme abgegeben, vor allem, da die wesentlichen Elemente der Datenspeicherung (Art der gespeicherten Daten, Dauer der Speicherung, Art der Speicherung, Rechtfertigung der Speicherung, Art der kriminellen Vergehen, deren Bekämpfung die Nutzung gespeicherter Daten rechtfertigt, Zweckbestimmungen usw.) nicht aufgeführt sind.

**Information der Öffentlichkeit**

Ebenfalls 2008 entwickelte die belgische Kommission mehrere Seiten ihrer Internetpräsenz auf Englisch, um insbesondere die Bürger über ihre internationalen Aktivitäten in diesem Bereich in dieser Sprache sowie auf Französisch und auf Niederländisch zu informieren.

## Bulgarien

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

Seit Anfang 2006 wurde die 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 durch das Gesetz über den Schutz personenbezogener Daten (GSPD) vollständig in bulgarisches Recht umgesetzt. Die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation wurde durch das Telekommunikationsgesetz in bulgarisches Recht umgesetzt, das im Staatsanzeiger, Ausgabe 41/2007, bekannt gemacht wurde.

Im Jahr 2008 wurde die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG im Hinblick auf die nationale Sicherheit und die Ermittlung von Straftaten durch die Verordnung Nr. 40 vom 7. Januar 2008 des Innenministers und des Vorsitzenden der staatlichen Behörde für Informationstechnologie und Kommunikation betreffend Datenkategorien, Verfahren für deren Vorratsspeicherung und Bestimmungen für Anbieter elektronischer Kommunikationsnetze und/oder -dienste, die im Staatsanzeiger, Ausgabe 9 vom 29. Januar 2008, bekannt gemacht wurde, in bulgarisches Recht umgesetzt.

### B. Bedeutende Rechtsprechung

Die typischen Fälle von Verletzungen der Richtlinie 95/46/EG und des GSPD betrafen im Jahr 2008 die illegale Verarbeitung personenbezogener Daten sowie die unrechtmäßige Weiterverarbeitung dieser Daten. In diesen Fällen wurde festgestellt, dass die Datenkontrolleure zur Bereitstellung einer bestimmten Art von Dienstleistung eine Kopie des Ausweises der betreffenden Person angefordert haben. Dies war bei einigen Beschwerden gegen Anbieter öffentlicher elektronischer Kommunikationsnetze und/oder -dienste der Fall, die auf der Grundlage des Telekommunikationsgesetzes bei der Kommission zum Schutz personenbezogener Daten eingingen.

Als spezielle Fälle unbefugter Verarbeitung personenbezogener Daten können die Fälle angesehen werden, in denen personenbezogene Daten von Versicherungsnehmern aufgrund eines Wechsels des Rentenversicherungsunternehmens verarbeitet wurden. In diesen Fällen gaben die betreffenden Personen an, dass sie keinen Wechselantrag eingereicht und zwecks Beglaubigung der Unterschrift vor einem Notar unterzeichnet haben. Gemäß dem Verfahren zur Übertragung von Versicherungsnehmern von einem Rentenversicherungsunternehmen in ein anderes schließt jedes Rentenversicherungsunternehmen Verträge mit natürlichen oder juristischen Personen ab, die beim Ausschuss für Finanzaufsicht als Versicherungsvertreter registriert sind. Bei einem Wechselantrag muss der Versicherungsnehmer den Antrag unterschreiben und seine Unterschrift von einem Notar beglaubigen lassen. Der Antrag wird dann bei dem Unternehmen eingereicht, zu dem die betreffende Person wechseln möchte. Dort wird dann lediglich eine Prüfung der erforderlichen Voraussetzungen durchgeführt. Die Praxis der Kommission zum Schutz personenbezogener Daten zielt darauf ab, die durch die Rentenversicherungsunternehmen ausgeübte Kontrolle der Versicherungsvermittler in ihrer Funktion als Verarbeiter personenbezogener Daten zu verbessern.

Im Jahr 2008 ergriff die Kommission zum Schutz personenbezogener Daten in Eigeninitiative Maßnahmen hinsichtlich der Organisation von Werbeveranstaltungen (Quizshows, Spiele sowie Erforschung der Kaufinteressen hinsichtlich bestimmter Produkte) sowie der Verarbeitung personenbezogener Daten von Teilnehmern solcher Veranstaltungen. Es wurde festgestellt, dass der Erhalt eines Preises mit der Bereitstellung zusätzlicher personenbezogener Daten verbunden war. Darüber hinaus war bereits zur Teilnahme an den Veranstaltungen die Angabe personenbezogener Daten erforderlich. In diesen Fällen hat die Kommission zum Schutz

personenbezogener Daten verpflichtende Anweisungen für die Kontrolleure personenbezogener Daten im Hinblick auf künftige Veranstaltungen ausgesprochen, damit das Prinzip der Verhältnismäßigkeit der verarbeiteten personenbezogenen Daten gewahrt wird und die erfassten Daten bei künftigen Veranstaltungen nicht mehr den betreffenden Personen zugeordnet werden können.

Die Kommission zum Schutz personenbezogener Daten hat Stellung zur Gewährung des Zugangs zur nationalen Bevölkerungsdatenbank für alle, die ein korrektes rechtliches Interesse nachweisen können, einschließlich Personen und staatlicher Behörden, zum Zwecke der Durchführung gesetzlich festgelegter Maßnahmen genommen. Außerdem gab es Stellungnahmen zu den Definitionen der Begriffe „Kontrolleur personenbezogener Daten" und „Verarbeiter" personenbezogener Daten.

Die Kommission beantwortete zahlreiche Anfragen von Einzelpersonen zu deren Rechten gemäß dem GSPD sowie zu den Pflichten von Kontrolleuren personenbezogener Daten. Diese Anfragen wurden per E-Mail, Brief und persönlich vorgebracht. Viele der bei der Kommission eingegangenen Fragen betrafen die Art und Weise, wie die Rechte des Einzelnen bei der Verarbeitung personenbezogener Daten geschützt und wie der Zugang zu diesen Daten geregelt wird.

Die Stellungnahmen sowie die spezifischen Fragen und Antworten der Kommission zur Anwendung des Gesetzes sind im Bekanntmachungsblatt der Kommission sowie auf der offiziellen Website veröffentlicht: www.cpdp.bg

Im Jahr 2008 wurde im Zusammenhang mit einem im Rahmen des PHARE-Programms finanzierten Partnerschaftsprojekt gemeinsam mit Experten der spanischen Datenschutzbehörde eine geplante Überprüfung des Bankensektors durchgeführt. Bei dieser Überprüfung wurde festgestellt, dass Bankkunden über die Daten (die den Kontrolleur und seine Vertreter identifizieren) informiert werden, mit dem Zweck der Verarbeitung der personenbezogenen Daten vertraut gemacht werden und Informationen darüber erhalten, dass ihre Daten an Dritte weitergegeben werden. Die Kunden werden jedoch nicht immer über die Empfänger ihrer Daten bzw. über die Kategorien der Empfänger ihrer Daten informiert. Es gab auch Fälle, in denen Kunden nicht darüber informiert wurden, ob die Bereitstellung von Daten verpflichtend oder freiwillig ist, bzw. über die Folgen einer Ablehnung des Datenkontrolleurs.

## C. Wichtige spezifische Themen

In Zusammenhang mit der durch die Kommission zum Schutz personenbezogener Daten durchgeführten Registrierung der von Kontrolleuren personenbezogener Daten gespeicherten Aufzeichnungen wurde Anfang 2008 ein System mit Namen eRALD eingeführt, das neben der traditionellen Einreichung von Registrierungsdokumenten auf Papier auch zum ersten Mal die Registrierung von Kontrolleuren personenbezogener Daten auf elektronischem Wege ermöglicht. eRALD ist eine webbasierte Anwendung, die allen Kontrolleuren ermöglicht, ihre eigenen Daten einzugeben und den Registrierungsprozess zu starten oder bereits eingegebene Informationen zu ändern. Die Kontrolleure erhalten einen Benutzernamen und ein Systempasswort. Der von ihnen gestartete Prozess unterliegt dann vollumfänglich ihrer Verwaltung und Kontrolle. Die volle Verantwortung für die Korrektheit sowie für die Aktualisierung der Daten liegt bei ihnen. Auf die eingegebenen Daten kann erst nach Abschluss der Registrierung zugegriffen werden.

Die Umsetzung eines elektronischen Registrierungssystems ist einer der größten Erfolge der Kommission zum Schutz personenbezogener Daten, da dieses System eine erhebliche Verbesserung und Vereinfachung des Prozesses ermöglicht und somit die Registrierungszeit deutlich reduziert. Darüber hinaus bietet es eine höhere Stabilität und rechtliche Sicherheit.

Im Laufe des Jahres hat sich die Kommission zum Schutz personenbezogener Daten aktiv an der Arbeit der speziell eingerichteten Gruppe „zum Schutz personenbezogener Daten" beteiligt, die als Teil der gemeinsamen Arbeitsgruppe des Ministerrates gebildet wurde, um die zur Gewährleistung der vollständigen Umsetzung der Bestimmungen des Schengen-Besitzstandes erforderlichen Maßnahmen zu ergreifen. Im Rahmen dieser Initiative diskutiert die Kommission zum Schutz personenbezogener Daten in Arbeitstreffen die Erfahrungen der neuen Schengen-Länder, tauscht Erfahrungen aus

und macht sich mit Schulungsprogrammen, durchgeführten Überprüfungen der zentralen SIS-Datenbank, der Erforschung der Anwendung der Rechtsgrundlage, der Zusammenarbeit zwischen den nationalen Datenschutzbehörden und den Auswirkungen der Erweiterung des Schengen-Raumes vertraut.

Am 5. Dezember 2008 stellten Experten des Innenministeriums, des Außenministeriums und der Kommission zum Schutz personenbezogener Daten beim Treffen der Arbeitsgruppe „Schengen-Bewertung" des Rates der Europäischen Union in Brüssel eine Zusammenfassung der Antworten des Fragebogens zur „Schengen-Bewertung" vor. Dadurch wurde die erste Phase des Beitrittsverfahrens der Republik Bulgarien zum Schengen-Raum vorbereitet – eine wichtige Priorität und Herausforderung für unser Land nach dem Beitritt zur Europäischen Union.

Ende 2008 genehmigte die Europäische Kommission einen Projektantrag (BG-2007/019-303.07.03.01) betreffend die Durchführung einer Komponente – des „verschlankten" Partnerschaftsprojektes (BG/2007/IB/JH/01/UE/TWL): „Zusammenarbeit zur zusätzlichen administrativen Stärkung der bulgarischen Kommission zum Schutz personenbezogener Daten sowie zur weiteren Verbesserung der Kontrollmaßnahmen im Bereich Branchenüberprüfungen".

Das Verfahren zur Partnerauswahl ist jetzt abgeschlossen. Als Partner wurde die spanische Datenschutzbehörde ausgewählt. Die für das Projekt festgelegten Aktivitäten sollen nach der Unterzeichnung des Vertrages beginnen.



## Zypern

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

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

Im parlamentarischen Ausschuss für europäische Angelegenheiten, im parlamentarischen Ausschuss für Gesetzgebung und im parlamentarischen Ausschuss für Menschenrechte gab es Diskussionen im Hinblick auf die Umsetzung der nationalen Datenschutzgebung, Gesetz 138(I)/2001.

Auf die Diskussion folgte ein vom Kommissar eingereichtes Memorandum, das sich mit folgenden Themen befasste:

- Bewertung der Einhaltung der Gesetzgebung;
- öffentliches Bewusstsein;
- Effektivität der Ausübung der Befugnisse des Kommissars sowie zur Steigerung der Effektivität erforderliche Maßnahmen;
- Probleme und Schwierigkeiten beim Betrieb des Büros des Kommissars (hauptsächlich im Hinblick auf die Einstellung von Personal).

Der parlamentarische Ausschuss für europäische Angelegenheiten veröffentlichte einen Bericht, in dem er unter anderem zu den oben genannten Themen Stellung nahm und die Rolle sowie den Beitrag der Arbeitsgruppe insbesondere im Hinblick auf die zunehmende Nutzung personenbezogener Daten beim Kampf gegen den Terrorismus betonte.

2. Das Gesetz zur Umsetzung der Richtlinie 2006/24/EG über die Vorratsspeicherung von Telekommunikationsdaten wurde geändert, um bei Entführungsfällen den Zugang zu gespeicherten Daten ohne Gerichtsbeschluss zu ermöglichen.

Ein Gerichtsbeschluss muss jedoch binnen 48 Stunden ab dem Zugriff auf diese Daten eingeholt werden. Falls ein solcher Beschluss nicht eingeholt wird, muss der zuständige Polizeibeamte die betreffenden Daten vernichten und den Kommissar für den Schutz personenbezogener Daten darüber informieren.

3. Ein Gesetz zur Verhinderung von Gewalt im Sport wurde in Kraft gesetzt. Dieses Gesetz schafft unter anderem die Grundlage für die Einrichtung und die Pflege einer Datenbank mit Einträgen zu personenbezogenen Daten von Personen, denen der Eintritt zu den betreffenden Sportstätten verboten wurde, um somit Gewalt an Sportstätten zu bekämpfen und zu kontrollieren, insbesondere bei Fußballspielen.

### B. Bedeutende Rechtsprechung

Mein Büro untersuchte eine Beschwerde hinsichtlich des Verlustes einer Patientenakte im Zentralkrankenhaus in Nikosia. Die Krankenhausverwaltung gab zu, die Akte des Beschwerdeführers nicht finden zu können. Es wurde eine Geldstrafe von 2 000 € verhängt.

Nachdem in meinem Büro eine Beschwerde einer Person eingegangen war, die behauptete, ihre in der Datenbank des Ministeriums für Bildung und Kultur eingetragenen personenbezogenen Daten seien von einer Studentenorganisation unrechtmäßig zu Marketingzwecken genutzt worden, fanden wir bei der Untersuchung der Beschwerde heraus, dass sich der Kontrolleur der betreffenden Datenbank seit zwei Jahren in Ruhestand befand und die zuständige Behörde keinen Nachfolger ernannt hatte.

Da dieses Versäumnis dazu geführt hatte, dass niemand für die rechtmäßige Verarbeitung der relevanten personenbezogenen Daten verantwortlich war, kamen wir zu dem Schluss, dass der Generaldirektor des Ministeriums für dieses Versäumnis verantwortlich ist und verhängten eine Geldstrafe in Höhe von 1 500 €.

### C. Wichtige spezifische Themen

- Im Laufe des Jahres 2008 haben wir die vom neuen Zentralkrankenhaus Nikosia zur Einhaltung unserer nach der im Jahr 2007 durchgeführten Prüfung ausgesprochenen Empfehlungen ergriffenen Maßnahmen verfolgt und überprüft. Wir überwachen die im Hinblick auf die Sicherheit der und den Zugang zu den vom Krankenhaus verarbeiteten personenbezogenen

Daten eingesetzten Verfahren und lassen uns über die Einrichtung und den Betrieb des betreffenden IT-Systems informieren.

- Es gab zahlreiche Beschwerden über den Einsatz von CCTV-Systemen am Arbeitsplatz und die Verwendung von Fingerabdrücken der Arbeitnehmer zur Kontrolle ihrer Anwesenheit am Arbeitsplatz. Da wir zu diesen beiden Themen bereits Leitlinien veröffentlicht hatten, überprüfen unsere Sonderdirektionen die Einhaltung dieser Leitlinien durch die Kontrolleure.
- Wir haben uns außerdem mit der Frage befasst, ob Lehrer Zugang zu ihren Akten erhalten sollen und ob die Beurlaubung von Beamten kategorisiert werden soll, so dass Anträge auf Krankheitsurlaub nur noch beschränkt genutzt werden und in einer separaten Datei gespeichert werden dürfen, zu der nur gesondert befugtes Personal nach schriftlicher Genehmigung durch die zuständige Behörde Zugang erhalten darf.



## Tschechische Republik

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

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

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

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

Bei der Umsetzung nationaler Gesetze und aufgrund der Erweiterung des EU-/EG-Rechts spielen Kontrollmaßnahmen, einschließlich Prüfungen vor Ort, noch immer eine wichtige Rolle. Die Inspektoren reagieren dabei auf Veranlassungen, die sich in zwei Hauptgruppen untergliedern lassen: Beschwerden bezüglich einmaliger Verstöße gegen das Gesetz sowie Beschwerden bezüglich systematischer Verstöße gegen das Gesetz. Im Falle einzelner Verstöße lässt sich die Angelegenheit oftmals in der „vorläufigen Untersuchungsphase" klären. In diesen Fällen können Maßnahmen ohne formale Kontrolle eingeleitet werden. Diese Vorgehensweise kann nicht in allen Fällen angewendet werden – sie kommt üblicherweise in Fällen zum Einsatz, bei denen die Unregelmäßigkeit nicht das Ergebnis eines vorsätzlichen Handelns war. Die Inspektoren müssen jedoch beim überwiegenden Großteil der Beschwerden ordnungsgemäße Prüfungen durchführen, einschließlich Prüfungen vor Ort.

Auch wenn Prüfungen weiterhin das Hauptinstrument zur Kontrolle sind, so wird zunehmend auch ein Schwerpunkt auf die Sensibilisierung für den Schutz personenbezogener Daten gelegt. Im letzten Jahr hielten Spezialisten des ASPD 260 Stunden Vorlesungen.

Außerdem wurde ein vom ASPD für Lehrer erarbeitetes und vom Ministerium für Bildung, Jugend und Sport für drei Jahre akkreditiertes Programm gestartet. In den Regionen wurden Seminare durchgeführt. Zusätzlich wurde der zweite Kunst- und Literaturwettbewerb für Kinder und junge Menschen mit dem Titel „Meine Privatsphäre! Nicht gucken, nicht herumschnüffeln!" ("My Privacy! Don't look, don't poke about!") durchgeführt. Dieses Mal nahmen auch Kinder aus SOS-Dörfern in der Tschechischen Republik, der Ukraine, Kasachstan, Russland sowie Bosnien und Herzegowina erfolgreich am Wettbewerb teil. Das Amt begrüßt diese Zusammenarbeit aufrichtig, da man es für notwendig erachtet, dass Kinder, die nicht in einer Familie aufwachsen und sich auf ihre Zukunft vorbereiten, hinreichend über ihre Rechte informiert sein sollten.

Nach der internationalen Zustimmung, die der Wettbewerb für die Kinder und das Projekt zur Lehrerschulung dem Amt im letzten Jahr eingebracht haben (Madrid, 2007, Preis für bewährte Verfahrensweisen für Datenschutz in öffentlichen Diensten Europas), wurden die Werke der Kinder zur Feier des Datenschutztages in der Eingangshalle des Europapalastes in Straßburg ausgestellt.

Das Amt setzte auch seine Arbeit mit der 3. medizinischen Fakultät der Karls-Universität fort und hielt ein

Seminar darüber ab, wie mit spezifischen Bedrohungen der Privatsphäre und des Datenschutzes im Hinblick auf ältere Menschen umzugehen ist.

## B. Bedeutende Rechtsprechung

Als Teil der **elektronischen Aktenablage der öffentlichen Verwaltung** und der Einführung von e-Government-Diensten wurde die Arbeit an der Vorbereitung von Gesetzen zu den neuen elektronischen Registern der öffentlichen Verwaltung fortgesetzt. Das ASPD setzte grundlegende Stellungnahmen und Beschränkungen durch und bestand darauf, dass technische Aspekte diskutiert und mit dem Schutz personenbezogener Daten in Zusammenhang stehende Risiken bewertet werden. Als Folge dessen wurde dem Amt oftmals vorgeworfen, den Prozess zu verlangsamen. Auch wenn das Amt es nicht geschafft hat, all seine Meinungen vorzutragen, so ist sein positiver Einfluss auf die erreichte Lösung trotzdem offensichtlich.

Es hatte auch einen positiven Einfluss auf die Erarbeitung des *Gesetzes zur Volkszählung 2011*. In diesem Zusammenhang konzentrierten sich die Stellungnahmen des Amtes darauf, zu gewährleisten, dass für die geplante elektronischen Volkszählung, für die Arbeit der Volkszählungsbeamten sowie gleichermaßen für den Fall einer Zusammenarbeit mit externen Unternehmen klare Regeln für den Zugang zu bestimmten Arten von Informationen sowie für den Schutz der Daten vor Missbrauch gelten sollten.

Im Gegensatz dazu waren die Versuche, Einfluss auf die Arbeit mit den **medizinischen Registern** zu nehmen, nicht so erfolgreich – das Gesundheitsministerium wies den Antrag des ASPD ab, das Konzept der Zentralregister vollumfänglich zu erläutern. Das Amt forderte eine Erklärung über die Rechtfertigung des definierten Datenspeicherungszeitraums in den einzelnen Registern sowie eine Erläuterung der Gründe dafür an, warum die Zustimmung der betroffenen Personen anders als in einigen anderen europäischen Ländern nicht berücksichtigt wird.

Beim von einer parlamentarischen Initiative erstellten Entwurf des **Gesetzes über Interessenkonflikte** wurden nicht alle Vorschläge des Amtes angenommen. Hier wurden dem Amt spezifische Kontrollbefugnisse zugesprochen. Es weist jedoch weiter darauf hin, dass das Gesetz nicht hinreichend deutlich unterscheidet zwischen verfassungsrechtlichen und anderweitig gewählten Beamten, für die als öffentliche Personen eine grundlegend reduzierte Garantie ihrer Privatsphäre gilt, und Beamten von öffentlichen Verwaltungen, deren Privatsphäre im Wesentlichen im Hinblick auf Angelegenheiten geschützt werden muss, die nicht direkt in Zusammenhang mit der Erledigung ihrer eigentlichen offiziellen Pflichten stehen.

## C. Wichtige spezifische Themen

Die *Kontrollaktivitäten* des ASPD umfassten im Jahr 2008 insgesamt 112 durchgeführte Kontrollen in Bezug auf Datenschutzgesetz Nr. 101/2000 Coll. (selbe Anzahl wie 2007) sowie 91 durchgeführte Kontrollen in Bezug auf unerbetene Werbenachrichten gemäß Gesetz Nr. 480/2004 Coll. über bestimmte Dienstleistungen der Informationsgesellschaft. Bei der Mehrzahl der von unabhängigen Prüfern und deren Kontrollteams durchgeführten Überprüfungen handelte es sich um *Ad-hoc*-Kontrollen aufgrund von Veranlassungen und Beschwerden seitens Privatpersonen. Lediglich etwas mehr als 10 % der Kontrollen wurden im Rahmen des Jahresplans für Kontrollaktivitäten durchgeführt, wobei derartige Kontrollaktionen in der Regel sehr viel komplexer sind und ein breiteres Spektrum an Datenverarbeitungsmerkmalen und -aspekten abdecken.

Der *Jahresplan für Kontrollaktivitäten 2008* konzentrierte sich auf 5 allgemeine Bereiche:

1. Verarbeitung personenbezogener Daten bei der Arbeit von Justiz- und Strafverfolgungsbehörden, mit besonderem Schwerpunkt auf Vollstreckungen und der richterlichen Praxis bei der Pflege des Insolvenzregisters;
2. Verarbeitung personenbezogener Daten in Bezug auf die gemeinsamen Informationssysteme der EU, nämlich das Zollinformationssystem (ZIS), EURODAC und das Schengener Informationssystem;
3. Informationssysteme öffentlicher Verwaltungen, die nicht anderweitig klassifiziert sind und deren Schwerpunkt auf diagnostischen Einrichtungen, Kinderheimen mit Schulen und Bildungszentren liegen, d. h. darauf, wie die Einrichtungen für Kinder, die

nicht in Familien aufwachsen, personenbezogene Daten verarbeiten, sowie des Finanzministeriums und der Steuerbehörden;
4. Verarbeitung personenbezogener Daten im Rahmen von Überwachungssystemen sowohl im öffentlichen als auch im privaten Bereich, und zwar in den Gebäuden des Kultusministeriums, in Krankenhäusern, Sozialpflegeeinrichtungen sowie in Büros privater Unternehmen;
5. Verarbeitung personenbezogener Daten im Hinblick auf den Verbraucherschutz, mit Schwerpunkt auf modernen Technologien zur schnellen Identifizierung, insbesondere RFID-Systemen.

Die auf der Grundlage von Beschwerden und sonstigen Veranlassungen durchgeführten Kontrollmaßnahmen befassten sich mit einem breiten Spektrum von Bereichen des öffentlichen und privaten Sektors. Ein wichtiger Bereich war auch hier wieder die öffentliche Verwaltung, wo es oftmals Probleme gibt, beispielsweise bei der Nutzung der Informationssysteme für Bevölkerungsdaten. Diese Quelle wird von zahlreichen Behörden der öffentlichen Verwaltung genutzt, sowohl im Rahmen des Gesetzes über Bevölkerungsdaten als auch auf der Grundlage Dutzender anderer Sondergesetze. Das Amt sieht sich hier oftmals Versuchen gegenüber, die Daten in breiterem Umfang zu nutzen als diese Gesetze es zulassen.

Beschwerden waren auch der Anlass für Kontrollen im Gesundheitssystem, wo eine Reihe von Verstößen gegen das Gesetz zum Schutz personenbezogener Daten festgestellt wurde.

Das Amt befasste sich insbesondere mit der Verarbeitung von personenbezogenen DNS-Daten. Im Jahr 2008 wurde eine Kontrolle im Institut für Kriminalistik der Polizei der Tschechischen Republik durchgeführt, dem Betreiber der nationalen DNS-Datenbank, die als Reaktion auf Beschwerden sowie auf der Grundlage des Kontrollplans des vorangegangenen Berichtszeitraums eingerichtet wurde. Es wurden Verstöße gegen das Gesetz zum Schutz personenbezogener Daten festgestellt, da sensible Daten in einem Umfang erfasst, verarbeitet und gespeichert wurden, der über die rechtlichen Befugnisse hinaus geht. In diesen Fällen erfordert das Gesetz die Zustimmung der betroffenen Person. Diese wurde jedoch nicht eingeholt. Ein Aspekt der aus den Kontrollen gezogenen Schlussfolgerungen war die Verhängung einer Geldstrafe sowie einer Korrekturmaßnahme, nämlich der Vernichtung der rechtswidrig verarbeiteten personenbezogenen Daten.

Auf der Grundlage von Beschwerden und sonstigen Veranlassungen wurde eine Kontrolle bestimmter privater Unternehmen durchgeführt, die Gentests zur Vaterschafts- und Verwandtschaftsbestimmung zu kommerziellen Zwecken sowie DNS-Analysen für die Forschung und zum Testen auf genetisch bedingte Krankheiten sowie zur Vorhersage der Effizienz der Behandlung dieser durchführen. Es wurden Verstöße gegen zahlreiche Vorschriften des Gesetzes (Meldepflicht, Zustimmung, die nicht die gesamte Nutzung der Daten betraf, bestimmte Aspekte der Verhältnismäßigkeit usw.) festgestellt. Es wurde eine Geldstrafe verhängt und eine Korrekturmaßnahme durchgeführt.

Überwachungssysteme (Kameras) im öffentlichen und privaten Sektor sind auch weiterhin Gegenstand zahlreicher Beschwerden und darauf folgender Kontrollen. Obwohl durch zahlreiche Kontrollen und intensive Sensibilisierung durch das Amt in Form von Meinungen, Konsultationen usw. bereits kleine Erfolge (z. B. stärkere Beschränkungen bei der Installation von Kameras in Schulen) verzeichnet werden konnten, ist hier dennoch ein zunehmender Trend zu erkennen.

Die zuvor genannten Kontrollmaßnahmen umfassen nicht die Maßnahmen, die sich mit *unerbetenen Werbenachrichten* („Marketing-Spam") befassen. Im Jahr 2008 gingen beim ASPD 1.458 Beschwerden und sonstige Veranlassungen ein. 1.311 davon wurden bearbeitet, 91 Kontrollen wurden abgeschlossen und 81 Sanktionen verhängt.

## Dänemark

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

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

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

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

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

### B. Bedeutende Rechtsprechung

Im Februar 2008 bat ein Nachtclub die DSB um die Genehmigung der Verarbeitung von Daten seiner Gäste gemäß Abschnitt 50 (1) des Gesetzes über die Verarbeitung personenbezogener Daten, um Sicherheit und eine friedliche Stimmung zu gewährleisten.

Um dies zu erreichen, wollte der Nachtclub die folgenden Maßnahmen umsetzen:
- Einrichtung eines elektronischen Zugangssystems auf der Grundlage von Fingerabdrücken (Vorlagen) und Fotos der Gäste;
- Erstellung einer internen Liste von Gästen, gegen die aufgrund von Gewalttaten, Vandalismus, Bedrohungen und dem Konsum und/oder dem Verkauf von Drogen ein Hausverbot ausgesprochen wurde. Auf der internen Liste würden auch Informationen zur Dauer des Hausverbots sowie zu den Gründen aufgeführt werden.

Nach Vorlage des Anliegens beim Rat kam die DSB zu dem Schluss, dass der Nachtclub die Fingerabdrücke (Vorlagen) und Fotos mit ausdrücklicher Zustimmung der Gäste verarbeiten dürfe.

Wenn ein Gast seine Zustimmung widerruft, ist der Nachtclub verpflichtet, den Fingerabdruck und das Foto zu löschen.

Die DSB kam außerdem zu dem Schluss, dass dem Nachtclub unter folgenden Bedingungen die Genehmigung zur Verarbeitung sensibler Daten (wie z. B. Daten zu Gesundheit (Drogenkonsum) und Straftaten) erteilt werden könne:
- Die Verarbeitung sensibler Daten im Zusammenhang mit der Verhängung eines Hausverbots darf nur mit Zustimmung des Gastes erfolgen. Die Zustimmung muss ausdrücklich sein und muss im Einklang mit dem Gesetz über die Verarbeitung personenbezogener Daten stehen. Das bedeutet, dass sie freiwillig, für diesen speziellen Fall und nach hinreichender Information gegeben werden muss.

- Wenn der Gast seine Zustimmung widerruft, müssen die Daten zu den Gründen für das Hausverbot gelöscht werden.
- Die Verarbeitung sensibler Daten muss im Einklang mit den festgelegten, in einem Anhang aufgelisteten Sicherheitsmaßnahmen erfolgen.

Die Angestellten des Nachtclubs müssen darüber informiert werden, dass die Verwendung der Liste von Gästen, gegen die ein Hausverbot ausgesprochen wurde, protokolliert wird und dass dieses Protokoll dazu verwendet werden kann, die unbefugte Verwendung dieser Liste festzustellen.

## C. Wichtige spezifische Themen

Im November 2007 wurde der DSB zugetragen, dass eingebettete sensible Daten über natürliche Personen in Zusammenhang mit PowerPoint-Präsentationen veröffentlicht wurden.

Daraufhin startete die DSB zahlreiche Untersuchungen von öffentlichen Behörden und privaten Kontrolleuren. Die meisten im Jahr 2007 gestarteten Untersuchungen wurden im Jahr 2008 beendet. Die DSB kritisierte die für die Veröffentlichung verantwortlichen Kontrolleure.

Aufgrund des Sicherheitsproblems forderte die dänische DSB die Behörden dazu auf, sicherzustellen, dass auf ihren Websites keine solchen eingebetteten Daten über natürliche Personen abrufbar sind.

Darüber hinaus empfahl die DSB, dass die öffentlichen Behörden überprüfen sollten, ob solche Daten Dritten (z. B. Teilnehmern von Meetings) auf andere Art und Weise zugänglich gemacht wurden. Falls dies der Fall sein sollte, müssten die öffentlichen Behörden Maßnahmen ergreifen, um die Daten zurückzuziehen oder den Empfänger auffordern, diese zu löschen.

***Beschreibung des Sicherheitsproblems und Möglichkeiten zur Vermeidung:***
Das Sicherheitsproblem tritt auf, wenn PowerPoint-Präsentationen Excel-Grafiken oder Tabellen in Form eines eingebetteten Objekts enthalten. Wird dieses Objekt geöffnet, so ist es möglich, auf die eingebetteten Daten zuzugreifen, die unter Umständen sensible Daten enthalten (um das Objekt zu öffnen, muss die .ppt-Datei auf dem PC gespeichert, das Objekt dann in der PowerPoint-Anwendung geöffnet und dann die betreffende Grafik oder Tabelle angeklickt werden).

Das Problem ist hauptsächlich bei PowerPoint-Präsentationen aufgetreten, kann jedoch auch bei anderen Office-Dateien wie z. B. Word-Dokumenten auftreten, wenn eine Datei aus einem anderen Programm (z. B. Excel) eingebettet wurde.

Das Sicherheitsproblem kann folgendermaßen vermieden werden:
1. Umwandlung der PowerPoint-Präsentation in das pdf-Format
2. Einbindung von Grafiken und Tabellen als Bilder anstatt als Objekte.

Dasselbe Verfahren wird angewendet, wenn Grafiken und Tabellen in Word-Dokumente eingebunden werden sollen.

# Estland

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

Im Berichtszeitraum 2008 gab es wesentliche Entwicklungen im Hinblick auf die Umsetzung des Gesetzes über den Schutz personenbezogener Daten (im Folgenden GSPD). Die neue Version des GSPD trat am 1. Januar in Kraft.

Die Änderung der Definition personenbezogener Daten sowie die Erweiterung auf sensible personenbezogene Daten durch die Verwendung biometrischer Daten könnte als das wichtigste Ergebnis des neuen GSPD betrachtet werden. Ebenso zu nennen sind der verbesserte Schutz bei der Verarbeitung personenbezogener Daten, d. h. Änderungen an Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten zur rechtmäßigen öffentlichen Nutzung, Verordnungen zur Verarbeitung personenbezogener Daten zu Forschungszwecken oder für Regierungsstatistiken sowie die Ernennung eines DSB (gemäß Richtlinie 95/46/EG: Datenschutzbeauftragter), der für den Schutz der personenbezogenen Daten verantwortlich ist.

Seit dem 1. Januar 2008 besteht die Kategorie private personenbezogene Daten nicht mehr. In der neuen Version des GSPD werden personenbezogene Daten nun in sensible personenbezogene Daten und personenbezogene Daten unterteilt. Mit der Aufhebung der Kategorie private personenbezogene Daten entfallt auch die oben erwähnte Verpflichtung, die Verarbeitung dieser Daten zu melden.

Wie zuvor erwähnt, werden seit dem 1. Januar 2008 biometrische Daten, vor allem Fingerabdrücke, Handabdrücke und Irisabbildungen, als sensible personenbezogene Daten behandelt, und der Begriff Daten in Bezug auf genetische Informationen wurde durch „genetische Daten" ersetzt.

Außerdem wurde eine neue Bestimmung hinsichtlich der Weitergabe von Daten vorgebracht. Seit Januar 2008 hat eine Person das Recht, die Beendigung der Weitergabe und jeder anderen Verwendung von personenbezogenen Daten, die in gesetzlich zulässiger Weise für öffentliche Verwendung bestimmt wurden, zu verlangen. Folglich wird eine Person die Kontrolle über die weitere Verwendung dieser Daten nach ihrer Weitergabe behalten, was nach dem früheren Gesetzestext nicht möglich war

Seit dem 1. Januar 2008 regelt das GSPD die Erhebung personenbezogener Daten zwecks Solvenzeinschätzung – personenbezogene Daten über Zahlungsverzug dürfen nur noch binnen drei Jahren ab der Nichterfüllung der Verpflichtungen verarbeitet und an Dritte weitergegeben werden. Die Daten im Kreditregister Estlands dürfen also nicht älter als drei Jahre sein. Ältere Daten werden aus dem Register entfernt. Diese Änderung soll im Wesentlichen sicherstellen, dass jeder Verarbeiter die Grundlage für die Verarbeitung der Daten kennt und gewährleistet, dass Verträge, Vereinbarungen und andere Dokumente den gesetzlichen Anforderungen nicht zuwiderlaufen.

Auch die Anforderungen bezüglich der Zustimmung des Datensubjekts haben sich geändert. Eine Person kann die Verarbeitung von Daten verbieten, wenn die Rechtsgrundlage für die Offenlegung und Verarbeitung nicht geprüft werden kann. Eine weitere Verarbeitung von Daten kann nur dann nicht verboten werden, wenn die ursprüngliche Offenlegung zu journalistischen Zwecken (das Gesetz enthält diesbezüglich neue Vorschriften) oder auf gesetzlicher Grundlage (zum Beispiel Datenbanken, die nur Regierungsstellen zugänglich sind) erfolgt ist.

## B. Bedeutende Rechtsprechung

**Die Verarbeitung personenbezogener Daten zu journalistischen Zwecken ohne die Zustimmung des Datensubjektes**

Die am 1. Januar 2008 in Kraft getretene neue Version des GSPD umfasst Änderungen der Vorschriften zur Verarbeitung personenbezogener Daten zu journalistischen Zwecken sowie zu Audio- und Videoaufzeichnungen an öffentlichen Orten.

Leider gab es bereits erste negative Erfahrungen zu diesem sensiblen Thema. So leitete die estnische Datenschutzinspektion (im Folgenden EDSI) ein

Ordnungswidrigkeitsverfahren auf der Grundlage einer Beschwerde einer Privatperson ein, die im Rahmen der Ausstrahlung eines TV-Senders zu sehen war. Laut der Beschwerde wurden die Privatperson und ihr Bauernhof von dem TV-Sender auf dem Gelände des Bauernhofs gefilmt, ohne dass zuvor die Genehmigung oder die Zustimmung der Person eingeholt worden war. Der Bericht wurde im Rahmen einer beliebten Nachrichtensendung des TV-Senders ausgestrahlt, obwohl die betroffene Person dies verboten hatte.

Die Verarbeitung personenbezogener Daten ist nur mit der Zustimmung des Datensubjektes erlaubt. Ferner muss eindeutig festgelegt werden, für welche Datenmenge die Genehmigung zur Verarbeitung erteilt wird, für welchen Zweck die Daten verarbeitet werden und für welche Personen eine Übertragung der Daten gestattet wird. Schweigen oder Untätigkeit ist nicht als Zustimmung einzustufen.

In diesem Fall kann die Annahme, dass die Person über den Besuch des Filmteams informiert war, nicht als Zustimmung dieser Person eingestuft werden. Daher hat das Filmteam die Aufnahmen ohne Zustimmung der Person gemacht. Außerdem wurde keine Zustimmung im Hinblick auf die Ausstrahlung des Berichts in der Nachrichtensendung eingeholt.

Die in der neuen Version des GSPD aufgeführte Ausnahme besagt, dass personenbezogene Daten ohne Zustimmung des Datensubjektes zu journalistischen Zwecken verarbeitet und in den Medien veröffentlicht werden dürfen, wenn das öffentliche Interesse überwiegt und die Verarbeitung und Veröffentlichung im Einklang mit den Prinzipien der journalistischen Ethik erfolgt. In diesem Fall war das öffentliche Interesse jedoch nicht klar, daher kam eine Ausnahmeregelung hier nicht in Frage.

Gegen den TV-Sender wurde für die Filmaufnahmen und die Ausstrahlung des Berichts ohne die Zustimmung der Person eine Geldstrafe in Höhe von 760 € verhängt.

## C. Wichtige spezifische Themen

Bereits zum zweiten Mal formulierte die EDSI auf eigene Initiative die Prioritäten im Bereich Aufsichtsaktivitäten für das Jahr. Es wurden zahlreiche Themen ausgewählt, die zu diesem Anlass eingehend behandelt wurden, und für jedes dieser Themen veröffentlichte die EDSI auf ihrer Website (http://www.aki.ee) eine Stellungnahme oder ein Anleitungsdokument. Es wurden die Themen ausgewählt, die nach Ansicht der Beamten der EDSI im Bereich des Schutzes personenbezogener Daten und der Informationsfreiheit am problematischsten erschienen.

Auf der Grundlage der Themen wurden Untersuchungen sowie gegebenenfalls Kontrollen vor Ort durchgeführt und anhand der Ergebnisse Leitlinien/Anleitungsdokumente erstellt.

Die ausgewählten Prioritäten und die im Berichtszeitraum erstellten Leitlinien lauten wie folgt: Verarbeitung personenbezogener Daten von Förderern politischer Parteien, Verarbeitung personenbezogener Daten durch Anbieter von Unterkünften, Verarbeitung personenbezogener Daten von Passagieren, Fotoaufnahmen in Bildungseinrichtungen, Registrierung der Verarbeitung sensibler personenbezogener Daten durch Sicherheitsfirmen, Veröffentlichung von Studenten- und Graduiertenlisten. Darüber hinaus hat die EDSI einen Fragebogen zur Selbstbewertung für Datenverarbeiter erstellt, um System und Verfahren zur Datenverarbeitung innerhalb des Unternehmens zu veranschaulichen und zu analysieren.

# Finnland

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

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

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

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

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

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

**Änderungen**

Im Berichtsjahr gab es keine eigentlichen Änderungen am Gesetz über personenbezogene Daten (523/1999), jedoch wurden einige Vorschriften bezüglich Kreditkartendaten in ein eigenständiges Gesetz übertragen. Die Übergangsphase für das Gesetz über die Kreditkartendaten endete am 1. November 2008. Teilweise bietet das Gesetz auch Datenschutz für juristische Personen und legt fest, dass insbesondere Datenkontrolleure hinreichende Datenschutzkompetenzen haben müssen. Das Gesetz zum Schutz der Privatsphäre im Arbeitsleben wurde um ein neues Kapitel 5a ergänzt, das detaillierte Vorschriften zur Verwendung persönlicher Kreditkartendaten im Arbeitsleben enthält.

Im Berichtsjahr wurden die von der Richtlinie (2006/24/EG) geforderten Änderungen in das Gesetz über Datenschutz im Bereich elektronische Kommunikation (516/2004) integriert. Frist für die Umsetzung ist der 15. März 2009.

Im Jahr 2006 beauftragte das finnische Parlament die Regierung mit der Erarbeitung von Gesetzen zum allgemeinen Schutz personenbezogener Daten im Bereich der biometrischen Identifizierung. Laut Justizministerium, das für die Erarbeitung des Gesetzes verantwortlich ist, werden die allgemeinen Vorschriften zur Verarbeitung der biometrischen Identifizierung in Zusammenhang mit der Überprüfung des Gesetzes über personenbezogene Daten (95/46/EG Artikel 8, Paragraph 7) erarbeitet. Diese Überprüfung wird zu einem späteren Zeitpunkt gestartet.

## B. Bedeutende Rechtsprechung

Am 17. Juli 2008 verkündete der Europäische Gerichtshof für Menschenrechte sein Urteil im Fall I gegen Finnland (Nr. 20511/03). Bei dem Fall ging es unter anderem um das Recht einer Person, auf der Grundlage von Protokolldaten herauszufinden, wer Zugang zu ihren Patientendaten hatte. Im finnischen Recht ist

festgelegt, dass der Datenschutz teilweise speziell zu dem Zweck gewährt wird, dass der Zugang zu dieser Art von Informationen sichergestellt werden kann. Das Datensystem des Krankenhauses wurde jedoch derart umgesetzt, dass die Verwaltung der Zugangsrechte und der Protokolldateien nicht im Detail die Personen zeigte, die Daten verarbeitet hatten. Als Folge dessen und unter Anwendung des Prinzips der obligatorischen Strafverfolgung konnte das Strafgericht keiner einzelnen Person eine Straftat nachweisen. In seinem Urteil gab der Europäische Gerichtshof für Menschenrechte an, dass eine Situation entstanden sei, die sich durch die funktionalen Eigenschaften eines Datensystems begründete, das nicht gemäß den rechtlichen Vorschriften kontrolliert werde und somit der Schutz des Privatlebens der betreffenden Person gemäß Artikel 8 der Europäischen Menschenrechtskonvention verletzt worden sei. Der Beschluss ist von besonderer Bedeutung, da der Europäische Gerichtshof für Menschenrechte die Menschenrechtskonvention auf ein elektronisches Datensystem und seine Mängel anwandte.

Der Gerichtshof der Europäischen Gemeinschaften (Große Kammer) hat am 16. Dezember 2008 ein Urteil zur Veröffentlichung von Daten zu beruflichem Einkommen verkündet. Der Fall betraf den Anwendungsbereich der Richtlinie 95/46/EG, die Verarbeitung und die Mobilität personenbezogener steuerlicher Daten, den Schutz von Einzelpersonen sowie das Recht auf freie Meinungsäußerung. Das Gericht überließ die Entscheidung hinsichtlich der in Artikel 9 der Richtlinie 95/46/EG genannten Verarbeitung zu journalistischen Zwecken den jeweiligen nationalen Gerichten. Andererseits muss die Datenschutzrichtlinie gemäß dem Urteil auf die Verarbeitung von aus öffentlichen Datenquellen gewonnenen personenbezogenen Daten und die Verwendung zuvor veröffentlichter Listen oder Dienstleistungen angewendet werden. Die Sache wird derzeit beim Obersten Verwaltungsgericht Finnlands behandelt.

Die zuständige Datenschutzbehörde gab ihren Beschluss zu dem vom Büro des Datenschutzombudsmannes eingeleiteten Verfahren zur Authentifizierung von Kunden bei Schnellkrediten per Mobiltelefon bekannt. In ihrem Beschluss entschied die Datenschutzbehörde, dass die Praxis, bei der der Kreditgeber die Antragsteller ausschließlich auf der Grundlage der per Textnachricht übermittelten Daten zu Namen, Sozialversicherungsnummer, Anschrift und Telefonnummer identifiziert und dies als Kreditantrag akzeptiert wird, nicht als hinreichend zuverlässige Praxis angesehen werden kann. Daher untersagte die Behörde dem Verfahrensgegner, der ein in der Branche übliches Authentifizierungsverfahren eingesetzt hatte, personenbezogene Daten auf die zuvor genannte Art und Weise zu verarbeiten. Der Verfahrensgegner reichte beim zuständigen Berufungsgericht eine Beschwerde zum Beschluss der Datenschutzbehörde ein. Zum Teil aufgrund dieses Falles wurde in Finnland der Vorschlag zur Inkraftsetzung eines allgemeinen Gesetzes zur Authentifizierung vorgebracht.

## C. Wichtige spezifische Themen

### Schwerpunkt auf Sondergesetzen

Gemäß Paragraph 10 der finnischen Verfassung muss der Schutz personenbezogener Daten gesetzlich gewährleistet sein. Aufgrund dieser Vorschrift existieren derzeit bis zu 650 Sondergesetze zur Regelung des Schutzes personenbezogener Daten. Im Hinblick auf die Übertragung von Daten zwischen Behörden ist das allgemeine, neben dem Datenschutzgesetz anzuwendende Gesetz das Gesetz über die Transparenz der Aktivitäten der Regierung. Die tragischen Schießereien an den Schulen in Jokela und Kauhajoki haben das Thema der Bearbeitung des gesamten gesetzlichen Rahmens betont. Ein besonderer Schwerpunkt lag hierbei auf Gesetzen über Studentenwerke, Schusswaffen und Gesundheitsversorgung. Es wurde festgestellt, dass die Behörden in verschiedenen Verwaltungsbereichen nicht hinreichend auf die aktuelle Gesetzgebung geachtet hatten. Andererseits war auch leicht zu beobachten, dass das Personal, das die Gesetze auf lokaler Ebene anwenden musste, keine ausreichenden Informationen und Anweisungen erhalten hatten. Aus diesem Grund war es ihm in Problemsituationen nicht möglich, innerhalb der gestatteten gesetzlichen Grenzen zu agieren.

### Durchgeführte Studien

Im Berichtsjahr führte das Büro des Datenschutzombudsmannes zahlreiche Studien durch. Das nationale Gesetz über die elektronische Verarbeitung von Kundendaten in den Bereichen Sozialhilfe und Gesundheitsversorgung enthält eine spezielle Vorschrift

zur Ernennung einer für den Datenschutz zuständigen Person pro Abteilung. Darüber hinaus verlangt das Gesetz, dass der Leiter jeder Abteilung spezifische Leitlinien erstellt, die im Hinblick auf den Datenschutz anzuwenden sind. Laut unserer Studie begann die Umsetzung der Vorschriften positiv, die Situation könnte jedoch noch immer verbessert werden. Gleichzeitig wurden weit reichende Bildungsmaßnahmen für die für den Datenschutz zuständigen Personen gestartet. Diese sind auf Hochschulebene am umfassendsten.

Im Rahmen der so genannten Umfrage zur Internetpolizei wurde die Legalität der Verarbeitung personenbezogener Daten bei finnischen Internetdiensten untersucht. Der Schwerpunkt der Umfrage lag beispielsweise auf Diensten, die soziale Netzwerke für Kinder und junge Leute anbieten sowie auf Diensten, die sensible personenbezogene Daten erfassen. Die Ergebnisse der Studie zeigten, dass es im Hinblick auf die Erfüllung der Informationspflichten noch immer viel zu tun gibt. Hinsichtlich einiger der Dienstanbieter wurden Sondermaßnahmen eingeleitet.

Unsere dritte Studie befasste sich mit der Funktionsweise des Gesetzes über personenbezogene Daten sowie zum Teil mit dem System der strafrechtlichen Sanktionen. Im Rahmen der Studie wurden unter anderem die von Gerichten verhängten Strafen sowie die von Staatsanwälten gefassten Beschlüsse untersucht. Die Studie zeigte, dass die Anzahl der Vergehen gegen das Datenschutzgesetz langsam aber sicher zunimmt. Es wird vermutet, dass dies in der verbesserten Kommunikation über die Rechte bezüglich und die Bedeutung des Datenschutzes, in zunehmend sicheren Datensystemen und der verbesserten beruflichen Kompetenz von Polizei und Staatsanwaltschaft begründet liegt. Andererseits gab es auch Diskussionen, ob das System der strafrechtlichen Sanktionen streng genug ist.

**Wissenschaftliche Forschung**

In der wissenschaftlichen Forschung wird oft mit sensiblen personenbezogenen Daten gearbeitet. Zu Forschungszwecken werden Daten oftmals aus verschiedenen Quellen benötigt. Unserer Erfahrung nach sind Forscher oftmals nur sehr unzureichend über die Anforderungen hinsichtlich des Datenschutzes bei wissenschaftlicher Forschung informiert. Aus diesem Grund haben wir in Zusammenarbeit mit zahlreichen Behörden ein umfangreiches und umfassendes Projekt für internetbasierte Leitlinien durchgeführt. Ziel des Projektes war die Verbesserung des Datenschutzniveaus in der wissenschaftlichen Forschung, um die Arbeit der Forscher zu erleichtern und die Verfahren von Behörden im Hinblick auf ihre Funktion als Datenquelle zu verbessern. Ergebnisse des Projektes waren unter anderem virtuelle Leitlinien sowie erforderliche Qualitätssicherungssysteme und zahlreiche Handbücher zu bewährten Verfahrensweisen.

## Frankreich

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

Frankreich hat die europäische Richtlinie vom 24. Oktober 1995 durch das Gesetz vom 6. August 2004 zur Abänderung des Gesetzes vom 6. Januar 1978 umgesetzt. Eine erste Durchführungsverordnung wurde am 20. Oktober 2005 verabschiedet und einer am 25. März 2007 verabschiedeten Änderung unterzogen, um insbesondere die erforderlichen verfahrenstechnischen Klarstellungen hinzuzufügen.

### B Bedeutende Rechtsprechung

**Die Verordnung des obersten Gerichtshofes vom 19. Februar 2008 legt die Rolle der CNIL als rechtsprechende Instanz fest.**
Die CNIL verfügt seit dem Gesetz vom 6. August 2004 über die Befugnis zur Einleitung von Verfahren und zur eventuellen Sanktionierung von für die Datenverarbeitung Verantwortlichen. Art und Status dieser Urteilsbefugnis wurden vom obersten Gerichtshof in einem Beschluss vom 19. Februar 2008 festgelegt. Der oberste Gerichtshof urteilte insbesondere, dass die „begrenzte Befugnis" der CNIL als „Rechtsprechung" angesehen werden müsse im Sinne des Artikel 6.1 der europäischen Konvention über die Menschenrechte und Grundfreiheiten. Diese bedeutsame Entscheidung zeigt, dass die CNIL sich, neben ihrer Rolle als Hüter der öffentlichen Freiheiten, als eine maßgebliche Behörde bewähren und so jedermanns Recht auf den Schutz personenbezogener Daten gewährleisten konnte.

### C. Wichtige spezifische Themen

**Annahme von Beschlüssen**
Im Verlauf des Jahres 2008 hat die CNIL im Rahmen von 36 Plenarsitzungen und 14 kleineren Gremien 50 Mal getagt. Auf diesen Sitzungen wurden insgesamt **586** Beschlüsse angenommen, d. h. **50 %** mehr als 2007.

Die CNIL hat 2008:
- **391** Genehmigungen erteilt (+ **84** % verglichen mit 2007;
- **18** Genehmigungen verweigert;
- **29** Stellungnahmen zur Verarbeitung von sensiblen oder Risikodaten verabschiedet.

**Anrufungen**
**Im Jahr 2008 wurde die CNIL mit 6.760 Fällen beauftragt;**
4.244 Beschwerden und 2.516 Anträge auf indirektes Zugangsrecht, (leicht rückläufig (-5%) verglichen mit 2007 (2.660 Anträge), jedoch noch immer deutlich steigend (+ 58%) verglichen mit 2006 (1.595 Anträge)).

Wenngleich die Zahl der Beschwerden leicht rückläufig ist, bestätigt diese nichtsdestotrotz die überaus starken Erwartungen der Bürger hinsichtlich der Wahrung der Freiheiten.

Die Meldung von Datenbanken erlebte 2008 eine außerordentliche Entwicklung. So gab es 71.990 Meldungen gegenüber 56.404 im Jahre 2007, was eine Steigerung um **27%** bedeutet.

**Kontrollen**
2008 **wurden 218 Kontrollen durchgeführt**, d. h. **33% mehr** als im Vorjahr. Anfang der 2000er-Jahre wurden nicht mehr als dreißig Kontrollen durchgeführt. Wir weisen darauf hin, dass eine Verweigerung einer Kontrolle durch die CNIL ein Delikt darstellt, das mit einer Gefängnisstrafe von einem Jahr und einer Geldbuße von 15.000 Euro bestraft wird. Diesbezüglich wurde im Januar 2009 eine erste Verurteilung wegen „Behinderung in der Ausübung der Tätigkeiten" durch das „Tribunal de Grande Instance" (~ Oberlandesgericht) in Paris ausgesprochen – aufgrund der Verweigerung von zwei Kontrollen im Februar und im April 2008.

Die Einhaltung des Gesetzes über „Informatik und persönliche Freiheit" wurden in **145 Einrichtungen** kontrolliert.

Die von der Kommission durchgeführten Kontrollen sollen die **Umsetzung des Jahresprogrammes** ermöglichen, das von der CNIL angenommen wurde und die von den Kommissaren als vorrangig bezeichneten Themen definiert.

In diesem Rahmen stand die elektronische Wahl im Mittelpunkt. Zwanzig Kontrollen wurden bei Stimmabgaben auf dem elektronischen Wege im Rahmen von Gewerkschaftswahlen durchgeführt. Es ging darum, die Geheimhaltung des Wahlergebnisses, den persönlichen, freien und anonymen Charakter der Wahl, die Aufrichtigkeit der Wahlvorgänge und die Überwachung der Wahl zu beurteilen.

Innerhalb des Sektors **der kommunalen Körperschaften** wurden ebenfalls Kontrollen durchgeführt angesichts der Vielzahl von Datenbanken mit diversen Zweckbestimmungen (Familienstand, Wählerverzeichnisse, sozialer Bereich, Stadt-/Gemeindepolizei, Bodenverwaltung, Schulanmeldungen – mitunter sensible Daten), über die sie verfügen, und der Art der gesammelten Daten.

2008 **wurde die Kontrolle der Datenbank der Kriminalpolizei (STIC)** (Datenverarbeitungssystem für festgestellte Vergehen), die dem Innenminister unterstellt ist, eingestellt. Etwa zwanzig Kontrollen wurden vor Ort bei Kommissariaten, regionalen Diensten der Gerichtspolizei, Gerichten, Präfekturen oder der regionalen Direktion des französischen Dienstes für allgemeine Informationen (Direction Régionale des Renseignements Généraux) durchgeführt und ermöglichten eine äußerst gründliche Funktionsanalyse.

Ein zweiter Schwerpunkt der durchgeführten Kontrollen bestand 2008 aus Vor-Ort-Überprüfungen im Rahmen der Beschwerden, die die CNIL empfangen hat. **25% der 2008 durchgeführten** Kontrollen fanden somit im Rahmen von Beschwerden statt.

**Sanktionen**
Seit dem Gesetz vom 6. August 2004 verfügt die CNIL über Sanktionsbefugnisse, aufgrund deren sie Geldstrafen in einer maximalen Höhe von 150.000 Euro (300.000 Euro im Wiederholungsfall) verhängen kann, wobei dieser Betrag 5% des Umsatzes nicht überschreiten darf.

Insgesamt hat die CNIL 2008:
- 9 Geldstrafen zwischen 100 und 30 000 Euro verhängt;
- 1 Warnung und
- 126 (+ 20 %) Mahnungen ausgesprochen.

**Der Datenschutzbeauftragte**
Artikel 22 des Gesetzes sieht vor, dass die Einrichtung im Falle der Anwesenheit eines „Beauftragten zum Schutz personenbezogener Daten", Datenschutzbeauftragter genannt, in der Einrichtung, von den üblichen Meldeformalitäten befreit ist. Diese Dateien sind nunmehr in ein vom Datenbeauftragten geführtes Register eingetragen. Die sogenannten „sensiblen" Verarbeitungen hingegen, die eine Vollmacht oder eine Stellungnahme erfordern, werden nach wie vor der CNIL unterworfen.

Am 31. Dezember 2008 hatten **3679** Einrichtungen einen Datenschutzbeauftragten benannt, was einer Steigerung von **104%** im Vergleich zum Jahr 2007 entspricht. Die Gesamtanzahl der Datenschutzbeauftragten zum 31. Dezember 2008 betrug 989, denn viele Einrichtungen benennen zusammen einen Datenschutzbeauftragten. **89%** der Benennungen betreffen den privaten Sektor. Der öffentliche Sektor hingegen nimmt einen Anteil von **11% ein**.

Der Datenschutzbeauftragte muss den für die Datenverarbeitung Verantwortlichen bei der Einhaltung der Auflagen unterstützen, insbesondere in Bezug auf die Wahrung der Rechte der betroffenen Personen: Zugangsrecht, Berichtigungs- und Löschungsrecht, Widerspruchsrecht. Er hat somit die Beratung des für die Datenverarbeitung Verantwortlichen zur Aufgabe, sodass die vorrangigen strategischen Orientierungen im Einklang mit dem „Datenschutzgesetz" sind. Er muss auch Verstöße aufzeigen, sodass jegliche strafrechtliche Sanktion vermieden werden kann. Der Datenschutzbeauftragte tritt als Quelle juristischer Sicherheit auf und zeugt von den ethischen Bestrebungen der Einrichtungen.

**Bedeutsame Entwicklungen 2008**
***Die Datei Edvige***
**Die CNIL hat sich 2008 zur Schaffung der polizeilichen Datei „Edvige" geäußert.**
Im März 2008 hat die CNIL vom Innenminister ein Projekt zur Schaffung eines nationalen Registers erhalten, das im Rahmen der Reform der französischen Nachrichtendienste realisiert werden sollte, und als solches der Zentraldirektion der französischen

Ordnungsdienste (Direction Centrale de la Sécurité Publique) unterstellt war.

Der Innenminister hatte den Wunsch geäußert, dass der Beschluss über die Schaffung der Datei „Edvige" nicht in den öffentlichen Medien veröffentlicht werden sollte. In der Besorgnis um die demokratische Transparenz und die Information der Bürger hat die CNIL darauf gedrängt, dass dieser Text dennoch veröffentlicht wird, um eine öffentliche Debatte zu ermöglichen. Mit der Veröffentlichung sowohl der Entstehungsakte der Datei als auch der Stellungnahme ist den Wünschen der CNIL entsprochen worden.

Die Veröffentlichung der Schaffung dieser Datei ermöglicht in weiterer Folge die Kontrolle der Datei vor Ort und mithilfe von Belegen durch die CNIL, was eine zusätzliche Garantie darstellt.

Die CNIL hat ferner bewirkt, dass die Verarbeitung in keinerlei Datenverbindung, keinerlei Vergleich oder Verknüpfung mit anderen Dateien geschieht, insbesondere jene der gerichtlichen Polizei.

Die CNIL ist ebenfalls dafür eingetreten, dass die Speicherung von Daten von öffentlichen, gewerkschaftlichen, religiösen oder politischen (örtlich oder auf nationaler Ebene) Personen deutlich eingegrenzt wird, da es sich insbesondere um die Speicherung von „verhaltensbezogenen" oder „mobilitätsbezogenen" Daten dieser Personen handelt.

Der ursprüngliche Entwurf der Durchführungsverordnung sah keine Begrenzung in der Aufbewahrungsfrist der erfassten Daten vor. Die CNIL hat sich demzufolge für eine Begrenzung der Aufbewahrungsfrist auf fünf Jahre eingesetzt, wenn es um Daten einer Person im Rahmen administrativer Nachforschungen beim Eintritt in bestimmte Berufe (Sicherheitsdienst usw.) geht.

### Die CNIL hat zu mehreren Aspekten Vorbehalte ausgesprochen

Im Bereich der Datenerfassung bei Minderjährigen hat die CNIL nachdrücklich auf ihren Grundsatz verwiesen, gemäß welchem eine solche Erfassung die Ausnahme und starken Sicherheitsvorkehrungen unterworfen sein muss. Sie hat den Wunsch vorgebracht, dass das Mindestalter für solche Erfassungen bei Minderjährigen von gegenwärtig 13 Jahren auf 16 Jahre angehoben wird.

Die Frage des Alters von Personen, die erfasst werden können, muss in Zusammenhang gebracht werden mit dem Fehlen einer Datenspeicherungsfrist. Wenngleich Minderjährige in der Tat Auslöser von *„Störungen der öffentlichen Ordnung"* sein können, so erscheint es doch nicht legitim, dass ihnen solche Vergehen noch 30 Jahre später zur Last gelegt werden können. Das „Recht auf Vergessen" muss für alle garantiert werden, auch für die Bürger von morgen.

Die CNIL urteilte des Weiteren, dass die Möglichkeit der Erfassung von Daten über ethnische Herkunft, Gesundheit und Sexualleben der Personen unzureichend abgesichert sei.

Sie hat außerdem hervorgehoben, dass sie weder über hinreichende Informationen über den Stand der technischen Sicherheit der Datei „Edvige" verfügt noch über die Existenz eines Mittels zur Rückverfolgbarkeit, mithilfe dessen die Zugriffsbedingungen auf die in der Datei enthaltenen Daten durch die öffentlichen Behörden kontrolliert werden können. Diese Informationen sind jedoch erforderlich, um ihr die Kontrolle in vollem Umfang zu ermöglichen.

Schließlich bedauerte die CNIL das Fehlen einer formalisierten Aktualisierung und Bereinigung der Dateien. Sie hat jedoch die dem Generaldirektor der nationalen Polizei obliegende jährliche Verpflichtung zu Protokoll genommen, der CNIL Rechenschaft abzulegen über seine Überprüfungsaktivitäten, die Aktualisierung und die Löschung von in der Datei „Edvige" enthaltenen Informationen.

Als Folge ihrer Bemerkungen und der Reaktionen auf die Veröffentlichung der Durchführungsverordnung EDVIGE hat die Regierung den Text zurückgezogen. Sie hat der CNIL neue Vorschläge vorgelegt, vor allem im Bezug auf die Speicherungsfrist bei Daten von Minderjährigen und die Registrierungsbedingungen bestimmter sensibler Daten. Sie hat auch angekündigt, von der Erfassung von Daten, die öffentliche Personen betreffen, in dieser Datei abzusehen.

*Die Entwicklung der Biometrie*
Biometrische Vorrichtungen, die einer Genehmigung oder einer Stellungnahme durch die CNIL unterliegen, befinden sich stetig im Vormarsch. So sind seit 2004 mehr als 1800 Anträge bei der CNIL eingegangen, wovon 1500 Vorrichtungen betreffen, die in Übereinstimmung mit den Auflagen der CNIL im Bezug auf die Erkennung der Handumrisse oder der Fingerabdrücke realisiert wurden.

Die CNIL spielt bei den Unternehmen eine betreuende Rolle bei der Zusammenstellung ihrer Systeme, sodass der Schutz personenbezogener Daten gewährleistet wird. Dieser Dienst hat sich im Besonderen auf die nachstehend beschriebenen Systeme konzentriert.

*Das biometrische Visum oder VISABIO*
Dieses neue biometrische Visumsystem wurde 2004 im Rahmen des Pilotprojektes BIODEV in einem Experiment getestet. VISABIO wird jedes Jahr mehr als zwei Millionen Personen betreffen, die aus Ländern kommen, die den Visumformalitäten unterliegen. Ziel ist die Erfassung und Speicherung biometrischer Daten in einer zentralen biometrischen Datenbank: das digitale Passfoto sowie die zehn Fingerabdrücke des Antragstellers in Kombination mit den beim vorangegangenen Visumantragsverfahren gesammelten Daten.

Wenngleich solche Daten unbestreitbar die Identitäts- und Ausweiskontrollen erleichtern, meint die CNIL, dass für dieses Verfahren sehr klare Grenzen erforderlich sind. Die CNIL bedauert vor allem, dass die Möglichkeit, biometrische Daten lediglich auf den biometrischen Visa und nicht etwa in einer zentralen Datenbank aufzubewahren, keinerlei Aufmerksamkeit bekommen hat. Die CNIL hebt auch die besondere Bedeutung hervor, die der Erfassung von Fingerabdrücken bei Minderjährigen über sechs Jahren zukommt. Diese Erfassung sollte nicht als einfache technische Maßnahme angesehen werden, sondern erfordert ganz im Gegenteil eine echte Grundsatzdiskussion.

*Der biometrische Pass*
2007 hatte die CNIL ihre Stellungnahme zum Entwurf der Durchführungsverordnung abgegeben. Die Durchführungsverordnung, deren Umsetzung vor dem 28. Juni 2009 erwartet wird, sieht die Ausstellung von Pässen vor, die mit einer elektronischen Vorrichtung versehen sind, die, in Übereinstimmung mit den Vorschriften des Rates der Europäischen Union vom 13. Dezember 2004, nicht nur ein digitales Passfoto enthält, sondern auch zwei Fingerabdrücke

Diese Durchführungsverordnung sieht im Übrigen die Speicherung des digitalen Passfotos des Antragstellers des Passes sowie acht seiner Fingerabdrücke vor. Diese Datenspeicherung bringt bedeutsame Veränderungen in dieser Datenbank mit sich.

Die CNIL hat auf die Vorbehalte hingewiesen, die dieses Projekt aufwirft, sobald die erste biometrische Datenbank für französische Bürger zu administrativen Zwecken errichtet wird. Sie hat insbesondere hervorgehoben, dass die automatische und zentralisierte Verarbeitung dieser Daten nur in dem Maße zugelassen werden kann, in dem die Wahrung der öffentlichen Ordnung oder der inneren Sicherheit dies rechtfertigen. In diesem Punkt urteilt die CNIL, dass die Argumente zur Rechtfertigung der Errichtung einer solchen Datenbank – die Verbesserung des Abgabe- oder Erneuerungsverfahrens bei Pässen oder allgemeiner, der Kampf gegen Betrug – nicht restlos überzeugend seien.

Die Speicherung digitaler Passfotos und Fingerabdrücke in einer zentralen Datenbank erscheint vor dem Hintergrund der genannten Ziele unverhältnismäßig. Angesichts der Vorbehalte der CNIL hat der Innenminister zugesichert, dass die digitalen Fingerabdrücke nicht zur Identifikation genutzt werden dürfen und dass keinerlei Erkennungssystem auf Grundlage der in der Datenbank enthaltenen digitalen Passfotos genutzt werden darf.

Die CNIL bedauerte ebenfalls, dass das neue Ausstellungsverfahren bei Pässen mittels Vorschrift angenommen wurde und nicht auf gesetzlichem Wege, da die so eingeführten Änderungen die Grenzen der europäischen Empfehlungen überschreiten. Der Umfang dieser Reformen und ihre erheblichen Folgen hätten einer öffentlichen Debatte bedurft und die Ausarbeitung eines Gesetzentwurfs erfordert.

***Stimmerkennung und venöse Erkennung***
2008 hat die CNIL erstmals die Verwendung einer Vorrichtung zur Erkennung des Venengeflechts des

Fingers genehmigt. Diese Genehmigungen wurden nach einer umfassenden technischen Begutachtung erteilt. Die CNIL hat sich auf diese Weise versichert, dass diese Vorrichtungen keinerlei Risiken im Bezug auf den Datenschutz bergen.

*Stimmerkennung*
Das Stimmerkennungssystem zielt auf die Sicherung und die Vereinfachung der Verwaltung von Passwörtern, die für den Zugriff auf das Informatiksystem, hier der Firma Michelin, erforderlich sind. Das Verfahren ermöglicht die automatische Erzeugung und Reinitialisierung von Passwörtern. Das System stützt sich auf die Erkennung des Stimmprofils, das digitalisiert und dann in abgetastete Einheiten unterteilt wird. Bei dem Stimmaufnahmeverfahren registriert jeder Mitarbeiter sein Stimmprofil. Zur Erneuerung seines Passwortes ruft er ein eigens dazu eingerichtetes Voice-Mail-System an. Das System führt dann einen Vergleich zwischen den wiederholten Wörtern des Nutzers und dem Referenzprofil durch.

Anlässlich dieser Begutachtung hat sich die Kommission davon überzeugt, dass die Mitarbeiter hinreichend informiert waren und alle Maßnahmen zur Vermeidung jeglichen Risikos des Identitätsmissbrauchs ergriffen worden waren.

*Venöse Erkennung*
Die CNIL hat außerdem 2008 erstmals die Verwendung von fünf Vorrichtungen auf Basis der Erkennung des Venengeflechts im Finger genehmigt, die dazu bestimmt sind, den Zugang zu Räumlichkeiten oder Informatiksystemen zu kontrollieren. Diese Technologie ist eine ernst zu nehmende Konkurrenz für nunmehr klassische Systeme (Fingerabdruck, Iris, Handkonturen ...). Es beruht auf der Erkennung der Verflechtung von Blutgefäßen. Dieses Verfahren bietet den Vorteil, dass es ein subkutanes Netz erkennen kann. Es ist jedoch zumindest momentan nicht möglich, dieses biometrische Kennzeichen ohne Mitwissen der betroffenen Person zu lesen und zu kopieren.

Ausgehend von einem technischen Gutachten urteilt die CNIL, dass das Venengeflecht zum heutigen Stand der Technik ein biometrisches Kennzeichen ist, das keine Spuren hinterlässt und dessen Speicherung in einer Datenbank weniger Risiken birgt als die Speicherung eines Fingerabdruckes.

*Videoüberwachung*
Die CNIL bemerkt seit den fünf letzten Jahren eine steigende Zahl der Anmeldung von Videoüberwachungsvorrichtungen. Allein 2008 wurden 2588 Anmeldungen eingereicht, gegenüber 1317 im Jahr 2007.

Die Anzahl der Beschwerden hat in dieser Periode ebenfalls eine starke Steigerung erfahren und liegt bei **173**, was eine **Steigerung um 43 % bedeutet**. In Übereinstimmung mit ihrer Aufgabe ist die CNIL zu zahlreichen Kontrollen vor Ort übergegangen und hat mehrere Mahnungen erteilt, da Einrichtungen Videoüberwachungssysteme ohne Rücksicht auf die gesetzlich vorgesehenen Formalitäten installiert hatten.

Außerdem erfordert die Bedeutung, die Videoüberwachungssysteme inzwischen einnehmen, eine Verdeutlichung der auf sie anwendbaren Texte.

***Ein komplexer gesetzlicher Rahmen, der rechtliche Unsicherheit schafft***
Gegenwärtig können Videoüberwachungssysteme zweierlei gesetzlichen Regelungen unterliegen:
- dem Gesetz vom 21. Januar 1995, gemäß dem Videoüberwachungssysteme, die öffentliche Orte beobachten, einer präfekturalen Genehmigung unterliegen;
- dem Gesetz „Informatik und Freiheiten" vom 6. Januar 1978, abgeändert 2004, das die Verwendung von Videoüberwachungssystemen an nicht-öffentlichen Orten (z. B. Firmen) regelt, oder auch von Systemen, die an öffentlichen Orten installiert sind und an biometrische Systeme (z. B. Gesichtserkennung) gekoppelt sind.

In der Praxis fehlt es diesem gesetzlichen Rahmen, in dem zwei Regelungen nebeneinander existieren, an Deutlichkeit. Seine Anwendung wird demzufolge schwierig, da die Mehrheit der Videoüberwachungsvorrichtungen nunmehr an digitale Systeme gekoppelt sind, die an sich eine automatisierte Verarbeitung personenbezogener Daten darstellen und folglich in den Zuständigkeitsbereich der CNIL fallen, unabhängig von dem Ort, an dem sie

installiert sind. Angesichts dieser Situation erachtet die CNIL die Klärung der aktuellen Regelung in Bezug auf die Videoüberwachung als erforderlich, um eine bessere Regulierung der Praktiken zu gewährleisten.

Die Frage der Kontrolle der Vorrichtungen zur Videoüberwachung durch ein wirklich unabhängiges Organ ist nunmehr in den modernen demokratischen Gesellschaften eine grundlegende Forderung.

Die Einrichtung von Videoüberwachungssystemen erfordert eine breite Zustimmung der Bevölkerung. Wenngleich bestimmte Meinungsumfragen zeigen, dass die Bevölkerung im Großen und Ganzen der Videoüberwachung positiv gegenübersteht, sind die Franzosen dennoch nicht bereit, auf den Schutz ihrer individuellen Rechte zu verzichten.

Darum beauftragt die CNIL IPSOS mit einer **Studie über die Meinung der Franzosen im Bezug auf Videoüberwachung**. Die im März 2008 durchgeführte Studie, in der eine repräsentative Stichprobe von 972 Personen im Alter von 18 Jahren und mehr befragt wurde, bestätigt, dass eine breite Mehrheit der Franzosen (71%) Videoüberwachungskameras an öffentlichen Orten positiv gegenübersteht. 65% davon sind der Meinung, dass die Erhöhung der Anzahl von Kameras zum Kampf gegen Delinquenz und Terrorismus erforderlich ist.

Dem Gedanken, dass diese Vorrichtungen zur Videoüberwachung der Kontrolle eines unabhängigen Organs unterliegen, steht eine breite Mehrheit der Franzosen (79%) positiv gegenüber. Sie sehen die CNIL als am besten geeignet für eine solche Kontrolle an.

In dieser Frage kann einzig unter der Bedingung, dass man sowohl über eine Regelung der Videoüberwachung mittels deutlicher Gesetzestexte zum Schutz der Person als auch über ein unabhängiges Kontrollorgan verfügt, von „Videoschutz" („vidéo protection"), wie es der Innenminister formulierte, gesprochen werden.



# Deutschland

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

### Gesetz zur Umsetzung der IPR Enforcement Richtlinie

Der Deutsche Bundestag hat am 11. April 2008 das Gesetz zur Umsetzung der IPR Enforcement Richtlinie (Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums) verabschiedet, das am 1. September 2008 in Kraft getreten ist (BGBl. I 2008, S. 1191). Es sieht eine Novellierung von mehreren Gesetzen zum Schutz des geistigen Eigentums vor:

Patentgesetz, Gebrauchsmustergesetz, Markengesetz, Halbleiterschutzgesetz, Urheberrechtsgesetz, Geschmacksmustergesetz, Sortenschutzgesetz werden weitgehend wortgleich geändert. Insbesondere gewährt es den Rechteinhabern, vor allem der Musik und Filmindustrie mit Blick auf „Piraterie" in Internettauschbörsen, nunmehr einen zivilrechtlichen Auskunftsanspruch gegen die Internet Zugangsprovider, um mögliche Rechteverletzer zu ermitteln. Die Auskunftserteilung setzt allerdings eine richterliche Anordnung voraus, was aus datenschutzrechtlicher Sicht mit Blick auf die Nutzung der Verkehrsdaten zur Auskunftserteilung unabdingbar ist.

Die Vorratsdaten dürfen zur Auskunftserteilung nicht genutzt werden. Der Gesetzgeber hat bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung deren Verwendung ausdrücklich auf Zwecke der Strafverfolgung und der Gefahrenabwehr, § 113b Absatz 1 Satz 1 TKG, beschränkt.

Klärungsbedarf besteht noch bei der Frage der Zulässigkeit der Ermittlung der IP-A, die Voraussetzung für die Identifizierung der Nutzer ist. Diese erfolgt z. B. durch Spähdateien, die vorgeben, die Verknüpfung zu bestimmten vom Tauschbörsennutzer gesuchten Medien zu enthalten, in Wahrheit aber nur die IP-A des Interessenten ermitteln. Ein Herunterladen z. B. von Musikstücken findet also tatsächlich nicht statt. Im anderen Fall werden Tauschbörsen anhand der Prüfsumme der urheberrechtlich geschützten Dateien abgesucht. Mit dem Rechner, der die gesuchten Dateien in seinem offenen Ordner vorhält, wird auch die jeweilige IP-A ermittelt. Auch hier handelt es sich um die heimliche Erhebung der IP-A von Tauschbörsenteilnehmern mit dem Ziel der anschließenden zweckfremden Verwendung dieser Daten.

### Gesetz zur Abwehr von Gefahren des internationalen Terrorismus

Durch das am 1. Januar 2009 in Kraft getretene Gesetz zur Abwehr von Gefahren des internationalen Terrorismus werden dem Bundeskriminalamt (BKA) erstmals umfassende polizeiliche Befugnisse zur Abwehr des internationalen Terrorismus eingeräumt.

Die Aufgabenzuweisung an das BKA bedeutet eine Zäsur in der bundesdeutschen Sicherheitsarchitektur. Die deutsche Polizei war in der Bundesrepublik Deutschland von Beginn an Ländersache. Die Zuweisung präventiver Befugnisse an das BKA verändert diese Kompetenzaufteilung.

Aus datenschutzrechtlicher Sicht sind zwei wesentliche Kritikpunkte zu nennen:

Zum einen ist zweifelhaft, inwieweit die dem BKA eingeräumten Datenerhebungs- und -verarbeitungsbefugnisse für die Erfüllung der ihm zugewiesenen Aufgaben angemessen, erforderlich und geeignet sind. Neben polizeilichen Standardbefugnissen erhält das BKA zusätzlich besondere Ermittlungsbefugnisse bis hin zur Online-Durchsuchung informationstechnischer Systeme. Schon im Hinblick auf die weiterhin bestehende Zuständigkeit der Länder bei der Abwehr von Gefahren des internationalen Terrorismus ist fraglich, ob für die wenigen Fälle, in denen das BKA selbst tätig werden wird, diese Fülle neuer Befugnisse wirklich angemessen ist. Das Nebeneinander von Zuständigkeiten des BKA und der Landespolizeibehörden für die Gefahrenabwehr sehe ich auch insofern kritisch, als es dazu führt, dass sowohl das BKA als auch die Länder parallele Abwehrmaßnahmen ergreifen können und dabei gleich mehrfach personenbezogene Daten verarbeiten.

Der andere wesentliche Kritikpunkt an dem Gesetz betrifft die Gewährleistung des Kernbereichs privater

Lebensgestaltung. Das Bundesverfassungsgericht hat in mehreren Entscheidungen in den letzten Jahren dem Gesetzgeber aufgegeben, diesen Kernbereich bei heimlichen Datenerhebungsbefugnissen abzusichern, insbesondere in dem Eingriffe in diesen Bereich soweit wie möglich von vornherein unterbleiben. Dieses Erhebungsverbot muss zudem durch Regelungen über die sofortige Löschung intimer Informationen und der Nichtverwertbarkeit ergänzt werden, wenn es ausnahmsweise doch zu einer Kernbereichsverletzung gekommen ist. Das BKA-Gesetz weist insofern Defizite auf.

## B. Bedeutende Rechtsprechung

### Urteil des Bundesverfassungsgerichts zur Zulässigkeit von Online-Durchsuchungen informationstechnischer Systeme

Das Bundesverfassungsgericht hat in seinem Urteil vom 27. Februar 2008 zur Online-Durchsuchung den heimlichen Zugriff auf informationstechnische Systeme nur unter bestimmten, engen Voraussetzungen für zulässig erklärt. So müssen bestimmte Tatsachen auf eine im Einzelfall drohende Gefahr für ein überragend wichtiges Rechtsgut hinweisen. Hierzu zählen Leib, Leben und Freiheit einer Person sowie die Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen betreffen. Der Gesetzgeber muss zudem den Grundrechtsschutz der Betroffenen durch geeignete Verfahrensvorkehrungen sicherstellen.

Die Befugnis zur Online-Durchsuchung informationstechnischer Systeme ist auf Bundesebene erstmals im Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt (siehe A) normiert worden.

Durch die vorgenannte Entscheidung hat das Bundesverfassungsgericht das neue Grundrecht auf die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme entwickelt. Dieses Grundrecht ist – ebenso wie das im Volkszählungsurteil 1983 entwickelte Recht auf informationelle Selbstbestimmung – eine besondere Ausprägung des allgemeinen Persönlichkeitsrechts. Das neue Grundrecht schützt die Bürgerinnen und Bürger vor neuartigen Gefahren, die mit der Nutzung informationstechnischer Systeme verbunden sind. Angesichts des rasanten technischen Fortschritts und der gewandelten Lebensverhältnisse sind derartige Systeme allgegenwärtig und vielfach unverzichtbar. Das Internet als komplexer Verbund von Rechnernetzen verdeutlicht exemplarisch diese Entwicklung. Folge dieser Nutzung ist die automatisierte und vielfach ohne das Wissen des Betroffenen vollzogene Erhebung und Verarbeitung von Daten über das Verhalten und die Eigenschaften des Nutzers. Hieraus können weit reichende Persönlichkeitsprofile gewonnen werden. Das neue Grundrecht gilt für alle informationstechnischen Systeme, die umfängliche oder aussagekräftige personenbezogene Daten enthalten können. Das Grundrecht schützt das Vertrauen der Berechtigten, selbstbestimmt über ihr System, dessen Leistungen, Funktionen und Inhalte entscheiden zu können. Können Dritte unberechtigt auf dieses System zugreifen, liegt bereits ein Grundrechtseingriff vor – unabhängig davon, ob der Zugriff leicht oder nur mit erheblichem Aufwand möglich ist.

### Einstweilige Anordnungen des Bundesverfassungsgerichts zur Vorratsdatenspeicherung

Mit einem Beschluss vom 28. Oktober 2008 schränkte das Bundesverfassungsgericht den Zugang zu Daten, die aufgrund des „Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ gespeichert wurden, weiter ein. Bereits im März 2008 hatte das Gericht entschieden, dass bis zur endgültigen Entscheidung in der Sache die gespeicherten Verkehrsdaten nur den zuständigen Behörden zur Verfügung gestellt werden dürfen, wenn sie für die Verfolgung von so genannten schweren Straftaten i. S. d. § 100a der Strafprozessordnung (z. B. Mord, Raub, Erpressung) genutzt werden. Da verschiedene Bundesländer innerhalb des letzten Jahres gesetzliche Ermächtigungsgrundlagen geschaffen haben, die ihren Nachrichtendiensten und Behörden im Bereich der Gefahrenabwehr den Zugang zu den Vorratsdaten ermöglicht, hat das Gericht in seiner Entscheidung vom Oktober die Beschränkung der Nutzungsmöglichkeit auf diese Behörden ausgedehnt.

**Verwaltungsgericht Berlin entbindet Provider von Pflicht zur Vorratsdatenspeicherung**

Mit einer einstweiligen Anordnung vom 17. Oktober 2008 untersagte das Berliner Verwaltungsgericht der Regulierungsbehörde (Bundesnetzagentur) einen Provider, der sich weigerte der Verpflichtung zur Vorratsdatenspeicherung nachzukommen, entsprechend der gesetzlichen Möglichkeiten mit einem Bußgeld zu belegen. Das Gericht begründet seine Entscheidung damit, dass es für die zur Datenspeicherung notwendigen technischen und personellen Investitionen der TK-Anbieter keine hinreichende Entschädigungsregelung auf Kostenseite gäbe. Daher wiege das Risiko des finanziellen Schadens für die Provider schwerer als die Vorteile des Staates, die er von der Möglichkeit des Zugangs auf gespeicherte Daten hätte. Der klagende Provider bietet seine Dienstleistungen vorwiegend für Geschäftskunden an, was die Wahrscheinlichkeit eines Zugriffs der Strafverfolgungsbehörden auf die gespeicherten Vorratsdaten erheblich reduziert. Die Entscheidung entfaltet zunächst nur gegenüber dem klagenden Anbieter Folgen. Um ebenfalls vorerst von der Verpflichtung zur Vorratsdatenspeicherung entbunden zu werden, haben andere TK-Anbieter jeweils auch einen entsprechenden Antrag gestellt. Die Regulierungsbehörde hat derweil die Entscheidung des VG Berlin beim zuständigen Berufungsgericht angefochten.

**Vorlagebeschluss des Verwaltungsgerichts Wiesbaden zur Vorratsdatenspeicherungs-Richtlinie**

Das Verwaltungsgericht Wiesbaden entschied mit Beschluss vom 27. Februar 2009 die Frage, ob die Richtlinie zur Vorratsdatenspeicherung (2006/24/EG) mit dem europäischen Recht vereinbar ist, dem Europäischen Gerichtshof für eine Vorabentscheidung vorzulegen. Das Gericht sieht in der Datenspeicherung auf Vorrat einen Verstoß gegen das Grundrecht auf Datenschutz. Der Einzelne würde keine Veranlassung für den mit der Vorratsdatenspeicherung verbundenen Eingriff geben, könne aber auch bei seinem legalen Verhalten wegen der Risiken des Missbrauchs und des Gefühls der Überwachung eingeschüchtert werden. Daher sei der nach Artikel 8 EMRK zu wahrende Verhältnismäßigkeitsgrundsatz durch die Richtlinie nicht gewahrt. http://www.vorratsdatenspeicherung.de/content/view/301/1/lang,de/

## C. Wichtige spezifische Themen

Das Jahr 2008 war durch das Bekanntwerden einer Reihe von schwerwiegenden Datenschutzverstößen geprägt. Bereits Anfang 2008 wurde in den Medien über die heimliche Überwachung von Mitarbeitern eines großen Lebensmitteldiscounters berichtet. Im Frühjahr und Sommer 2008 wurden in immer rascherer Folge die Ausmaße des illegalen Handels mit Anschriften, aber auch Bankverbindungsdaten aufgedeckt. Ein großes deutsches Telekommunikationsunternehmen war gleich mehrfach vertreten, von der Kommunikationsüberwachung bei Spitzenmanagern und Betriebsräten bis hin zu betrügerischen Call-Centern und schlichten Datenpannen erheblichen Ausmaßes. Aber auch Meldeämter und andere öffentliche Stellen waren betroffen.

Die Bundesregierung legte daraufhin Ende des Jahres eine Novelle des BDSG vor, derzufolge insbesondere die Privilegierung des Handels mit personenbezogenen Daten zu Werbezwecken abgeschafft werden soll. Die Betroffenen sollen nunmehr regelmäßig einwilligen müssen, bevor ihre Daten zu Werbezwecken genutzt und weitergegeben werden dürfen. Neben weiteren Maßnahmen soll zudem ein Datenschutzaudit eingeführt werden. Unternehmen, die sich einem Prüfregime unterwerfen und - noch zu definierende - strengere Datenschutzanforderungen erfüllen, sollen danach mit einem Gütesiegel belohnt werden. Am vorgelegten Gesetzentwurf ist zum Teil erheblicher Änderungsbedarf angemeldet worden. Er wird derzeit im Bundestag beraten. Sein Ausgang ist ungewiss.

Das Bundeskabinett hat am 14. Januar 2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BR 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, insbesondere im Hinblick auf die Speicherung und Auswertung von Verkehrs- und Nutzungsdaten des Internet. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder warnte in einer Entschließung davor, dass die zur Stärkung der IT-Sicherheit vorgesehenen Maßnahmen nicht zu Lasten des Datenschutzes gehen dürfen.

Das Bundeskabinett hat ferner am 4. Februar 2009 den Entwurf eines Bürgerportalgesetzes beschlossen. Der Entwurf verfolgt die Ziele, die Vertraulichkeit, die Integrität und die Authentizität im E-Mail Verkehr zu gewährleisten. Im Kern geht es bei den Bürgerportalen um die Schaffung einer sicheren Infrastruktur für die E-Mail-Kommunikation (De-Mail) und die Speicherung persönlicher Daten (De-Safe), die bei der Kommunikation zwischen Bürger und Verwaltung benötigt werden, etwa Urkunden und Bescheinigungen. Die Realisierung und der Betrieb der Dienste sollen allein privaten Unternehmen obliegen. Der BfDI hat vorgeschlagen, die Kommunikation durch eine Ende-zu-Ende-Verschlüsselung zwischen Absender und Empfänger zu sichern. Auch die Ablage persönlicher Daten in einem elektronischen Safe ist nur wirklich sicher, wenn die Daten verschlüsselt gespeichert werden und ausschließlich der Betroffene den elektronischen Schlüssel dazu besitzt.



## Griechenland

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

**Neues Gesetz zur Verbesserung der Privatsphäre bei Telefongesprächen**

Nach einem Skandal, der im Jahr 2005 durch die Medien ging, als bekannt wurde, dass etwa 200 Mobiltelefone abgehört und Gespräche aufgezeichnet wurden (darunter auch die des griechischen Premierministers und anderer Regierungsmitglieder), wurde im Jahr 2008 ein neues Gesetz (Gesetz 3674/2008) zur Verbesserung der Privatsphäre bei Telefongesprächen verabschiedet.

Das neue Gesetz umfasst die folgenden wesentlichen Vorschriften:

- Alle Telekommunikationsanbieter müssen eine Sicherheitspolitik vorweisen können. Jede Politik sowie Änderungen/Aktualisierungen müssen von der griechischen Behörde für das Kommunikationsgeheimnis (ADAE, diese Behörde unterscheidet sich von der Datenschutzbehörde GDSB) genehmigt und der GDSB sowie der Regulierungsbehörde für Telekommunikation und Post gemeldet werden.
- Alle Anbieter müssen einen Angestellten bestimmen, der dafür zuständig ist, dass die Privatsphäre bzw. das Telekommunikationsgeheimnis eingehalten und geschützt wird. Der Name dieses Angestellten ist den zuständigen Behörden mitzuteilen.
- Anbieter von Telekommunikationsdiensten sind verpflichtet, alle erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Privatsphäre sämtlicher Telekommunikationen zu gewährleisten sowie regelmäßige Prüfungen ihrer Systeme und Infrastruktur durchzuführen.
- Alle Angestellten des Anbieters sind zur Geheimhaltung verpflichtet.
- Sämtlicher Sprechverkehr, der über Kanäle außerhalb des Aufsichtsbereichs des Anbieters erfolgt, muss durch Verschlüsselungstechniken geschützt werden.
- Im Falle von Mobilfunk-/digitalen Vermittlungszentralen müssen alle Verwaltungsprozesse auf der Software jedes Zentrums in Sicherheitsprotokollen gespeichert werden. Diese Protokolle sind auf ordnungsgemäß geschützten Medien zu speichern, die die Integrität der Protokolle gewährleisten können. Jeglicher direkter oder indirekter Zugang zu diesen Dateien ist streng verboten. Weitere Einzelheiten zur Pflege dieser Protokolle werden in einer Verordnung der ADAE festgelegt.
- Die ADAE muss regelmäßige Kontrollen/Prüfungen der Hard- und Software-Infrastruktur des Anbieters durchführen, um die Einhaltung der Gesetze zu gewährleisten.
- Im Fall einer Verletzung der Sicherheitsbestimmungen oder bei einem Risiko einer Verletzung der Sicherheitsbestimmungen muss der für die Gewährleistung der Gemeinhaltung zuständige Angestellte des Anbieters den Anbieter oder den gesetzlichen Vertreter des Anbieters, den Staatsanwalt, die ADAE sowie alle potenziell betroffenen Kunden informieren. Die Meldung muss schriftlich erfolgen. Ist eine direkte Kommunikation nicht möglich, kann eine andere geeignete Methode gewählt werden.
- Nach der Meldung über die Verletzung der Sicherheitsbestimmungen und bis zu dem Zeitpunkt, an dem der Staatsanwalt und die ADAE spezifische Maßnahmen anordnen, darf kein Angestellter des Anbieters Informationen zur Verletzung der Sicherheitsbestimmungen oder des Risikos einer Verletzung der Sicherheitsbestimmungen offen legen. Alle Angestellten müssen geeignete Maßnahmen zur Sicherung jedweder Beweise ergreifen.
- Als Teil dieses neuen griechischen Gesetzes wurde das Strafgesetzbuch entsprechend abgeändert. Verstöße gegen die Geheimhaltung von Telefongesprächen, einschließlich Daten zu Inhalt, Traffic und Standort, werden als Ordnungswidrigkeit eingestuft. Etwaige durch diese Verstöße erhaltene Beweise sind in Strafsachen vor Gericht nicht zugelassen.
- Letztlich muss ein nationaler Sicherheitsplan zum Schutz der elektronischen Kommunikation (nicht nur für Telefongespräche) im öffentlichen Sektor sowie für die Anbieter von elektronischen Kommunikationsnetzen und -diensten erarbeitet werden. Die Empfänger des Sicherheitsplans müssen die Maßnahmen innerhalb von 6 Monaten umsetzen. Zu diesem Zweck wurde ein Gesetzgebungsausschuss eingerichtet, in dem auch die GDSB vertreten ist. Bisher hat die griechische Regierung jedoch noch nicht die Initiative ergriffen.

**Rechtmäßiges Abfangen elektronischer Kommunikationen in Fällen von Kinderpornografie**
Im Einklang mit Gesetz 3625/2007 wird das Fakultativprotokoll zum Übereinkommen der UN über die Rechte des Kindes betreffend den Verkauf von Kindern, die Kinderprostitution und die Kinderpornografie vom griechischen Parlament ratifiziert. Nach diesem Gesetz wird Artikel 348A des griechischen Strafgesetzbuches abgeändert, so dass Kinderpornografie über elektronische Systeme oder über das Internet als Straftat eingestuft wird.

Im Einklang mit Gesetz 3666/2008 (Artikel 2, Paragraph 7a) wird die Liste der Straftaten, bei denen eine rechtmäßige Überwachung elektronischer Kommunikationen gestattet ist, abgeändert und Kinderpornografie aufgenommen.

**Richtlinie 2006/24/EG**
Der Gesetzgebungsausschuss des Justizministeriums hat einen Gesetzesentwurf zur Umsetzung der Richtlinie 2006/24/EG in nationales Recht abgeschlossen. Der Entwurf wurde noch nicht vom Parlament verabschiedet.

## B. Bedeutende Rechtsprechung

**Entscheidung 27/2008**
Die griechische Datenschutzbehörde (DSB) wurde über einen Zeitungsartikel über an Sekundarschulen in der Präfektur Karditsa installierte CCTV-Systeme informiert. Die DSB stufte die durch die Kameraüberwachung des Schulhofes und der Gänge erfolgende Verarbeitung der personenbezogenen Daten von Schülern und Lehrern als gesetzeswidrig ein. Es wurde entscheiden, dass eine solche Verarbeitung unverhältnismäßig sei, da der Zweck (Sicherheit auf dem Gelände sowie Zugangskontrolle im Hinblick auf Fahrzeuge und Dritte) auch durch weniger in die Rechte der Betroffenen eingreifende Maßnahmen hätte erreicht werden können.

**Entscheidung 30/2008**
Nach einer von einem Betroffenen eingereichten Beschwerde und einer daraufhin von der GDSB durchgeführten Prüfung wurde bestätigt, dass ein Unternehmen seinen Kunden einem Lügendetektordienst (Anwendung zur technischen Stimmanalyse, LVA = Layer Voice Analysis) einer dritten Partei unterzog, um herauszufinden, ob der Betroffene die Wahrheit sagte oder nicht. Die DSB entschied, dass die Verwendung dieser speziellen Anwendung zur Beantwortung der Frage, ob eine Person die Wahrheit sagt, während eines Telefonats und ohne vorherige Information der betreffenden Person gegen Artikel 4 von Gesetz 3471/2006 verstößt.

**Entscheidung 48/2008**
Auf einen Antrag des Nationalen Sozialversicherungsinstituts (NSVI) hin gab die GDSB eine Stellungnahme zu folgendem Thema ab. Der Vorsitzende der oben genannten Behörde stellte 330 Arbeitsverträge zwischen Einzelpersonen und dem NSVI aus. Die GDSB befand, dass es nicht gegen das Datenschutzgesetz verstoße, den zuständigen Mitgliedern des Parlaments den Zugang zu oben genannter Entscheidung, einschließlich der Namen und Adressen der 330 für die spezifischen Verträge ausgewählten Personen sowie aller zu diesem Zweck eingereichten Bewerbungen und dazugehörigen Unterlagen zu gewähren, damit die Mitglieder des Parlaments die Legitimität der Entscheidungen überprüfen können. Darüber hinaus wurde entschieden, dass die Methode, nach der die zuständigen Mitglieder des Parlaments Zugang zu den relevanten Daten erhalten würden, vom NSVI und dem Parlament vereinbart werden sollte. Die Entscheidung der GDSB gründete auf der Idee, dass die Gewährung des Zugangs zu den oben genannten Daten für die zuständigen Mitglieder des Parlaments zum Zwecke der parlamentarischen Kontrolle erforderlich sei, die darauf abzielt, zu verifizieren, ob nach dem Vergleich der Qualifikationen ausgewählter und abgelehnter Bewerber auch tatsächlich die qualifiziertesten Personen zum Abschluss von Arbeitsverträgen mit dem NSVI ausgewählt wurden.

**Entscheidung 50/2008**
Auf einen Antrag eines früheren Bewohners eines Waisenhauses hin entschied die GDSB, dass einem adoptierten Erwachsenen rechtmäßig Zugang zu den in der Adoptionsakte vermerkten personenbezogenen Daten seiner biologischen Eltern gewährt werden darf, damit er sie suchen kann. Dies umfasst sämtliche Informationen zur Identität der biologischen Eltern sowie alle sonstigen Informationen, die dazu beitragen könnten, dass der Adoptierte seine Eltern finden kann.

**Entscheidung 52/2008**
Bei der GDSB ging ein Antrag einer Investmentbank auf Genehmigung für die Installation und den Betrieb eines biometrischen Systems eins, das den Zugang zu spezifischen elektronischen Anwendungen der Bank auf der Grundlage von Fingerabdrücken der Angestellten kontrolliert. Die GDSB entschied mit Mehrheitsbeschluss, dass diese spezielle Datenverarbeitung im Prinzip nicht gegen die Bestimmungen von Gesetz 2472/1997 verstößt, da sie ausschließlich der Zugangskontrolle für bestimmte Angestellte dient, die Transaktionen größerer Geldmengen durchführen. Die GDSB entschied, dass eine Verarbeitung von Daten rechtmäßig ist, wenn es Ziel der Verarbeitung ist, die sichere Durchführung von Transaktionen zu gewährleisten und Geldwäsche oder sonstige illegale Handlungen zu verhindern. Die Behörde entschied außerdem, dass die spezielle Verarbeitung von Daten aus den folgenden Gründen nicht unverhältnismäßig ist: a) das betreffende System wird in einer Umgebung mit hohen Sicherheitsstandards und für spezifische Anwendungen bei der Transaktion von Geldbeträgen verwendet, der Anteil der Angestellten, die das System nutzen ist im Verhältnis zu dem durch die Verarbeitung verursachten Eingreifen in die Privatsphäre der Angestellten nur gering; b) das System ist verhältnismäßig im Hinblick auf die spezifischen Bankangelegenheiten, bei denen es hauptsächlich um Investmentaktivitäten von Transportfirmen geht; und c) der Betrieb des Systems dient den Angestellten selbst, da es andere von einer illegalen Verwendung ihrer Identität abhält und gleichzeitig bei falschen oder rechtswidrigen Transaktionen sicherstellt, dass der Verantwortliche zur Rechenschaft gezogen werden kann.

**Entscheidung 66/2008**
Bei der GDSB ging eine Beschwerde einer Person gegen eine Bank ein, die der Person den Zugang zu ihren Daten nicht gestattet hatte. Die GDSB entschied, dass der Kontrolleur nicht befugt ist, einer Person mitzuteilen, dass ein Untersuchungsverfahren hinsichtlich der Legalisierung von Einkommen aus Straftaten gegen sie läuft oder dass Informationen für den Abschluss der Untersuchungen an den zur Bewertung und Untersuchung der oben genannten Informationen zuständigen Ausschuss weitergegeben wurden (Artikel 31 von Gesetz 3691/08). Die Beschränkung des Rechts auf Zugang zu den Daten endet jedoch, wenn die Bank die erfassten Daten und Informationen zu einer Person aufgrund der Einschätzung, dass die erfassten Informationen kein Beweis für die Legalisierung von Einkommen aus Straftaten sind, nicht an den zuständigen Ausschuss überträgt. Wenn zudem auch personenbezogene Daten von Dritten vom Kontrolleur verarbeitet wurden, die die Art und Weise beeinflussen, auf die die Daten der betroffenen Person verarbeitet wurden, dann betreffen die spezifischen Daten allein die betreffende Person und diese hat dann das Recht auf Zugang zu ihren Daten.

## Ungarn

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

**Richtlinie 95/46/EG**
Keine nennenswerten Ereignisse.

**Richtlinie 2002/58/EG**
Die allgemeinen Vorschriften für elektronische Werbung wurden stark abgeändert. Gemäß Gesetz XLIII aus dem Jahr 2008 über die Kriterien und die Beschränkungen betreffend Werbeaktivitäten von Unternehmen *„darf Werbung an natürliche Personen als Empfänger einer Direktmarketing-Maßnahme nur dann per elektronischer Post oder vergleichbarem Instrument verschickt werden, wenn der Empfänger zuvor unmissverständlich seine ausdrückliche Zustimmung erteilt hat"*, solche Werbung zu erhalten. In diesen Fällen ist die nationale Kommunikationsbehörde für die Aufsicht zuständig und befugt, zu entscheiden, ob die betreffende elektronische Kommunikation als Werbung einzustufen ist oder nicht und ob durch den Versand gegen das Gesetz verstoßen wurde. Die wichtigste Änderung ist die, dass Beschränkungen nur für Werbung gelten, die an natürliche Personen verschickt wird. Daten, die nicht zu natürlichen Personen gehören, werden nicht so streng geschützt.

### B. Bedeutende Rechtsprechung

Im Jahr 2006 beantragte eine zivile Organisation eine Untersuchung von Philip Morris Hungary Ltd. durch den Datenschutzbeauftragten im Hinblick auf die Verarbeitung personenbezogener Daten im Rahmen einer Direktmarketing-Kampagne (z. B. Punkte sammeln). Die erfassten personenbezogenen Daten wurden darüber hinaus verwendet, um individualisierte Broschüren mit Informationen zu Tabakprodukten zu verschicken. Der Datenschutzbeauftragte beantragte eine Stellungnahme der ungarischen Wettbewerbsbehörde zur Frage, ob solche Direktmarketingmethoden als Werbung für Tabakprodukte eingestuft werden können.

Gemäß Abschnitt 13 (1) - (2) von Gesetz LVIII aus dem Jahr 1997 über Werbeaktivitäten von Unternehmen *„ist es verboten, für Tabak zu werben oder indirekt für Tabakprodukte zu werben"*. Auf der Grundlage der Stellungnahme der Wettbewerbsbehörde kam der Datenschutzbeauftragte zu dem Schluss, dass selbst mit Zustimmung der betreffenden Person keine personenbezogenen Daten erfasst und für den Versand individualisierter Broschüren zur Bewerbung von Tabakprodukten weiterverwendet werden dürfen. Aus diesem Grund riet der Datenschutzbeauftragte dem Datenverarbeiter, diese Praxis einzustellen und beauftragte ihn per Verordnung, unrechtmäßig verarbeitete Daten zu sperren, zu löschen oder zu vernichten.

Gegen diese Verordnung kann über administrative Kanäle kein Widerspruch eingelegt werden, daher hat Philip Morris Hungary Ltd. vor dem zuständigen Gericht Klage gegen die Verordnung eingereicht. Laut der Entscheidung des Gerichts „können die Informationen nicht als Werbung eingestuft werden, da der Empfänger selbst gewünscht hatte, dass sie in einem verschlossenen Umschlag zugeschickt werden". In Anbetracht der Entscheidung des Gerichts nahm der Datenschutzbeauftragte die Verordnung zurück. Der Fall wurde vom Gericht abgewiesen. Später trat das Gesetz XLIII aus dem Jahr 2008 über die Kriterien und die Beschränkungen betreffend Werbeaktivitäten von Unternehmen in Kraft.

Angesichts des neuen Gesetzes hielt es der Datenschutzbeauftragte für notwendig, den Fall neu aufzurollen und die Aktivitäten zur Datenverarbeitung zu untersuchen. Nach dem neuen Gesetz gelten Informationen, die zweifelsfrei dem Empfänger zugeschickt werden, als verbotene Werbung für Tabakprodukte. Daher werden die erfassten Daten auf eine Art und Weise weiterverwendet, die mit den angegebenen, expliziten und legitimen Zwecken nicht vereinbar ist. Als Folge dessen hat der Datenschutzbeauftragte die Datenverarbeitung per Verordnung verboten. Dieses Mal wurde seitens Philip Morris Hungary Ltd. keine Berufung vor Gericht eingelegt.

### C. Wichtige spezifische Themen

Der Datenschutzbeauftragte hat eine Stellungnahme zu einem Dekret des Finanzministeriums veröffentlicht, das den psychologischen Eignungstest vor einer Anstellung im öffentlichen Dienst bei der ungarischen

Zoll- und Finanzkontrollverwaltung (APEH) regelt. Laut dem Dekret dürfen Personen, die sich in psychiatrischer Behandlung befinden oder vermutlich (wahrscheinlich) an einer psychischen Krankheit leiden, die ihre Anpassung und Integration in die Behörde behindert oder die ihre Effizienz durch die Beeinflussung der Aktivitäten der Behörde beeinträchtigt, nicht in einer solchen Position arbeiten. Der Datenschutzbeauftragte betonte, dass Sonderkategorien für Daten wie z. B. Gesundheitsdaten – sofern nicht per Gesetz angeordnet – nur nach schriftlicher Genehmigung der betreffenden Person verarbeitet werden dürften. Die Rechtsgrundlage selbst ermögliche die Verarbeitung nicht. Es müssten auch andere Kriterien erfüllt sein, insbesondere hinsichtlich der Zweckbeschränkung bezüglich der Verarbeitung. Die Tatsache, dass sich eine Person in psychiatrischer Behandlung befunden habe, bedeute nicht zwangsläufig, dass die Anstellung dieser Person die rechtmäßige Aktivität der Behörde beeinflusst oder gefährdet. Er betonte weiterhin, dass die Würde des Menschen gefährdet sei, wenn einer Person aufgrund einer wahrscheinlichen Krankheit eine Anstellung verwehrt würde. Die Vorschrift des betreffenden Dekrets könnte zu Diskriminierungen führen, die eindeutig gegen die ungarische Verfassung und die Bestimmungen von Gesetz CXXV aus dem Jahr 2003 über die Förderung der Gleichbehandlung und die Chancengleichheit verstoßen. Er betonte, dass ein solches ministerielles Dekret als Rechtsquelle nicht die Rechtsgrundlage für die Verarbeitung von Daten bieten könne. Lediglich ein von der Nationalversammlung verabschiedetes Gesetz könne dies. Aus diesem Grund bat der Datenschutzbeauftragte den Finanzminister, das Dekret zurückzunehmen.

In einem anderen Fall untersuchte der Datenschutzbeauftragte die Datenverarbeitungsaktivitäten eines multinationalen Unternehmens, das GPS-Systeme einsetzt. Die GPS-Systeme wurden in Firmenwagen von Angestellten mit flexiblen Arbeitszeiten eingesetzt, um den Standort der Fahrzeuge jederzeit bestimmen zu können. Es wurde jedoch nicht zwischen Daten unterschieden, die während bzw. die außerhalb der Arbeitszeiten erfasst wurden. Somit verarbeitete das Unternehmen also personenbezogene Daten ohne Zustimmung des betreffenden Datensubjektes. Die Verarbeitung erfolgte außerdem nicht im Einklang mit dem Prinzip der Zweckbeschränkung, da die Standortdaten außerhalb der Arbeitszeiten erfasst wurden. Der Datenschutzbeauftragte gab in seiner Stellungnahme an, dass GPS-Systeme Daten ausschließlich während der Arbeitszeiten übertragen dürften. Außerhalb dieser Zeiten dürften keine personenbezogenen Daten vom Arbeitgeber verarbeitet werden. Um die Verarbeitung gesetzmäßig zu gestalten, müsste den Angestellten die Möglichkeit gegeben werden, den GPS-Sender abzuschalten, wenn der Wagen zu privaten Zwecken genutzt wird.

Im Oktober erhielt der Datenschutzbeauftragte den Gesetzesentwurf zur Einrichtung des zentralen Kreditmeldesystems. In seiner Stellungnahme gab der Datenschutzbeauftragte an, er sei gegen die Einführung der so genannten „Positivliste".

# Irland

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

Beide Richtlinien wurden vollständig in irisches Recht umgesetzt. Zu den Entwicklungen in der Gesetzgebung, die eine signifikante Auswirkung auf den Datenschutz in Irland haben, zählten im Jahr 2008 neue Verordnungen zur Änderung der Gesetzgebung zur Inkraftsetzung der Richtlinie über den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG) in Irland. Die neuen Richtlinien sehen höhere Strafen für Vergehen im Hinblick auf unaufgeforderte Kommunikation vor und gewährleisten, dass die Beweislast für den Vertragsschluss durch einen Abonnenten beim Beklagten liegt.

Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden (zur Änderung der Richtlinie 2002/58/EG) war bis Ende 2008 noch nicht in irisches Recht umgesetzt worden. Die Verabschiedung eines Gesetzes durch das Parlament zur Inkraftsetzung der Richtlinie wird im Laufe des Jahres 2009 erwartet.

## B. Bedeutende Rechtsprechung

In den meisten Fällen, in denen Beschwerden im Einklang mit Abschnitt 10 der irischen Datenschutzgesetze von 1988 und 2003 beim Datenschutzbeauftragten eingereicht wurden, kam es zu einer gütlichen Einigung ohne formalen Beschluss oder Vollstreckungsmaßnahme. Eine solche gütliche Einigung kann beispielsweise einen finanziellen Beitrag durch den betreffenden Datenschützer an den Geschädigten oder an eine geeignete wohltätige Einrichtung bedeuten. Gegebenenfalls können auch Vollstreckungsmaßnahmen angewendet werden – so zum Beispiel, wenn der Dateninhaber die Zugangsrechte der Geschädigten nicht respektiert. In einigen Fällen werden Dateninhaber auch in Fallstudien im Jahresbericht des Kommissars namentlich erwähnt. Im Laufe des Jahres 2008 war der Datenschutzbeauftragte an Gerichtsverfahren zu den Rechten von Personen im Rahmen der Datenschutzgesetze von 1988 und 2003 sowie der Rechtsverordnung 535 des Jahres 2003 (zur Umsetzung der Richtlinie 2002/58/EG in Irland) beteiligt. Hierzu gehörten:

**Beschwerde gegen eine Aufforderung des Datenschutzbeauftragten zur Löschung von Daten**

Im November 2008 ließ das zuständige Gericht (Dublin Circuit Court) eine Berufung eines Datenkontrolleurs gegen einen durch den Datenschutzbeauftragten gemäß Artikel 10 der Datenschutzgesetze von 1988 und 2003 (der die Befugnis zur Aufforderung einer Löschung von Daten gemäß Artikel 28 von Richtlinie 95/46/EG überträgt) erlassenen Vollstreckungsbescheides zu. In dem Fall ging es um bestimmte Aufzeichnungen bei psychiatrischen Behandlungen, die vom Datenkontrolleur einbehalten wurden. Im Einklang mit Abschnitt 6A der Datenschutzgesetze (der Artikel 14 a der Richtlinie umsetzt) beantragte der Betroffene die Löschung dieser Aufzeichnungen aufgrund der durch die Einbehaltung verursachten Belastung. Der Antrag wurde vom Datenkontrolleur abgelehnt. Der Datenschutzbeauftragte kam zu dem Schluss, dass der Betroffene einen berechtigten Grund hatte, der schwerer wiegt als die durch den Datenkontrolleur vorgebrachten Gründe für die Einbehaltung der Aufzeichnungen. Dementsprechend erließ der Datenschutzbeauftragte einen Bescheid zur Löschung der Daten. Der Datenkontrolleur legte Berufung gegen den Bescheid ein. Die Berufung wurde zugelassen.

**Datenschutzbeauftragter verteidigt erfolgreich die Berufung gegen eine gesetzliche Informationsmitteilung**

Der Datenschutzbeauftragte hat die Berufung einer Zeitung gegen eine Informationsmitteilung, die im Zusammenhang mit einer Untersuchung der Unterlassung der Zeitung, personenbezogene Daten zu einem Bürger herauszugeben, erfolgreich verteidigt. Die Zeitung hatte angeführt, dass sie gemäß der in Abschnitt 22A der irischen Datenschutzgesetze (der Artikel 9 der Richtlinie umsetzt) genannten Ausnahme nach dieser Mitteilung keine weiteren Daten herausgeben müsse. Die Zeitung argumentierte, dass die Herausgabe dieser Informationen die Ausnahme in Abschnitt 22A untergraben würde. Das Gericht wies die Berufung mit der Begründung zurück, dass die

Ausnahme nicht für die Untersuchungsbefugnisse des Datenschutzbeauftragten gemäß Abschnitt 10 und Abschnitt 12 der Datenschutzgesetze gelte.

**Strafverfolgung wegen des Versands unaufgeforderter Textnachrichten (SMS) – Zusammenarbeit mit dem Datenschutzbeauftragten der Isle of Man**

Nach Beschwerden über unaufgeforderte Text nachrichten startete die Datenschutzbehörde die Untersuchung eines Unternehmens mit Hauptsitz außerhalb der irischen Gerichtsbarkeit (auf der Isle of Man). Das Unternehmen beschäftigte jedoch Personal in Dublin und hatte technische Infrastruktur in Irland zum Versand der Nachrichten verwendet. Ein Team der Datenschutzbehörde sammelte im Rahmen einer Prüfung vor Ort Beweise. Mit der Unterstützung des Datenschutzbeauftragten der Isle of Man konnten weitere Beweise aus dieser Gerichtsbarkeit gesammelt werden. Im November 2008 fand eine strafrechtliche Verfolgung gemäß Verordnung 535 aus dem Jahr 2003 statt (die Richtlinie 2002/58/EG in Irland umsetzt). Das Gericht verhängte Geldstrafen, nachdem sich das betreffende Unternehmen für schuldig bekannt hatte und nachdem zugegeben wurde, dass die betreffenden Mobilfunknummern nicht korrekt für den Empfang von Werbe-Textnachrichten registriert waren.

**Strafrechtliche Verfolgung aufgrund der Nichteinhaltung der Befugnisse des Datenschutzbeauftragten im Hinblick auf den Zugang zu Daten**

Nach wiederholten Versuchen, Informationen von einem staatlichen Unternehmen im Hinblick auf die Untersuchung einer Beschwerde zu erhalten, erließ die Datenschutzbehörde eine Informationsmitteilung, die das Unternehmen dazu aufforderte, zu kooperieren und die zur Erfüllung der rechtlichen Pflichten der Datenschutzbehörde erforderlichen Daten herauszugeben. Das Unternehmen verabsäumte es, die angefragten Informationen innerhalb der Frist von 21 Tagen herauszugeben. Die Datenschutzbehörde hat aufgrund dieses Versäumnisses im Juni 2008 eine strafrechtliche Verfolgung eingeleitet. Das Unternehmen bekannte sich nicht schuldig im Sinne der Anklage, wurde jedoch zu einer Geldstrafe verurteilt. Zum ersten Mal fühlte sich die Datenschutzbehörde verpflichtet, eine strafrechtliche Verfolgung gegen eine Organisation einzuleiten, da diese eine im Zusammenhang mit der Befugnis des Datenschutzbeauftragten zur Einsichtnahme in Daten ausgestellte Mitteilung ignorierte.

## C. Wichtige spezifische Themen

Wie bereits im Vorjahresbericht erwähnt, führte die Behörde im Sommer 2007 „Razzien" bei einer Reihe von Unternehmen durch, die im Bereich des SMS-Marketing tätig sind. Diese Verdachtskontrollen erfolgten in Reaktion auf zahlreiche Beschwerden, die die Datenschutzbehörde über diese Unternehmen erhielt, und im Rahmen einer Strategie, die vollen Befugnisse der Behörde einzusetzen, um gegen unerbetene Textnachrichten vorzugehen. Im Anschluss an diese Razzien wurden Strafverfahren gegen diese Unternehmen eingeleitet. Eines der Unternehmen hat die Rechtsgrundlage für diese Strafverfahren angefochten. Diese Anfechtung wurde vom Obersten Gerichtshof abgewiesen. Die Strafverfahren werden nunmehr weiter verfolgt.

# Italien

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

Die Richtlinie 95/46/EG wurde per Gesetz vom 31. Dezember 1996 (Gesetz Nr. 675), das ein halbes Jahr später in Kraft trat, in nationales Recht umgesetzt. Im Juni 2003 wurde ein neues Gesetz (Datenschutzgesetzbuch) verabschiedet, das die bestehenden Gesetze zusammenfasste und vollständig ersetzte. Letzteres Gesetz trat am 1. Januar 2004 in Kraft.

Die Richtlinie 2002/58/EG wurde mit dem genannten Datenschutzgesetzbuch in nationales Recht übernommen. Titel X des Gesetzbuches trägt die Überschrift „Elektronische Mitteilungen" (Paragraphen 121 bis 132).

### Neue Gesetzgebung

***Umsetzung der Richtlinie 2006/24/EG –*** Die Gesetzgebung über die Vorratsspeicherung von Traffic-Daten wurde mit der Hilfe der Datenschutzbehörde zur Umsetzung der Richtlinie 2006/24/EG geändert. Derzeit dürfen Traffic-Daten zu Zwecken der Strafverfolgung 24 Monate (Telefontraffic-Daten) bzw. 12 Monate (Traffic-Daten bei elektronischer Kommunikation) lang gespeichert werden – und zwar unabhängig von der zu verfolgenden Straftat. Durch die Gesetzesänderungen wurden die Rolle der italienischen Datenschutzbehörde (DSB) in diesem Bereich verdeutlicht und spezielle Strafen im Zusammenhang mit der Nichteinhaltung von Anforderungen hinsichtlich der Vorratsspeicherung von Traffic-Daten eingeführt (Abschnitt 162-bis des Datenschutzgesetzbuches).

***Vereinfachte Anforderungen für Sicherheitsmaßnahmen und -meldungen –*** Im Jahr 2008 wurden vereinfachte Maßnahmen betreffend bestimmte, von Selbständigen und KMU (einschließlich Handwerkern) zu erfüllende Datenschutzanforderungen eingeführt. Es wurden einige Bestimmungen des Datenschutzgesetzbuches geändert, um hinderliche Verfahren zu eliminieren, die insbesondere für die Annahme eines Mindestmaßes an Sicherheitsmaßnahmen gelten. Der Mechanismus zur Meldung von Verarbeitungsverfahren bei der italienischen DSB wurde ebenfalls weiter vereinfacht, insbesondere durch die Angabe, welche Informationen auf dem Meldeformular (im Einklang mit Artikel 17 der Richtlinie 95/46/EG) angegeben werden müssen. Darüber hinaus wurden spezielle Entscheidungen von der DSB veröffentlicht, um durch die Gewährleistung der Tatsache, dass die Rechte des Einzelnen gewahrt werden, zur Vereinfachung beizutragen (siehe unten).

***Grenzüberschreitende Datenflüsse*** – Bei grenzüberschreitenden Datenflüssen in Drittländer gab es eine wesentliche rechtliche Innovation. Weiterhin wurde auf einen von der italienischen DSB beim Parlament eingereichten Antrag die Formulierung des Datenschutzgesetzbuches dahingehend geändert, dass die Anwendung bindender Vorschriften in dieser Hinsicht ausdrücklich aufgeführt wurde. Dementsprechend besagt Abschnitt 44 des Datenschutzgesetzbuches nun, dass Datenübertragungen in Drittländer gestattet sind, wenn sie von der DSB genehmigt wurden und die Rechte der Datensubjekte angemessen schützen „wie von der Garante festgelegt, auch in Zusammenhang mit vertraglichen Schutzmaßnahmen bzw. andernfalls durch Verhaltensregeln, die für alle Unternehmen gelten, die demselben Konzern angehören."

***Sanktionen*** – Im Hinblick auf die Sanktionen, die die italienische DSB auferlegen darf, gab es signifikante Änderungen. Der Schwerpunkt dieser Änderungen, die die der DSB übertragenen Befugnisse erheblich erweiterten, liegt hauptsächlich auf verwaltungsrechtlichen Sanktionen, da die im Datenschutzgesetzbuch vorgesehenen strafrechtlichen Sanktionen praktisch unverändert geblieben sind. Im Allgemeinen sahen die Änderungen folgendermaßen aus: a. Erhöhung der Geldstrafen für die einzelnen Verstöße; b. Einführung neuer Kategorien strafbaren Verhaltens; c. Einführung von Mechanismen zur besseren Anpassung der Sanktionen an die jeweiligen Gegebenheiten je nach Schwere und Bedeutung des Vergehens und/oder der Größe der vom Verstoß betroffenen Datenbank, nach der Beteiligung einer großen Anzahl an Datensubjekten sowie nach dem finanziellen Status des Täters.

***Amtszeit der Mitglieder unabhängiger Aufsichtsbehörden*** – Bis ein Gesetz zur Angleichung der Verordnungen für unabhängige Aufsichtsbehörden in Kraft tritt, hat das Parlament die Amtszeit aller Mitglieder/Kommissare

solcher Behörden angeglichen – die Amtszeit wurde auf sieben Jahre festgelegt, eine weitere Amtszeit ist nicht möglich.

***Übereinkommen über Computerkriminalität*** – Italien hat das Übereinkommen des Europarates über Computerkriminalität aus dem Jahr 2001 ratifiziert. Die Ratifizierungsurkunde erforderte keine Integration einer allgemeinen Klausel in die Strafverfahrensvorschriften zur Gewährleistung des Schutzes der grundlegenden Menschenrechte, insbesondere des „Prinzips der Verhältnismäßigkeit" gemäß Artikel 15 des Übereinkommens. Diese Anforderung wurde von der italienischen DSB unter anderem entsprechend der Stellungnahme, die die Artikel 29 Datenschutzgruppe zum Entwurf des Übereinkommens veröffentlicht hatte, betont. Unsere DSB schlug vor, dass eine *Ad-hoc*-Klausel in jede rechtliche Bestimmung zur Regulierung von Untersuchungs- und Vorbereitungsmaßnahmen bei Strafverfahren integriert werden sollte, wodurch bei allen von der zuständigen Justiz- oder Polizeibehörde durchgeführten Untersuchungen und eingeleiteten verfahrensbezogenen Schritten die Relevanz und Verhältnismäßigkeit der Daten berücksichtigt und verhältnismäßige Maßnahmen ergriffen werden müssten. Die Ratifizierungsurkunde änderte auch die Bestimmungen über Traffic-Daten (Abschnitt 132 des Datenschutzgesetzbuches) und ermächtigte die Polizeibehörden, unter bestimmten Umständen IT- und/oder Internet-Dienstleistungsanbieter und -betreiber aufzufordern, Internet-Traffic-Daten – mit Ausnahme von Inhaltsdaten – maximal 90 Tage lang zu speichern und zu schützen, um Untersuchungen im Vorfeld von Gerichtsverfahren durchführen zu können bzw. im Hinblick auf die Feststellung und Vermeidung bestimmter Straftaten. Die von den Polizeibehörden ausgesprochene Aufforderung ist dem zuständigen Staatsanwalt zu melden und von ihm bestätigen zu lassen.

***Verwendung von Daten aus Telefonverzeichnissen zu Werbezwecken*** – Ein Regierungsdekret führte eine vorübergehende Ausnahmeregelung zur geltenden Gesetzgebung betreffend Telefonverzeichnisse ein, nachdem die Verarbeitung von Daten solcher Verzeichnisse zu Werbe- und/oder Marketingzwecken nur nach der vorherigen, freiwilligen, informierten und ausdrücklichen Zustimmung des Datensubjekts gestattet ist. Diese Ausnahmeregelung wurde von der italienischen DSB negativ aufgenommen, da sie die Sicherheitsmaßnahmen für Datensubjekte beeinträchtigt, die unter anderem durch Maßnahmen und Vorschriften unserer Behörde geschaffen wurden. Die neuen Vorschriften gestatten die rechtmäßige Verwendung personenbezogener Daten aus vor dem 1. August 2005 erstellten öffentlichen Telefonverzeichnissen zu Werbezwecken bis zum 31. Dezember 2009 ausschließlich durch entsprechende Datenkontrolleure, da besagte Datenbanken vor dem 1. August 2005 erstellt wurden.

***Videoüberwachung in Eigentumswohnungen*** – Die italienische DSB lenkte die Aufmerksamkeit des Parlaments und der Regierung auf die Zweckmäßigkeit der Inkraftsetzung von Gesetzen zur Regulierung bestimmter Fragen in Zusammenhang mit der Verarbeitung personenbezogener Daten, die durch den Einsatz von Ausrüstung zur Videoüberwachung in Eigentumswohnungen erfasst wurden. Insbesondere sprach sich die DSB für eine Regulierung des Prozesses zur Entscheidungsfindung im Hinblick auf die Installation von Videokameras in Eigentumswohnungen sowie für eine Festlegung der zur Genehmigung eines solchen Beschlusses erforderlichen Anzahl von Stimmen der Eigentümer aus.

***Parlamentarische Anhörungen*** – Die DSB wurde im Jahr 2008 einige Male zu wichtigen Fragen angehört, mit denen sich die zuständigen parlamentarischen Ausschüsse entweder im Rahmen von Untersuchungsmaßnahmen oder einer Debatte zur Verabschiedung von Gesetzen zur Umsetzung des Schutzes personenbezogener Daten befassten. Insbesondere wurde die Behörde zu Fragen angehört, mit denen sich der Justizausschuss im Abgeordnetenhaus (Unterhaus) im Rahmen einer Anhörung zum Gesetzesentwurf der Regierung zur Reform der Gesetzgebung über das Abfangen von Kommunikationen befasste. Die DSB trug im Rahmen einer Anhörung vor dem zuständigen Zweikammerausschuss auch zur Klärung von Fragen bei, die aus der Verarbeitung von und dem Zugang zu Daten des Steuerzahlerregisters entstanden. Weiterhin sind zwei informelle Anhörungen zu Fragen betreffend die Versicherungsbranche sowie zu Gesetzesentwürfen betreffend die Einführung eines Systems zur Betrugsprävention im Bereich Verbraucherkredite zu nennen.

## B. Bedeutende Rechtsprechung

***Strafrechtliche Verantwortung bei einer Veröffentlichung von Informationen über die Gesundheit eines Kindes durch einen Journalisten*** – Der italienische Kassationshof (die letztinstanzliche Justizbehörde) entschied, dass ein Journalist und der Geschäftsführer einer wöchentlichen Veröffentlichung strafrechtlich für die Veröffentlichung von Informationen über die Gesundheit der Tochter eines bekannten Nachrichtensprechers verantwortlich seien. Insbesondere wandte der Kassationshof die für Fälle unrechtmäßiger Verarbeitung von Daten, in denen gegen die „journalistischen Verhaltensregeln" verstoßen wird, vorgesehenen strafrechtlichen Maßnahmen an, die dem Datenschutzgesetzbuch beigefügt sind. Diese Entscheidung bestätigte den besonderen rechtlichen Status dieser Verhaltensregeln, da gemäß dem italienischen Datenschutzgesetz die Einhaltung des geltenden Datenschutzgesetzbuches eine Grundvoraussetzung für die rechtmäßige Verarbeitung personenbezogener Daten ist.

***Die vorsorgliche Beschlagnahmung von Bildern, die die Privatsphäre verletzen, ist rechtmäßig*** – Der Kassationshof entschied, dass ein Gericht rechtmäßig die vorsorgliche Beschlagnahmung von Bildern und Negativen in einer Zeitungsredaktion angeordnet hatte (Entscheidung Nr. 17408/2008), auf denen ein bekannter Politiker im Park seiner Villa zu sehen war. Das Thema wurde zuvor vor der italienischen DSB angesprochen, die feststellte, dass die Privatsphäre durch die Veröffentlichung der auf aufdringliche Art und Weise gemachten Bilder verletzt worden sei und verbat dementsprechend die weitere Veröffentlichung. Der Kassationshof entschied, dass die darauf hin von einem Gericht gegenüber einer anderen Zeitung, die die Bilder trotz des Verbotes der italienischen DSB erneut veröffentlicht hatte, angeordnete Beschlagnahmung rechtmäßig sei. Das Gericht befand – im Einklang mit den von der italienischen DSB vorgebrachten Gründen –, dass die Privatsphäre des Datensubjektes verletzt worden sei, da die betreffenden Bilder das Privatleben des Politikers gegen seinen Willen und auf seinem Privatbesitz zeigten und auf eine die Privatsphäre verletzende Art und Weise sowie unter Zuhilfenahme spezieller technischer Ausrüstung gemacht worden seien.

***Konkursverfahren und Strafregisterauszüge*** – Der Kassationshof entschied, dass – gemäß der kürzlich in Kraft gesetzten Gesetzgebung zu Konkursverfahren (Dekret Nr. 5/2006) – sämtliche Einträge zu Konkurserklärungen aus den von der für die Strafregisterauszüge zuständigen Behörde ausgestellten Bescheinigungen auf Antrag des Datensubjektes zu löschen sind, wenn das Konkurs-/Abwicklungsverfahren beendet wurde, sofern das betreffende Dekret die Bestimmungen zu den Entlastungen eines Konkursschuldners ausdrücklich außer Kraft gesetzt hat (Entscheidung Nr. 40675/2008).

## C. Wichtige spezifische Themen

### Gewährleistung der Sicherheit öffentlicher und privater Datenbanken

***Verarbeitung von Traffic-Daten durch Telefon- und Internetdienstanbieter:*** Die italienische DSB verabschiedete gemäß Abschnitt 132 des italienischen Gesetzes über die Privatsphäre eine allgemeine Vorschrift (mit Datum vom 17. Januar 2008) über die Speicherung und Verarbeitung von durch Telefon- und Internetdienstanbieter erzeugten Traffic-Daten. Ziel war es, eine bessere Sicherheit im Hinblick auf von Anbietern aus rechtlichen Gründen gespeicherten Traffic-Daten (auch zu Strafverfolgungszwecken) zu gewährleisten.

Die von der Garante entwickelten Maßnahmen verdeutlichen, wer welche Daten speichern darf und legen technische und organisatorische Maßnahmen zur Gewährleistung einer sicheren Speicherung der betreffenden Daten fest.

Insbesondere wurde klargestellt, dass Anbieter von Internetinhalten, Betreiber von Suchmaschinen, öffentliche Behörden/Organisationen, die ihrem Personal Telefon- und Internetnetzwerke zur Verfügung stellen und/oder Server anderer Organisationen zur Bereitstellung dieser Systeme verwenden, Internetcafés und vergleichbare Einrichtungen gemäß den in Richtlinie 2002/22/EG über den Universaldienst und in den Richtlinien 2002/58/EG und 2006/24/EG festgelegten Definitionen nicht in den Anwendungsbereich der betreffenden Verpflichtungen zur Vorratsspeicherung fallen. Zahlreiche technische Maßnahmen zum Schutz von Daten wurden bestimmt – unter anderem starke Authentifizierungs- und biometrische

Verfahren, eine gründliche Prüfung von Datenbanken und Computersystemen, die Verschlüsselung von Datenbanken, zentrale und geschützte Protokollierung sowie physische Sicherheitsmaßnahmen zum Schutz von Computerräumen und Datenzentren.

Unbeschadet der oben beschriebenen rechtlichen Änderungen müssen Telekommunikationsbetreiber besagte Maßnahmen bis 30. April 2009 umsetzen.

Diese Verlängerung wurde von der italienischen DSB als Reaktion auf im Juli von Gewerkschaften von Anbietern elektronischer Kommunikationsdienste eingereichte Anträge gewährt, da diese eine längere Frist zur vollständigen Umsetzung der betreffenden komplexen Sicherheitsmaßnahmen beantragt hatten.

***Systemverwalter:*** Die italienische DSB hielt es für notwendig, eine spezifische Maßnahme zu so genannten „Systemverwaltern" durchzuführen, um deren Bedeutung im Hinblick auf die Verarbeitung personenbezogener Daten zu betonen und sowohl Datenkontrolleuren als auch der breiten Öffentlichkeit die Sensibilität der von ihnen erledigten Aufgaben bewusst zu machen. Auf der Grundlage der in den vergangenen Jahren durch die italienische DSB durchgeführten Prüfungen könnte der Eindruck entstehen, dass die meisten Unternehmen sowie öffentliche und private Organisationen Systemverwaltern eine besondere Bedeutung zugemessen haben. Dies war jedoch nicht immer der Fall. Hieraus ergab sich das Risiko einer Unterschätzung der sich aus unbeaufsichtigten Aktivitäten von Verwaltern, die auch die angemessene Nutzung von IT-Systemen überwachen und kontrollieren sollten, ergebenden Folgen. Dementsprechend wurden alle Kontrolleure von Verarbeitungsverfahren, die vollständig oder teilweise mithilfe elektronischer Werkzeuge durchgeführt werden, aufgefordert, die Notwendigkeit zu berücksichtigen, die Risiken und Gefahren abzuwägen, die eine Beauftragung von Systemverwaltern mit sich bringt. Gleichzeitig wurde eine erste Reihe organisatorischer Maßnahmen zur besseren Sensibilisierung öffentlicher und privater Behörden und Organisationen für die Existenz bestimmter technischer Funktionen, für die mit diesen Funktionen einhergehende Verantwortung sowie in einigen Fällen für die Identität der Personen, die im Zusammenhang mit den betreffenden Diensten und Datenbanken als Systemverwalter tätig sind, festgelegt. Zu diesen Maßnahmen gehören unter anderem die Notwendigkeit einer sorgfältigen Bewertung der persönlichen Qualifikationen von Bewerbern, die individuelle Ernennung von Systemverwaltern, die Pflege einer Liste aktueller Systemverwalter (insbesondere wenn Personaldaten bearbeitet werden) sowie die Bereitstellung relevanter Informationen zu Datensubjekten und Personal, die Gewährleistung des Vorhandenseins von Systemen zur Protokollierung der durch Systemverwalter getätigten Zugriffe (über Computerauthentifizierung) auf Verarbeitungssysteme und elektronische Datenbanken.

**Steuerdaten und Privatsphäre**

***Verbreitung der Steuererklärungsdaten im Internet durch das italienische Finanzamt:*** Die italienische DSB verbat dem italienischen Finanzamt die Veröffentlichung der Steuererklärungsdaten aller Italiener im Internet. Wenige Tage zuvor waren diese Daten auf der Website des Finanzamtes veröffentlicht worden. Die Verbreitung der Daten verstoße gegen die sektorspezifische Gesetzgebung, die andere Mechanismen zur Beschaffung von Informationen zum Einkommen der Steuerzahler vorsehen, die weniger in die Privatsphäre eingreifen. Die Veröffentlichung der Daten im Internet wurde vor dem Hintergrund des Zwecks der Veröffentlichung der betreffenden Daten im Internet als unverhältnismäßig eingestuft.

Die Folgen dieser pauschalen, ungefilterten Offenlegung von Daten zu allen italienischen Steuerzahlern waren vielfältig. Eine beträchtliche Anzahl von Benutzern in Italien sowie im Ausland konnte innerhalb weniger Stunden auf eine gewaltige Datenmenge zugreifen, da die Daten über eine einzige Quelle abrufbar waren. So konnten sie Daten kopieren, ihre eigenen Datenbanken erstellen, die Daten abändern und/oder verarbeiten, Profillisten erstellen und die Daten mit allen Risiken betreffend ihre Korrektheit weiter verbreiten.

Außerdem konnte festgestellt werden, dass das Finanzamt versäumt hatte, vor der Verabschiedung der Entscheidung, die Daten im Internet zu veröffentlichen, eine – gesetzlich vorgeschriebene – Stellungnahme der italienischen DSB einzuholen.

Steuerzahlerregister: Mit einer im September 2008 verabschiedeten Entscheidung wurden die von der italienischen DSB im Rahmen zahlreicher Prüfungen hinsichtlich des Steuerzahlerregisters festgestellten Gefahren inventarisiert. Millionen von Daten zu italienischen Steuerzahlern können von einer erheblichen Anzahl von Benutzern öffentlicher und privater Behörden aufgerufen werden. Außerdem wurden technologische und organisatorische Maßnahmen zur Verbesserung der Zugangssicherheit und zur Anpassung der Verarbeitung an die Datenschutzgesetzgebung festgelegt. Angesichts der Tatsache, dass die wesentlichen Gefahren auf eine mangelnde Information der insgesamt zugangsberechtigten Benutzer, eine schlechte Überwachung der Zugriffe, die Verwendung nicht geeigneter Passwörter und Benutzerkennungen sowie die nicht zur Gewährleistung der Datensicherheit geeigneten technologischen Maßnahmen zurückführen sind, hat die italienische DSB eine regelmäßige Überwachung der zugangsberechtigten Behörden und Organisationen angeordnet. Es wurde eine Untersuchung aller Datenflüsse vom und zum Register, einschließlich Details zu den zugangsberechtigten Behörden, der geltenden Rechtsgrundlage und der Art der übertragenen Daten durchgeführt. Außerdem wurden Daten in Kategorien untergliedert, um zu gewährleisten, dass der betreffende Benutzer nur auf die Daten zugreifen kann, für die er tatsächlich zugangsberechtigt ist. Ferner wurden Warnsysteme zur Erkennung und Vermeidung von Verstößen gegen die Sicherheitsauflagen sowie Authentifizierungsmechanismen/verbesserte Authentifizierungsmechanismen implementiert, die Protokollierung der Zugriffsdaten sowie eine Beschränkung der Zugriffshäufigkeit eingeführt, sichere Verbindungskanäle für die Verwaltung des webbasierten Datenflusses geschaffen und für die zeitnahe Sperrung von Benutzern gesorgt, die nicht mehr auf die relevanten Daten zugreifen dürfen.

**Maßnahmen zur Vereinfachung**

Wie bereits erwähnt, wurden die Maßnahmen zur Vereinfachung hinsichtlich bestimmter Datenschutzanforderungen auch im Jahr 2008 mit der Unterstützung der italienischen DSB fortgesetzt. In einer Anfang des Jahres veröffentlichten Entscheidung wurden praktische Maßnahmen zur weiteren Erleichterung von standardmäßigen Verwaltungs- und Buchhaltungsaufgaben im öffentlichen und privaten Sektor festgelegt, insbesondere dort, wo keine sensiblen oder juristischen Daten verarbeitet werden. Hierzu wurden vereinfachte Mechanismen im Hinblick auf die Informationspflichten gegenüber Datensubjekten festgelegt, ohne dabei den vom Gesetz gewährleisteten Umfang des Schutzes zu gefährden. Außerdem wurden Datenkontrolleure aufgefordert, nicht die Zustimmung von Datensubjekten einzuholen, wenn sie personenbezogene Daten lediglich zu standardmäßigen Verwaltungs- und/oder Buchhaltungszwecken oder im Zusammenhang mit der Erfüllung vertraglicher, vorvertraglicher und/oder rechtlicher Verpflichtungen verarbeiten. Im Sinne des Prinzips des Interessenausgleichs sowie im Einklang mit spezifischen Bedingungen entschied die DSB, dass Datenkontrolleure im privaten Sektor die von einem Datensubjekt zur Verfügung gestellten Informationen zur E-Mail-Adresse ohne die Zustimmung dieser Person verwenden dürfen, wenn die betreffende Person ein Produkt und/oder eine Dienstleistung vom Datenkontrolleur bezogen hat, unter der Voraussetzung, dass diese Daten zu standardmäßigen Verwaltungs- und/oder Buchhaltungszwecken verwendet werden und das Mailing dazu genutzt wird, eigene Direktwerbung und/oder Verkaufsmaterialien zu verschicken, eigene Marktumfragen durchzuführen und/oder Werbenachrichten bereitzustellen. In einer weiteren Entscheidung legte die italienische DSB vereinfachte Maßnahmen zur Umsetzung von Mindestmaßnahmen zur Gewährleistung der Sicherheit im Hinblick auf bestimmte Kategorien der Datenverarbeitung fest. Ziel war – im Einklang mit den Bestimmungen in der bereits auf eine Vereinfachung hin ausgelegten Gesetzgebung (siehe oben) – ein angemessenes Maß an Sicherheit durch die Berücksichtigung der Situation kleiner Unternehmen sowie der Datenverarbeitungen zu gewährleisten, die lediglich zu Buchhaltungs- und/oder Verwaltungszwecken durchgeführt werden.

**Gesundheitsversorgung und sensible Daten**

***Leitlinien für die Verarbeitung von Daten im Rahmen klinischer Medikamentenversuche:*** Diese Leitlinien wurden im Jahr 2008 herausgegeben, um die Sicherheitsmaßnahmen festzulegen, die Datenkontrolleure bei der Verarbeitung personenbezogener Daten von Patienten, die an klinischen Medikamentenversuchen teilnehmen, ergreifen müssen. Im Anschluss wurde auch eine öffentliche

Konsultation zu diesen Leitlinien gestartet. Die Leitlinien fordern insbesondere, dass Daten und biologische Proben kürzer gespeichert werden sollen, dass eindeutiger zwischen der Einwilligung in eine medizinische Behandlung und der Zustimmung zur Verarbeitung personenbezogener Daten unterschieden werden muss, dass eine spezielle Klausel formuliert werden soll, nach der die Zustimmung der Patienten einzuholen ist, damit sich die betreffenden Personen auch im Hinblick auf die etwaige Verarbeitung durch andere Organisationen äußern können, die an der betreffenden Forschung beteiligt sind (eventuell auch im Ausland), und dass strengere Sicherheitsmaßnahen eingeführt werden müssen. Die DSB entwarf außerdem eine Vorlage für ein Meldeformular, das von Pharmaunternehmen verwendet werden könnte, die solche Studien finanziell unterstützen, um die Patienten über die Verarbeitung ihrer Daten durch die beteiligten Testzentren zu informieren. Die Sicherheitsmaßnahmen wurden insbesondere in Bezug auf elektronische Datenübertragungen verschärft. Obligatorische Authentifizierungsverfahren für den Zugriff auf Daten sowie Bestimmungen zur Nutzung von Datenspeicherungs- und -archivierungssystemen auf der Grundlage verschlüsselter und sicherer Kommunikationsprotokolle für die Übertragung von Daten zwischen Testzentren, der Datenbank des Pharmaunternehmens sowie den Studienbetreuern wurden festgelegt.

*Anti-Doping:* Auf eine Beschwerde des Verbandes italienischer Radprofis (ACCPI) bei der italienischen DSB, dass die vom italienischen olympischen Komitee (CONI) angewandte Regelung, Dopingkontrollen auch außerhalb des Wettkampfzeitraums durchzuführen, gegen die Gesetzgebung zum Schutz der Privatsphäre verstoße, veröffentlichte die DSB eine Entscheidung hinsichtlich der Verarbeitung personenbezogener Daten im Bereich Anti-Doping. Die DSB betonte, dass die Verarbeitung personenbezogener Daten durch das CONI (eine öffentliche Behörde) im Einklang mit allen geltenden Gesetzen stehen und relevante internationale Instrumente berücksichtigen muss. Die DSB forderte das CONI auf, die zur Information der Datensubjekte (in diesem Fall die Sportler) verwendeten Informationsblätter zu ändern, so dass sie spezifische Informationen zu den bereitzustellenden Daten enthalten. Es sollte angegeben werden, ob der Test obligatorisch oder freiwillig durchgeführt wird und welche Folgen das Versäumnis der Bereitstellung der Daten mit sich bringt, insbesondere im Hinblick auf detaillierte Informationen zum Aufenthaltsort. Außerdem musste der Kommunikationsumfang der betreffenden Daten durch die Angabe (der Kategorien) der Empfänger sowie die Beantwortung der Frage, ob die Daten auch ins Ausland übertragen werden, verdeutlicht werden.

**Justiz**

Auch im Jahr 2008 wurde weiter daran gearbeitet, den Respekt für das Prinzip des Datenschutzes in Zusammenhang mit Maßnahmen der Justiz zu gewährleisten. In diesem Kontext verabschiedete die DSB „Leitlinien zur Datenverarbeitung durch vom Gericht bestimmte Experten", die verdeutlichen, welche Pflichten diese Fachleute bei der Bearbeitung großer Mengen personenbezogener Daten im Zusammenhang mit unterschiedlichen gerichtlichen Verfahren einhalten müssen. Im Jahr 2008 wurden auch „Verhaltensregeln für Untersuchungen der Verteidigung durch Rechtsbeistände oder Privatdetektive" verabschiedet. Diese Regeln legen die Sicherheitsvorschriften fest, an die sich Rechtsbeistände und Privatdetektive zu halten haben, wenn sie personenbezogene Daten von Klienten verarbeiten – und zwar von den ersten Vorbereitungen zur Einreichung einer Klage bis nach Abschluss des Verfahrens. Insbesondere legen die Regeln vereinfachte Maßnahmen im Hinblick auf Informationsmitteilungen, strenge technische und organisatorische Maßnahmen zum Schutz der Daten sowie einen beschränkten Speicherzeitraum für die zu besagten Zwecken erfassten Daten fest.

**Unternehmensinformationen**

Die DSB veröffentlichte eine Entscheidung zur Verarbeitung von Daten durch ein Unternehmen, das eine eigene Datenbanken betrieb, die durch die Extraktion von Informationen aus anderen (von öffentlichen oder privaten Organisationen eingerichteten) Ablagesystemen generiert wird, um seinen Kunden – meist Experten und Fachleuten wie z. B. Banken, Finanzunternehmen, Informationsunternehmen und -agenturen – informationsbezogene Dienste mit Schwerpunkt auf so genannten Unternehmensinformationen zu bestimmten Zielorganisationen (andere Unternehmen, Fachleute usw.) zu bieten. Durch eine Entscheidung vom 30. Oktober 2008 forderte die DSB das Unternehmen auf,

alle erforderlichen Maßnahmen zu ergreifen und die Datensubjekte angemessen zu schützen, um: a. zu verhindern, dass Informationen, die nicht direkt dem betreffenden Datensubjekt zugeordnet werden können, da sie auch andere Organisationen betreffen, dem besagtem Datensubjekt zugeordnet werden; b. zwischen den Fällen, in denen auf der Grundlage der zur Verfügung stehenden Daten in Zusammenhang mit der Zielorganisation keine schädlichen Dinge gefunden werden, und den Fällen, in denen die Zuverlässigkeitsrate des Unternehmens auf „niedrig" gesetzt wird, zu unterscheiden. Außerdem verbat die DSB dem Unternehmen: a. Informationen zu verwenden, die irrelevant sind und in jedem Fall nicht direkt mit den Zielorganisationen in Zusammenhang stehen; b. ihren Kunden Daten zur Anzahl der Abfragen der Akte einer bestimmten Zielorganisation zur Verfügung zu stellen; c. die aus Wählerverzeichnissen zur Durchführung von Konsistenzkontrollen erfassten Daten bei der Bereitstellung ihrer Dienstleistungen zu verarbeiten; d. personenbezogene Daten zu für das Jahr 2005 eingereichten und nach deren Veröffentlichung durch das italienische Finanzamt gespeicherten Steuererklärungen (siehe Abschnitte oben) zu verarbeiten. Das Unternehmen wurde außerdem aufgefordert, besagte Daten unverzüglich zu löschen.

**Elektronische Kommunikation**

*Elektrischer und elektronischer Abfall und Datenschutz:* Durch eine Entscheidung vom 13. Oktober 2008 lenkte die Garante die Aufmerksamkeit juristischer Personen, öffentlicher Verwaltungsbehörden sowie anderer Behörden und natürlicher Personen, die Geräte, die personenbezogene Daten enthalten, nicht zerstören, sondern diese nach der Erledigung der betreffenden Aufgaben lediglich entsorgen, auf die Notwendigkeit der Einführung geeigneter Vorkehrungen und geeigneter Maßnahmen (auch mit Hilfe dritter Parteien, die über die geeigneten technischen Fähigkeiten verfügen) zur Verhinderung eines unbefugten Zugriffs auf die auf elektrischen und elektronischen Geräten gespeicherten personenbezogenen Daten. Wer elektrische und elektronische Ausrüstung oder Teile davon wieder verwenden und/oder recyceln will, muss sicherstellen, dass sich keine personenbezogenen Daten darauf befinden und/oder wiederhergestellt werden können und außerdem, sofern machbar, die Vollmacht erhalten, solche Daten zu löschen und/oder dafür zu sorgen, dass sie nicht wiederhergestellt werden können.

*Einzelgebührennachweis:* Durch eine Entscheidung vom 13. März 2008 bevollmächtigte die Garante alle Anbieter öffentlicher elektronischer Kommunikationsdienste gemäß Abschnitt 124(5) des entsprechenden Gesetzes, ab dem 1. Juli 2008 die vollständigen Rufnummern auf den von den Kunden angeforderten Einzelverbindungsnachweisen aufzuführen, unter der Voraussetzung, dass sie ihren Kunden ermöglichen, über eine andere Zahlungsmethode als per Rechnung von jedem beliebigen Anschluss aus Kommunikationen durchzuführen und Dienste zu beantragen und unter der Voraussetzung, dass sie allen Anschlussinhabern geeignete Informationsmitteilungen zusammen mit mindestens zwei Rechnungen zukommen lassen und diese auch auf ihrer Website veröffentlichen.

*Telefonwerbung:* Nach zahlreichen Beschwerden und Berichten über unerbetene Telefonanrufe, die von verschiedenen Telefonanbietern selbst und/oder im Namen dieser Anbieter und/oder von Unternehmen, die Waren und Dienstleistungen anbieten, durchgeführt wurden, verbat die italienische DSB zahlreichen auf die Entwicklung und den Verkauf von Datenbanken spezialisierten Unternehmen die Weiterverarbeitung der personenbezogenen Daten (d. h. der Telefonnummern) von Millionen von Nutzern. Die betreffenden Telefonnummern wurden unrechtmäßig erfasst und verwendet, da die Datensubjekte vorher nicht informiert wurden und sie keine ausdrückliche Zustimmung für die Übertragung ihrer Daten an andere Unternehmen erteilt hatten.

Dieses Verbot galt auch für andere Unternehmen, die die Datenbanken von dem betreffenden Unternehmen gekauft hatten, um Nutzer zu kontaktieren und ihre Produkte und Dienstleistungen über Call Center zu vermarkten. Auf das Verbot folgten zahlreiche Warnungen und Prüfungen durch die DSB. Die Prüfungen wurden im Hinblick auf die Telefonbetreiber und -unternehmen, die die Datenbanken gekauft hatten, in den Geschäftsräumen der Unternehmen durchgeführt, die diese Datenbanken erstellt und verkauft hatten. Darüber hinaus wurden auch die Call Center überprüft, die die betroffenen Personen kontaktiert hatten.

Interessant war, dass ein Unternehmen auf seiner Website Daten von über 15 Millionen italienischen Familien,

sortiert nach Einkommen und Lebensstil, veröffentlicht hatte, ohne die Datensubjekte zu informieren und ihre Zustimmung zur Übermittlung ihrer Daten an Dritte einzuholen.

An dieser Stelle sollte an eine aktuelle Gesetzesänderung (siehe Teil 1) erinnert werden, die eine Ausnahme betreffend die Einholung der Zustimmung der Anschlussinhaber im Hinblick auf die oben genannten Bestimmungen enthält. Hiernach dürfen personenbezogene Daten aus Datenbanken, die vor dem 1. August 2005 aus öffentlichen Telefonverzeichnissen erstellt wurden, bis zum 31. Dezember 2009 rechtmäßig von Datenkontrolleuren zu Werbezwecken verwendet werden, jedoch ausschließlich dann, wenn besagte Datenbanken vor dem 1. August 2005 erstellt wurden.

***Standortdaten und in Bussen installierte Kontrollinstrumente:*** In einer nach dem Abschluss vorheriger Prüfmaßnahmen veröffentlichten Entscheidung genehmigte die italienische DSB die Verarbeitung von Standortdaten durch lokale öffentliche Verkehrsdienste. Die DSB genehmigte außerdem die Verarbeitung zusätzlicher Informationen zum „Fahrverhalten" sowie einiger weiterer Parameter (z. B. Öldruck der Bremse bei Beginn und Ende des Bremsvorgangs, Fahrzeuggeschwindigkeit während des Bremsvorgangs usw.), die bei Unfällen über einen so genannten „Datenrekorder für Vorfälle" erfasst werden.

Die DSB gestattete die Verarbeitung der betreffenden Daten unter der Voraussetzung der Einhaltung einer Reihe von Anforderungen: Den Datensubjekten (Fahrern) muss detailliert erklärt werden, welche Daten verarbeitet werden, welche Funktionen das System hat und welcher Zweck damit verfolgt wird. Der Zugang zu den verarbeiteten Daten darf nur Personen gestattet werden, die vom Unternehmen damit beauftragt wurden und die zur Erfüllung ihrer Aufgaben rechtmäßig zugangsberechtigt wurden. Die Daten dürfen nicht länger als für den betreffenden Zweck erforderlich gespeichert werden. Durch gegebenenfalls erforderliche Anonymisierung sollen die Daten zu Standortinformationen ausschließlich als Datenverbund im Hinblick auf die Überwachung und Planung des öffentlichen Verkehrsdienstes verarbeitet werden. Hinsichtlich der Daten zum „Fahrverhalten", die verarbeitet werden sollten, um die Fahrer mit Boni zu belohnen, die ihr Fahrverhalten an die Vorgaben des Unternehmens anpassen, sollte die Verarbeitung im Einklang mit den geltenden rechtlichen Bestimmungen erfolgen – insbesondere mit den in Abschnitt 10 der Verordnung (EG) Nr. 561/2006 vom 15. März 2006 aufgeführten. Die gemäß Abschnitt 4(2) von Gesetz Nr. 300/1970 einzuführenden Verfahren – nach dem zur Fernüberwachung von Angestellten die Genehmigung eingeholt und/oder eine Verordnung einer lokalen Agentur des Arbeitsministeriums beantragt werden muss – müssen bereits vor der Einführung eingehalten werden. Das Unternehmen muss der italienischen DSB die Verarbeitung melden, insbesondere die Verarbeitung der Standortdaten, und außerdem den Dienstleistungsanbieter als Datenverarbeiter gemäß Abschnitt 29 des Datenschutzgesetzbuches bestimmen.

**Formale Beschwerden**

***Online-Zeitungsarchive:*** Die DSB befasste sich mit einigen Beschwerden über die Verfügbarkeit (alter) Zeitungsartikel im historischen Online-Archiv einer Zeitung. In den Beschwerden wurde darauf hingewiesen, dass die archivierten Berichte nicht mehr die aktuelle Situation wiedergäben, da die betreffenden Personen ihr Leben zum Positiven hin geändert hatten. Die DSB stellte fest, dass die Verfügbarkeit solcher Berichte dem Zwecke (historischer) Forschung und Analyse diene, dementsprechend keine Zustimmung der Datensubjekte erforderlich sei und die Daten somit im Hinblick auf den ursprünglichen Zweck auch zu einem späteren Zeitpunkt verarbeitet werden dürften. Die Verarbeitung ist rechtmäßig und relevant, die Daten müssten nicht, wie von den Beschwerdeführern beantragt, gelöscht und/oder anonymisiert werden. Die Mechanismen zur Datenbeschaffung externer Suchmaschinen beeinträchtigen die Rechte der Beschwerdeführer jedoch unverhältnismäßig, da sie die betreffende Person für immer vergangenen Ereignissen und Verhaltensweisen zuordnen. Außerdem können die betreffenden Informationen im Internet aufgrund aktueller Speichermechanismen und Sucheingaben zu Zwecken verbreitet werden, die nicht mit historischer Forschung in Zusammenhang stehen. Den Beschwerden wurde teilweise stattgegeben – d. h. die Websites, die personenbezogene Daten der Beschwerdeführer enthielten, durften nicht unter Verwendung der Namen der Beschwerdeführer bei den beliebtesten Suchmaschinen

indiziert werden. Sie sollten jedoch innerhalb des (über die Website des Herausgebers erreichbaren) Online-Archivs des Herausgebers unverändert bleiben. Die technischen Werkzeuge zur Erfüllung dieser Anforderung sind derzeit verfügbar („Robots Exclusion Protocol"; Verwendung des „Robots Meta Tag"). Der Herausgeber wurde aufgefordert, die Anforderungen binnen 60 Tagen umzusetzen. Die DSB behielt sich das Recht vor, weitere gründliche Untersuchungen der weitergehenden Auswirkungen dieses Themas in Zusammenarbeit mit allen relevanten Interessengruppen durchzuführen.

*Vaterschaftstests zu gerichtlichen Zwecken ohne die Einwilligung des Kindes:* Bei einer Beschwerde ging es um den Fall eines Vaters, der im Zusammenhang mit Untersuchungen zur Feststellung der Blutsverwandtschaft einen Gentest zu seinem Sohn durchgeführt hatte, ohne ihn zuvor darüber zu informieren. Eine private Detektei hatte im Auftrag und als Rechtsbeistand des Mannes zwei von seinem Sohn weggeworfene Zigarettenstummel eingesammelt. Die biologischen Proben wurden ohne Information des Datensubjektes getestet, um die genetische Verwandtschaft zwischen Vater und Sohn zu untersuchen. Die italienische DSB entschied, dass ein Vaterschafts-/Mutterschaftstest nicht ohne die Einwilligung des Kindes erfolgen darf, sofern ein solcher Test nicht zu gerichtlichen Zwecken unabdingbar ist. Die DSB erinnerte daran, dass genetische Daten nur nach „vorheriger, schriftlicher" und informierter Genehmigung des Datensubjektes erfasst und verarbeitet werden dürfen. Von dieser Anforderung darf nur dann abgewichen werden, wenn eine gerichtliche Klage bestätigt oder abgewehrt werden muss. Dies gilt jedoch nur dann, wenn der Test absolut „unabdingbar" ist und gemäß den von der italienischen DSB festgelegten Bedingungen durchgeführt wird. Dies beinhaltet insbesondere die Verpflichtung, spezifische Informationen zum Datensubjekt bereitzustellen, wenn der Gentest zur Ermittlung der Vaterschaft/Mutterschaft dienen soll. Die DSB entschied, dass die Datenschutzrechte des Sohnes verletzt wurden und verbat daher sowohl seinem Vater als auch dessen rechtlichem Beistand die weitere Verarbeitung der auf die oben genannte Art und Weise unrechtmäßig erlangten genetischen Informationen.

*Unternehmensinformationen:* Im vergangenen Jahr gingen zahlreiche Beschwerden über ein Unternehmen ein, das die größte Datenbank mit Unternehmensinformationen in Italien betreibt und Banken, Finanzagenturen, Experten und Unternehmen Informationen zur Zuverlässigkeit und Leistung anderer Unternehmen anbietet. Neben der Bearbeitung der zahlreichen Beschwerden zu diesem Thema befasste sich die italienische DSB auch etwas allgemeiner mit dem Thema und veröffentlichte eine Entscheidung über das betreffende Unternehmen (siehe oben).

**Prüfungen**

Die Prüfmaßnahmen wurden im Einklang mit dem für die vergangenen Jahre berichteten allgemeinen Aufwärtstrend im Jahr 2008 weiter verbessert. Der Schwerpunkt der Maßnahmen lag auf Fragen von allgemeinem Interesse für verschiedene Kategorien von Datensubjekten. Insbesondere wurden anspruchsvolle, gründliche Prüfungen durchgeführt im Hinblick auf die Verarbeitungsprozesse von a. Finanz- und Steuerbehörden; b. Kreditinstituten; c. Unternehmen, die Informationen zu anderen Unternehmen anbieten; d. Telekommunikationsbetreibern in Zusammenhang mit unerbetener Werbung sowie in Zusammenhang mit der Erstellung von Kundenprofilen auf der Grundlage von Traffic-Daten; Verbraucherkredit-Organisationen; e. Unternehmen, die öffentliche Daten wiederverwenden, insbesondere Wählerverzeichnisse und Daten aus öffentlichen Registern betreffend bewegliches und nicht bewegliches Eigentum. Zahlreiche Prüfungen öffentlicher und privater Organisationen wurden durchgeführt, um den Einsatz von Videoüberwachungssystemen und die rechtmäßige Verarbeitung der Daten sowie die Einhaltung der allgemeinen Entscheidung der DSB zu diesem Thema zu kontrollieren. Ein besonderes Augenmerk lag auch auf den in privaten Krankenhäusern durchgeführten Prüfungen zur Kontrolle der Verarbeitung sensibler Daten im Hinblick auf die Einhaltung von Mindest-Sicherheitsstandards.



## Lettland

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

**Gesetz zum Schutz personenbezogener Daten**
Die Richtlinie 95/46/EG wurde durch das Gesetz zum Schutz personenbezogener Daten in nationales Recht umgesetzt, das am 20. April 2000 in Kraft trat. Die letzten Änderungen traten am 6. März 2008 in Kraft. Das Gesetz zum Schutz personenbezogener Daten wurde am 21. Februar 2008 geändert. Die wesentlichen Änderungen betrafen die Ausnahme des Rechts eines Datensubjektes auf Zugang zu Daten, wenn diese Daten durch den Staat im Hinblick auf Steuerfragen oder durch Versicherungsunternehmen zum Zwecke der Geltendmachung einer Entschädigung gemäß einem Versicherungsvertrag verarbeitet wurden.

**Gesetz über die Datenaufsichtsbehörde**
Um die vollständige Unabhängigkeit der lettischen Datenaufsichtsbehörde zu gewährleisten, wurde das Verfahren zum Entwurf eines Gesetzes über die Datenaufsichtsbehörde abgeschlossen. Angesichts der Notwendigkeit einer Überprüfung der für die Arbeit der unabhängigen Datenschutzbehörde erforderlichen Mittel vor dem Hintergrund der wirtschaftlichen Situation in Lettland wurde der Gesetzesentwurf Ende 2008 und Anfang 2009 aktualisiert. Bis Mitte 2009 soll er der Regierung vorgelegt werden.

**Verordnung betreffend die Übermittlung von Daten an Drittländer**
Im Jahr 2008 führte die lettische Datenaufsichtsbehörde ihre Aktivitäten zum Entwurf einer Kabinettsverordnung zu Standard-Anforderungen für Vereinbarungen betreffend die Übermittlung personenbezogener Daten an Drittländer fort. Die Verordnung setzt die in den Entscheidungen 2001/497/EG und 2004/915/EG der Kommission bezüglich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer festgelegten Anforderungen in Bezug auf den Inhalt von Verträgen um.

**Verordnung betreffend die Schulung und Überprüfung von Datenschutzbeauftragten**
Das Gesetz zum Schutz personenbezogener Daten regelt die Meldung von Datenverarbeitungen. Seit 2008 gibt es eine Alternative hierzu – den Datenschutzbeauftragten in privaten und öffentlichen Institutionen. Aus diesem Grund hat die Datenaufsichtsbehörde die Kabinettsverordnung „Verfahren zur Schulung von Datenschutzbeauftragten" (5. Februar 2008 Nr. 80) erlassen, die am 9. Februar 2008 in Kraft trat. Die Verordnung legt das Verfahren zur Schulung und Überprüfung von Datenschutzbeauftragten sowie die betreffenden Schulungsprogramme fest. Die Schulung kann durch die Datenaufsichtsbehörde und sonstige Institutionen des öffentlichen oder privaten Sektors durchgeführt werden. Die Prüfung kann jedoch ausschließlich von der Datenaufsichtsbehörde durchgeführt werden. Im Jahr 2008 organisierte die lettische Datenaufsichtsbehörde zwei Prüfungen. Für sieben Datenschutzbeauftragte, die den privaten Sektor und die Regierung vertreten, wurden Bescheinigungen ausgestellt.

**Höhere Geldstrafen für Vergehen betreffend personenbezogene Daten**
Am 3. Juli 2008 wurde das lettische Ordnungswidrigkeitengesetz geändert, um höhere Geldstrafen für Verstöße betreffend personenbezogene Daten festzulegen. Die Änderung trat am 7. August 2008 in Kraft. Die höchste Geldstrafe, die gegen juristische Personen verhängt werden kann, liegt nunmehr bei 10.000 Lats (etwa 14.230 €).

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

Seit 2007 ist die Datenaufsichtsbehörde für die Zusammenfassung der Statistiken über die Vorratsspeicherung jener Daten zuständig, die im Zusammenhang mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden. Grundlage dafür sind Paragraph 19 des Gesetzes über elektronische Kommunikation und Artikel

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

## B. Bedeutende Rechtsprechung

Im Laufe des Jahres 2008 gingen 140 Beschwerden bei der Datenaufsichtsbehörde ein. Die meisten betrafen die Verarbeitung personenbezogener Daten ohne Rechtsgrundlage sowie die Verarbeitung von Daten, die über den eigentlichen Zweck der Datenverarbeitung hinausgeht. Als Ergebnis von Untersuchungen betreffend den Schutz personenbezogener Daten wurden in 28 Fällen Verstöße gegen das Gesetz zum Schutz personenbezogener Daten bestätigt. In 18 % der Fälle wurden Verwarnungen ausgesprochen. Im Jahr 2007 wurden nur in 10 % der Fälle Verwarnungen ausgesprochen. Es ist also ein prozentualer Anstieg zu verzeichnen. Außerdem hat sich die Zahl der im Jahr 2008 gegen die Gesetzesübertreter verhängten Verwaltungsgebühren verglichen mit dem Jahr 2007 um etwa 40 % erhöht. Die Beschwerden betrafen zumeist die Verarbeitung von Daten ohne Rechtsgrundlage und Verstöße gegen die Rechte der Datensubjekte (Artikel 10 und 11 der Richtlinie 95/46/EG) sowie Verstöße gegen das Prinzip der Verhältnismäßigkeit bei der Verarbeitung von Daten.

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

- Veröffentlichungen personenbezogener Daten im Internet;
- Videoüberwachung;
- Kopieren von Ausweisen;
- Verarbeitung von Daten von Hausmeisterdiensten;
- Verarbeitung von Daten durch Kreditvermittlungsagenturen sowie Datenübermittlung an Dritte.

Verglichen mit 2007 ist die Zahl der Verstöße betreffend die Veröffentlichung personenbezogener Daten im Internet gestiegen. Zudem wurde die Zusammenarbeit mit der Polizei im Hinblick auf Fälle verstärkt, in denen Personen bei Verfahren zur Klärung der Identität von Verdächtigen die personenbezogenen Daten einer anderen Person anstelle ihrer eigenen nutzen.

## C. Wichtige spezifische Themen

Nachstehend sind die wesentlichen Themen des Jahres 2008 aufgeführt, bezüglich deren sich die Datenaufsichtsbehörde an Diskussionen auf nationaler Ebene beteiligte. Die wesentlichen Themen betrafen Folgendes:

- Entwurf eines Konzepts für das nationale System zur Online-Gesundheitsfürsorge (E-Health);
- Organisation des Systems zum Online-Abschluss von Kraftfahrzeugversicherungen sowie Lösung des Problems der Gewährleistung des Rechts behinderter Menschen auf eine Vergünstigung bei der Kraftfahrzeugversicherung, da dies den Zugriff auf sensible Daten erfordert;
- Überlegungen auf nationaler Ebene betreffend die Übermittlung von Passagierdaten an die USA sowie den Austausch personenbezogener Daten mit den USA als Teil des Programms für visumfreies Reisen;
- Einrichtung der gemeinsamen Datenbank biometrischer Daten sowie die Verarbeitung biometrischer Daten in Ausweisen.

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

1. Ein großer Anteil der eingegangenen Beschwerden betraf die Kreditvermittlung. Personenbezogene Daten von Kreditnehmern werden zur Einziehung von Forderungen an Dritte übermittelt. Zusätzlich werden aktuelle und frühere Daten ohne Einwilligung

des Datensubjektes an Dritte übermittelt. In den meisten Fällen wird die Übermittlung personenbezogener Daten als Verarbeitung von Daten ohne Rechtsgrundlage eingestuft und liegt somit außerhalb des zulässigen Bereichs der Datenverarbeitung.

2. Die Veröffentlichung personenbezogener Daten im Internet ohne die Einwilligung der betreffenden Datensubjekte kann oftmals als Verstoß gegen das Gesetz zum Schutz personenbezogener Daten ausgelegt werden. Eine solche Handlung eines Datenkontrolleurs ist als Verarbeitung von Daten ohne Rechtsgrundlage einzustufen.
3. Der Arbeitgeber hat Kopien von Ausweisdokumenten seiner Angestellten und Kunden an Dritte übermittelt. Das Kopieren von Ausweisdokumenten ist als unverhältnismäßige Verarbeitung personenbezogener Daten einzustufen, eine Übermittlung an Dritte als Verarbeitung von Daten ohne Rechtsgrundlage. Beides ist somit als unrechtmäßige Datenverarbeitung einzustufen.

**Entwurf von Empfehlungen**

Im Jahr 2008 entwarf die Datenaufsichtsbehörde zwei Empfehlungen. Unter Berücksichtigung der Anzahl von Beschwerden bezüglich Videoüberwachung und SPAM sowie im Hinblick auf die Förderung des Verständnisses dieser Themen entwarf die Datenaufsichtsbehörde Folgendes:

- die Empfehlung zur Verarbeitung von Daten durch Videoüberwachung;
- die Empfehlung zu Werbenachrichten.

**Schengener Informationssystem (SIS).**

Im Jahr 2008 überprüfte die Datenaufsichtsbehörde Institutionen und Behörden, die Zugang zum Schengener Informationssystem (SIS) haben. Die Überprüfungen wurden im Einklang mit den Artikeln 96, 97 und 98 des Übereinkommens von Schengen durchgeführt.

**Datenschutz in Schulen**

Im Jahr 2008 organisierte die Datenaufsichtsbehörde zahlreiche Workshops für Lehrer und sonstiges Schulverwaltungspersonal zum Thema Datenschutz in Schulen. Die allgemeinen Datenschutzprinzipien wurden erläutert und spezifische Themen diskutiert, unter anderem auch die Ergebnisse des Projekts zum Zugang zu Schulen („e-class-Projekt"), die Veröffentlichung von Informationen auf Schulwebsites, die Speicherung medizinischer Daten, Videoüberwachung usw.

## Litauen

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

Am 1. Februar 2008 verabschiedete das Parlament (Seimas) der Republik Litauen eine Änderung des Gesetzes über den rechtlichen Schutz personenbezogener Daten (der neue Wortlaut wird am 1. Januar 2009 in Kraft treten).

Der neue Wortlaut legt die Bestimmungen des Gesetzes über den rechtlichen Schutz personenbezogener Daten fest und regelt die Verarbeitung des persönlichen Identifizierungscodes. Datenkontrolleure, die gesundheitsbezogene Daten zum Zwecke der Gesundheitsvorsorge automatisch verarbeiten und die personenbezogene Daten zu wissenschaftlichen medizinischen Zwecken verarbeiten, müssen dies der staatlichen Datenschutzbehörde melden, damit diese eine Vorprüfung durchführen kann. Der Begriff Videoüberwachung wurde definiert, und Vorschriften zur Verarbeitung personenbezogener Bilddaten sowie zur Verarbeitung personenbezogener Daten für Direktwerbung und Solvenzbewertung wurden verabschiedet. Darüber hinaus wurden Vorschriften zum Status einer für den Datenschutz und die Bearbeitung von Beschwerden verantwortlichen Person oder Abteilung verabschiedet. Der Wortlaut des neuen Gesetzes über den rechtlichen Schutz personenbezogener Daten schreibt die Unabhängigkeit der staatlichen Datenschutzbehörde fest, die als Aufsichtsbehörde für den Datenschutz fungiert (gemäß den Bestimmungen der Richtlinie 95/46/EG) und deren Behördenleiter für eine Amtszeit von jeweils 5 Jahren eingesetzt wird.

Am 14. November 2008 wurde das Gesetz zur Änderung und Ergänzung des Gesetzes über elektronische Kommunikation der Republik Litauen (Inkraftsetzung: 15. März 2009) zur Umsetzung der Bestimmungen der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG verabschiedet.

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

Sind die oben genannten Daten für die Geschäftstätigkeit der Behörden, für vorgerichtliche Untersuchungen, für den Staatsanwalt, das Gericht oder den Richter zur Ermittlung und Feststellung von Straftaten oder für von der Regierung bevollmächtigte Institutionen erforderlich, so müssen die Betreiber elektronischer Kommunikationsnetzwerke und/oder -dienste diese Informationen für einen längeren Zeitraum speichern, jedoch nicht länger als 6 weitere Monate. Für diese Speicherung ist aus staatlichen Mitteln gemäß dem von der Regierung festgelegten Verfahren (Artikel 77(2) des Gesetzes über elektronische Kommunikation der Republik Litauen) eine Entschädigung zu zahlen.

Am 12. November 2008 wurden mit der Verordnung Nr. 1T-71 (1.12) „Zur Genehmigung allgemeiner Anforderungen für organisatorische und technische Maßnahmen zum Datenschutz“ allgemeine

Anforderungen für organisatorische und technische Maßnahmen zum Datenschutz ratifiziert. Sie legen allgemeine Anforderungen für organisatorische und technische Maßnahmen zum Datenschutz fest, die von Datenkontrolleuren und Datenverarbeitern umgesetzt werden müssen, um zu gewährleisten, dass personenbezogene Daten vor einer versehentlichen oder unrechtmäßigen Vernichtung, Änderung, Offenlegung oder sonstigen unrechtmäßigen Verarbeitungen geschützt sind.

## B. Bedeutende Rechtsprechung

**Veröffentlichung personenbezogener Daten betrunkener Menschen im Internet**

Bei der staatlichen Datenschutzbehörde gingen zwei Beschwerden über die Veröffentlichung personenbezogener Daten auf der Website des Polizeipräsidiums der Stadt Wilna ein. Nach einer Untersuchung der Sachlage stellte die Staatliche Datenschutzbehörde fest, dass der Leiter des Polizeipräsidiums der Stadt Wilna entschieden hatte, personenbezogene Daten (Vorname, Nachname, Geburtsjahr, Zeit und Ort der Ordnungswidrigkeit, Grad der Trunkenheit sowie verhängte Strafmaßnahme) der Personen, die wegen Trunkenheit am Steuer belangt worden waren, auf der Website des Polizeipräsidiums der Stadt Wilna zu veröffentlichen. Die Veröffentlichung dieser personenbezogenen Daten sollte der Information und Bildung der Öffentlichkeit sowie der Verhinderung weiterer Ordnungswidrigkeiten dienen.

Die staatliche Datenschutzbehörde entschied, dass solche Maßnahmen der Polizei illegal seien, da der Zweck der Erfassung personenbezogener Daten der Beschwerdeführer lediglich die Verhängung einer Strafmaßnahme sei. Später wurden die personenbezogenen Daten der Beschwerdeführer auch im Register für Verstöße gegen die Straßenverkehrsordnung und Verkehrsunfälle verarbeitet. Gemäß Paragraph 2 von Artikel 6 des Gesetzes über Polizeiaktivitäten ist es verboten, in den Informationssystemen der Polizei gespeicherte persönliche Informationen offen zu legen oder an andere Personen weiterzugeben, sofern dies nicht durch entsprechende Gesetze oder sonstige rechtliche Vorschriften festgelegt ist. Gemäß Paragraph 1, Absatz 1 von Artikel 3 des Gesetzes über den rechtlichen Schutz personenbezogener Daten muss der Datenkontrolleur gewährleisten, dass die erfassten personenbezogenen Daten zu speziellen und legitimen Zwecken verarbeitet werden und nicht anschließend zu Zwecken verarbeitet werden, die nicht im Einklang mit den vor der Erfassung der betreffenden personenbezogenen Daten festgelegten Zwecken stehen. Die staatliche Datenschutzbehörde entschied, dass solche personenbezogenen Daten aus folgenden Gründen nicht zum Zwecke der Information und Bildung der Öffentlichkeit sowie zur Vermeidung von Ordnungswidrigkeiten im Internet veröffentlicht werden dürfen:

- Diese Zwecke entsprechen nicht den vor der Erfassung der personenbezogenen Daten festgelegten Zwecken;
- gemäß dem Gesetz über Polizeiaktivitäten ist es verboten, im Register gespeicherte persönliche Informationen offen zu legen;
- es gab keine Kriterien für eine rechtmäßige Verarbeitung der personenbezogenen Daten.

Die staatliche Datenschutzbehörde erließ eine Anweisung an das Polizeipräsidium der Stadt Wilna zur Beendigung der Veröffentlichung von Daten (Vorname, Nachname, Geburtsjahr, Zeit und Ort der Ordnungswidrigkeit, ermittelter Grad der Trunkenheit, Artikel des Ordnungswidrigkeitengesetzes der Republik Litauen betreffend die Haftbarkeit für begangene Ordnungswidrigkeiten sowie die für den Verstoß verhängte Strafmaßnahme) zu Personen, gegen die ein Bußgeld wegen eines Verstoßes gegen die Straßenverkehrsordnung verhängt wurde, auf der Website zum Zwecke der Information und Bildung der Öffentlichkeit sowie zur Vermeidung von Ordnungswidrigkeiten.

Das Polizeipräsidium der Stadt Wilna legte vor Gericht Widerspruch gegen die Entscheidungen der staatlichen Datenschutzbehörde ein. Das Verwaltungsgericht des Bezirks Wilna entschied, dass Paragraph 1, Absatz 6 von Artikel 5 des Gesetzes über den rechtlichen Schutz personenbezogener Daten angewendet werden müsse (personenbezogene Daten dürfen verarbeitet werden, wenn eine Verarbeitung für die vom Datenkontrolleur verfolgten legitimen Interessen oder für Interessen einer dritten Partei, der die personenbezogenen Daten offen gelegt wurden, erforderlich ist, sofern die Interessen des Datensubjektes nicht über diesen Interessen stehen). Das

Gericht stellte außerdem fest, dass Daten wie z. B. Zeit und Ort der Ordnungswidrigkeit, Grad der Trunkenheit sowie verhängte Strafmaßnahmen nicht als personenbezogene Daten eingestuft werden können.

Gegen die Entscheidung des Verwaltungsgerichtes des Bezirks Wilna wurde Berufung beim Obersten Verwaltungsgericht Litauens eingelegt.

Das Oberste Verwaltungsgericht Litauens entschied, dass Daten wie z. B. Zeit und Ort der Ordnungswidrigkeit, Grad der Trunkenheit sowie verhängte Strafmaßnahmen als personenbezogene Daten einzustufen sind, wenn diese Daten zusammen mit dem Vor- und Nachnamen des Datensubjektes veröffentlicht werden.

Das Gericht entschied weiterhin, dass das Polizeipräsidium der Stadt Wilna personenbezogene Daten unter dem Vorwand legitimer Interessen auf seiner Website veröffentlicht habe (Paragraph 1, Absatz 6, Artikel 5 des Gesetzes über den rechtlichen Schutz personenbezogener Daten). Als Zusammenfassung der im Ordnungswidrigkeitengesetz festgelegten Bestimmungen ist festzuhalten, dass das Ordnungswidrigkeitengesetz staatliche Institutionen, einschließlich der Polizei, dazu verpflichtet, die begangenen Verstöße nicht nur zu erklären und eine geeignete Strafmaßnahme zu verhängen, sondern auch Maßnahmen zur Vermeidung von Ordnungswidrigkeiten zu erarbeiten und umzusetzen. Darüber hinaus besagt das Ordnungswidrigkeitengesetz, dass die Vermeidung von Verstößen einer der Zwecke der Verhängung von Ordnungsstrafen ist. Daher ist es offensichtlich, dass die in Zusammenhang mit den verhängten Strafmaßnahmen ergriffenen Maßnahmen zur Verhinderung von Verstößen auf der Grundlage von Informationen, einschließlich personenbezogener Daten, erarbeitet und umgesetzt werden dürfen, die im Rahmen von Ordnungswidrigkeiten erfasst wurden.

Entsprechend gerichtlicher Praxis gilt das Fahren eines motorbetriebenen Fahrzeugs unter Einfluss von Alkohol als schwerer Verstoß gegen die Straßenverkehrsordnung. Das Ordnungswidrigkeitengesetz sieht für diese Verstöße die härtesten Strafmaßnahmen vor, da diese direkt die Gesundheit und Sicherheit der anderen Verkehrsteilnehmer gefährden. Daher wurde im Hinblick auf das Wertegleichgewicht verglichen: Auf der einen Seite stand die vorübergehende Veröffentlichung (einen Monat) personenbezogener Daten einer Person, die eine schwere Ordnungswidrigkeit begangen hatte, auf der anderen Seite die Vermeidung einer Gefahr für Leben, Gesundheit und Sicherheit von Verkehrsteilnehmern. Das Gericht kam zu dem Schluss, dass das Recht des Datensubjektes auf Schutz der Privatsphäre in diesem Fall dem öffentlichen Interesse zur Vermeidung schwerer Verstöße gegen die Straßenverkehrsordnung untergeordnet ist. Die Interessen des Datensubjektes stehen nicht über den legitimen Interessen der Polizei.

**Veröffentlichung personenbezogener Daten zu Wahlzwecken**

Der zentrale Wahlausschuss der Republik Litauen meldete der staatlichen Datenschutzbehörde die Verarbeitung personenbezogener Daten von Parlamentskandidaten im Internet im Hinblick auf eine Vorabprüfung und Genehmigung dieser Verarbeitung durch die Datenschutzbehörde. Gemäß den vom zentralen Wahlausschuss der Republik Litauen festgelegten Vorschriften sind die personenbezogenen Daten (Vorname, Nachname, politische Partei, Geburtsdatum und -ort, Staatsangehörigkeit, Nationalität, Familienstand, Namen der Familienmitglieder, Erklärungen zu Eigentum und privaten Interessen usw.) der Kandidaten auf der Website des zentralen Wahlausschusses der Republik Litauen ohne zeitliche Beschränkung abrufbar. Der unbeschränkte Veröffentlichungszeitraum der personenbezogenen Daten hängt nicht davon ab, ob die Kandidaten tatsächlich zu Mitgliedern des Parlaments gewählt wurden.

Gemäß Artikel 4 des Gesetzes über den rechtlichen Schutz personenbezogener Daten dürfen personenbezogene Daten nicht länger als für die Zwecke der Datenverarbeitung erforderlich gespeichert werden. Werden personenbezogene Daten nicht mehr zu Verarbeitungszwecken benötigt, so sind sie zu vernichten. Entsprechend dieser Bestimmung erließ die staatliche Datenschutzbehörde eine Anweisung an den zentralen Wahlausschuss der Republik Litauen, um festzulegen, wie lange die personenbezogenen Daten der Kandidaten im Internet zu veröffentlichen sind. Der zentrale Wahlausschuss der Republik Litauen lehnte es ab, eine zeitliche Grenze festzulegen, und die

staatliche Datenschutzbehörde entschied, dem zentralen Wahlausschuss der Republik Litauen die Genehmigung der Veröffentlichung personenbezogener Daten auf seiner Website zu verweigern.

Der zentrale Wahlausschuss der Republik Litauen legte Widerspruch gegen die Entscheidung der staatlichen Datenschutzbehörde ein.

Das Verwaltungsgericht des Bezirks Wilna entschied, dass die Entscheidung der staatlichen Datenschutzbehörde korrekt sein und dass es keine Gründe gebe, warum dem zentralen Wahlausschuss der Republik Litauen die Genehmigung erteilt werden sollte, diese personenbezogenen Daten für einen unbegrenzten Zeitraum auf seiner Website zu veröffentlichen.

Gegen die Entscheidung des Verwaltungsgerichtes des Bezirks Wilna wurde Berufung beim Obersten Verwaltungsgericht von Litauen eingelegt.

Das Oberste Verwaltungsgericht Litauens entschied in dieser Sache anders.

Der zentrale Wahlausschuss der Republik Litauen verarbeite personenbezogene Daten, um die Wähler zu informieren, so dass diese von ihrem Wahlrecht Gebrauch machen können. Es gebe keinen Zweifel daran, dass die Daten der Parlamentskandidaten im Rahmen des Wahlkampfes erforderlich sind. Informationen zu Parlamentskandidaten, zu gewählten Mitgliedern des Parlaments sowie zu den Personen, die nicht gewählt wurden, seien für den Prozess der Berechnung und Verkündung des Wahlergebnisses unbestreitbar wichtig. Wenn ein Mitglied des Parlaments seinen Eid abgelegt habe, so habe der Wähler das vertretbare Recht, zu wissen, wer ihn vertritt. Gleichermaßen sei es im Prinzip auch während der Amtszeit der gewählten Mitglieder des Parlaments auch den Kandidaten, die nicht ins Parlament gewählt wurden, möglich, einen freien Posten zu besetzen. Vor diesem Hintergrund seien die Daten zu den Parlamentskandidaten und den tatsächlich gewählten Mitgliedern des Parlaments von großer Bedeutung für die Wähler und blieben vom Zeitpunkt der Entscheidung für eine Parlamentskandidatur bis zum Ende der Amtszeit relevant.

Der unbegrenzte Zeitraum der Veröffentlichung der Daten über die Kandidaten könne durch die Bedeutung von Wahlen als Form der Staatsführung durch die Beteiligung der Bürger gerechtfertigt werden. Demokratische Wahlen seien eine wichtige Form der Staatsführung durch die Beteiligung der Bürger und aus diesem Grund auch eine wertvolle Einrichtung zur Bildung der Vertretungsinstitutionen des Staates. Wahlen seien nicht als demokratisch und Ergebnisse nicht als korrekt und rechtmäßig einzustufen, wenn sie organisiert würden, ohne dass dabei die in der Verfassung festgelegten Prinzipien für demokratische Wahlen berücksichtigt würden, und somit gegen die demokratischen Wahlverfahren verstoßen würden.

Die Gewährleistung der korrekten Information der Wähler sei eine Grundvoraussetzung für die Gewährleistung korrekter und rechtmäßiger Wahlen. Darüber hinaus bedeuteten mehr Daten auch ein stärkeres Vertrauen der Wähler nicht nur in bestimmte Kandidaten, sondern auch in die Vertretungsbehörde selbst: Die Wähler könnten auf Daten zu früheren Wahlen und deren Organisation zugreifen, Informationen zu früheren Kandidaten abrufen, Daten zuordnen und nicht nur eine Wahl hinsichtlich geeigneter Kandidaten treffen, sondern auch überprüfen, ob die Organisation der Wahlverfahren vertrauenswürdig ist und auf dieser Grundlage entscheiden, ob sie an den Wahlen teilnehmen wollen. Daher könnten die Erstellung spezieller Archive zu Wahlen und eine Offenlegung von Daten durch den zu erreichenden legitimen Zweck – nämlich die Steigerung des Vertrauens der Wähler in die Vertretungsbehörde selbst – gerechtfertigt werden.

Unter Berücksichtigung der Tatsache, dass die Offenlegung von Informationen über die Mitglieder des Parlaments einem legitimen Zwecke dient – nämlich der Steigerung des Vertrauens der Wähler in die Bildung der Vertretungsinstitutionen – und somit gewährleistet, dass die Wahlverfahren rechtmäßig und transparent sind, sowie unter Berücksichtigung der Tatsache, dass die Erreichung dieser Ziele nicht nur während bestimmter Wahlen von Bedeutung ist, stellte das Oberste Verwaltungsgericht Litauens fest, dass die Daten zu den Wahlen für einen unbegrenzten Zeitraum veröffentlicht werden dürfen.

## C. Wichtige spezifische Themen

### Verarbeitung personenbezogener Daten bei Kreditinstituten

Die Staatliche Datenschutzbehörde führte Prüfungen der rechtmäßigen Verarbeitungen personenbezogener Daten in sechs Kreditinstituten durch, um den Umfang und die Rechtmäßigkeit der Verarbeitung der Daten einzelner Personen zu überprüfen, die sich im Hinblick auf schnelle Kreditdienste per Internet oder SMS an Kreditinstitute wenden. Im Rahmen der Prüfungen wurden die Methoden zur Identifizierung der Personen (Kunden) festgestellt: Eine Person erstellt ein Dokument zur Bestätigung der Identität; eine Person registriert sich und zahlt einen Betrag von ihrem persönlichen Bankkonto zur Bestätigung der Daten; eine Person erhält eine SMS-Nachricht mit einem Anmeldepasswort; eine Person füllt einen Antrag im Internet oder über das Telefon aus und muss danach persönlich beim Kundendienst vorstellig werden, um unter Vorlage eines Identifikationsdokumentes einen Vertrag zu unterschreiben; eine Person registriert sich per SMS-Nachricht und zahlt einen Betrag von ihrem während der Registrierung angegebenen persönlichen Bankkonto; wenn die Daten übereinstimmen, erhält die Person eine SMS-Nachricht mit einem Anmeldepasswort; eine Person gibt ihre Telefonnummer im Internet an und erhält eine SMS-Nachricht mit einem Code, der auf der Website eingegeben werden muss, füllt dann ein Antragsformular aus und zahlt eine feste Gebühr von ihrem persönlichen Bankkonto. Ein Kreditinstitut forderte Kopien persönlicher Dokumente der Personen an, die kein elektronisches Homebanking-System nutzen. Diese Dokumente sollten zur Identifizierung der Person per Fax oder E-Mail zugeschickt werden. Laut der staatlichen Datenschutzbehörde dürfe eine solche Fernübertragung eines persönlichen Identifikationsdokumentes nicht als korrekte Maßnahme zur Identifikation einer Person eingestuft werden.

Die von den betreffenden Personen bereitgestellten Daten werden durch den Abgleich mit verschiedenen Datenkontrolleuren überprüft: Ein Unternehmen erhält Daten über die Einkünfte, die die Personen vom staatlichen Sozialversicherungsfonds des Ministeriums für soziale Sicherheit und Arbeit der Republik Litauen erhalten; drei Kreditinstitute erhalten Daten des Einwohnermeldeamtes des Innenministeriums der Republik Litauen zum Zwecke der Identifikation der Person, der Prüfung der Daten sowie der Prüfung der Korrektheit; das Konsortium „Creditinfo Lietuva" stellt allen Kreditinstituten Daten über private Schulden zur Verfügung. Drei Kreditinstitute erhalten vom Grundbuchamt Daten zu Immobilien, die sich im Besitz der betreffenden Person befinden. Eines der Kreditinstitute erhält diese personenbezogenen Daten illegal vom Grundbuchamt; vier Kreditinstitute erhalten Daten zum Zwecke der Identifikation und Überprüfung der betreffenden Person von Kreditinstituten (Banken).

Im Laufe der Prüfungen wurden verschiedene Verstöße gegen das Gesetz der Republik Litauen über den rechtlichen Schutz personenbezogener Daten (hinsichtlich der Menge an personenbezogenen Daten, der unrechtmäßigen Verarbeitung ohne die vorherige Einholung der Zustimmung des Datensubjektes, der Verordnung über Direktwerbung und deren Umsetzung (ohne die Möglichkeit für das Datensubjekt, seine Zustimmung zu äußern zur, der Verarbeitung personenbezogener Daten zu Direktwerbezwecken, oder die Möglichkeit, lediglich ein Ablehnungsrecht geltend zu machen) sowie der Umsetzung korrekter organisatorischer und technischer Maßnahmen) festgestellt. Die staatliche Datenschutzbehörde erließ Anweisungen für die untersuchten Kreditinstitute.

### Aufklärung der Öffentlichkeit

Am 23. Januar 2008 veranstaltete die Staatliche Datenschutzbehörde in Zusammenarbeit mit dem Menschenrechtsausschuss des Parlaments (Seimas) der Republik Litauen eine Konferenz mit dem Thema „Der Europäische Datenschutztag für Jugendliche".

Die Veranstaltung wurde aus Anlass des traditionell am 28. Januar stattfindenden Europäischen Datenschutztages organisiert. Ziel der diesjährigen Veranstaltung war es, die Aufmerksamkeit junger Menschen in Litauen zu erhalten und diesen die Themen eines Bereiches vorzustellen, der für alle Menschen von größter Bedeutung ist, nämlich die Themen Menschenrechte und Schutz der Privatsphäre. Der Bericht über die aktuellen, dem Vertreter des Zentrums zur Personalisierung von Identitätsdokumenten des Innenministeriums der Republik Litauen zugeschickten Identitätsdokumente

weckte Neugier und reges Interesse bei den jungen Leuten. Durch die Organisation dieser Veranstaltung wurde auch deutlich, dass es sehr wichtig ist, herauszufinden, wie bewusst sich junge Menschen – Teenager – der Themen Menschenrechte und Datenschutz sind und welche Themen sie derzeit am meisten verärgern.

An der Veranstaltung nahmen 80 Schüler im Alter von 14 bis 18 Jahren aus Schulen in Wilna teil. Ihnen wurden Broschüren mit präzisen Informationen zur sicheren Nutzung des Internets sowie weiteres Informationsmaterial ausgehändigt.

# Luxemburg

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

**Gesetz vom 2. August 2002 über den Schutz von Personen im Hinblick auf die Verarbeitung personenbezogener Daten (Umsetzung der Richtlinie 95/46/EG)**
Im Jahr 2008 gab es keine Änderungen an oben genanntem Gesetz.

**Gesetz vom 30. Mai 2005 über Sonderregelungen zum Schutz der Privatsphäre im Bereich elektronische Kommunikation (Umsetzung der Richtlinie 2002/58/EG)**
Im Jahr 2008 gab es keine Änderungen an oben genanntem Gesetz.

**Verordnungen und abgeleitetes Recht**
In der luxemburgischen Verordnung vom 7. Oktober 2008 wird die Erneuerung von Mandaten für jedes der drei Mitglieder der luxemburgischen Datenschutzkommission (CNPD) sowie die Ernennung zwei neuer stellvertretender Mitglieder befürwortet.

Die Regierung setzte außerdem eine Verordnung vom 1. Dezember 2008 über die technischen Spezifikationen zur Überwachung elektronischer Kommunikationen in Luxemburg in Kraft.

**Weitere Entwicklungen in der Gesetzgebung**
Der Gesetzesentwurf zur Festlegung der „*Bedingungen, unter denen Richter und Polizeibeamte Zugang zu bestimmten Datenbanken erhalten können, die von juristischen Personen des öffentlichen Rechts betrieben werden*" wurde vom Parlament verabschiedet und am 27. August 2008 im Amtsblatt veröffentlicht. Der erste Entwurf dieses Gesetzestextes war im Jahr 2006 von der CNPD kommentiert worden. Die Regierung folgte den ausgesprochenen Empfehlungen und integrierte eine große Zahl der von der CNPD vorgeschlagenen Sicherheitsmaßnahmen. In den Parlamentsdebatten haben zusätzliche, vom Beratungsausschuss für Menschenrechte vorgebrachte Bedenken zu weiteren restriktiven und schützenden Bestimmungen geführt. Das verabschiedete Gesetz umfasst ein breites Spektrum an Beschränkungen und wertvollen Garantien im Hinblick auf einen möglichen Missbrauch personenbezogener Daten. Es scheint jedoch, als seien die Bestimmungen zu restriktiv für die Polizei im Hinblick auf die Erledigung ihrer alltäglichen Aufgaben. Daher könnte es möglich es, dass das Parlament im Laufe des Jahres 2009 wieder zusammenkommt, um Änderungen an diesen restriktiven Bestimmungen vorzunehmen.

Die Datenschutzkommission beriet die Regierung zu zahlreichen Gesetzesentwürfen und Verordnungen, so z. B. zum Entwurf einer Verordnung hinsichtlich der Erfassung und Verarbeitung personenbezogener Daten von Schülern, zur Verordnung betreffend die Bedingungen und Modalitäten für die Herausgabe von Katasterunterlagen oder zum Gesetzesentwurf zur Änderung des Wahlgesetzes aus dem Jahr 2003. Weitere Themen waren der Gesetzesentwurf über den freien Personenverkehr und Einwanderung sowie der Entwurf einer entsprechenden Verordnung. Letztere legt genau fest, zu welchen Kategorien personenbezogener Daten der für Einwanderung zuständige Minister Zugang erhalten darf, um alle gesetzlich vorgeschriebenen Kontrollen durchzuführen. Außerdem beriet die CNPD die Regierung zum Gesetzesentwurf über die Ausübung des Arzt-, Zahnarzt- und Tierarztberufes sowie zum Entwurf der entsprechenden Verordnung.

Die Datenschutzkommission beriet die Regierung außerdem im Hinblick auf die Erfassung von Notfallnummern im Einklang mit dem Gesetz über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der elektronischen Kommunikation.

## B. Bedeutende Rechtsprechung

**Zivil- und Strafverfahren**
*Entscheidung des Bezirksgerichts Luxemburg, Berufungsgericht, 5. Strafkammer, über die Wirksamkeit von unter Verletzung des Datenschutzgesetzes von 2002 gesammelten Beweisen (Videoüberwachungsbilder)*

Im Jahr 2007 erklärte das Oberste Berufungsgericht („*Cour de Cassation*") eine Entscheidung des Berufungsgerichts über die Wirksamkeit von unter Verletzung des Datenschutzgesetzes gesammelten Beweisen für ungültig. Grundlage der Entscheidung des Obersten

Berufungsgerichts war die Verletzung des Rechts auf einen fairen Prozess (Artikel 6 der Europäischen Menschenrechtkonvention).

Am 26. Februar 2008 entschied das Berufungsgericht (andere Zusammensetzung), dass die Kombination der Vorlage von unrechtmäßig erworbenen Beweisen (*d. h. ohne vorherige Genehmigung durch die CNPD*) in Gerichtsverfahren und ein Verfahren, das an sich nicht im Einklang mit den Bestimmungen über die Durchführung von strafrechtlicher Verfolgung und gerichtlichen Ermittlungen steht, das Recht auf einen fairen Prozess verletze.

*Bezirksgericht Luxemburg, 16. Strafkammer, über die Verletzung von Artikel 10, 11 und 14 des Datenschutzgesetzes von 2002*

Am 27. Oktober 2008 veröffentlichte die 16. Strafkammer des Bezirksgerichts Luxemburg eine neue Rechtsprechung im Hinblick auf die strafrechtliche Verurteilung einer Person auf der Grundlage des Gesetzes aus dem Jahr 2002. Ein Angestellter eines Friedhofes hatte auf besagtem Friedhof, in der Umgebung sowie in der Leichenhalle ein System zur Videoüberwachung installiert. Die Verarbeitung personenbezogener Daten war jedoch nicht gemäß den Bestimmungen des abgeänderten Gesetzes aus dem Jahr 2002 von der *Datenschutzkommission* genehmigt worden. Da der Angestellte jedoch weiter die personenbezogenen Daten verarbeitete (Videoüberwachung in Echtzeit, Speicherung der Bilddaten auf seinem Computer sowie Erstellung von Kopien zum „*eigenen Vergnügen*"), stellte das Gericht fest, dass er eindeutig gegen die Bestimmungen des Datenschutzgesetzes aus dem Jahr 2002 verstoßen habe, und zog ihn für diese Taten zur Verantwortung.

## C. Wichtige spezifische Themen

### Cyberüberwachung von Angestellten durch den Arbeitgeber

Die CNPD entwarf eine grundlegende Entscheidung zur Cyberüberwachung von Angestellten, um so das Gleichgewicht zwischen dem Schutz der Privatsphäre eines Datensubjektes am Arbeitsplatz und den legitimen Interessen des Arbeitgebers zu gewährleisten.

Die in dieser Entscheidung festgelegten Prinzipien berücksichtigen die gewaltige Anzahl an Genehmigungs- und Informationsanträgen, die zu diesem Thema bei der CNPD eingegangen sind. Die Entscheidung befürwortet den angemessenen Einsatz von Überwachungsinstrumenten und definiert den erlaubten Bereich für solche Sicherheitsmaßnahmen, die ein Arbeitgeber ergreifen darf. Daher darf eine solche Überwachung nur zu bestimmten Zwecken durchgeführt werden, wie z. B. zur Sicherstellung der Funktionalität des IT-Systems, zur Wahrung der Betriebsgeheimnisse und zum Schutz vertraulicher Informationen sowie zur Verhinderung unlauteren Wettbewerbs.

Eine wesentliche Schwierigkeit bei der Cyberüberwachung in diesem Bereich besteht in der Unterscheidung zwischen privater und beruflicher Nutzung. Die CNPD legte fest, dass auf dem Computer des Angestellten gespeicherte Dateien und Nachrichten als berufsbezogen einzustufen sind, sofern sie nicht als privat gekennzeichnet sind.

Private Nachrichten dürfen nicht vom Arbeitgeber geöffnet oder gelesen werden, selbst wenn die Nutzung von Mailsystemen zu privaten Zwecken vorher verboten wurde. Außerdem darf der Arbeitgeber Dateien nicht öffnen oder lesen, die im Beisein des Angestellten als privat gekennzeichnet wurden.

Auf berufsbezogene Dateien und Nachrichten darf jedoch in Abwesenheit des Angestellten oder nach seinem Ausscheiden aus dem Unternehmen zugegriffen werden, um die Aufrechterhaltung des Arbeitsflusses im Unternehmen zu gewährleisten (jedoch nicht, um den Angestellten zu bewerten oder rechtliche Schritte gegen ihn einzuleiten).

Um das Gleichgewicht zwischen den legitimen Interessen der Parteien zu wahren, ist eine vollständige oder permanente Überwachung verboten. Cyberüberwachung darf daher nur begrenzt eingesetzt werden und nur auf der Grundlage gerechtfertigter und greifbarer Beweise für einen Missbrauch ausgeweitet werden.

**E-Catering – automatische Erfassung der Kantinenbesuche von Kindern**

Auf Antrag der CNPD reduzierte das Bildungsministerium die Anzahl der erfassten Datenkategorien sowie den Zeitraum der Speicherung dieser Daten. Außerdem wurde das Recht der Datensubjekte garantiert, gegen die Erfassung und Verarbeitung ihrer Daten Widerspruch einlegen zu können. Diese Maßnahme ist Teil einer europäischen Bemühung zur Stärkung der Rechte von Kindern auf Privatsphäre an Schulen.

**Prüfung der wichtigsten luxemburgischen Telekommunikationsunternehmen**

Im Berichtszeitraum 2007-2008 führte die CNPD eine umfassende Prüfung der wichtigsten luxemburgischen Telekommunikationsunternehmen durch. Ziel war es, einen Überblick darüber zu erhalten, wie Telekommunikationsbetreiber ihre Geschäftstätigkeit in Einklang mit den Bestimmungen des Gesetzes vom 30. Mai 2005 zur Umsetzung der Richtlinie 2002/58/EG bringen.

**Informations- und Aufklärungskampagnen**

Im Laufe des Jahres 2008 führte die Datenschutzkommission ihre Informations- und Aufklärungskampagnen unter anderem durch die aktive Teilnahme an der Arbeit des nationalen Ethikausschusses für die Forschung sowie am zweiten, vom Europarat organisierten Datenschutztag fort. Die Datenschutzkommission stellte über ihre Website und in Interviews in den luxemburgischen Medien Informationen zu den neuen gesetzlichen Bestimmungen zur Verfügung.

# Malta

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

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

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

**Weitere Entwicklungen in der Gesetzgebung**
Die Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG wurde durch zwei Rechtsinstrumente zur Änderung der genannten Verordnungen in lokales Recht umgesetzt. Die gesetzliche Mitteilung 198 aus dem Jahr 2008 zur Änderung der gesetzlichen Mitteilung 16 aus dem Jahr 2003 sowie die gesetzliche Mitteilung 199 aus dem Jahr 2008 zur Änderung der gesetzlichen Mitteilung 19 aus dem Jahr 2003 wurden beide im Amtsblatt veröffentlicht und traten am 29. August 2008 in Kraft.

Die Verordnungen verpflichten Dienstleistungsanbieter, die im Rahmen der Richtlinie erfassten Informationen für einen Zeitraum von einem Jahr (bei Telefonie- und Mobilfunkdaten) bzw. für den Zeitraum von sechs Monaten (bei internetbezogenen Daten) zu speichern. Diese Informationen dürfen ausschließlich der Polizei oder dem Sicherheitsdienst auf Antrag offen gelegt werden, und zwar nur dann, wenn ein schweres Verbrechen vorliegt.

## B. Bedeutende Rechtsprechung

Keine nennenswerte.

## C. Wichtige spezifische Themen

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

Im Laufe des Jahres 2008 gingen 31 Beschwerden beim Datenschutzbeauftragten ein. Jeder Fall wurde untersucht und die Entscheidung gemäß dem Ergebnis der Untersuchungen und unter Berücksichtigung aller Faktoren kommuniziert. Häufigste Beschwerdegründe waren die Anbringung von CCTV-Systemen durch Privatpersonen, die Versendung elektronischer Mitteilungen zu Zwecken der Direktvermarktung ohne Einhaltung der gesetzlichen Vorschriften sowie die Einführung biometrischer Systeme am Arbeitsplatz ohne vorherige Mitteilung an die Datenschutzbehörde.

Im Berichtszeitraum führte der Datenschutzbeauftragte zahlreiche Prüfungen von Verarbeitungen personenbezogener Daten durch Datenkontrolleure durch. Diese Prüfungen wurden auf Anregung des Datenschutzbeauftragten sowie zur Einhaltung der europäischen Verpflichtungen als Teil der Strategie der Datenschutzbehörde zur Bewertung einer bestimmten Branche im Rahmen von Untersuchungen hinsichtlich eingegangener Beschwerden durchgeführt.

Im Laufe des Jahres hat die Datenschutzbehörde durch die Teilnahme an der Artikel 29 Datenschutzgruppe, der Europäischen Konferenz der Datenschutzbehörden, der Internationalen Konferenz zur Privatsphäre und zum Schutz personenbezogener Daten, an Treffen der gemeinsamen Aufsichtsbehörden für das Schengener Abkommen, den Zoll, Europol und Eurodac, am Workshop zur Fallbehandlung und an Eurojust (Europarat) sowie an der Arbeit des Büros des Beratungsausschusses der Konvention zum Schutz von Privatpersonen im Hinblick auf die automatische Erfassung personenbezogener Daten ihren Beitrag zu europäischen und internationalen Foren geleistet.

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

Am 28. Januar feierte der Datenschutzbeauftragte zusammen mit den anderen europäischen Datenschutzbehörden den Europäischen Datenschutztag. An diesem Tag verteilte die Datenschutzbehörde Poster und Mauspads in Schulen, um die jüngere Generation für das Thema Datenschutz zu sensibilisieren. Dies verdeutlicht das starke Engagement der Datenschutzbehörde, den Kindern die neue Datenschutzkultur zu vermitteln, damit sie ihre Grundrechte schätzen und anwenden lernen.

Die Botschaft dieses Jahres befasste sich mit der Nutzung des Internets und der Bedeutung des Bewusstseins für potenzielle Risiken für die Privatsphäre, denen die personenbezogenen Daten ausgesetzt sein können, wenn sie im Internet angegeben werden. Die Datenschutzbehörde betonte, dass die Identität jedes Einzelnen wertvoll sei und sie daher unbedingt geschützt werden müsse. Als Teil der Aktivitäten sprach der Datenschutzbeauftragte mit Unterstützung des Büros des Premierministers auch mit allen Datenschutzbeauftragten des öffentlichen Dienstes.

Im Juni wurde ein Gesetz zur Informationsfreiheit („Freedom of Information Act") im Parlament vorgestellt. Es etabliert das Recht auf Informationen, die bei öffentlichen Behörden gespeichert sind, um so eine bessere Transparenz und stärkere Rechenschaftspflicht der Regierung zu erreichen. Das Gesetz wird dem Datenschutzbeauftragten nach Inkrafttreten zusätzliche Funktionen und die Pflichten eines Informationsbeauftragten übertragen.

Im Laufe des Jahres verlor die Datenschutzbehörde den Datenschutzbeauftragten Paul Mifsud-Cremona, der am 14. August verstarb. Herr Mifsud-Cremona hatte dieses Amt seit 1. Januar 2004 inne. Im Dezember ernannte der Premierminister, nach vorheriger Beratung und in Absprache mit dem Oppositionsführer, Herrn Joseph Ebejer zum neuen Datenschutzbeauftragten. Der neue Datenschutzbeauftragte soll Anfang kommenden Jahres formal ernannt werden.

## Niederlande

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

Die Richtlinie 95/46/EG wurde per *Wet bescherming persoonsgegevens* (Wbp, niederländisches Datenschutzgesetz] in nationales Recht umgesetzt. Das Gesetz vom 6. Juli 2000[18] trat am 1. September 2001 in Kraft und ersetzte damit das alte Datenschutzgesetz *Wet persoonsregistraties* (*Wpr*) vom 28. Dezember 1988.

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

### B. Bedeutende Rechtsprechung und wichtige spezifische Themen

Im vergangenen Jahr konnte die niederländische Datenschutzbehörde (DSB – College bescherming persoonsgegevens) ihre Position als Aufsichtsbehörde deutlich stärken. Der Schwerpunkt ihrer Arbeit liegt auf der Überprüfung der Einhaltung von Vorschriften zur Verarbeitung personenbezogener Daten sowie auf Vollstreckungsmaßnahmen im Falle von Verstößen gegen diese Vorschriften. Im Jahr 2008 begann die DSB damit, systematisch die Dinge anzugehen, die im vorangegangenen Jahr angekündigt worden waren: Vor allem wurden Personal und Ressourcen zur Durchführung von Untersuchungen zur Einhaltung der relevanten gesetzlichen Vorschriften sowie zur Durchführung von Vollstreckungsmaßnahmen im Fall von Verstößen gegen diese Vorschriften eingesetzt. Die DSB traf im Jahr 2008 auf der Grundlage von Risikoanalysen auch klarere Entscheidungen zur Bearbeitung der großen Anzahl verschiedener Themen, die ihr vorgetragen wurden. Vorrangig für die niederländische DSB waren strukturelle Themen und Verstöße, die viele Menschen betreffen – insbesondere Risikogruppen. Die Risikoanalyse wurde auf der Grundlage eines von uns entwickelten und von Experten getesteten Systems sowie auf der Grundlage von Warnungen erstellt, die uns über verschiedene Wege erreichen. Ziel war die Bestimmung der Sektoren, in denen (1) viele Bürger einem (2) großen Risiko von (3) schweren und strukturellen Verstößen gegen das Datenschutzgesetz ausgesetzt sind. Der Politikplan der DSB für das Jahr 2008 nahm auf dieser Grundlage konkrete Formen an.

Die Zahlen für 2008 sind vielversprechend: Die niederländische DSB führte in ihrer Funktion als Aufsichtsbehörde in 95 Fällen (50 % mehr als im Jahr 2007) Untersuchungen durch und verhängte in 68 Fällen Strafmaßnahmen oder drohte deren Verhängung an. Diese Zahl ist fast doppelt so hoch wie die aus dem Jahr 2007 (2007: 39; 2006: 2!).

**Das Internet**

Im vergangenen Jahr ging bei der DSB eine große Anzahl von Beschwerden und Hinweisen zur Veröffentlichung personenbezogener Daten im Internet ein. Hierzu gehörten insbesondere Anträge auf Löschung der Daten sowie Fragen zu den Rechten, die eine Person hat, wenn ihre Daten im Internet veröffentlicht werden. Mithilfe von Vollstreckungsmaßnahmen gegen Websites, die strukturell gegen das Datenschutzgesetz (Wet bescherming persoonsgegevens, Wbp) verstoßen, möchte die DSB die Aufmerksamkeit sowohl der Datenkontrolleure als auch der Datensubjekte erhöhen. Beide Parteien müssen sich über die Rechte von Datensubjekten sowie die Notwendigkeit der Einhaltung dieser Rechte im Klaren sein.

Eine Sofortmaßnahme gegen eine Website, auf der personenbezogene Daten von Beamten und Politikern abrufbar waren, führte in Rekordzeit zum Erfolg: Der Zugang zu der Website wurde innerhalb nur eines Tages gesperrt. Eine Maßnahme gegen eine Gemeinde, die die Anträge auf eine Planungsgenehmigung zusammen mit

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

[19] Gesetz vom 19. Oktober 1998 bezüglich der im Telekommunikationsbereich geltenden Regelungen (Telecommunicatiewet – Telekommunikationsgesetz), Staatsblad van het Koninkrijk der Nederlanden (Amtsblatt der Gesetze, Gesetzesverordnungen und Erlasse) 2004, 189.

personenbezogenen Daten und der Unterschrift des Antragstellers sowie Namen und Unterschrift des zuständigen Beamten auf ihrer Website veröffentlichte, führte zur Entwicklung eines neuen Online-Antragsformulars, das in den ganzen Niederlanden verwendet werden soll. Die unrechtmäßige Veröffentlichung dieser personenbezogenen Daten wurde beendet.

Die heimliche Speicherung der IP-Adressen von Besuchern der Website Geencommentaar.nl („Kein Kommentar") zum Zwecke der Veröffentlichung dieser Liste für andere wurde von der DSB für unrechtmäßig erklärt. Als Reaktion hierauf gab der Datenkontrolleur an, dass die Liste vernichtet und die Software von der Website entfernt worden sei. Auch die Website beoordeelmijnleraar.nl („Bewerte meinen Lehrer") wurde für unrechtmäßig erklärt. Darauf hin nahm der Eigentümer der Website zahlreiche Änderungen an ihr vor. Zusammen mit der unabhängigen Post- und Telekommunikationsbehörde (Onafhankelijke Post- en Telecommunicatie Autoriteit, OPTA) konnte die DSB erfolgreich gegen Dienste vorgehen, die Inverssuchen – Angabe der Telefonnummer, um den dazugehörigen Namen und die Adresse herauszufinden – anbieten und Spezifikationen erarbeiten, unter welchen Bedingungen virales Marketing gestattet ist.

**Unternehmen und Arbeit**

Das Thema medizinische Daten von Angestellten ist äußerst heikel. Nach einer Untersuchung eines Arbeitsschutzdienstes vermutete die niederländische DSB, dass andere Arbeitsschutzdienste diese Daten ebenfalls systematisch an Arbeitgeber weitergeben könnten. Aus diesem Grund wurde die Entscheidung getroffen, die Verarbeitung dieser Daten auch bei anderen Arbeitsschutzdiensten zu untersuchen. Die Untersuchung wird im Jahr 2009 fortgesetzt.

Im Hinblick auf Daten zu sensiblen Informationen zur finanziellen Lage einer Person muss mit größtmöglicher Sorgfalt vorgegangen werden. Das nationale Schuldeninformationssystem (Landelijk Informatiesysteem Schulden) reichte den Entwurf eines Registrierungssystems bei der DSB zweimal zur Bewertung ein. Der Entwurf wurde in beiden Fällen von der DSB zurückgewiesen. Die Datenverarbeitung wäre unzureichend abgegrenzt gewesen, und die Gruppe von Personen, die Zugang zu diesen Daten gehabt hätte, wäre zu groß gewesen und hätte somit das Risiko eines Schadens für versehentlich in das System eingegebene Personen geborgen.

Eines der strukturellen Probleme beim Schutz der Privatsphäre ist die Tatsache, dass viele Menschen nicht wissen, wohin ihre Daten gelangen und was damit geschieht. Werden Ermittlungen zu Personen durchgeführt – sei es von einer privaten Detektei oder von der Abteilung für Sozialversicherungsbetrug (Afdeling Sociale Recherche) –, so müssen diese Personen nach Beendigung der Ermittlungen darüber informiert werden. Nach einer Untersuchung stellte die DSB fest, dass die Verpflichtung, diese Information offen zu legen, in vielen Fällen nicht eingehalten wird. Die DSB wird diesbezüglich auch weiterhin wachsam bleiben. Auch die Erfassung von Daten im Hinblick auf eine effizientere und bewusstere Energienutzung muss im Einklang mit dem Datenschutzgesetz erfolgen. Nach einer Kritik der DSB wurde eine Reihe von Maßnahmen zum Schutz der Privatsphäre in den Gesetzesvorschlag betreffend die Einführung intelligenter Energieverbrauchszähler integriert.

**Verkehr**

Nach jahrelangen Streitigkeiten betreffend die Verwendung von Reisedaten zu Werbezwecken in Folge der Einführung einer Chipkarte für den öffentlichen Verkehr (OV-chipkaart) und der Veröffentlichung einer Studie der DSB zur Verwendung der Karte für das U-Bahn-System in Amsterdam schlugen die öffentlichen Verkehrsunternehmen schließlich ein System vor, das die Anforderungen des Datenschutzgesetzes respektiert. Die DSB wird die Umsetzung des Systems und die Einhaltung der festgelegten Standards überwachen. Eine im Jahr 2008 durchgeführte offizielle Untersuchung der Verarbeitung personenbezogener Daten betreffend die Chipkarte, die ab 29. Januar 2009 in der U-Bahn in Rotterdam zur Pflicht wird, kam zu dem Schluss, dass es keinen Grund gebe, zum gegenwärtigen Zeitpunkt weitere Schritte einzuleiten. Das auf einem Kilometerpreis basierende System könnte auch zu einem detaillierteren Bild des Reiseverhaltens führen, in diesem Falle hinsichtlich einzelner Kraftfahrer. Die DSB hat sich im Unterhaus für eine Minimierung der Daten ausgesprochen.

Die Überwachung von Autos, die bestimmte Strecken fahren, betrifft alle Bürger, die ein Auto fahren, also auch die, die nichts zu verbergen haben. Die DSB hat Leitlinien zur automatischen Nummernschilderkennung (ANPR) entwickelt, die die Frage, was bei der Umsetzung dieser Methode erlaubt ist und was nicht, endgültig klären sollen. Die Polizei darf gescannte Daten nicht speichern und verarbeiten. Es muss verhindert werden, dass alle Kraftfahrer als potenzielle Verdächtige angesehen werden.

**Gesundheitswesen**

Bei der Verarbeitung von gesundheitsbezogenen Daten sind besondere Sorgfalt und geeignete Sicherheitsmaßnahmen erforderlich. Im Gesetzesvorschlag betreffend eine elektronische Patientenakte wird dieser sehr wichtige Rat der DSB berücksichtigt. Prinzipiell haben nur Fachleute Zugang zu den Krankenakten, die die betreffenden Patienten auch tatsächlich behandeln.

Die DSB betont die Notwendigkeit, dass Bürger (und insbesondere Patienten) das Recht haben müssen, zu wissen, wer, wann und wie Zugang zu ihren Daten hat. Außerdem müssen sie das Recht haben, zu wissen, dass diese Daten in anderen Bereichen des Gesundheitswesens, in denen ebenfalls personenbezogene daten ausgetauscht werden, sicher verarbeitet werden. Dieses Recht gilt, wenn Versicherungsunternehmen Daten zu versicherten Parteien, die gesundheitliche Probleme und Anspruch auf eine Kostenübernahme haben, an die allgemeine Verwaltungsstelle übertragen. Es gilt auch, wenn ein Versicherer einem anderen Versicherer personenbezogene Daten weitergibt, wenn Bündelverträge übertragen werden. Es gilt für die nationale Verarbeitung von Daten zur allgemeinen Pflegeanmeldung im Rahmen des Gesetzes über außergewöhnliche medizinische Ausgaben (Algemene wet bijzondere ziektekosten). Es gilt bei der Ausgabe von Daten an die Pflegeversicherungsbehörde (College voor Zorgverzekeringen) zum Zwecke der Erfassung ausstehender Krankenversicherungsprämien. Es gilt auch für die Nutzung der Bürgerservicenummer (Burgerservicenummer, BSN) im Gesundheitswesen: Bei der Verarbeitung und Bereitstellung personenbezogener Daten muss ein bestimmtes Maß an Informationssicherheit gewährleistet werden.

Die Einhaltung des erforderlichen Maßes an Informationssicherheit kann nicht immer vorausgesetzt werden, wie die Untersuchung der Inspektion für das Gesundheitswesen (Inspectie voor de Gezondheidszorg) durch die DSB zeigte. Keines der 20 untersuchten Krankenhäuser erfüllte diese Anforderung. Dies könnte schwer wiegende Folgen für die Qualität der bereitgestellten Versorgungsleistungen und für die Privatsphäre der Patienten haben. Die Krankenhäuser müssen zeigen, dass sie diese Anforderung erfüllen und müssen darlegen, wie sie dies erreichen wollen.

**Junge Menschen**

Die digitale Verarbeitung personenbezogener Daten im Allgemeinen sowie deren Verarbeitung durch die Regierung im Besonderen erfordert ausdrücklich Sicherheitsmaßnahmen. Dies gilt umso mehr, wenn es um Informationen zu Kindern und jungen Menschen geht.

Im Jahr 2008 gab die DSB einen äußerst dringlichen Rat zu einem Gesetzesvorschlag, der die Schaffung eines Referenzindexes für gefährdete junge Menschen (Verwijsindex Risicojongeren) zur Folge hätte. Laut der DSB steht dieser Vorschlag im Widerspruch zum Datenschutzgesetz. Der Schwerpunkt der Kritik liegt insbesondere auf dem nicht hinreichend spezifischen Gegenstand des Referenzindexes sowie auf seinen unklaren Kriterien für die Registrierung eines jungen Menschen durch seinen Versorgungsanbieter. Dies bringt ein fast unvermeidbares Risiko für Willkür mit sich. Obwohl der am 6. Februar 2009 eingereichte Gesetzesvorschlag die Kritik der DSB – unter anderem – berücksichtigt, so ist er doch im Wesentlichen leider unverändert geblieben.

Oft wird behauptet, dass die Vorschriften zur Privatsphäre die korrekte Umsetzung von Kinderschutzmaßnahmen verhindern. Dieser Mythos wurde im Rahmen einer Rundtischkonferenz im April 2007 widerlegt, an der die DSB und Experten aus dem Bereich der Kinderpflege teilnahmen. Die DSB ist bereit, dem Entwurf für einen Gesetzesvorschlag zur Änderung der Kinderschutzmaßen zuzustimmen. Dieser Entwurf umfasst ein *Recht*, sich zu äußern. Wenn es im Interesse des Kindes erforderlich ist, die Schweigepflicht eines Arztes (in der Arzt-Patienten-Beziehung) aufzuheben, so muss es dem Pflegeanbieter möglich sein, sich zu äußern.

Grundschulen stellen Entwicklungsberichte über ihre Schüler für Sekundarschulen aus. Die DSB hat die Einhaltung der Auskunftspflicht gegenüber den Eltern der Kinder in dieser Situation überprüft. Dies ist im Hinblick auf die Möglichkeit der Korrektur eines Berichtes unerlässlich, der einen langfristigen negativen Effekt auf das betreffende Kind haben kann, wenn er falsche oder veraltete Informationen enthält.

**Polizei und Justizbehörden**

Eine schwere Form des Missbrauchs personenbezogener Daten kommt in den Niederlanden immer häufiger vor – der Identitätsbetrug. Um diesen Diebstahl von personenbezogenen Daten zu bekämpfen, ist die Einhaltung der Auskunftspflicht von größter Bedeutung, damit das Datensubjekt auch darüber informiert ist, dass eine Organisation seine personenbezogenen Daten verarbeitet und welche Daten verarbeitet werden. Im Jahr 2008 erforschte die DSB im Rahmen von Treffen mit Experten sowie durch eine Literaturstudie die unterschiedlichen Möglichkeiten zur Vermeidung und Bekämpfung des Identitätsbetruges.

Die Sicherstellung der korrekten und transparenten Verwendung personenbezogener Daten ist auch im Hinblick auf die erweiterten Befugnisse wichtig, die Polizei und Justizbehörden bei der Verarbeitung personenbezogener Daten gewährt wurden. Im Jahr 2007 vertrat die DSB den Standpunkt, dass eine Gesetzgebung, die die Möglichkeit einer Verwandtschaftsbestimmung per DNS-Test als Teil eines Strafverfahrens zulässt, gegen das Datenschutzgesetz verstoße. In einem zweiten Vorschlag (Oktober 2008) berücksichtigte der Minister die Kritik der DSB.

Hinsichtlich des Vorschlags der Staatsanwaltschaft (Openbaar Ministerie) zur Erweiterung der Untersuchungsberichte – z. B. durch die Nutzung von Internet und Telefon – empfahl die DSB die Integration geeigneter Sicherheitsmaßnahmen, um zu gewährleisten, dass diese Berichte nicht über Suchmaschinen zu finden sind und dass etwaige Fehler schnell korrigiert werden. Der Bericht „Anleitungen zu den Untersuchungsberichten" (*Aanwijzing opsporingsberichtgeving*) wird als Reaktion auf diese Kritik hin abgeändert werden. Die DSB erteilte auch einen dringenden Rat zur Bereitstellung von Verbrechensdaten aus Datenbanken der Staatsanwaltschaft an Datensubjekte und Dritte für Zwecke, die nicht mit dem Strafverfahren in Zusammenhang stehen. Die DSB ist der Ansicht, dass dies nur in bestimmten Fällen gestattet sein sollte und dann auch nur, wenn es absolut erforderlich ist. Eine Zweckmäßigkeit allein ist nicht ausreichend.

Die DSB veröffentlichte einen Untersuchungsbericht über den internen Austausch personenbezogener Daten über das Informationssystem bei der Polizei. Die überwältigende Mehrheit der Polizeibezirke war nicht hinreichend ausgerüstet, um die Anforderungen des Polizei-Datenschutzgesetzes (Wet politiegegevens) einzuhalten, das am 1. Januar 2008 in Kraft getreten ist.



## Polen

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

Im Berichtszeitraum führte der Generalinspektor für den Schutz personenbezogener Daten Maßnahmen zur Einführung von Änderungen des Datenschutzgesetzes durch, die *unter anderem* Folgendes betreffen: Verbesserte Effizienz der Umsetzung administrativer Entscheidungen der Datenschutzbehörde im Hinblick auf nicht-finanzielle Verpflichtungen; Integration einer Strafbestimmung in das Datenschutzgesetz für den Fall der Verhinderung oder Behinderung von Prüfungen; Spezifizierung der Bestimmungen des Datenschutzgesetzes im Hinblick auf die Inhalte des Prüfprotokolls; Regelung der Widerrufs der Zustimmung zur Verarbeitung personenbezogener Daten (Artikel 7 (5) des Gesetzes); Möglichkeit der Einrichtung lokaler Einheiten (Zweigstellen) des Büros des Generalinspektors für den Schutz personenbezogener Daten; so genannte Kontaktaufnahmen mit öffentlichen Behörden, Selbstverwaltungseinheiten sowie natürlichen und juristischen Personen, die personenbezogene Daten verarbeiten (Einführung einer Verpflichtung zur Reaktion auf eine solche Kontaktaufnahme binnen 30 Tagen ab Eingang der Kontaktaufnahme); Aufhebung von Artikel 29 des Datenschutzgesetzes (über die Möglichkeit der Offenlegung personenbezogener Daten zum Zwecke der Integration dieser Daten in ein Datenablagesystem oder zu anderen Zwecken) – eine Offenlegung personenbezogener Daten darf nur gemäß den in Artikel 23 oder 27 des Datenschutzgesetzes genannten Bestimmungen erfolgen.

Auf Initiative des Generalinspektors wurde eine Verordnung vom Minister für Inneres und Verwaltung hinsichtlich der Vorlage für ein Antragsformular zur Anmeldung des Datenablagesystems für eine Registrierung beim Generalinspektor verabschiedet. Zweck dieser neuen Bestimmungen ist es, Antragstellern dabei zu helfen, Anmeldeformulare zum Zeitpunkt der Anmeldung von Datenablagesystemen für eine Registrierung auszufüllen, da die frühere Praxis gezeigt hat, dass ihnen dies oftmals ernste Probleme bereitet (die meisten Felder wurden durch Auswahlbuttons ersetzt), sowie zur Gewährleistung einer besseren Transparenz des Formulars und der Einhaltung der grundlegenden Pflichten des Kontrolleurs. Es ist erwähnenswert, dass der Generalinspektor zuvor bereits oftmals die Registrierung eines Datenablagesystems abgelehnt hatte, wenn Fehler in den Anmeldeformularen gefunden wurden. Dies hatte negative Auswirkungen auf die wirtschaftliche Tätigkeit des Antragstellers oder verhinderte die Fortführung dieser Tätigkeit sogar gänzlich.

### B. Bedeutende Rechtsprechung

Im Berichtszeitraum wurde der Rechtsstreit betreffend eine kommerzielle Weitergabe personenbezogener Daten von Anschlussinhabern von Telekomunikacja Polska S.A. (Telekommunikationsbetreiber), die eingewilligt hatten („Opt-Out"), dass ihre personenbezogenen Daten in einem Telefonverzeichnis veröffentlicht werden, an Dritte beendet. Das Verwaltungsgericht entschied, dass gemäß dem Standpunkt des Generalinspektors die unausgesprochene Einwilligung (d. h. nicht erfolgter Widerspruch) zur Veröffentlichung der Daten im Telefonverzeichnis keine unabhängige Voraussetzung für die Weitergabe dieser Daten an Dritte ist. In anderen Fällen, in denen es um die Erhebung von Gebühren für die Bereitstellung von Informationen zu Datensubjekten durch das Kreditregister (BIK S.A.) ging, stützte das Gericht die Ansicht des Generalinspektors, der zufolge die Erhebung einer Gebühr illegal ist. Der Fall wurde an das Oberste Verwaltungsgericht übergeben und ist derzeit anhängig. Eine weitere wichtige Entscheidung betraf das Verbot der Verarbeitung personenbezogener Daten in Backup-Dateien ab dem Zeitpunkt, an dem sie aus dem Datenablagesystem gelöscht wurden. Das Gericht entschied, dass eine solche Praxis nicht zulässig sei. Es wurde bemerkt, dass eine Organisation, die entscheidet, Daten zu löschen, diese auch vollständig löschen muss. Darüber hinaus erließ das Verwaltungsgericht eine Entscheidung zur Legalität der Verarbeitung personenbezogener Daten von Bankkunden durch das Kreditregister (BIK S.A.) zu statistischen Zwecken für einen Zeitraum von 12 Jahren (gemäß Paragraph 5, Artikel 105 des Bankengesetzes). Der Generalinspektor für den Schutz personenbezogener Daten untersuchte aus der Perspektive der Verpflichtung zur Offenlegung öffentlicher Informationen die Frage des Schutzes von in Erklärungen zur finanziellen Lage von Personen mit Ämtern in öffentlichen

Verwaltungsbehörden aufgeführten personenbezogenen Daten. Der Generalinspektor stufte die Offenlegung der Wohnadressen von Personen, die Erklärungen zu ihrer finanziellen Lage sowie Adressen ihres Eigentums einreichen, als illegal ein. Der Generalinspektor untersuchte außerdem die Veröffentlichung von Verordnungen des Gemeinderates einschließlich Vornamen, Nachnamen oder Wohnadressen der Personen, für die die Verordnung gilt, auf der Website des öffentlichen Informationsblattes. Es wurde festgelegt, dass die Offenlegung von Daten, die eine vollständige Identifikation der betreffenden Person ermöglichen, zur Einhaltung der Verpflichtung zur Bereitstellung von Informationen im Rahmen des Gesetzes über den Zugang zu öffentlichen Informationen nicht erforderlich ist. Es wurde entschieden, dass diese Praxis das Recht der betreffenden Personen auf Privatsphäre verletzt und dass der Umfang der veröffentlichten Daten für den Zweck der Veröffentlichung von Verordnungen nicht relevant ist. Der oben genannte Standpunkt wurde durch die Entscheidung des Verwaltungsgerichtes gestützt. Im Jahr 2008 untersuchte der Generalinspektor auch die Legitimität von bei Zeitungsverlagen eingereichten Anträgen. Hierunter war auch ein Antrag auf Herausgabe personenbezogener Daten von Journalisten, die für die Einreichung einer Zivilklage gegen diese Personen wegen der Verletzung persönlicher Rechte in Presseveröffentlichungen erforderlich waren. In den meisten Fällen ordnete der Generalinspektor die Herausgabe dieser Daten an, sofern die Daten für die Einreichung einer Zivilklage gegen die betreffenden Datensubjekte tatsächlich erforderlich waren und die Herausgabe somit im Einklang mit Paragraph 2, Artikel 29 des Datenschutzgesetzes stand.

## C. Wichtige spezifische Themen

In Zusammenhang mit Polens Beitritt zum Schengen-Raum war es erforderlich, die Genauigkeit der Verarbeitung personenbezogener Daten im Schengener Informationssystem (SIS) zu untersuchen. Die Organisationen, denen der direkte Zugang zum nationalen Informationssystem gewährt wurde, um Einträge im SIS vorzunehmen und auf Daten des SIS zuzugreifen (Polizei, Grenzschutz, Zollkammern und Konsulate), wurden überprüft. Im Laufe der Überprüfungen wurden einige Unregelmäßigkeiten festgestellt (z. B. wurden die Personen, die auf Daten des SIS zugreifen konnten, nicht aufgelistet, es gab keine schriftlichen Genehmigungen, keine Spezifikation des Umfangs der Genehmigung zur Verarbeitung personenbezogener Daten und keine Ausweise für zugangsberechtigtes Personal). Diesbezüglich übersandte der Generalinspektor dem Obersten Polizeichef, dem Chef des Grenzschutzes und dem Leiter des Zollamtes einen schriftlichen Antrag mit der Aufforderung, Maßnahmen zur Korrektur der angegebenen Versäumnisse zu ergreifen.

Darüber hinaus wurden einige Änderungen an der zum Ausfüllen der Anmeldeformulare verwendeten Software vorgenommen, die zum Zeitpunkte der Anmeldung von Datenablagesystemen zur Registrierung verwendet wurde, um die Anzahl der von den Antragstellern gemachten Fehler beim Ausfüllen eines solchen Registrierungsformulars zu minimieren und es auch jenen, die über keine elektronische Signatur verfügen, zu ermöglichen, einen Antrag einzureichen. Die Änderungen werden den Prozess der Registrierung von Datenablagesystemen erheblich verbessern und die Einhaltung der Pflicht, Datensysteme zur Registrierung anzumelden, für die betreffenden Antragsteller vereinfachen. Die betreffende Software bildet zusammen mit dem Online-Register für Datenablagesysteme die „Elektronische Plattform des Generalinspektors für den Schutz personenbezogener Daten" (e-GIODO-Plattform).

Als Reaktion auf die steigende Anzahl von Fragen zur Verarbeitung personenbezogener Daten im Zusammenhang mit der Nutzung moderner Technologien führte das Büro des Generalinspektors eine Analyse einer geeigneten Interpretation der Begriffe IP-Adresse, elektronische Post, Cookie-Dateien, IMEI-Nummer, Benutzername und Login durch. Die Analyse soll ein hilfreiches Instrument für eine rechtliche Bewertung der Frage sein, ob die oben genannten Informationen im Einzelfall als personenbezogene Daten einzustufen sind. Außerdem wurde eine Sonderarbeitsgruppe für moderne Technologie innerhalb des Büros eingerichtet, die Standpunkte von Behörden, rechtliche Stellungnahmen, Leitlinien, Anmerkungen, Politiken usw. zu Fragen der Verarbeitung personenbezogener Daten mit Hilfe von Informations- und Kommunikationstechnologien im weitesten Sinne des Begriffes erarbeiten soll.

Weiterhin organisierte der Generalinspektor vom 1. bis 4. Juni 2008 das 10. Treffen der mittel- und osteuropäischen Datenschutzbehörden. *Unter anderem* wurden die Themen Schutz der Online-Privatsphäre von Kindern, Aufgaben der mittel- und osteuropäischen Datenschutzbehörden im Rahmen der Erweiterung des Schengen-Raumes, Qualifikationen, Aufgaben und Befugnisse von Datenschutzbeauftragten diskutiert, und das Forum der mittel- und osteuropäischen Datenschutzbehörden bewertete die Arbeit der vergangenen zehn Jahre. Zwei endgültige Erklärungen zur weiteren Zusammenarbeit im Rahmen des Forums sowie zur Gleichbehandlung der Landessprachen aller EU-Mitgliedstaaten wurden verabschiedet.

Im Bereich Bildungsmaßnahmen führte das Büro des Generalinspektors 62 Schulungskurse zum Thema Schutz personenbezogener Daten durch, *unter anderem* in folgenden Institutionen: Ministerien, Gerichte, Steueraufsicht, nationaler Rat der Rechtsberater, Konsulat der Republik Polen in Brüssel, nationale Kammer der Steuerberater sowie Amt für öffentliches Beschaffungswesen (insgesamt wurden etwa 1.700 Personen geschult). Im Zusammenhang mit Polens Beitritt zum Schengen-Raum wurden spezielle Schulungskurse hinsichtlich der Verarbeitung personenbezogener Daten im SIS für die Ausbilder in Polizeipräsidien und beim Grenzschutz durchgeführt.

Darüber hinaus wurde die neue E-Learning-Plattform „eduGIODO" gestartet, um Kenntnisse zum Schutz personenbezogener Daten praktisch und mit Hilfe moderner Technologie zu vermitteln. Sie bietet allen interessierten Parteien ein breites Spektrum an Informationen zum Thema Datenschutz und ist in spezielle Module untergliedert, die sich jeweils mit speziellen Themen befassen (so genannte „ABCs"). Diese „virtuelle Universität" bietet verschiedene Schulungskurse mit Schwerpunkt auf dem jeweiligen spezifischen Aspekt des Datenschutzes (Rechte von Datensubjekten, allgemeine Prinzipien des Datenschutzes sowie die Pflichten der Datenkontrolleure). Zum Start der „eduGIODO"-Plattform wurden zwei landesweite Konferenzen (in Warschau und Danzig) veranstaltet, bei denen die wesentlichen Ziele der Plattform hinsichtlich des Schutzes personenbezogener Daten vorgestellt wurden.

Der Generalinspektor für den Schutz personenbezogener Daten organisierte im Rahmen des TAIEX-Programms einen Workshop zu den in der EU-Datenschutzgesetzgebung im Zusammenhang mit der Umsetzung des gemeinschaftlichen Besitzstandes (*acquis communautaire*) im Bereich des Schutzes personenbezogener Daten festgelegten Änderungen. Der Workshop richtete sich hauptsächlich an Richter und Staatsanwälte.

Im vergangenen Jahr nahmen die Angestellten des Büros des Generalinspektors für den Schutz personenbezogener Daten am Projekt zum Erfahrungsaustausch zwischen Angestellten von Datenschutzbehörden teil. Das Projekt wurde im Rahmen des Leonardo da Vinci-Programms zum lebenslangen Lernen mit dem Titel „Neue Kompetenzen für mit der Umsetzung von Datenschutzbestimmungen betraute Personen" durchgeführt. Das Projekt trug zur Verbesserung des Kenntnisstandes und der Fähigkeiten in den Bereichen Umsetzung von Gemeinschaftsrecht, Austausch von Erfahrungen zum Betrieb von Datenschutzbehörden, Integration von in Partnerländern angewendeten Verfahren in das polnische System, Verbesserung der Mobilität der Angestellten sowie Sprachkenntnisse bei.

Der Generalinspektor und der Verband für Direkt-Marketing unterzeichneten eine Vereinbarung zur Zusammenarbeit mit dem Ziel der Verbesserung des Schutzes personenbezogener Daten sowie der Gewährleistung des Rechtes der Bürger auf Privatsphäre im Bereich Direkt-Marketing.

Bildungsmaßnahmen spielen bei den Aufgaben des Generalinspektors für den Schutz personenbezogener Daten eine besondere Rolle. Diese wurden *unter anderem* durch eine breite Zusammenarbeit mit den Medien umgesetzt. Im Jahr 2008 gab der Generalinspektor etwa 100 Interviews, in denen er seine Standpunkte darlegte oder verschiedene Fragen zum Schutz personenbezogener Daten kommentierte und erläuterte.

## Portugal

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

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

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

Die Richtlinie 2006/24/EG (Richtlinie über die Vorratsspeicherung von Daten) wurde per Gesetz 32/2009, das im August 2009 in Kraft trat, in nationales Recht umgesetzt. Das Gesetzgebungsverfahren wurde im Jahr 2008 gestartet, und die Datenschutzbehörde (DSB) wurde von der Regierung sowie später vom Parlament gebeten, Stellung zum Gesetzesentwurf zu nehmen. Die Überlegungen und Vorschläge der DSB wurden im endgültigen Gesetzestext umfassend berücksichtigt. Der maximale Zeitraum zur Speicherung von Daten wurde auf ein Jahr festgelegt. Die Verbrechen, bei denen eine Untersuchung von Traffic-Daten gestattet ist, sind im Gesetz angegeben. Ebenso ist die Verpflichtung für Richter angegeben, diese Daten nach Feststellung der Rechtsgrundlage direkt bei den Telekommunikationsanbietern anzufordern. Eine Liste des Personals, das zu rechtlichen Zwecken auf die Traffic-Daten zugreifen darf, sowie regelmäßige Berichte zu den untersuchten Daten wurden der DSB übermittelt. Die Kommunikation zwischen den Richtern und den Telekommunikationsanbietern erfolgt online über ein spezielles Formular.

### B. Bedeutende Rechtsprechung

Keine nennenswerte.

### C. Wichtige spezifische Themen

**Allgemeine Aktivitäten**
Die portugiesische DSB steigerte ihre Aktivitäten im Jahr 2008 erheblich. Die Anzahl von Meldungen bezüglich der Verarbeitung von Daten hat sich auf 10.000 verdoppelt.

Um dieses gewaltige Arbeitspensum erledigen zu können, ergreift die DSB Maßnahmen zur Vereinfachung und Beschleunigung der Entscheidungsfindung, ohne dabei die im Falle einiger Fragen erforderlichen gründlichen Analysen zu beeinträchtigen.

Die DSB führt Änderungen an dem von unserem eigenen IT-Personal erstellten und entwickelten Informationssystem durch, um es an die anhaltende Entmaterialisierung interner Verfahren anzupassen und dadurch künftig ohne Papierkopien auskommen zu können.

Während die DSB das elektronische Meldeverfahren für alle Arten von Datenverarbeitungen entwickelt, um so das Verfahren für Datenkontrolleure zu vereinfachen und die Erteilung von Genehmigungen zu beschleunigen, führte sie im Jahr 2008 auch zwei spezielle elektronische Meldungen als Teil eines voll automatisierten Verfahrens ein – für ein Videoüberwachungsprogramm in Schulen sowie für die Verarbeitung sensibler Daten im Bereich Opferschutz von Kindern.

Ein weiterer wichtiger Aspekt der Aktivitäten der DSB ist die Bereitstellung von Beratung für sowie die Sensibilisierung von Datenkontrolleuren und Datensubjekten. Darüber hinaus sollte auch die verstärkte Teilnahme der DSB an öffentlichen Seminaren und Konferenzen zum Thema Datenschutz in verschiedenen Bereichen betont werden.

**Stellungnahmen zu Gesetzesentwürfen**
Die DSB wurde in 59 Fällen gebeten, Stellungnahmen zu Gesetzesentwürfen betreffend Datenschutzfragen abzugeben. Die relevantesten betrafen hierbei die Umsetzung der Richtlinie 2005/60/EG über Geldwäsche und Terrorismusbekämpfung, Volkszählung, Änderung der Datenbank des Wählerverzeichnisses, Verarbeitung von Daten im Justizsystem, Änderung des Arbeitsgesetzes sowie Fahrzeug-Ereignissätze. Innerhalb ihrer Kompetenzen zur Abgabe von Stellungnahmen wurde die DSB auch vom Parlament zu Gesetzesentwürfen angehört.

Die Frage der Umsetzung des als „elektronischer Nummernschildsensor" bekannten Gerätes entfachte eine große öffentliche Diskussion. Die DSB fungierte

hierbei als Referenzstelle für die Diskussion, da sie Bedenken zu diesem Projekt äußerte. Nach dem entsprechenden Gesetzesentwurf soll das Gerät für alle Fahrzeuge verpflichtend sein und verschiedene Zwecke erfüllen: Feststellung von Verstößen gegen die Straßenverkehrsordnung (z. B. fehlender Versicherungsschutz, eingezogener Führerschein oder nicht bezahlte Strafzettel) sowie Zahlung von Mautgebühren in Portugal sowie im europäischen elektronischen Mautsystem. Als Technologie wurde die dedizierte Nahbereichskommunikation (Dedicated Short Range Communications, DSRC) mit einer Reichweite von 1.000 Metern gewählt.

Die DSB stellte zwei wesentliche Fragen zum Gesetzesentwurf: Obwohl die ausgewählte Technologie weniger in die Privatsphäre eingreifen würde als die GPS-Alternativen, so müsste dennoch entschieden werden, wie viele Sensorscanner installiert werden, um sicherzustellen, dass die Fahrstrecke eines Fahrzeugs nicht verfolgt werden kann. Andererseits sollte es aufgrund des verpflichtenden Einbaus dieses Gerätes in allen Fahrzeugen dem Fahrer auch möglich sein, die Maut anonym zu zahlen, ohne dabei eine elektronische Spur seines Aufenthaltsortes zu hinterlassen.

Das Gesetz wurde letzten Februar von der Regierung verabschiedet, und es wurde entschieden, dass das Gerät vorerst nur zur Zahlung von Mautgebühren eingesetzt werden soll. Andere Zwecke wurden ausgeschlossen. Es sind noch einige Regulierungsarbeiten zu erledigen, und die DSB wird an diesem Prozess sowie an der der darauf folgenden Erteilung der Genehmigungen zur Datenverarbeitung beteiligt sein.

**DADUS-Projekt**

Nach einer Vereinbarung mit dem Bildungsministerium und den regionalen Bildungsbehörden der Azoren und Madeiras startete die portugiesische DSB im Januar 2008 am europäischen Datenschutztag ein Pionierprojekt mit dem Namen DADUS-Projekt, um unter anderem Datenschutzfragen in Lehrpläne an Schulen zu integrieren.

Ziel ist die Sensibilisierung für Rechte im Bereich Datenschutz sowie die Bereitstellung von Ratschlägen für junge Menschen zur Frage, wie IKT sicherer genutzt werden können. Dies soll insbesondere durch ein strukturiertes, landesweites und langfristiges Projekt erreicht werden, dass weiter geht als eine gelegentliche Kampagne.

Dieses Projekt richtet sich an Kinder im Alter von 10 bis 15 Jahren. Die Inhalte basieren auf Internetplattformen. Die DSB entwickelte eine speziell auf das Projekt ausgerichtete Seite, auf der Lehrer ein grundlegendes Datenschutzhandbuch und zahlreiche unterstützende Materialien zur Arbeit im Unterricht abrufen können, sowie einen Blog mit Spielen, Tipps, Texten, Schularbeiten, Schülerkommentaren und Cartoons, über den die Schüler in der Schule oder von zu Hause aus interaktiv am Projekt teilnehmen können.

Die DADUS-Website enthält auch einen speziellen Bereich für Eltern, der einfache und klare Informationen zum Thema Datenschutz bietet und ihnen ermöglicht, ihre Kinder zu überwachen. Außerdem können sie über ein Diskussionsforum Erfahrungen austauschen und Probleme sowie entsprechende Lösungsansätze diskutieren.

Im vergangenen Jahr lag der Schwerpunkt darauf, den Schulen das Projekt zu präsentieren und den Lehrern gedrucktes Material auszuhändigen. Die ersten Reaktionen waren sehr positiv, und viele Lehrer – auch in Privatschulen – führten das Projekt unmittelbar im Schuljahr 2007/2008 ein. Im Laufe des ersten Jahres des DADUS-Projekts meldeten sich etwa 1.700 Lehrer zum Projekt an, und Website sowie Blog verzeichneten über 100.000 Zugriffe.

## Rumänien

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

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates wurde in Rumänien am 12. Dezember 2001 durch die Annahme des Gesetzes Nr. 677/2001 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr umgesetzt.

Gesetz Nr. 677/2001 wurde durch Gesetz Nr. 102/2005 über die Einrichtung, Organisation und Funktionsweise der nationalen Aufsichtsbehörde für die Verarbeitung personenbezogener Daten geändert. Die bedeutendste Änderung betrifft die Aufhebung der Bestimmungen zur Notwendigkeit der Einholung einer Vorvereinbarung der Ermittlungsbehörde oder des zuständigen Gerichtes in Fällen, in denen die Aufsichtsbehörde eine Untersuchung betreffend die Verarbeitung personenbezogener Daten im Bereich des Strafrechts durchführen möchte.

Eine weitere Änderung des Gesetzes 677/2001 wurde durch Gesetz 278/2007 dadurch durchgeführt, dass die Meldegebühr für die Verarbeitung personenbezogener Daten im Rahmen des Gesetzes 677/2001 abgeschafft wurde.

Im Laufe des Jahres 2008 wurden keine weiteren Änderungen am Gesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vorgenommen.

Die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation wurde durch das Gesetz Nr. 506/2004 über die Verarbeitung personenbezogener Daten und den Schutz des Privatlebens im Bereich der elektronischen Kommunikation in nationales Recht umgesetzt.

Das Gesetz Nr. 506/2004 garantiert den Schutz personenbezogener Daten, die von Anbietern öffentlicher Kommunikationsnetzwerke, von Anbietern von Mehrwertdiensten sowie von Anbietern von Abonnentenregistern verarbeitet werden. Dieses Gesetz ergänzt und spezifiziert den vom Gesetz 677/2001 über die besonderen Anforderungen des Sektors der elektronischen Kommunikation festgelegten gesetzlichen Rahmen.

Die Richtlinie 2006/24/EG wurde durch Gesetz Nr. 298/2008 in nationales Recht umgesetzt. Zweck dieses Gesetzes war die Festlegung einer nationalen Regelung betreffend die Pflichten von Anbietern öffentlicher Kommunikationsnetze und -dienste zur Speicherung von im Rahmen ihrer Tätigkeiten erfassten oder verarbeiteten Daten für einen Zeitraum von 6 Monaten ab dem Datum, an dem die elektronische Kommunikation stattfand, um den zuständigen Behörden somit im Rahmen ihrer Tätigkeiten zur Ermittlung in Strafsachen sowie zur Vermeidung von Straftaten diese Daten zugänglich zu machen.

Angesichts Rumäniens Status als EU-Mitgliedstaat bezog die Aufsichtsbehörde im Rahmen ihrer regulatorischen Aktivitäten im Bereich des Schutzes personenbezogener Daten die bei ihren alltäglichen Aktivitäten beobachteten Dinge ein. Folgende Entscheidungen wurden demzufolge verabschiedet: Entscheidung Nr. 90/2008 über ein angemessenes Maß an Schutz personenbezogener Daten in Jersey, Entscheidung Nr. 95/2008 über die Einführung eines standardisierten Meldeformulars, das durch das Gesetz Nr. 677/2001 eingeführt wurde, Entscheidung Nr. 101/2008 über die Verarbeitung personenbezogener Daten betreffend den Gesundheitszustand sowie über die Einführung eines Genehmigungsmodells für die Verarbeitung personenbezogener Daten betreffend den Gesundheitszustand.

Um die nationalen Gesetzgebungsverfahren zur Umsetzung und Harmonisierung des Besitzstandes der Gemeinschaft zu beschleunigen, die für zahlreichen Tätigkeitsfelder maßgeblich sind, hat die Aufsichtsbehörde durch die Bereitstellung von Expertenmeinungen zu bestimmten Gesetzgebungsakten während der betreffenden Annahmeverfahren ständig mit nationalen Institutionen zusammengearbeitet. In dieser Hinsicht ist Folgendes bemerkenswert: Entwurf einer Entscheidung der Regierung über das Genehmigungsverfahren für die Anbieter öffentlicher Dienste zur elektronischen Authentifizierung, Entwurf einer Eilverordnung der

Regierung über die Änderung und Ergänzung des Gesetzes über das Recht auf freien Verkehr für rumänische Bürger außerhalb Rumäniens, Entwurf einer Eilverordnung der Regierung zur Regulierung der Nutzung personenbezogener Daten im Polizeibereich – Umsetzung der Empfehlung 87 (15) vom 17. September 1987 des Ministerkomitees des Europarates.

Die Aufsichtsbehörde hat außerdem zahlreiche Stellungnahmen, Standpunkte, Empfehlungen sowie Anweisungen gemäß den sowohl in gemeinschaftlichen als auch nationalen Gesetzgebungsakten festgelegten Prinzipien und Bestimmungen zur Verarbeitung personenbezogener Daten ausgesprochen.

## B. Bedeutende Rechtsprechung

Es wurde festgestellt, dass die Gerichte im Jahr 2008 in den Fällen, die im Zusammenhang mit dem Schutz personenbezogener Daten standen, eine einheitliche Praxis verfolgt haben.

Trotz der unterschiedlichen Art der vor Gericht gebrachten Anliegen und der zur gerichtlichen Kontrolle gemeldeten Situationen wurde die Gesetzgebung zum Schutz personenbezogener Daten ähnlich der Auslegung der Aufsichtsbehörde interpretiert.

So wurde nach einer Untersuchung eines privaten Unternehmens durch die Aufsichtsbehörde bemerkt, dass das Unternehmen personenbezogene Daten über E-Mails verarbeite. Für die Übermittlung unerbetener Werbenachrichten auf elektronischem Wege wurde ein Bußgeld verhängt. Der Datenkontrolleur reichte Beschwerde gegen den Untersuchungsbericht ein.

Angesichts der in diesem Fall vorgelegten Beweise stellte das Gericht fest, dass der Datenkontrolleur die personenbezogenen Daten der betreffenden Personen, an die er die Werbenachrichten übermittelt hatte, verarbeitet habe, ohne dass der Empfänger die Möglichkeit gehabt hätte, ein Widerrufsrecht geltend zu machen. Insbesondere erhielt der Empfänger wiederholt Werbenachrichten ohne vorherige Zustimmung, solche Nachrichten tatsächlich erhalten zu wollen.

Angesichts dieser Feststellungen entschied das Gericht, dass die Aufsichtsbehörde das Vergehen korrekt eingestuft habe und das Bußgeld rechtskräftig sei.

Im Rahmen der Untersuchung eines Sportvereins stellte die Aufsichtsbehörde fest, dass der Verein die persönliche Identifikationsnummer sowie Vor- und Nachnamen von Mitgliedern, die dem Verein beigetreten waren, sowohl manuell als auch automatisch verarbeitet hatte, ohne vorher über die Verarbeitung der personenbezogenen Daten zu informieren und ohne die Datensubjekte über ihre gesetzlichen Rechte zu informieren.

Die Aufsichtsbehörde verhängte für das Ausbleiben der Information über die Verarbeitung der personenbezogenen Daten der Mitglieder sowie für die nicht erfolgte Information, die die Datensubjekte betreffend ihre Rechte und die Art und Weise, wie sie diese Rechte geltend machen können, hätten erhalten müssen, ein Bußgeld gegen den Datenkontrolleur.

Als Reaktion auf das Bußgeld reichte der Datenkontrolleur eine Meldung bezüglich der Verarbeitung der personenbezogenen Daten ein und stellte die gemäß Gesetz Nr. 677/2001 erforderlichen Daten zur Verfügung.

## C. Wichtige spezifische Themen

Der Schwerpunkt der Kontrollaktivitäten des Jahres 2008 lag auf der Durchführung von Untersuchungen gemäß dem Jahresplan sowie auf der Untersuchung möglicher illegaler Verarbeitungen personenbezogener Daten, auf die in bei der Aufsichtsbehörde eingegangenen Beschwerden und Meldungen hingewiesen wurde.

Der Großteil der von Amts wegen *(ex officio)* durchgeführten Untersuchungen erfolgte auf der Grundlage des aus den Aktivitäten der Behörde abgeleiteten Jahresplans in Tätigkeitsbereichen, in denen Verstöße gegen das Gesetz Nr. 677/2001 festgestellt wurden bzw. bezüglich deren Meldungen eingegangen waren.

Insbesondere wurden bei den im Rahmen des Jahresplans durchgeführten Untersuchungen vier wesentliche Tätigkeitsbereiche festgestellt:

- SWIFT
- Gesundheitsversorgungs- und Pflegezentren
- Onlinehandel
- Videoüberwachung

SWIFT – Als Reaktion auf verschiedene von der Artikel 29 Datenschutzgruppe vorgebrachten Fragen wurde entschieden, dass bestimmte Untersuchungen von Amts wegen in den Jahresplan für Untersuchungen integriert werden müssen, insbesondere die Kontrolle der im Rahmen des Systems für internationale Finanztransaktionen (SWIFT) verarbeiteten personenbezogenen Daten.

In Fortführung ihrer Überwachungs- und Kontrollaktivitäten gemäß Gesetz Nr. 677/2001 überprüfte die Aufsichtsbehörde die Einhaltung der rechtlichen Verpflichtungen von Finanzinstitutionen bei der Übertragung von Daten im Rahmen von SWIFT-Transaktionen in die USA und überprüfte Anfang 2008 außerdem die Einhaltung der Verpflichtung zur Information der betreffenden Datensubjekte.

Die Untersuchungen zeigten, dass die Daten auf der Grundlage eines Standardvertrages zwischen jedem Teilnehmer und SWIFT an SWIFT-Zentralen übermittelt werden. Der Vertrag legt für alle Teilnehmer vergleichbare Klauseln fest und gewährleistet damit ein standardisiertes Vorgehen hinsichtlich der Verarbeitung und Übertragung personenbezogener Daten an die SWIFT-Zentralen.

Hinsichtlich der Information der Datensubjekte bezüglich der Übermittlung der Daten über SWIFT hängten die Banken Informationsmitteilungen in ihren Geschäftsräumen aus und veröffentlichten diese auf ihren Websites, um so die betreffenden Informationen zu verbreiten. Diese Mitteilungen enthielten auch Informationen, dass personenbezogene Daten zu nach dem 11. September 2001 über SWIFT durchgeführten Transaktionen auf Anfrage von US-Behörden an diese übermittelt werden können. Die Informationsmitteilung enthielt überdies Informationen zur Tatsache, dass das US-Finanzministerium ausschließlich zu Zwecken der Terrorismusbekämpfung Zugang zu den in der SWIFT-Zentrale gespeicherten personenbezogenen Daten von Bankkunden beantragen kann und dass die personenbezogenen Daten so lange in einer sicheren Umgebung gespeichert werden, wie sie für diesen Zweck zugänglich sein müssen.

Die durchgeführten Prüfungen zeigten, dass einige Datenkontrolleure keine Meldung bezüglich der Verarbeitung personenbezogener Daten zu diesen Zwecken eingereicht hatten und dass einige Finanzinstitutionen die Datensubjekte nicht angemessen gemäß Artikel 12 des Gesetzes Nr. 677/2001 informierten. Dementsprechend wurden sie aufgefordert, diese Mängel zu beheben.

Die Datenkontrolleure sind den Empfehlungen der Aufsichtsbehörde nachgekommen.

Gesundheitsversorgungs- und Pflegezentren – Die im Rahmen von Untersuchungen durchgeführten Prüfungen zeigten, dass nicht alle Datenkontrolleure Meldungen bezüglich der Verarbeitung personenbezogener Daten vor dem Beginn der eigentlichen Verarbeitung eingereicht hatten.

**Beispiel:** Gegen Unternehmen X wurde ein Bußgeld verhängt, da es vor dem eigentlichen Beginn der Verarbeitung keine Meldung der Verarbeitung personenbezogener Daten zur Bereitstellung von Waren und Dienstleistungen eingereicht hatte. Außerdem war die Verarbeitung der personenbezogenen Daten illegal, da die Datensubjekte nicht über ihre gesetzlichen Rechte informiert worden waren.

Im Untersuchungsbericht wurde die Empfehlung für den Datenkontrolleur ausgesprochen, eine Meldung bezüglich der Verarbeitung personenbezogener Daten einzureichen, die Datensubjekte über ihre gesetzlichen Rechte zu informieren und das Personal, das Zugang zu personenbezogenen Daten hat, Geheimhaltungsvereinbarungen unterschreiben zu lassen.

Da festgestellt worden war, dass das Unternehmen auch die persönliche Identifikationsnummer sowie die Kontonummer der Kunden verarbeitete, wurde entschieden, dass die Verarbeitung der Identifikationsnummer sowie der Kontonummer der Kunden einzustellen sei, da dies im Hinblick auf den Zweck der Verarbeitung zur

„Bereitstellung von Waren und Dienstleistungen" sowie zu „Werbe-, Marketing- und kommerziellen Zwecken" unverhältnismäßig sei und die vor dieser Entscheidung verarbeiteten Daten gelöscht werden müssten.

Weitere in diesem Fall durchgeführte Prüfungen zeigten, dass der Datenkontrolleur die im Untersuchungsbericht festgelegten Maßnahmen eingehalten hatte – er hatte die Verarbeitung der persönlichen Identifikationsnummer sowie der Kontonummer zur „Bereitstellung von Waren und Dienstleistungen" sowie zu „Werbe-, Marketing- und kommerziellen Zwecken" eingestellt und die bis zu diesem Punkt verarbeiteten Daten gelöscht.

Nach den Untersuchungen in diesem speziellen Bereich stieg die Anzahl der eingereichten Meldungen durch Datenkontrolleure deutlich an, was für eine bessere Sensibilisierung hinsichtlich der Pflichten betreffend den Schutz personenbezogener Daten spricht.

**Onlinehandel** – Unter Berücksichtigung der Tatsache, dass diese Aktivität die Verarbeitung personenbezogener Daten, einschließlich sensibler Daten (z. B. persönliche Identifikationsnummer sowie Ausweisdokumente und deren Nummern) von Einzelpersonen voraussetzt, führte die Aufsichtsbehörde zahlreiche Untersuchungen privater Unternehmen durch, die in diesem Bereich tätig sind.

Die auf den Websites der Datenkontrolleure veröffentlichten „Allgemeinen Geschäftsbedingungen" und die „Geheimhaltungsvereinbarungen" enthalten Informationen zu den Gründen, warum die personenbezogenen Daten erfasst und gespeichert werden, sowie die Angabe, dass die Daten nicht an Dritte weitergegeben werden. Diese Dokumente enthielten jedoch keine Informationen über die in Gesetz Nr. 677/2001 festgeschriebenen Rechte.

Die durchgeführten Prüfungen zeigten, dass die meisten Datenkontrolleure vor der Untersuchung keine Meldung bezüglich der zu diesem Zweck erfolgten Verarbeitung personenbezogener Daten eingereicht hatten, dieser Verpflichtung jedoch nach der Untersuchung nachkamen.

**Beispiel:** Eine im Jahr 2006 durchgeführte Untersuchung eines Unternehmens, das im Bereich Onlineverkauf tätig war, hatte gezeigt, dass der Datenkontrolleur über eine eigens hierfür eingerichtete Website persönliche Informationen über diejenigen verarbeitete, die an den Angeboten des Unternehmens interessiert waren, sowie außerdem Informationen über seine Kunden (natürliche Personen), und sowohl elektronisch als auch auf Papier Aufzeichnungen erstellte, die in den Geltungsbereich des Gesetzes Nr. 677/2001 fielen. Die betreffenden Personen wurden über ein Onlineformular gebeten, personenbezogene Daten anzugeben, so zum Beispiel folgende: Vorname, Nachname, persönliche Identifikationsnummer, Lieferadresse, E-Mail-Adresse und Telefonnummer. Erklärungen von Vertretern des Unternehmens zufolge sei die Angabe einer persönlichen Identifikationsnummer nicht verpflichtend zur Ausstellung einer Rechnung. Es wurden keine weiteren Gründe genannt, die eine Verarbeitung dieser Art von Daten rechtfertigen würden.

Darüber hinaus enthielt der Abschnitt „Allgemeine Geschäftsbedingungen" der Website eine Informationsmitteilung mit einer Auflistung der Kategorien von Datensubjekten (Kunden – natürliche Personen), jedoch keinen Hinweis auf das Gesetz Nr. 677/2001 oder die Rechte der Datensubjekte und die Möglichkeiten, wie diese ihre Rechte gemäß Paragraph (1), Artikel 12 des Gesetzes Nr. 677/2001 gelten machen können.

Angesichts der im Rahmen der Untersuchung festgestellten Dinge wurde gegen den Datenkontrolleur eine Geldbuße wegen der nicht erfolgten Meldung der Verarbeitung personenbezogener Daten und der illegalen Verarbeitung personenbezogener Daten ohne eine angemessene (vollständige) Information der Datensubjekte verhängt.

Nach der Untersuchung wurde bemerkt, dass das auf der Website veröffentlichte Bestellformular dahingehend abgeändert wurde, dass die Angabe einer persönlichen Identifikationsnummer nicht mehr verpflichtend war.

Auf der Grundlage der Ergebnisse der Untersuchung erließ die Aufsichtsbehörde eine Entscheidung, durch die sie die Löschung der in der Datenbank des Unternehmens

gespeicherten persönlichen Identifikationsnummern anordnete, da der Datenkontrolleur keinen bestimmten, präzisen und legitimen Zweck angeben konnte, der die Verarbeitung der persönlichen Identifikationsnummer gemäß den Bestimmungen der Artikel 4 und 8 des Gesetzes 677/2001 rechtfertigen würde.

Der Datenkontrolleur erfüllt nunmehr die von der Behörde auferlegten Anordnungen.

**Videoüberwachung** – Bei der Aufsichtsbehörde gingen im Jahr 2008 zahlreiche Meldungen zur Prüfung der Einhaltung der Meldepflicht verschiedener öffentlicher und privater Behörden ein, die Videoüberwachungsanlagen nutzen.

Als Reaktion führte die Aufsichtsbehörde eine Reihe von Untersuchungen betreffend die Verarbeitung personenbezogener Daten durch Videoüberwachungsanlagen durch – entweder von Amts wegen oder auf Beschwerden bzw. Meldungen von Datensubjekten hin.

Im Rahmen der Untersuchungen wurde im Wesentlichen Folgendes kontrolliert: Einhaltung von Mindest-Sicherheitsmaßnahmen durch die Datenkontrolleure, Vorhandensein eines legitimen und ausdrücklichen Zwecks, Vermeidung übermäßiger Speicherung von durch Videoüberwachungsanlagen verarbeiteten personenbezogenen Daten, Gewährung der Möglichkeit zur Ausübung der (gesetzlich festgeschriebenen) Rechte für Datensubjekte sowie Verhinderung einer Weitergabe von auf diese Art und Weise verarbeiteten Daten ohne Rechtsgrundlage.

Die von den Datenkontrolleuren zur Rechtfertigung der Installation von Kameras zur Videoüberwachung angeführten Gründe waren die Verhinderung von Diebstählen und anderen illegalen Aktivitäten. Die erfassten Bilder werden abhängig von der Kapazität der Speichereinheit für einen bestimmten Zeitraum auf Servern gespeichert. Danach werden sie automatisch gelöscht. Die Bilder werden nur dann an die Polizei weitergegeben, wenn Straftaten begangen wurden und ein offizieller Antrag vorliegt.

Beispiel: Der auf eine Meldung hin untersuchte Datenkontrolleur verarbeitete personenbezogene Daten, nämlich Bilder, die über in einem Restaurant installierte Videoüberwachungskameras erfasst worden waren.

Die Untersuchung zeigte, dass auch auf den Toiletten Kameras installiert worden waren und eine Identifizierung einzelner Personen möglich war. Der vom Datenkontrolleur angegebene Zweck des Überwachungssystems war die Gewährleistung der „Sicherheit der Geschäftsräume und der Waren sowie die Verhinderung von Straftaten".

Ein Hinweis zur Videoüberwachung war lediglich im Eingangsbereich des Restaurants angebracht.

Da der Datenkontrolleur die Verarbeitung personenbezogener Daten nicht gemeldet hatte, wurde gegen ihn wegen der ausgebliebenen Meldung und des nicht korrekten Hinweises ein Bußgeld verhängt.

Nach der Untersuchung sowie unter Berücksichtigung der Tatsache, dass Toiletten als privater Raum ausschließlich für diejenigen gedacht sind, die sie zu einer beliebigen Zeit benutzen, stufte die Aufsichtsbehörde die Installation des Videoüberwachungssystems in diesen Räumen im Einklang mit den Bestimmungen von Artikel 29 von WP 67/2002 über die Verarbeitung personenbezogener Daten durch Videoüberwachungsanlagen als unverhältnismäßig ein.

Angesichts der oben genannten Feststellungen erließ die Aufsichtsbehörde eine Entscheidung zur Einstellung der Verarbeitung der Bilder von Einzelpersonen beim Besuch der Toiletten des Restaurants und forderte die Löschung der bis zu diesem Zeitpunkt erfassten Daten.

Im Fall von zur Einhaltung der im Gesetz Nr. 4/2008 zur Verhinderung von Gewalt bei Sportveranstaltungen genannten Bestimmungen installierten Videoüberwachungssystemen führte die Aufsichtsbehörde Untersuchungen bei großen Fußballvereinen in Bukarest und anderen Städten durch. Die Ergebnisse zeigten, dass die Verarbeitung personenbezogener Daten (Bilder) vor dem Beginn dieser Verarbeitung in den meisten Fällen nicht gemeldet wurde. Gegen die betreffenden Datenkontrolleure wurden Bußgelder verhängt.

Außerdem hatten die Datenkontrolleure in den meisten Fällen Maßnahmen ergriffen, um zu gewährleisten, dass die Zuschauer über die Videoüberwachung im Fußballstadion informiert sind. Die Information erfolgte sowohl durch schriftliche Hinweise an sichtbaren Stellen sowie durch mündliche Hinweise während der Sportveranstaltungen.

Im Laufe des Jahres 2008 wurden zusätzlich zu den im Rahmen des verabschiedeten Jahresplans durchgeführten Untersuchungen auch Untersuchungen in den folgenden Bereichen durchgeführt:

- Nationales Programm zur Bewertung des Gesundheitszustandes der Bevölkerung in der medizinischen Grundversorgung – Verarbeitung personenbezogener Daten im Rahmen dieses Programms sowie
- Klassifizierungssystem für Diagnosegruppen (DRG) – Verarbeitung personenbezogener Daten von Patienten.

Nach den Untersuchungen war ein deutlicher Anstieg der Anzahl an eingegangenen Meldungen von Datenkontrolleuren zu verzeichnen, deren Aktivitäten in den Aufgabenbereich der nationalen Aufsichtsbehörde für die Verarbeitung personenbezogener Daten (NSAPDP) fallen.

Die Bearbeitung von Beschwerden und entsprechende Lösungsansätze, die sich aus den Aktivitäten der Aufsichtsbehörde ergeben, sind von größter Bedeutung. Im Jahr 2008 stieg die Anzahl der eingegangenen Beschwerden im Vergleich zum Jahr 2007 um den Faktor 11. Dies zeigt deutlich, dass die Befugnisse der Aufsichtsbehörde sowie das Thema Schutz personenbezogener Daten insgesamt besser von der breiten Öffentlichkeit wahrgenommen werden und dass Bürger sich zunehmend für die Aktivitäten unserer Behörde interessieren. Beim Großteil der Beschwerden ging es um unerbetene kommerzielle Nachrichten, die Weitergabe personenbezogener Daten von Schuldnern an das Kreditbüro und das Zentrum für Risikoanalyse von Banken sowie die illegale Weitergabe solcher Daten in anderen Situationen.

# Slowakei

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

Eine kleine, aber äußerst wichtige Änderung zur gesetzlichen Regelung der faktischen Existenz und Funktionsweise der Behörde zum Schutz personenbezogener Daten der Republik Slowakei (im Weiteren „Datenschutzbehörde" genannt) wurde vorgenommen. Durch diese spezifische Änderung wurde das Gesetz Nr. 428/2002 Coll. über den Schutz personenbezogener Daten (im Weiteren „Gesetz Nr. 428/2002 Coll." genannt) im Hinblick auf das „Haushaltsprogramm zum Schutz personenbezogener Daten" geändert, das von der Haushaltskategorie der Regierung der Slowakischen Republik in die Kategorie der allgemeinen Finanzverwaltung übertragen wurde. Diese Übertragung stärkte formal die Unabhängigkeit der Behörde im Haushalt. Im nächsten Haushaltsjahr wird es nicht mehr erforderlich sein, den Haushalt als Teil des Regierungshaushalts zur Genehmigung vorzulegen. Diese Gesetzesänderung lässt jedoch weiterhin die Möglichkeit offen, dass finanzielle Anforderungen der Behörde ignoriert werden, da die Kategorie der allgemeinen Finanzverwaltung dem Finanzministerium der Slowakischen Republik untersteht, dessen Haushalt dem nationalen Rat der Slowakischen Republik zur Verhandlung und Genehmigung vorgelegt wird.

## B. Bedeutende Rechtsprechung

Im Jahr 2005 erließ die Behörde eine Anordnung für die staatliche Verwaltungsbehörde als Kontrolleur des Ablagesystems zur Beendigung der Veröffentlichung der nationalen Identifikationsnummer (eine Identifikationskennung zur allgemeinen Anwendung) von Datensubjekten auf der Website des Amtsblattes. Der Kontrolleur wurde außerdem angewiesen, zuvor veröffentlichte nationale Identifikationsnummern von der Website zu entfernen. Der Empfänger dieser Anweisung legte bei der Behörde Widerspruch gegen diese Entscheidung ein. Der Widerspruch wurde als nicht akzeptabel abgewiesen. Der Kontrolleur reichte Klage bei Gericht ein und beantragte die Aufhebung der Entscheidung der Behörde. Das Gericht wies die Klage ab und gab als Begründung an, die Veröffentlichung personenbezogener Daten sei eine sehr spezifische Art der Datenverarbeitung. Eine Besonderheit dieser Tätigkeit bestehe hauptsächlich darin, dass es sich um einen Prozess handle, der nicht vollständig rückgängig gemacht werden könne (Wiederherstellung eines Zustandes als wäre nichts geschehen) und der eine Reihe möglicher Konsequenzen mit sich bringe, die im Falle einer unrechtmäßigen Veröffentlichung negative Auswirkungen auf das Datensubjekt haben könnten. Die Veröffentlichung nationaler Identifikationsnummern sei sogar als noch sensibler einzustufen. Letztlich verbiete auch das Gesetz ausdrücklich die Veröffentlichung von „Identifikationskennungen zur allgemeinen Anwendung". Nach Ansicht des Gerichts basierte die Entscheidung der Behörde auf angemessenen Gründen und stand im Einklang mit den der Behörde gesetzlich zugestandenen Kompetenzen.

## C. Wichtige spezifische Themen

**Prüfaktivitäten und Bearbeitung von Meldungen**
Die Abteilung für Prüfungen der Behörde kontrolliert unabhängig den Schutz personenbezogener Daten und stärkt durch ihre Tätigkeiten den Schutz anderer Grundrechte und Freiheiten natürlicher Personen. Der Schwerpunkt der Aktivitäten der Abteilung für Prüfungen liegt hauptsächlich auf der Prüfung der Ablagesysteme von Kontrolleuren und der Bearbeitung der Meldungen von Datensubjekten und anderen Personen bezüglich einer direkten Verletzung ihrer in Gesetz Nr. 428/2002 Coll. festgelegten Rechte.

**Kontrolle des Schutzes personenbezogener Daten in Zahlen**
Im Jahr 2008 gingen 113 Meldungen von Datensubjekten und anderen natürlichen Personen bezüglich einer Verletzung des Schutzes ihrer personenbezogenen Daten bei der Behörde ein. 65 weitere Meldungen gingen von anderen Personen ein, die den Verdacht eines Verstoßes gegen das Datenschutzgesetz vorbrachten. Der Oberinspektor der Behörde ordnete von Amts wegen 74 Verfahren gegen die Kontrolleure von Ablagesystemen an. 21 weitere Meldungen waren noch aus dem Jahr 2007 anhängig. Insgesamt bearbeitete die Behörde im Jahr 2008 273 Meldungen. Diesbezüglich führte die Abteilung für Prüfungen 105

Prüfungen von Kontrolleuren und Bearbeitern von Ablagesystemen durch und forderte 34 „Einreichungen von Erklärungen" an. Insgesamt 75 Mal wurde die Behebung von im Rahmen der Prüfungen festgestellten Mängeln angeordnet. Das Recht, Widerspruch gegen diese Anordnung einzulegen, wurde nur von einem Kontrolleur in Anspruch genommen. Der Widerspruch wurde abgewiesen.

Im Jahr 2008 betrafen 142 der 252 neu eingegangenen Meldungen Kontrolleure aus dem privaten Bereich und 61 Meldungen Kontrolleure in öffentlichen Verwaltungen, hauptsächlich in anderen öffentlichen Verwaltungsbehörden. In 28 Fällen untersuchte die Behörde Meldungen betreffend Selbstverwaltungsbehörden. 8 Fälle betrafen zivilgesellschaftliche Organisationen, Stiftungen, politische Parteien oder Bewegungen sowie eingetragene Kirchen oder Religionsgruppen. In 4 Fällen wurden Einrichtungen der öffentlichen Verwaltung untersucht. In 9 Fällen wurde eine Meldung zu einem Subjekt eingereicht, das nicht der Kontrolleur des Ablagesystems gemäß Gesetz Nr. 428/2002 Coll. war.

Von den 113 im Jahr 2008 von Datensubjekten eingereichten Meldungen konnte die Behörde 99 Fälle abschließen, 71 davon innerhalb des gesetzlich vorgeschriebenen Basiszeitraums von 60 Tagen. Die längeren Untersuchungen der anderen Meldungen ergaben sich durch die Notwendigkeit der Konsultation anderer Institutionen, die Prüfungen von Ablagesystemen in den Geschäftsräumen der Datenkontrolleure zur Sammlung weiterer Beweise oder durch den Antrag auf Zusammenarbeit durch die Antragsteller selbst. Insgesamt 50 Meldungen wurden nach ihrer Bewertung als grundlos abgewiesen.

Ist ein Informant mit der Bearbeitung seiner Meldung durch die Behörde nicht zufrieden, so kann er binnen einer gesetzlich festgelegten Frist von 30 Tagen eine erneute Meldung bei der Behörde einreichen. Unter den 99 im Jahr 2008 abgeschlossenen Fällen waren lediglich 2 Meldungen, die erneut eingereicht worden waren. Die übrigen 97 Informanten, deren Meldungen im Jahr 2008 untersucht wurden, waren mit der endgültigen Entscheidung der Behörde zufrieden. Dies entspricht über 96 %. Im Laufe des Jahres 2008 übergab die Abteilung für Prüfungen 4 Meldungen an die Strafverfolgungsbehörden.

Im Jahr 2008 verhängte die Behörde 14 Bußgelder in Höhe von insgesamt 1.045.000 SKK (34.687,65 €). Die Bußgelder bewegten sich normalerweise im unteren Bereich, da die Behörde bei der Verhängung von Bußgeldern über einen Handlungsspielraum verfügt. Das höchste verhängte Bußgeld belief sich auf 250.000 SKK (8.298,50 €).

**Landesweite Prüfaktivitäten der Behörde**

*Überprüfungen von Videoüberwachungssystemen in Städten und Gemeinden*

Im Jahr 2008 führte die Abteilung für Prüfungen die Überprüfung von Videoüberwachungssystemen durch. Ziel der landesweiten Überprüfungen war die Untersuchung von durch Städte und Gemeinde betriebenen Videoüberwachungssystemen. Diesbezüglich führte die Abteilung für Prüfungen 12 Überprüfungen durch, 7 davon bereits im Jahr 2007. Bei allen Überprüfungen wurden Mängel festgestellt. Die Behörde erließ entsprechende Anordnungen für die Kontrolleure. Der typischste Mangel bestand darin, dass in den überwachten für die Öffentlichkeit zugänglichen Bereichen nicht eindeutig auf die Videoüberwachung hingewiesen wurde, dass keine Aufzeichnungen über das Ablagesystem gemacht wurden, dass die Aufzeichnungen nicht nach Ablauf der im Gesetz Nr. 428/2002 Coll. genannten Frist gelöscht wurden und dass keine ausreichenden technischen, organisatorischen oder persönlichen Maßnahmen in Form einer Sicherheitsrichtlinie für Kameraablagesysteme ergriffen wurden.

*Überprüfungen der Verarbeitung personenbezogener Daten durch Gerichtsvollzieher, Notare und Anwälte*

Im Jahr 2007 wurde festgestellt, dass zahlreiche Gerichtsvollzieher sich durch die Veröffentlichung von nationalen Identifikationsnummern von Datensubjekten am offiziellen Aushang (Verkündung des Beginns der Vollstreckung, Auktionsmitteilung) außerhalb des durch die Bestimmungen des Gesetzes Nr. 428/2002 Coll. festgelegten Rahmens bewegten. Im Rahmen der im Jahr 2008 durchgeführten Überprüfungen der Büros der Gerichtsvollzieher wurden außerdem Mängel bei der Anwendung der Bestimmungen des Gesetzes Nr. 428/2002 Coll. im Hinblick auf die Sicherheit der

Verarbeitung personenbezogener Daten aufgedeckt, insbesondere in den Fällen, in denen das Ablagesystem zur Verarbeitung der personenbezogenen Daten mit dem Internet verbunden ist.

Die Abteilung für Prüfungen überprüfte, inwieweit ausgewählte Notare und Anwälte in der gesamten Slowakischen Republik die Bestimmungen des Gesetzes Nr. 428/2002 Coll. einhalten.

Untersucht wurde insbesondere Folgendes:
- Information berechtigter Personen;
- Inhalt von Verträgen zwischen Kontrolleuren und Bearbeitern;
- Aufzeichnungen zu Personal, Gehaltsablagesystemen und Mandanteninformationssystemen;
- Ernennung eines Beauftragten für den Schutz personenbezogener Daten;
- Vorhandensein und Qualität eines Sicherheitsprojekts oder von Sicherheitsrichtlinien.

Die Anordnungen wurden ausgesprochen, um die Mängel zu beseitigen, und nach einer gründlichen Analyse des gesamten Falles vom Oberinspektor mit den zuständigen Vertretern der slowakischen Rechtsanwaltskammer, der slowakischen Kammer der Gerichtsvollzieher und der Notarkammer der Slowakischen Republik, die den zuständigen Subjekten von ihrem Standpunkt aus Hilfe zur schnellstmöglichen Lösung ihrer Situation bieten können, diskutiert.

*Überprüfungen der Verarbeitung personenbezogener Daten durch Kontrolleure im Gesundheitswesen*
Im Jahr 2008 bearbeitet die Behörde zahlreiche Meldungen von Datensubjekten betreffend Kontrolleure im Gesundheitswesen. Aufgrund der kritischen Anzahl und der besonderen Bedeutung dieser Meldungen entschied der Oberinspektor, Überprüfungen durchzuführen, um festzustellen, in welchem Umfang die Kontrolleure im Gesundheitswesen die Bestimmungen des Gesetzes Nr. 428/2002 Coll. betreffend die Verarbeitung personenbezogener Daten von Patienten einhalten. Die Abteilung für Prüfungen untersuchte staatliche und private Einrichtungen des Gesundheitswesens (Krankenhäuser und Arztpraxen), Apotheken und Krankenversicherungsgesellschaften. In den meisten Fällen hatten die Kontrolleure versäumt, Sicherheitsrichtlinien zur Festlegung des Umfangs der Kompetenzen und der Beschreibung der Funktionen der berechtigten Personen sowie des Umfangs ihrer Verantwortlichkeiten hinsichtlich der Verarbeitung personenbezogener Daten auch in außergewöhnlichen Situationen (z. B. bei Schließung oder Umzug einer Arztpraxis oder eines Krankenhauses) bereitzustellen. In vielen Fällen stellte die Behörde fest, dass personenbezogene Daten in Einrichtungen des Gesundheitswesens und Apotheken auf indiskrete Art und Weise erfasst oder weitergegeben wurden. Außerdem untersuchte die Behörde auch Verdachtsmomente hinsichtlich der Weitergabe personenbezogener Daten von Neugeborenen an Krankenversicherungsgesellschaften.

*Sonderprüfungen im Hinblick auf den Beitritt der Slowakischen Republik zum Schengen-Raum*
Im Zusammenhang mit den Vorbereitungen für den Beitritt der Slowakischen Republik zum Schengen-Raum führte die Abteilung für Prüfungen im Jahr 2008 weitere Untersuchungen ausgewählter Botschaften der Slowakischen Republik im Ausland durch. Ziel der Untersuchungen war es, zu überprüfen, ob die von den Kontrolleuren der Ablagesysteme angewandten Verfahren zur Ausstellung von Schengen-Visa sowie zur Erfüllung der Anforderungen des Schengen-Kataloges (Empfehlungen und bewährte Verfahrensweisen) betreffend die Ausstellung von Visa im Einklang mit den Bestimmungen des Gesetzes Nr. 428/2002 Coll. stehen. Im März 2008 wurden die Konsulate der Botschaften der Slowakischen Republik in Kuwait und Damaskus überprüft, im Mai 2008 die Konsulate in Prag und Brünn. Im Hinblick auf die Überwachung der rechtmäßigen Verarbeitung personenbezogener Daten im Einklang mit der aktuellen Version des Schengener Informationssystems (SIS I) wurden Überprüfungen im nationalen SIRENE-Büro, im Büro für die internationale Zusammenarbeit der Polizei sowie im Polizeipräsidium durchgeführt.

**Internationale Zusammenarbeit**
Die Behörde nimmt jeweils im Frühling und im Herbst regelmäßig an internationalen Workshops für Inspektoren von Behörden für den Schutz personenbezogener Daten teil. Bei dem Workshop im Herbst 2007, der von der portugiesischen Behörde für den Schutz personenbezogener Daten in Lissabon organisiert wurde, wurde entschieden,

dass der XVIII. Internationale Workshop für Inspektoren im Jahr 2008 in der Slowakei stattfinden sollte. Der von der Behörde organisierte Workshop fand am 29. und 30. September 2008 in Bratislava statt. Außer den Inspektoren der Mitgliedstaaten der Europäischen Union nahmen auch Inspektoren der Beitrittskandidaten am Workshop teil, die sich auf den Beitritt zur Europäischen Union vorbereiten. Insgesamt waren 63 Teilnehmer aus dem Ausland sowie 10 Angestellte der Behörde am Workshop anwesend. Das Büro des Europäischen Datenschutzbeauftragten wurde durch zwei Delegierte vertreten. Die Veranstaltung wurde vom Vorsitzenden des parlamentarischen Ausschusses für Menschenrechte, Minderheiten und den Status von Frauen sowie vom Vorsitzenden der Behörde eröffnet. Während des Treffens diskutierten die Inspektoren fünf grundlegende Themen:

1. Bearbeitung von Beschwerden: Befugnisse von Aufsichtsbehörden bei der Bearbeitung von Beschwerden;
2. Austausch bewährter Verfahrensweisen der Untersuchungen der Botschaftskonsulate hinsichtlich der Ausstellung von Schengen-Visa;
3. Interessenausgleich: Schutz personenbezogener Daten vs. Massenmedien;
4. Anwendung von Sicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten;
5. Verarbeitung personenbezogener Beschäftigungsdaten.

Die Abteilung für Prüfungen präsentierte die folgenden Themen:

- Durchführung von Überprüfungen und interne Regeln für die Überprüfungen;
- Bereitstellung von Erklärungen sowie Ernennung eines Datenschutzbeauftragten;
- Berechtigte Personen; organisatorische und persönliche Maßnahmen;
- Rechtlicher Rahmen und Bedingungen für die Vorbereitung eines Sicherheitsprojektes;
- Rechtlicher Rahmen für die Verarbeitung personenbezogener Daten durch ein Videoüberwachungssystem sowie Erfahrungen der Behörde bei der Durchführung von Überprüfungen von Videoüberwachungssystemen.

**Grenzüberschreitender Verkehr personenbezogener Daten**

Im Berichtszeitraum erteilte die Behörde 3 Genehmigungen eines grenzüberschreitenden Verkehrs personenbezogener Daten. Subjekte des grenzüberschreitenden Verkehrs personenbezogener Daten waren im Rahmen von Beschäftigung, Personalverwaltung und Auslagerung von Verarbeitungstätigkeiten verarbeitete personenbezogene Daten. Eine Entscheidung zur grenzüberschreitenden Übertragung von Daten an Länder, die keinen ausreichenden Schutz personenbezogener Daten garantieren, wurde dem Kontrolleur – einem in Indien ansässigen Importeur – zugestellt. Er wurde angewiesen, die rechtlichen Bestimmungen durch die Integration von Standard-Vertragsklauseln einzuhalten. Die Behörde erließ zwei Entscheidungen zur Übertragung personenbezogener Daten betreffend Importeure in den USA nach erfolgter Selbstbescheinigung der Importeure gemäß Nichtbeanstandungsregelung. Aus den eingegangenen Dokumenten ging deutlich hervor, dass die Kontrolleure die relevanten Entscheidungen der Europäischen Kommission zur Bereitstellung hinreichender Sicherheitsmaßnahmen zum Schutz personenbezogener Daten während und nach deren Übertragung in Drittländer nicht korrekt anwenden und interpretieren konnten. Die Behörde befasste sich außerdem mit Anträgen zur „Sonderregistrierung" von Systemen zur Meldung von Verdachtsmomenten hinsichtlich gesetzeswidriger oder unethischer Handlungen (Whistleblower-System) sowie mit zugehörigen Anträgen zur Genehmigung der Übertragung entsprechender Daten an Verarbeiter in den USA. Die Behörde stellte auch zahlreiche Stellungnahmen zur Interpretation des Gesetzes Nr. 428/2002 Coll. sowie zur Interpretation der diesbezüglichen Stellungnahmen der Artikel 29 Datenschutzgruppe zur Verfügung. Im Berichtszeitraum erließ die Behörde eine Entscheidung zur Ablehnung einer Sonderregistrierung auf der Grundlage von durch ein Whistleblower-System verarbeiteten Daten. Nach der Beseitigung der festgestellten Mängel gestattete die Behörde schließlich die „Sonderregistrierung" in diesem Fall. Im Hinblick auf die Whistleblower-Systeme wurde keine Übertragung entsprechender Daten an Drittländer von der Behörde genehmigt. Nach Prüfung der Anträge auf Genehmigung der Übertragung personenbezogener Daten kam die Behörde zu dem Schluss, dass keine Gründe genannt wurden, die die Erteilung einer

Genehmigung des vorgelegten Antrags rechtfertigten. Diese sehr breit ausgelegten Whistleblower-Systeme gingen weit über den Anwendungsbereich des Gesetzes Nr. 428/2002 Coll. hinaus. In dieser Hinsicht beträfe dies ausschließlich im Ausland entwickelte Whistleblower-Systeme, die bereits eingerichtet sind und seit geraumer Zeit betrieben werden.

**Internationale Zusammenarbeit**

Zum Zwecke der Auseinandersetzung mit speziellen Fragen, der Einrichtung von Kooperationen sowie zum Austausch bewährter Verfahrensweisen werden bilaterale Treffen veranstaltet. An diesen Treffen nehmen der Vorsitzende der Behörde sowie zuständige Experten teil.

*Mai 2008* – Bilaterales Treffen mit der Datenschutzbehörde der Tschechischen Republik in der Slowakei, einberufen von der slowakischen Behörde. Themen des Treffens waren Fragen zum Austausch bewährter Verfahrensweisen betreffend die Durchführung von Prüfaktivitäten:

- Verwendung offizieller Dokumente in der Praxis: Ausweis und Reisepass als europäische Dokumente. Gesetzgebung betreffend offizielle Dokumente; Umfang der in offiziellen Daten aufgeführten personenbezogenen Daten
- Verarbeitung und Veröffentlichung personenbezogener Daten aus Zentralregistern (Ablagesystemen) des Justizministeriums der Slowakischen Republik im Hinblick auf den Zuständigkeitsbereich (z. B. Amtsblatt der Gerichtsentscheidungen, Dokumentensammlung)
- Durchführung von Überprüfungen in den Geschäftsräumen des kontrollierten Subjektes (Kontrolleur/Verarbeiter) ohne die Notwendigkeit einer vorherigen Ankündigung. Zusammenarbeit der staatlichen Verwaltungsbehörden und anderer öffentlicher Verwaltungsbehörden mit der DSB der Slowakischen und Tschechischen Republik.

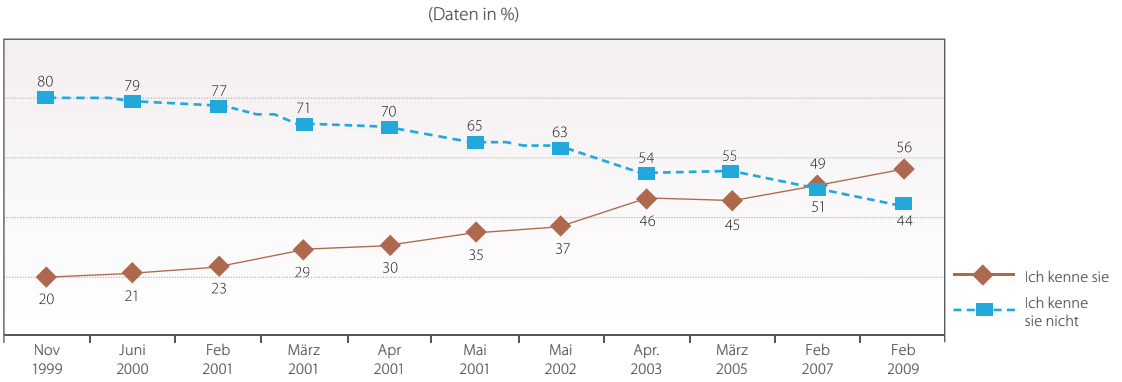
*April 2008 – Besuch der Behörde des Generalinspektors für den Schutz personenbezogener Daten in Warschau, Polen.*

Zweck des Besuchs war es, sich mit der Organisationsstruktur und den Aktivitäten der polnischen DSB (GIODO) vertraut zu machen. Zu diesem Anlass gaben die Vorsitzenden beider DSB ein Interview in der Tageszeitung „Rzeczpospolita".

*April 2008 – Besuch der nationalen Behörde für den Schutz personenbezogener Daten in Bukarest, Rumänien.*

Das Programm des Besuchs stand in Zusammenhang mit dem zuvor veranstalteten bilateralen Treffen in Bratislava und befasste sich mit der Frage, wie sich Rumänien auf den Beitritt zum Schengen-Raum vorbereitet. Das Programm wurde um den Austausch bewährter Verfahrensweisen erweitert, die beispielsweise mit den Besonderheiten hinsichtlich der Unabhängigkeit der rumänischen DSB in Zusammenhang stehen.

**Kennen Sie Ihre in Gesetz Nr. 428/2002 Coll. zum Schutz personenbezogener Daten festgeschriebenen Rechte betreffend den Schutz personenbezogener Daten?**



**Sensibilisierung der Öffentlichkeit für den Schutz personenbezogener Daten**

Das Meinungsforschungsinstitut des statistischen Amtes der Slowakischen Republik führt auf Anweisung der DSB seit 1999 wiederholt öffentliche Meinungsumfragen zu Fragen des Schutzes personenbezogener Daten durch. Die letzte Umfrage wurde im Februar 2009 durchgeführt.

Wie in der Grafik zu erkennen ist, hat die Sensibilisierung der Bürger hinsichtlich aller Kategorien des Schutzes personenbezogener Daten in den vergangenen zwei Jahren – von Februar 2007 bis Februar 2009 – um 5 % zugenommen. Insgesamt stieg die Zahl von November 1999 bis Februar 2009 um 36 %.

Im Allgemeinen kann festgehalten werden, dass der höchste Grad an Sensibilisierung (höher als der Durchschnitt für die gesamte Slowakische Republik) bei Bürgern im Alter zwischen 30 und 39 Jahren (68 %), gefolgt von denen im Alter zwischen 40 und 49 Jahren (66 %) zu verzeichnen ist. Außerdem ausgewertet: Befragte mit Hochschulabschluss (87 %), Befragte mit abgeschlossener Sekundarschulbildung (67 %), Unternehmer (70 %), Angestellte (74 %) sowie Bürger von Städten mit über 100.000 Einwohnern (76 %).

## Slowenien

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

Durch die Verabschiedung des Gesetzes zum Schutz personenbezogener Daten[20], des Gesetzes über den Datenschutzbeauftragten[21] und die Einrichtung der Stelle des Datenschutzbeauftragten[22] wurde die Richtlinie 95/46/EG vollständig in slowenisches Recht umgesetzt.

Gemäß der Sonderbestimmung von Artikel 48 des GSPD gab der Datenschutzbeauftragte zahlreiche vorläufige Stellungnahmen zu Gesetzen zur Vorbereitung der Einhaltung der Datenschutzbestimmungen heraus. Im Jahr 2008 wurden die Gesetze über persönliche Identifikationskarten, Ausländer, Strafregister, elektronische Kommunikation sowie verschiedene Verordnungen in den Bereichen öffentliche Gesundheit und Krankenversicherung, kostenlose Rechtshilfe usw. bearbeitet.

Bei der Ausübung seiner Pflichten sah sich der Datenschutzbeauftragte einem Problem hinsichtlich der Beschaffung von Standortdaten für Mobiltelefone bei einer Gefahr für Leib und Leben der betreffenden Person gegenüber, wenn diese Gefahr nicht in Verbindung mit einem Strafverfahren steht und die Polizei den Standort aufgrund eines Notrufes ermitteln möchte. In diesem Zusammenhang schlug der Datenschutzbeauftragte Änderungen am Gesetz über elektronische Kommunikation vor[23]. Gemäß den vorgeschlagenen Änderungen hätte die Polizei in der beschriebenen Situation das Recht, die Daten zum letzten bekannten Standort des Mobilfunkgerätes einer Person zu ermitteln, deren Leib und Leben in Gefahr ist. Die Polizei würde diese Daten permanent speichern und der Datenschutzbeauftragte würde mindestens einmal jährlich eine Überprüfung der Datenspeicherung durchführen. Diese Änderung setzt außerdem Artikel 5f der Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG angemessen um.

### B. Bedeutende Rechtsprechung

Im Jahr 2008 befasste sich der Datenschutzbeauftragte mit zahlreichen **Fällen**, über die von den nationalen Medien **ausführlich berichtet** wurde.

**Missbrauch von Traffic-Daten zu Telefonkommunikationen durch das Außenministerium**
Der Datenschutzbeauftragte erließ eine rechtliche Entscheidung in einem Fall gegen das Außenministerium hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Beschaffung einer Kopie von Festnetztelefonnummern, einschließlich der gewählten Rufnummern sowie der Rufnummern von eingegangenen Anrufen. Das Ministerium wurde aufgefordert, die CD zu vernichten, auf der die betreffende Liste mit Telefonnummern gespeichert war.

Im Rahmen einer internen Untersuchung innerhalb des Ministeriums sowie zum Zwecke der Identifizierung des Angestellten, der eine diplomatische Mail an einen Journalisten einer Tageszeitung weitergegeben hatte, wurden sämtliche Traffic-Daten eines bestimmten Zeitraums gesammelt. Zu diesem Zweck wurde eine Datenbank mit etwa 110.000 Traffic-Daten erstellt.

Im Einklang mit dem Gesetz über elektronische Kommunikation wurde den Traffic-Daten der doppelte Schutz gewährt, nämlich der Schutz der Privatsphäre von Korrespondenz sowie anderer Kommunikationsmittel gemäß Artikel 37 der Verfassung der Republik Slowenien (im Folgenden: Verfassung) sowie außerdem der Schutz personenbezogener Daten gemäß Artikel 38 der Verfassung. Da Traffic-Daten als personenbezogene Daten einzustufen sind, weil sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, liegt bei einer illegalen Intervention, wie sie in diesem Fall vorlag, auch ein doppelter Verstoß gegen

[20] 2004 verabschiedet, 2007 geändert (Amtsblatt der Republik Slowenien, Nr. 94/2007 – offizielle konsolidierte Fassung), nachstehend: GSPD.

[21] Amtsblatt der Republik Slowenien, Nr. 113/2005.

[22] Amtsantritt: 1. Januar 2006.

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

die entsprechenden Rechte vor, nämlich bezüglich der Angestellten des Ministeriums sowie bezüglich der Personen, die von den Angestellten angerufen wurden bzw. derer, die die Telefonnummern letzterer gewählt haben.

Gemäß Paragraph 1 von Artikel 37 der Verfassung ist die Privatsphäre von Korrespondenz sowie anderer Kommunikationsmittel geschützt. Paragraph 2 dieses Artikels besagt, dass lediglich ein Gesetz vorschreiben kann, dass die Unverletzbarkeit der Privatsphäre von Korrespondenz sowie anderer Kommunikationsmittel und die Unverletzbarkeit der persönlichen Privatsphäre auf der Grundlage eines Gerichtsbeschlusses für einen bestimmten Zeitraum aufgehoben werden kann, sofern dies für eine Ermittlungsbehörde bzw. im Rahmen einer strafrechtlichen Ermittlung oder aus Gründen der nationalen Sicherheit erforderlich ist. Der Umfang des Schutzes der Privatsphäre von Kommunikationen gemäß Artikel 37 der Verfassung ergibt sich aus der Notwendigkeit des Schutzes der Privatsphäre von Beziehungen, die eine Person während einer Kommunikation aufbaut und nicht aus einer bestimmten Art, einem bestimmten Status oder den Eigentumsverhältnissen des Mediums bzw. des Kommunikationsmittels. Dieser Schutz gilt für alle Personen, da die Verfassung hier nicht zwischen der Privatsphäre im privaten oder öffentlichen Bereich unterscheidet.

Der Datenschutzbeauftragte gab an, dass das Ministerium die Daten zum nicht zulässigen Zweck der Untersuchung von Traffic-Daten beschafft und verwendet hatte, um herauszufinden, welche Angestellten die Zeitung angerufen hatten. Darüber hinaus wurde festgestellt, dass in diesem Fall klar unverhältnismäßig gehandelt wurde, da durch die Beschaffung der genannten Daten keine Beweise dafür gefunden werden konnten, dass tatsächlich jemand ein bestimmtes Dokument weitergegeben hatte.

**Wettbewerbsbehörde**

Der Datenschutzbeauftragte entschied, dass es der Wettbewerbsbehörde nicht gestattet sei, personenbezogene Daten weiterzuverarbeiten, die sich auf den Festplatten von Computern befinden, die im Rahmen einer Untersuchung kopiert wurden, um zu ermitteln, ob die größten drei Einzelhändler Sloweniens Absprachen getroffen hatten.

Im Rahmen der Überprüfung gab der Datenschutzbeauftragte an, dass Artikel 29 des Gesetzes über Wettbewerbsbeschränkung keine hinreichende Rechtsgrundlage für den Zugriff auf elektronische Korrespondenz und zugehörige Traffic-Daten darstelle. Im Einklang mit der Strenge der Verfassung (Artikel 37) gibt das Gesetz die Verarbeitung von E-Mails nicht als Ermittlungsform an. Somit würde der Zugriff auf E-Mails eine Verletzung der verfassungsrechtlich gewährten Privatsphäre bei der Kommunikation bedeuten. Der Datenschutzbeauftragte forderte die Wettbewerbsbehörde auf, den Zugang zu den beschafften elektronischen Dateien, die auch illegal beschaffte personenbezogene Daten umfassen, zu sperren und binnen fünf Tagen die Teile, die zur weiteren Ermittlung noch verwendet werden können, vom Speichermedium der elektronischen Dateien zu übertragen. Jeder Zugriff auf die beschafften Dateien soll in Gegenwart des Datenschutzbeauftragten erfolgen. Nach einer gerichtlichen Überprüfung der Entscheidung wies das Verwaltungsgericht den Antrag der Wettbewerbsbehörde ab, die Untersuchung der auf den Kopien der Festplatten befindlichen personenbezogenen Daten bis zur Rechtskraft der Entscheidung zu gestatten und bestätigte somit die Entscheidung des Datenschutzbeauftragten. Der Oberste Gerichtshof verweigerte der Wettbewerbsbehörde für den Rechtsstreit jeglichen rechtlichen Schutz als Verwaltungsbehörde, da die Kompetenzen und Mandate einer Verwaltungsbehörde bei der Durchführung ihrer Verwaltungstätigkeiten nicht als Rechte oder Vorteile eingestuft werden können, die ein Gericht bei einem Verwaltungsrechtsstreit schützen müsste.

**Schutz sensibler personenbezogener Daten**

Der Datenschutzbeauftragte hat sich mit gravierenden Fällen unzureichend geschützter sensibler personenbezogener Daten befasst. Während des Transports zu dem Ort, an dem Daten (Anordnungen für Laboruntersuchungen) vernichtet werden sollten, fielen Pappkartons mit Daten vom Lastwagen und wurden über die Autobahn verstreut. Der Datenkontrolleur – eine Ambulanz – hatte einen Datenverarbeiter mit dem Transport und der Vernichtung der Dateien mit personenbezogenen Daten beauftragt, der für die Durchführung von Abfallsammlungen und -transporten registriert ist. Die Ambulanz hatte jedoch

keine gemäß dem GSPD erforderlichen gegenseitigen Verpflichtungen hinsichtlich der vertraglichen Datenverarbeitung abgeschlossen. Sie hatte keine ausreichenden Anweisungen hinsichtlich des Schutzes der Daten während des Transports und der Vernichtung ausgesprochen und die Durchführung der Verfahren und Maßnahmen zum Schutz der personenbezogenen Daten durch den Auftragnehmer auch nicht überwacht. Aufgrund des unzureichenden Schutzes personenbezogener Daten sowie der Nichteinhaltung der gesetzlichen Bestimmungen betreffend die vertragliche Verarbeitung personenbezogener Daten verhängte der Datenschutzbeauftragte sowohl gegen den Datenkontrolleur (die Ambulanz) als auch gegen den Datenverarbeiter (das mit dem Transport und der Vernichtung der Daten betraute Unternehmen) eine Geldstrafe.

Im Rahmen einer Überprüfung des Instituts für Onkologie wurde ein weiterer Fall unzureichenden Schutzes sensibler personenbezogener Daten aufgedeckt, über den berichtet wurde. Es wurde festgestellt, dass die medizinischen Unterlagen – medizinische Akten mit Daten über verstorbene Patienten – in über 100 offenen, ungeschützten Pappkartons auf den Fluren gelagert wurden. Außerdem befanden sich im selben, jedermann zugänglichen Flur zwei Schränke mit Unterlagen über aktuell in Behandlung befindliche Patienten. Gegen den Datenkontrolleur, der die Daten gemäß den gesetzlichen Bestimmungen angemessen hätte schützen müssen, wurde vom Datenschutzbeauftragten eine Geldstrafe verhängt.

**Bürgermeister**

Dem Bürgermeister einer slowenischen Gemeinde wurde eine Wählerinitiative zu einer Volksabstimmung betreffend den Bau von Wohngebäuden in der Gemeinde vorgelegt. Die Anhänge zur Initiative enthielten eine Liste von über 400 Wählern, die ihre Unterschrift und ihre personenbezogenen Daten für die Initiative angegeben hatten. Der Bürgermeister übergab eine Kopie der Initiative dem Rechtsanwalt des Unternehmens, das die Wohngebäude bauen sollte. Später verwendete der Rechtsanwalt die personenbezogenen Daten der Unterzeichner der Liste zu einem anderen als zu dem der ursprünglichen Erfassung der Daten zugrunde liegenden Zweck. Der Rechtsanwalt informierte die Unterzeichner der Initiative nämlich, dass gegen sie eine Schadenersatzklage eingereicht worden sei und forderte sie auf, die für die Initiative geleistete Unterschrift zurückzunehmen. Sowohl gegen den Bürgermeister als auch gegen den Rechtsanwalt wurden Geldstrafen wegen unrechtmäßiger Verarbeitung personenbezogener Daten verhängt.

**Steuerverwaltung der Republik Slowenien**

Der Datenschutzbeauftragte überwachte auch den Schutz personenbezogener Daten durch die Angestellten unterschiedlicher Register der öffentlichen Verwaltung, so z. B. die Zugangsberechtigungen zum zentralen Register der Steuerzahler. Gemäß dem GSPD ist der Datenkontrolleur, in diesem Fall also die Steuerverwaltung der Republik Slowenien, verpflichtet, nachweisen zu können, wann personenbezogene Daten in das Ablagesystem eingegeben, verwendet oder anderweitig verarbeitet wurden. Daher war der Datenschutzbeauftragte in der Lage, sämtliche Zugriffe auf die Computerdatenbank der Steuerzahler im Hinblick auf 15 bekannte Persönlichkeiten aus Slowenien zu untersuchen. Die Steuerverwaltung übergab dem Datenschutzbeauftragten eine Liste von Angestellten, die innerhalb eines Zeitraums von 8 Monaten im Jahr 2008 auf die Daten der 15 genannten Personen zugegriffen hatten. Jeder der Angestellten wurde aufgefordert, die Verarbeitung der Daten zu begründen, und es wurde festgestellt, dass lediglich 47 von 200 Angestellten die Daten rechtmäßig verarbeitet hatten, nämlich zum Zwecke der Durchführung eines Steuerverfahrens. Die restlichen Angestellten hatten keinen rechtmäßigen Grund, auf die Daten zuzugreifen. Als Grund für die Zugriffe auf die Daten zum Alter und zur Adresse der Personen wurde meist Neugierde angegeben. Der Datenschutzbeauftragte verwarnte die Beamten, die ohne hinreichende Rechtsgrundlage auf die Daten zugegriffen hatten, um klarzustellen, dass ohne einen legitimen Grund nicht auf personenbezogene Daten zugegriffen werden darf.

**Überprüfung der Verfassungsmäßigkeit**

Auf der Grundlage der Bestimmungen von Artikel 23a des Gesetzes über das Verfassungsgericht, die den Datenschutzbeauftragten befugen, ein Verfahren zur Überprüfung der Verfassungsmäßigkeit bzw. Legalität von Verordnungen durchzuführen, wenn

die Verfassungsmäßigkeit bzw. Legalität eines von ihm durchgeführten Verfahrens fraglich ist, wurden im Jahr 2008 zwei weitere Anträge auf verfassungsrechtliche Überprüfung bestimmter Vorschriften des Bankengesetzes sowie des Gesetzes über den slowenischen Nachrichten- und Sicherheitsdienst eingereicht. Der erste Fall betraf die Vorschrift des Bankengesetzes betreffend die verpflichtende Einrichtung eines Informationssystems zur Kreditsituation von Kunden sowie den Pflichtbeitrag der Banken zu diesen Informationen. Er wurde im März 2009 aufgrund erfolgreicher Verhandlungen mit dem Finanzministerium hinsichtlich einer Gesetzesänderung, nämlich der Auflistung der im System zu speichernden Daten sowie des Speicherzeitraums, zu den Akten gelegt.

Hinsichtlich der Überprüfung des slowenischen Nachrichten- und Sicherheitsdienstes reichte der Datenschutzbeauftragte einen Antrag auf verfassungsrechtliche Überprüfung des Gesetzes über den slowenischen Nachrichten- und Sicherheitsdienst sowie auf Überprüfung der Vorschriften zur strategischen Überwachung der Telekommunikation ein, was die Einrichtung eines Ablagesystems für personenbezogene Daten zur Folge hätte. Der Datenschutzbeauftragte beantragte beim Verfassungsgericht die Feststellung der Diskrepanzen zwischen bestimmten Vorschriften des Gesetzes und Artikel 38 der Verfassung (Grundrecht des Menschen auf Datenschutz und Privatsphäre von Informationen). Der Datenschutzbeauftragte beantragte außerdem beim Gericht die Beantwortung der Frage, ob die Bestimmungen des Gesetzes im Einklang mit Artikel 37 der Verfassung stehen, der die Privatsphäre der Kommunikation regelt und die Bedingungen und Grenzen für Verstöße dieses Grundrechts definiert. Die Privatsphäre der Kommunikation darf für eine Ermittlungsbehörde bzw. im Rahmen einer strafrechtlichen Ermittlung oder aus Gründen der nationalen Sicherheit nur unter sehr strengen Bedingungen aufgehoben werden. Die Aufhebung muss in einem Gesetz geregelt sein und auf der Grundlage eines Gerichtsbeschlusses erfolgen.

Das Verfassungsgericht wies den Antrag des Datenschutzbeauftragten aus formalen Gründen ab, da der Antragsteller nicht nachgewiesen habe, dass die Fragen hinsichtlich der verfassungsrechtlichen Prüfung in Zusammenhang mit einem von ihm durchgeführten Verfahren stünden. Somit seien die verfahrensrechtlichen Bedingungen nicht erfüllt. Das Verfassungsgericht war der Ansicht, das Gesetz über den Sicherheitsdienst sei im Hinblick auf die Abhörung internationaler Kommunikationen (die so genannte strategische Überwachung internationaler Kommunikationen) präzise genug, die gemäß dem Gesetz nur dann gestattet ist, wenn die Telefonnummer und die betreffende Person nicht definiert werden. Es ist erwähnenswert, dass der Datenschutzbeauftragte im Rahmen der Überprüfung herausfand, dass die Überwachung anhand einer spezifischen Telefonnummer erfolgte und die Person somit identifizierbar war. Das Gesetz gestattet diese Vorgehensweise zwar nicht für strategische Überwachung internationaler Kommunikationen, die verfassungsrechtliche Frage dieses Falles war jedoch, ob die strategische Überwachung der internationalen Kommunikation, wie vom Gesetz vorgesehen, vom Direktor der betreffenden Behörde gestattet werden kann oder ob dieses Recht nach der Verfassung nur dem Gericht zusteht. Die Frage wurde noch nicht beantwortet. Der Datenschutzbeauftragte war der Ansicht, dass der Artikel, der dem Direktor die Befugnis zur Anordnung einer Überwachung überträgt, verfassungswidrig sei.

## C. Wichtige spezifische Themen

Zusätzlich zur Funktion der Prüf- und Aufsichts- sowie Strafverfolgungsbehörde führte der Datenschutzbeauftragte zahlreiche weitere Aufgaben bezüglich der Bestimmungen des GSPD durch.

Da die Umsetzung **biometrischer Maßnahmen** nur nach Erhalt der Entscheidung des Datenschutzbeauftragten gestattet ist, gingen im Jahr 2008 insgesamt lediglich 16 Anträge (verglichen mit insgesamt 40 Anträgen im Jahr 2007) ein. Im Verhältnis wurde ein Rückgang der erlassenen Entscheidungen verzeichnet – 17 Entscheidungen im Jahr 2008, verglichen mit 35 Entscheidungen im Jahr 2007.

Bei der Zahl der erteilten Genehmigungen zur **Verbindung von Ablagesystemen** wurde ein leichter Anstieg verzeichnet. Im Jahr 2008 erließ der Datenschutzbeauftragte insgesamt 8 (verglichen mit

7 im Jahr 2007) Entscheidungen zur Verbindung von Ablagesystemen.

Im Rahmen der **Prüfmaßnahmen** (seit Dezember 2007 gibt es zehn staatliche Datenschutzinspektoren – die dem Datenschutzbeauftragten unterstehen) gingen im Jahr 2008 beim Datenschutzbeauftragten 635 (256 aus dem privaten und 379 aus dem öffentlichen Bereich) Anträge und Beschwerden betreffend vermutete Verstöße gegen das Gesetz zum Schutz personenbezogener Daten ein. Verglichen mit früheren Jahren (406 Fälle im Jahr 2007 und 231 im Jahr 2006) lässt sich eine konstante, deutliche Zunahme verzeichnen (76 % im Jahr 2007 und 56 % im Jahr 2008). Wie in früheren Jahren betrafen die meisten Beschwerden die Weitergabe personenbezogener Daten (PD) an nicht befugte Verwender, die unrechtmäßige Erfassung von PD, illegale Videoüberwachung, unzureichenden Schutz von PD, die unrechtmäßige Veröffentlichung von PD usw. Dementsprechend wurde eine deutliche Zunahme der aufgrund von Ordnungswidrigkeiten eingeleiteten Verfahren verzeichnet: 279 Fälle im Jahr 2008 verglichen mit 133 Fällen im Jahr 2007 und 41 Fällen im Jahr 2006.

Im Jahr 2008 belief sich die Anzahl der Anträge auf **schriftliche Stellungnahmen** und Klarstellungen auf 853. Obwohl ein leichter Rückgang verglichen mit den 1.144 Fällen aus dem Jahr 2007 verzeichnet wurde, liegen diese Zahlen noch immer über denen des Jahres 2006 (616 Fälle). Dies lässt auf einen hohen Sensibilisierungsgrad der Öffentlichkeit hinsichtlich des Rechts auf Privatsphäre schließen, das durch ein modernes Gesetz zum Schutz personenbezogener Daten garantiert wird. Der hohe Sensibilisierungsgrad ist wahrscheinlich auf die transparente Arbeit und die intensiven öffentlichen Kampagnen des Datenschutzbeauftragten zurückzuführen.

Als Folge dessen genießt der Datenschutzbeauftragte ein hohes Ansehen, das Vertrauen der Öffentlichkeit und hat für eine Sensibilisierung für seine Aktivitäten gesorgt. Dies spiegelt sich sowohl in den Ergebnissen öffentlicher Meinungsumfragen als auch im Bericht über die Ergebnisse der Flash-Eurobarometer-Umfrage zum Thema Datenschutz vom Januar 2008 wider. Die Ergebnisse dieser Umfrage zeigten, dass Slowenien im Hinblick auf die Sensibilisierung von Bürgern und Datenkontrolleuren zum Thema Datenschutz sowie im Hinblick auf die Sensibilisierung zu rechtlichen und institutionellen Regelungen in diesem Bereich zu den erfolgreichsten EU-Ländern gehört.

Im Dezember 2008 erhielt der Datenschutzbeauftragte den nationalen Netko-Preis für die beste unternehmerische bzw. administrative Website in der Kategorie „öffentliche Verwaltungsinstitutionen".

Zusätzlich zur Veröffentlichung nicht-bindender Stellungnahmen in Form schriftlicher Erklärungen auf der Website sowie zusätzlich zur Veröffentlichung einer Reihe von Broschüren zu Datenschutzfragen begann der Datenschutzbeauftragte im Jahr 2008 mit der Veröffentlichung von **Leitlinien** zu spezifischen Datenschutzfragen. Zweck der Leitlinien des Datenschutzbeauftragten ist die Bereitstellung allgemeiner und praktischer Anleitungen und Informationen für Datenkontrolleure in Form typischer häufig gestellter Fragen und Antworten. Mithilfe dieser Antworten und Leitlinien sollten die Datenkontrolleure entsprechend in der Lage sein, die gesetzlichen Bestimmungen des Gesetzes zum Schutz personenbezogener Daten einzuhalten. Im vergangenen Jahr erarbeitete und veröffentlichte der Datenschutzbeauftragte auf seiner Website Leitlinien betreffend den Schutz personenbezogener Daten in Informationssystemen von Krankenhäusern, Leitlinien betreffend Biometrie, Leitlinien betreffend den Schutz personenbezogener Daten in Beschäftigungsverhältnissen sowie Leitlinien betreffend Videoüberwachung.

Im Rahmen des zweiten Europäischen **Datenschutztages** organisierte der Datenschutzbeauftragte eine Rundtischdiskussion zur sicheren Nutzung des Internets und anderer moderner Technologien. Der Schwerpunkt der Diskussion lag auf jungen Nutzern dieser Technologien sowie auf dem Datenschutz in diesem Bereich. Eine Broschüre zur Information von jungen Menschen, Eltern und Lehrern wurde erstellt, auf der Website des Datenschutzbeauftragten veröffentlicht und in großem Umfang an alle Schulen in Slowenien verteilt. Bei dieser Gelegenheit vergab der Datenschutzbeauftragte die Preise für bewährte

Verfahrensweisen im Bereich Schutz personenbezogener Daten im privaten und öffentlichen Bereich.

**Internationale Zusammenarbeit**
Der Datenschutzbeauftragte veranstaltete im Jahr 2008 zwei wichtige internationale Treffen. Im Frühjahr organisierte er den **16. Workshop zur Fallbehandlung**, der sich mit Fragen der Biometrie im öffentlichen und privaten Bereich sowie mit dem Thema Datenschutz im Internet befasst. Die Veranstaltung fand in Ljubljana statt. Im September 2008 veranstaltete der Datenschutzbeauftragte außerdem die **Dritte Europäische Konferenz der Datenschutzbeauftragten**, deren Schwerpunkt auf einer effektiveren und vor allem schnellen Umsetzung des Rechts auf Zugang zu öffentlichen Informationen lag.

Im Rahmen der **Schengen-Bewertung der Schweiz** im Hinblick auf ihren Beitritt zum Schengen-Raum leitete der slowenische Datenschutzbeauftragte das Team von EU-Experten im Bereich Datenschutz. Die Bewertung wurde im Herbst mit einem Abschlussbericht erfolgreich beendet.

Die Vertreter des Datenschutzbeauftragten nahmen aktiv an einer Reihe **internationaler Treffen und Veranstaltungen** teil, so z. B. unter anderem an der Frühjahrskonferenz der europäischen Datenschutzbehörden in Rom (April), an der 30. Internationalen Konferenz der Datenschutzbeauftragten mit dem Titel „Der Schutz der Privatsphäre in einer grenzenlosen Welt" in Straßburg (Oktober), am Forum der mittel- und osteuropäischen Datenschutzbehörden in Polen, am Treffen der internationalen Arbeitsgruppe für Datenschutz im Bereich Telekommunikation sowie an vielen anderen Veranstaltungen.

Die Vertreter des Datenschutzbeauftragten haben regelmäßig in folgenden **EU-Gremien** mitgearbeitet, die sich mit dem Schutz personenbezogener Daten befassen: Artikel 29 Datenschutzgruppe, Gemeinsame Kontrollinstanz von Europol, Gemeinsame Kontrollinstanz von Schengen, Gemeinsame Kontrollinstanz Zoll und Aufsicht über EURODAC durch die nationalen Datenschutzbehörden – Koordination durch die Datenschutzbeauftragten. Mit dem **Europarat** wurde regelmäßig hauptsächlich im Rahmen des Beratungsausschusses des Übereinkommens zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten zusammengearbeitet.

## Spanien

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

Aufgrund der im vergangenen Jahr in Spanien durchgeführten Wahlen (beide legislativen Kammern wurden aufgelöst und nach den Wahlen neu gebildet) erließ das Parlament keine Gesetze betreffend Datenschutz zur Umsetzung der Richtlinie 95/46/EG oder im Bereich Telekommunikation.

### B. Bedeutende Rechtsprechung

**Nationaler Gerichtshof**
Im Laufe des Jahres 2008 wies der Nationale Gerichtshof 166 Berufungen gegen Beschlüsse der Datenschutzbehörde ab und bestätigte diese vollumfänglich (72 %). 76 dieser Urteile bezogen sich auf Anträge zur Löschung von Taufbucheinträgen. In 14 Urteilen wurden die Berufungen zum Teil zugelassen (6 %). In 48 Urteilen wurde den Anträgen auf Abweisung der Beschlüsse der Datenschutzbehörde stattgegeben (21 %), 22 davon betrafen gemäß dem Urteil des Obersten Spanischen Gerichtshofes vom 19. September 2008 abgeschlossene Taufbücher (Erklärung folgt). In einem Fall ließ das Gericht ein Rechtsmittelverfahren nicht zu. Folgende interessante Urteile sind hervorzuheben:

- Das Urteil vom 17. Dezember 2008 besagt, dass die bloße Angabe von Urlaubszeit keine Angabe von Gesundheitsdaten darstellt und somit diesbezüglich keine hohen Sicherheitsmaßnahmen erforderlich sind.
- Das Urteil vom 10. Juli 2008 erläutert das Konzept öffentlich zugänglicher Quellen unter Berücksichtigung der Tatsache, dass das Internet als Ganzes nicht als „Massenmedium" angesehen werden kann.
- Die Urteile vom 26. Februar und 23. Juli bezüglich öffentlichem bzw. privatem Eigentum an Ablagesystemen von Berufsverbänden und öffentlichen Gesundheitszentren.
- Drei Urteile vom 1. Oktober 2008 zu den Berufungen betreffend die Verarbeitung von Daten von Menschen, die in der Öffentlichkeit stehen, durch soziale Massenmedien.

**Oberster Gerichtshof**
Der Oberste Gerichtshof bestätigte alle Beschlüsse der Datenschutzbehörde mit Ausnahme derer, die die Taufbücher der katholischen Kirche betreffen.

Mit dem Urteil vom 19. September 2008 hob der Oberste Gerichtshof das Urteil des Nationalen Gerichtshofes auf und bestätigte die von der Datenschutzbehörde (AEPD) seit 2004 vertretene Ansicht, dass Taufbücher als organisierte Sätze personenbezogener Daten als Ablagesysteme einzustufen sind und dass auf die Taufbücher somit das Prinzip der Datenqualität im Hinblick auf Korrektheit und Aktualität der Daten anzuwenden ist.

Auf der Grundlage dieser Kriterien stellte die AEPD fest, dass Beschwerden von Bürgern einen entsprechenden Vermerk in den Taufbüchern zur Folge haben sollten, der ihr Recht auf Löschung widerspiegelt. Darüber hinaus legte der Nationale Gerichtshof in seinem ersten Urteil fest, dass Anträge von Menschen, die ihre Gewissensfreiheit ausüben möchten, wenn sie mit dem Inhalt des Taufbuches nicht einverstanden sind, und nicht als Mitglied der katholischen Kirche eingetragen sein möchten, entsprechend zu bearbeiten sind.

Dennoch kam der Oberste Gerichtshof zu dem Schluss, dass Taufbücher nicht, wie oben erwähnt, als Ablagesysteme einzustufen sind. *„Taufbücher stellen lediglich eine Sammlung von Daten dar, die schwierig zu durchsuchen sind, auf die nicht jeder zugreifen kann und über die eine Identifikation nur schwer erfolgen kann, da sie nicht alphabetisch oder nach Geburtsdatum, sondern lediglich nach dem Taufdatum sortiert sind".*

Die AEPD legte gemeinsam mit dem Generalstaatsanwalt einen Antrag beim Verfassungsgericht vor, demzufolge die Interpretation des Begriffs „Ablagesystem" den Anwendungsbereich der Datenschutzbestimmungen unverhältnismäßig beschränken könnte und den Anwendungsbereich des durch die Rechtsprechung des Verfassungsgerichtes zugestandenen Grundrechtes ignoriert.

Er besagte, dass die Berufungen gegen Urteile des Nationalen Gerichtshofes zur Bestätigung der Beschlüsse der Datenschutzbehörde betreffend das Recht auf

Löschung aus den Taufbüchern der Katholischen Kirche in 9 Fällen angemessen gewesen seien.

Er besagte, dass die Berufungen gegen Urteile zur Bestätigung der Beschlüsse der Datenschutzbehörde in 8 Fällen nicht angemessen gewesen seien.

In einem Fall wurde eine Berufung gegen ein Urteil zur Bestätigung der Beschlüsse der Datenschutzbehörde nicht zugelassen.

**Beschlüsse der spanischen Datenschutzbehörde**

Die größere Sichtbarkeit der AEPD hat bei den Bürgern zu einer drastischen Erhöhung der gemeldeten Verstöße geführt. Dementsprechend haben sich die vor der Verhängung von Strafmaßnahmen durchgeführten Überprüfungen um 45,4 % erhöht und die prozeduralen Beschlüsse fast verdoppelt (Erhöhung um 94,1 %). Die meisten Überprüfungen finden noch immer in den Bereichen Telekommunikation, Finanzinstitute und Videoüberwachung statt. Auf diese Bereiche entfallen insgesamt 50,9 % aller durchgeführten Überprüfungen.

Auch im Hinblick auf Beschlüsse zu Strafmaßnahmen gegen private Unternehmen entfielen die beiden ersten Plätze auf die Bereiche Telekommunikation und Finanzinstitute. Zudem wurde hier eine wesentlich stärkere Zunahme gegenüber dem Vorjahr verzeichnet (81,3 % verglichen mit 45 % und 58,8 % verglichen mit 104 %). Der Bereich, in dem jedoch die größte Zunahme an Strafmaßnahmen verzeichnet wurde, ist der Bereich Videoüberwachung (mit einer Zunahme von 633,3 %), wenngleich auch nur in 61,3 % der Fälle ein tatsächlicher Verstoß festgestellt werden konnte. Die Zahl der Beschlüsse zu Verstößen von öffentlichen Verwaltungen gegen das spanische Datenschutzgesetz (LOPD) stieg um 19,7 %. Ebenso nahmen auch Beschlüsse zur Einstellung von Verfahren (113 %) sowie zur Abweisung von Meldungen (138,3 %) zu. Bei den tatsächlich verhängten Strafmaßnahmen war eine Zunahme von Strafmaßnahmen für schwere Vergehen zu verzeichnen (551 verglichen mit 350). Die Anzahl der Fälle, in denen ein deutlicher Rückgang der Haftbarkeit derer verzeichnet wurde, die einen Verstoß begangen hatten, belief sich auf 229. Das entspricht 42 % der Beschlüsse, die zur Verhängung eines Bußgeldes geführt haben (verglichen mit 32 % im Jahr 2007). Was die Bürger am meisten betraf, war der Erhalt unerbetener Telefonanrufe. Wie später noch erläutert werden wird, führte die Datenschutzbehörde von Amts wegen zwei sektorale Überprüfungen von Telefonanrufen und Textnachrichten auf Mobiltelefone durch und stellte Mängel der Mechanismen fest, die Bürgern zur Verfügung stehen, um sich gegen den Empfang solcher Anrufe zu wehren. Außerdem warnte sie vor den Risiken zusätzlicher Gebühren, die die Buchung von SMS-Diensten mit sich bringen.

Zwei interessante Beschlüsse sind hervorzuheben.

- Mit dem Beschluss 00281/2007 verhängte die AEPD Bußgelder gegen zwei Unternehmen für die Erfassung von Daten eines Minderjährigen ohne Zustimmung der Eltern über ein Formular auf einer Website sowie für die Verwendung dieser Daten zum Versand von Werbung für eine Kreditkarte ohne die Zustimmung des bzw. der Erziehungsberechtigten des Kindes.

  Das Unternehmen hatte bei der Verarbeitung der Daten unter Berücksichtigung des Geburtsdatums des Kindes keine hinreichende Sorgfalt walten lassen. Die AEPD stellt zwei Verstöße des Unternehmens gegen das Datenschutzgesetz fest. Der erste war ein schwerer Verstoß aufgrund der Erfassung der Daten des Minderjährigen ohne Zustimmung der Eltern bzw. eines Erziehungsberechtigten sowie ein schwerer Verstoß aufgrund der Weitergabe der personenbezogenen Daten des Kindes an ein zweites Unternehmen, das diese Daten zu Werbezwecken verwendete. Außerdem stellte die Datenschutzbehörde einen schweren Verstoß durch das zweite Unternehmen fest, da es die Daten als Datenkontrolleur ohne Zustimmung zu Werbezwecken verwendete.

- Laut AEPD sowie den geltenden Bestimmungen in Bezug auf Minderjährige unter 14 Jahren, die noch nicht reif genug sind, um volles Verständnis hinsichtlich einer Zustimmung zu garantieren, ist es erforderlich, dass die Zustimmung der Eltern bzw. Erziehungsberechtigten eingeholt werden muss und darüber hinaus geeignete Informationen zur Bestätigung des Alters des Kindes vorliegen müssen. Im Zweifel ist von der Verarbeitung der Daten abzusehen.

- In Beschluss AP/00061/2007 stellte die AEPD einen schweren Verstoß gegen das Datenschutzgesetz durch eine öffentliche Verwaltungsbehörde fest. Diese hatte durch die Veröffentlichung eines Beschlusses mit Daten zu Empfängern von Zuschüssen zur Behandlung einer Drogensucht einschließlich Vornamen, Nachnamen sowie Ausweisnummern im Amtsblatt gegen die Geheimhaltungspflicht verstoßen. Die AEPD war der Ansicht, dass es zur Einhaltung der gesetzlichen Anforderungen der „Transparenz, Objektivität und Zustimmung" nicht erforderlich sei, die Begünstigten der Zuschüsse für die Behandlung ihrer Drogensucht identifizieren zu können. Tatsächlich gebe es Alternativen wie z. B. eine Anonymisierung oder Dissoziierung, damit die betreffenden Personen nicht identifiziert werden können. Obwohl die Veröffentlichung in Amtsblättern nach geltendem Recht erlaubt ist, müssen die Kriterien für die Integration von Daten in Veröffentlichungen von öffentliche Behörden und Institutionen laut der APED überprüft werden.

## C. Wichtige spezifische Themen

Im Jahr 2008 lag der Schwerpunkt der Arbeit der AEPD auf folgenden Themenbereichen.

**Mehr Mittel zur Umsetzung der Gesetze**
Eine der effektivsten Möglichkeiten, die Bürger zu schützen, ist, zu gewährleisten, dass diejenigen, die ihre Daten verarbeiten, wissen, wie sie diese zu verarbeiten haben. Das bedeutet die Förderung der Umsetzung der Gesetze durch eine Verstärkung der Bemühungen zur Information der Öffentlichkeit sowie die Beantwortung etwaiger Fragen zu diesem Thema. Bisher geschah dies über die Abteilung für Bürgerfragen und die Beantwortung von Fragen an die Rechtsabteilung.

Das Jahr 2008 stellte aufgrund einer entschlossenen Politik mit dem Ziel der Verbesserung des Informationsangebotes durch Instrumente wie z. B. die Veröffentlichung von Leitlinien zur Verbreitung der grundlegenden Aspekte des Datenschutzes in einer klaren, einfachen und verständlichen Sprache diesbezüglich jedoch einen Wendepunkt dar. Dies war das Ziel der Veröffentlichung der *„Datenschutzleitlinien für Datenkontrolleure"* sowie der *„Leitlinien für Datensicherheit"* als Reaktion auf die gestiegene Nachfrage nach Informationen zu diesem Thema. Da sich die Anforderungen der Datenschutzbehörde betreffend die Kenntnis der geltenden Kriterien durch die Umsetzung einer Bestimmung des Datenschutzgesetzes erhöhten, wurden außerdem *„Öffentliche AEPD-Sitzungen"* eingerichtet, die hinsichtlich der Teilnahme (2.000 Personen) erfolgreich waren.

Diese Aktivitäten haben die traditionellen nationalen Politiken zur Vorbeugung auf der Grundlage der von Amts wegen durchgeführten sektoralen Überprüfungen wie z. B. der im Jahr 2008 durchgeführten Überprüfung von „Werbeanrufen und Textnachrichten auf Mobiltelefone" ergänzt. Zusätzlich zu diesen Überprüfungen wurden Berichte bzw. Erklärungen über neue Herausforderungen im Bereich Datenschutz erstellt, insbesondere im Hinblick auf Internetdienste.

Diese Leitlinien sind unter folgenden Links abrufbar:
*„Datenschutzleitlinien für Datenkontrolleure"*
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_responsable_ficheros.pdf
*„Leitlinien für Datensicherheit"*
https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/guia_seguridad_datos_2008.pdf

**Information als wichtigstes Element bei der Sensibilisierung der Bürger**
Vorrangiges Ziel der AEPD ist es, zu gewährleisten, dass die Bürger die ihnen zustehenden Rechte kennen, sie darüber zu informieren, wie sie diese Rechte geltend machen können und Instrumente zur Vorbeugung und Umsetzung einzusetzen, um die Effektivität dieser Rechte zu garantieren.

Das erste dieser Ziele erfordert die Unterstützung der Medien und die Gewährleistung der Tatsache, dass die Medien eine aktive Rolle bei der Verbreitung von Informationen zu den Auswirkungen spielen, die der Bereich Datenschutz auf das alltägliche Leben der Bürger hat, insbesondere im Hinblick auf die neuen Realitäten der Dienste der Informationsgesellschaft. Die von der AEPD unternommenen Anstrengungen zur Verbesserung der Kommunikation haben zu einer

Verbesserung der Qualität geführt. Die gesteigerte Präsenz der Datenschutzbehörde sowie des Themas Datenschutz in den Medien ist zur Realität geworden: Die Anzahl an Interviews und Informationsanfragen hat sich im Jahr 2008 auf über 800 verdoppelt.

Quantitativ gesehen beantwortete die Rechtsabteilung im Jahr 2008 insgesamt 690 Anfragen (25 % mehr als im Vorjahr). 279 (40 %) davon wurden von öffentlichen Verwaltungen gestellt, 411 (60 %) kamen aus dem privaten Bereich. Hinsichtlich der Registrierung von Ablagesystemen wurden 250.000 im Allgemeinen Datenschutzregister (RGPD) registriert, 31 % mehr als im Vorjahr. Dort sind nunmehr 1.267.579 Systeme registriert (85.083 der öffentlichen Hand sowie 1.182.496 in privatem Besitz).

Bei den im RGPD registrierten Ablagesystemen der öffentlichen Hand war ein deutlicher Zuwachs – um mehr als 23.500 – zu verzeichnen. Dies entspricht einem Zuwachs von 300 %. An dieser Stelle muss betont werden, dass die Registrierung aller Ablagesysteme durch den Allgemeinen Ausschuss der rechtsprechenden Gewalt in Zusammenhang mit Justizbehörden steht (11.965). Diese Initiative muss als solide Grundlage zur Förderung der Anpassung des Datenschutzgesetzes an die Justizverwaltung gesehen werden.

**Besondere Konzentration auf Minderjährige**

Der Schutz personenbezogener Daten von Minderjährigen hat sich als Themenbereich etabliert, auf den die AEPD einen besonderen Schwerpunkt legt. Es wurden zahlreiche Anstrengungen unternommen, um in der Gesellschaft für dieses Thema zu sensibilisieren. So wurde beispielsweise das Dokument „Leitfaden über die Rechte von Jungen und Mädchen sowie die Pflichten von Müttern und Vätern", ein Dokument mit grundlegenden Empfehlungen zur Sensibilisierung für das Thema Datenschutz in der Familie und der Schule, am Tag des Internets am 17. Mai vorgestellt.

Im Rahmen ihrer Teilnahme an der 30. Internationalen Konferenz der Datenschutzbehörden erklärte die spanische Datenschutzbehörde außerdem, dass die Schulung zur grundlegenden Nutzung von Computertools sowie zu deren Risiken und Vorteilen unzureichend sei. Auf jeden Fall müsse man sofort entsprechende Maßnahmen ergreifen: Es müssten effektive Werkzeuge entwickelt werden, mit deren Hilfe festgestellt werden kann, ob die Nutzer von Internetdiensten Minderjährige sind, was die Unterstützung ihrer Eltern erfordern würde.

In dieser Hinsicht ist die AEPD einen Vergleich in einem ersten Fall illegaler Verarbeitung von Daten eines Minderjährigen ohne vorherige Überprüfung des Alters eingegangen, der zur Verhängung einer Geldstrafe aufgrund mangelnder Sorgfalt bei der Altersüberprüfung führte.

Der Link zum „*Leitfaden über die Rechte von Jungen und Mädchen sowie die Pflichten von Müttern und Vätern*" lautet:
https://www.agpd.es/portalweb/canal_joven/common/pdfs/recomendaciones_menores_2008.pdf

**Internet vs. Privatsphäre**

Das so genannte Web 2.0 hat das Angebot neuer Internetdienste für Internetnutzer um ein Vielfaches erhöht, da es den Nutzern ermöglicht, miteinander in Kontakt zu treten.
Es muss jedoch erwähnt werden, dass soziale Netzwerke – leistungsfähige Kanäle für Kommunikation und Interaktion, die eine große Zahl junger Nutzer, einschließlich Minderjährigen, miteinander vernetzen, – Risiken für den Schutz personenbezogener Daten bergen können. Die AEPD war sich dessen bewusst und startete im Jahr 2008 eine Analyse der Auswirkungen sozialer Netzwerke und stellte nach einer ersten Bewertung Folgendes fest:

- Informationen zu Datenschutzrichtlinien und allgemeinen Geschäftsbedingungen sind nicht besonders klar und zugänglich.
- Es fehlen Anwendungen zur Überprüfung des Alters von Minderjährigen, die diese Dienste nutzen wollen.
- Es können auch Dritte, die nicht als „Freunde" oder „direkte Kontakte" der Nutzer eingestuft sind, auf die Profile der betreffenden Nutzer zugreifen.

**Eine dringende Aufgabe: Entwicklung internationaler Standards zum Schutz der Privatsphäre**

Die Vielfalt der Systeme zum Schutz von Daten und der Privatsphäre bzw. das Fehlen solcher Systeme hat zu unterschiedlichen Problemen geführt, die durch die

Annahme von internationalen (Mindest-)Standards als Garantien für die Datenflüsse in einer globalisierten Welt gelöst werden können.

Laut AEPD ist es an der Zeit, Maßnahmen zu ergreifen, damit greifbare Fortschritte im Hinblick auf die Erreichung dieser internationalen Standards erzielt werden können. Diesbezüglich wurde der Schweizer Behörde bei der 30. Internationalen Konferenz zum Schutz von Daten und der Privatsphäre ein gemeinsamer Vorschlag betreffend die unbedingte Notwendigkeit, die Privatsphäre in einer Welt ohne Grenzen zu schützen, vorgelegt. Der Behörde, die die internationale Konferenz im Jahr 2009 organisiert, wurde die Einrichtung einer Arbeitsgruppe vorgeschlagen, deren Ziel die Erarbeitung und Einreichung eines *„Gemeinsamen Vorschlages für den Entwurf internationaler Standards zum Schutz von Privatsphäre und personenbezogenen Daten"* in der nicht öffentlichen Sitzung im Rahmen der 31. Konferenz sein sollte.

Der Vorschlag wurde einstimmig von der Konferenz angenommen, wodurch die AEPD mit der Bildung der Arbeitsgruppe und der Leitung des Projekts zur Erarbeitung internationaler Standards zum Schutz der Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten betraut wurde. Letztendlich sollte der auf der im November in Madrid stattfindenden Konferenz vorgestellte Text mit breiter Zustimmung angenommen werden und als Grundlage für ein internationales Instrument zum Schutz von Privatsphäre und personenbezogenen Daten dienen.

**Zusammenarbeit mit den Datenschutzbehörden der autonomen Gemeinschaften**

Hinsichtlich der Überprüfungen wurde die Zusammenarbeit zwischen den Datenschutzbehörden im Bereich der Analyse von Maßnahmen verbessert, um die Effektivität der gefassten Beschlüsse und die Koordination der Überprüfungen zu gewährleisten, wenn die Untersuchungen die Kompetenzen mehrerer Behörden betreffen. Ebenso wurden Kriterien hinsichtlich Fragen zum Thema Videoüberwachung, im Internet veröffentlichte Urteile sowie in Amtsblättern veröffentlichte Informationen ausgetauscht. Die Behörden haben sich auf die gemeinsame Priorität verständigt, die Bildung von Minderjährigen zu fördern und die Bewerbung der AEPD um die Organisation der 31. Internationalen Konferenz zum Schutz von Daten und der Privatsphäre zu unterstützen. Zusätzlich zu dieser Unterstützung hat man sich verpflichtet, bei der Entwicklung gemeinsamer Standards für den Datenschutz in einer globalisierten Welt zusammenzuarbeiten.

**Umsetzung: Verbesserung von Präventionsmaßnahmen**

*Ex officio-Sektorplan betreffend Telefonwerbung*

Die AEPD hat einen *ex officio*-Sektorplan betreffend Telefonwerbung umgesetzt, im Rahmen dessen die Praktiken der größten Mobilfunk- und Festnetztelefonieanbieter in Spanien sowie der Unternehmen, die Zusatzdienste (Premiumdienste) über SMS-Nachrichten oder Abonnements anbieten, untersucht wurden.

Als allgemeines Ergebnis stellte die AEPD Mängel bei den Systemen fest, die garantieren sollen, dass Bürger keine Telefonwerbung erhalten. Als eine der wesentlichen Schlussfolgerungen der durchgeführten Analyse betonte die AEPD die Mängel der Mechanismen, die den Bürgern zur Verfügung stehen, um den Erhalt von Werbemitteilungen über Nachrichten und Anrufe an Festnetz- und Mobilfunknummern zu verhindern bzw. dies in bestimmten Fällen auch abzulehnen. Außerdem warnte sie vor den Risiken der Buchung von Zusatzdiensten. Dem Bericht zufolge lauten die im Rahmen der Überprüfung festgestellten Mängel wie folgt:

- Gemäß den Daten des Sektorplans entnahmen 53 % der untersuchten Unternehmen Daten aus Telefonbüchern, um die Festnetznummern der Empfänger ihrer Kampagnen zu sammeln. Diesbezüglich wurde besonders betont, dass lediglich 1 % der in den Telefonbüchern gelisteten Anschlussinhaber angegeben hat, keine Werbeanrufe erhalten zu wollen.
- Wegen einiger Praktiken von Betreibern, wie z. B. die Verwendung von Daten zu „empfohlenen Personen", wurden bereits Strafmaßnahmen durch die AEPD verhängt.
- Es wurde festgestellt, dass es im Rahmen von Mobiltelefonkampagnen üblich ist, die Rufnummer nicht zu übermitteln. Die AEPD hält es für dringend erforderlich, einen rechtlichen Rahmen zu schaffen, um diese Praxis zu verbieten.

- Absender von Nachrichten sind verpflichtet, klare Informationen sowie einfache Methoden zur Ausübung des Rechts auf Ablehnung des Erhalts dieser Nachrichten bereitzustellen.
- Betreiber sollten Kontrollmechanismen zur Begrenzung des massiven Zuflusses unerbetener Werbenachrichten aus nichteuropäischen Ländern einführen, die die spanischen Vorschriften nicht erfüllen.
- In Bezug auf die Premiumdienste betont der *ex officio*-Sektorplan, dass die Informationsklauseln in der Werbung für diese Dienste nur sehr wenige Informationen enthalten, da in Werbenachrichten an Mobilfunknummern üblicherweise unvollständige oder abgekürzte Wörter vorkommen und Symbole verwendet werden, die schwer zu lesen sind. Somit werden die Empfänger nicht über die Kosten der Nachrichten, das Verfahren zur Abbestellung, die Verarbeitung der Daten usw. informiert. Die AEPD spricht hinsichtlich dieser Dienste eine besondere Warnung bezüglich der Bestellung dieser Dienste durch Minderjährige aus, da diese leichter zu täuschen sind als Erwachsene und somit eine der größten Risikogruppen darstellen.

Nach Umsetzung des Sektorplans sowie als Reaktion auf die festgestellten Mängel erarbeitete die AEPD eine Reihe von **Empfehlungen für Bürger, damit diese ihre Rechte geltend machen können, sowie Empfehlungen für den Sektor**, damit die Praktiken verbessert werden können.

Der vollständige *ex officio*-Plan sowie die Empfehlungen sind unter folgendem Link abrufbar:
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/plan_sectorial_publicidad_telefonica_2008.pdf
https://www.agpd.es/portalweb/canaldocumentacion/recomendaciones/common/pdfs/recomendaciones_sms_llamadas_11_2008.pdf

**Videoüberwachung**
Im Jahr 2008 startete die AEPD eine Untersuchung von Amts wegen *(ex officio)* betreffend verschiedene Websites, die Bilder von in öffentlichen Bereichen installierten Überwachungskameras in Echtzeit übertrugen, um klarzustellen, ob das für den Zugriff auf diese Bilder erforderliche Passwort korrekt installiert wurde oder ob die gemäß den Datenschutzbestimmungen erforderlichen Sicherheitsmaßnahmen mangelhaft waren.

**Verhaltensregeln**
Die Selbstregulierung durch bei der betreffenden Behörde gemeldete und registrierte Standardregeln ist ein ergänzendes Instrument zur Förderung der Einhaltung des Datenschutzgesetzes sowie zur Verbesserung der rechtlichen Sicherheit. Während des gesamten Jahres 2008 wurden Initiativen zur Selbstregulierung in den Bereichen private Versicherungsvermittlung, Versicherung auf Gegenseitigkeit von Angestellten gegen Berufskrankheiten und Unfälle am Arbeitsplatz, klinische Forschung und pharmazeutische Überwachung sowie in Sicherheitsunternehmen und Anwaltskanzleien gestartet.

**Die wichtigsten Entwicklungen in Drittländern**
*Aktivitäten Spaniens innerhalb des Ibero-Amerikanischen Datenschutznetzes*
Die Notwendigkeit, auf neue internationale Herausforderungen reagieren zu müssen, hat zu einem qualitativen Wandel der Aktivitäten des Ibero-Amerikanischen Datenschutznetzes geführt, dessen Leitlinien wie folgt lauten:
- Stärkung der institutionellen Vertretung der teilnehmenden Länder sowie Stärkung von deren Effektivität.
- Förderung der exekutiven Organisation von Vertretern lateinamerikanischer Länder.
- Öffnung der Treffen des Netzes für die Teilnahme von Drittländern, die nicht dem Ibero-Amerikanischen Raum angehören.
- Förderung eines Meinungsaustausches zwischen politischen Institutionen und privaten Unternehmen.
- Ermöglichung eines flexiblen Dialogs zwischen lateinamerikanischen Ländern und der Europäischen Kommission betreffend Bemühungen hinsichtlich einer Erklärung über geeignete Länder, die den Schutz personenbezogener Daten garantieren.
- Integration des Ibero-Amerikanischen Netzes in den Prozess der Formulierung internationaler Datenschutzstandards.

Auf der VI. Ibero-Amerikanischen Konferenz zum Thema Datenschutz, die vom 27. bis 30. Mai 2008 in Cartagena de Indias (Kolumbien) stattfand, wurde der

Grundstein für die Erreichung dieser Ziele gelegt. Es nahmen Vertreter von Institutionen lateinamerikanischer Länder sowie US-Behörden in Nordamerika und Redner aus multinationalen ausländischen Konzernen teil. Eine Bestimmung des Netzes wurde aktualisiert, der zufolge die AEPD die Sekretariatstätigkeiten und die Präsidentschaft für einen Zeitraum von zwei Jahren übernehmen soll. Weitere spezielle Funktionen werden von den Mitgliedern Argentinien, Chile, Mexiko und Portugal übernommen. Ab März 2009 wird das Ibero-Amerikanische Netz als Beobachter an den halbjährlich stattfindenden Treffen des Beratungsausschusses für das Übereinkommen 108 des Europarates teilnehmen.

Die Behörde hat die Entwicklung der bilateralen Zusammenarbeit fortgesetzt. Dies hat zur Unterzeichnung einer Absichtserklärung zur gegenseitigen Zusammenarbeit zwischen der internationalen Behörde für die Entwicklung der Informationsgesellschaft in Bolivien (ADSIB) und der AEPD sowie der „Gemeinsamen Absichtserklärung" des chilenischen Verbandes zur Produktionsförderung (COFRO) und der AEPD geführt.

## Schweden

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

In Schweden wurde die Richtlinie 95/46/EG durch das Gesetz zum Schutz personenbezogener Daten (Personal Data Act, PDA, 1998:204) umgesetzt, das am 24. Oktober 1998 in Kraft trat. Das Gesetz zum Schutz personenbezogener Daten wird durch die Datenschutzverordnung ergänzt (1998:1191), die am gleichen Tag in Kraft trat. Das Gesetz findet wie die Richtlinie auf die automatisierte ebenso wie auf die manuelle Datenverarbeitung Anwendung. Dieses Gesetz gilt zwar grundsätzlich für die Verarbeitung personenbezogener Daten in allen Bereichen der Gesellschaft, jedoch gibt es in bestimmten Bereichen mehrere spezielle Gesetze und Beschlüsse für die Datenverarbeitung, entweder anstelle des Gesetzes zum Schutz personenbezogener Daten oder ergänzend zu diesem. Auch beim Entwurf dieser speziellen Gesetze und Beschlüsse wurde der Richtlinie Rechnung getragen.

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

Im Jahr 2004 beschloss die Regierung die Einsetzung eines Ausschusses (*Integritetsskyddskommittén* – Ausschuss für den Schutz der Privatsphäre), der sich aus Experten und Mitgliedern des *Riksdag* (schwedisches Parlament) zusammensetzte und dessen Aufgabe in der Durchführung einer Umfrage zur schwedischen Gesetzgebung in Bezug auf die Privatsphäre und in ihrer Analyse bestand. Der Ausschuss wurde später auch damit beauftragt zu beurteilen, ob zusätzlich zu den bestehenden Rechtsvorschriften auch allgemein gültige Vorschriften zum Schutz der Privatsphäre aufgestellt werden sollten. Wie im letzten Jahresbericht erwähnt, legte der Ausschuss im Frühjahr 2007 einen umfangreichen Bericht vor, der die Umfrage und die Analyse enthielt. Der Ausschuss äußerte mehrere Kritikpunkte systematischer und methodischer Art und beantwortete die direkte Frage, ob der Schutz der Privatsphäre als zufrieden stellend geregelt betrachtet werden kann, eindeutig abschlägig. Der zweite und letzte Bericht des Ausschusses wurde im Januar 2008 vorgelegt. In diesem Bericht analysierte der Ausschuss, auf welche Art und Weise der verfassungsrechtliche Schutz der Privatsphäre geregelt werden sollte und welche weiteren Maßnahmen erforderlich sind. Einer der Vorschläge des Ausschusses war die Stärkung des verfassungsrechtlichen Schutzes der Privatsphäre. Diesbezüglich schlägt der Ausschuss einen Schutz vor der Überwachung und Auskundschaftung der persönlichen Umstände einer Person durch öffentliche Behörden vor. Der Ausschuss führt unter anderem heimliche Überwachung und die Vorratsspeicherung von Traffic-Daten als Beispiele für Gesetzesverstöße an. In diesen Bereichen sollten gründlichere Untersuchungen durchgeführt werden als dies aktuell der Fall ist.

Wie bereits im vergangenen Jahr berichtet, war die *EG-Richtlinie über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden*, noch nicht in schwedisches Recht umgesetzt worden. Dies ist bis heute nicht geschehen. Die Regierung wird dem Parlament voraussichtlich im Juni dieses Jahres einen Gesetzesentwurf vorlegen.

Im Juli 2008 trat ein neues Gesetz über Patientenakten und das Gesundheitswesen, das *Patientendatengesetz*, in Kraft. Das Gesetz soll den Umgang mit personenbezogenen Daten im Gesundheitswesen einheitlich regeln.

Im Juni 2008 verabschiedete das Parlament den Vorschlag der Regierung für ein neues *Gesetz über Signalüberwachung* für militärische Aufklärungsdienste. Das Gesetz gilt für sämtliche Signalüberwachungsmaßnahmen zu militärischen Aufklärungszwecken – und zwar

unabhängig davon, ob sie per Funk oder telegrafisch übertragen werden. Das Gesetz enthält eine Reihe von Vorschriften zum Schutz der Privatsphäre von Einzelpersonen. Das Parlament fordert jedoch weitere Kontrollmechanismen, um unter anderem den Schutz von Einzelpersonen noch zu stärken. Die Datenschutzbehörde wird speziell beauftragt werden, die Aktivitäten des Nationalen Technischen Verteidigungsdienstes zu beobachten und der Regierung bis Dezember 2010 Bericht zu erstatten. Das neue Gesetz trat am 1. Januar 2009 in Kraft.

Die dritte *EG-Richtlinie über Geldwäsche* wurde im Jahr 2008 in schwedisches Recht umgesetzt und trat am 15. März 2009 in Kraft.

Im Dezember 2008 reichte die Regierung einen Vorschlag für ein neues Gesetz zur Umsetzung der *Richtlinie zur Durchsetzung der Rechte des geistigen Eigentums* (2004/48/EG) in schwedisches Recht ein. Das Parlament genehmigte den Vorschlag, und das Gesetz wird am 1. April 2009 in Kraft treten. Eine Besonderheit des Gesetzes ist, dass sich Organisationen, die geistiges Eigentum schützen, an ein Gericht wenden und Internetanbieter auffordern können, Informationen zum Nutzer einer betreffenden IP-Adresse herauszugeben, wenn ein Verdacht vorliegt, dass ein illegaler Datenaustausch stattgefunden hat.

Im Dezember 2006 wurde ein Untersuchungsausschuss eingerichtet. Dem Ausschuss wurde die Aufgabe übertragen, das Monopol des nationalen schwedischen Apothekenverbandes (Apoteket AB) für den Verkauf von Pharmaprodukten aufzuheben und anderen Betreibern zu ermöglichen, solche Produkte zu verkaufen. Der Auftrag umfasst beispielsweise auch Fragen zur Registrierung von Rezepten. Die Datenschutzbehörde wurde um eine Stellungnahme insbesondere hinsichtlich Fragen zu Datenbanken gebeten. Die Regierung legte dem Parlament kürzlich einen Gesetzesentwurf mit einem Vorschlag für ein neues Gesetz vor, das Gesetz über *Apothekendaten*. Das neue Gesetz tritt voraussichtlich im Juli 2009 in Kraft.

Im September 2008 nahm die Datenschutzbehörde zu Vorschlägen für Änderungen des *Kreditinformationsgesetzes* Stellung und stellte fest, dass für Kreditinformationen im Internet in der Praxis die gleichen Anforderungen gelten wie für andere Formen von Kreditinformationen. Hintergrund für die Vorschläge war die Änderung des *Grundrechtes auf freie Entfaltung* (verfassungsrechtliches Gesetz) im Jahr 2003, die es ermöglicht hat, Kreditinformationen auf Websites zu veröffentlichen, ohne dabei die strengen Regeln des *Kreditinformationsgesetzes* einhalten zu müssen. Dies führte zu Verletzungen der Privatsphäre und zahlreichen Beschwerden.

Im Februar 2008 richtete die Regierung einen Untersuchungsausschuss ein, der die Gesetze im Bereich Videoüberwachung überprüfen sollte. Der Auftrag umfasste die Durchführung einer Umfrage sowie eine Analyse der Anwendung der aktuellen Gesetze. Im Rahmen der Untersuchung soll unter anderem festgestellt werden, ob im Bereich Videoüberwachung weitere Maßnahmen zur Verbesserung des Schutzes der Privatsphäre von Einzelpersonen erforderlich sind.

## B. Bedeutende Rechtsprechung

Die Datenschutzbehörde hat in den beiden vorangegangenen Jahresberichten Fälle präsentiert, in denen biometrische Daten in Schulen verwendet worden waren. Es wurden Fingerabdrücke von Schülern erfasst und in einer entsprechenden Maschine zwecks Zugangskontrolle zur Schulkantine verarbeitet. Im Dezember 2008 entschied das Oberste Verwaltungsgericht, dass Schulen die Fingerabdrücke von Schülern verwenden dürfen, um zu überprüfen, ob sie ihr Essen bezahlt haben oder nicht. Die Schüler müssen jedoch ihre Einwilligung geben, und es muss eine Alternative für diejenigen geben, die ihre Fingerabdrücke nicht erfassen lassen wollen.

In einer Entscheidung aus dem Jahr 2007 beschloss die Datenschutzbehörde, dass die Gewerkschaft der schwedischen Bauarbeiter die Verarbeitung von Lohndaten von Arbeitern, die nicht Mitglied dieser Gewerkschaft sind, einstellen müsse. Gegen diese Entscheidung wurde beim Bezirksverwaltungsgericht Berufung eingelegt. Die Berufung wurde im Dezember 2008 abgewiesen und die Entscheidung der Datenschutzbehörde bestätigt. Die Gewerkschaft der schwedischen Bauarbeiter hat beim zuständigen Verwaltungsgericht Berufung eingelegt. Der Fall ist anhängig.

Die Datenschutzbehörde hat von 2006 bis 2008 Überprüfungen von Fahrkartensystemen öffentlicher Verkehrsunternehmen durchgeführt. Diese (auf RFID-Techniken basierenden) Systeme nutzen so genannte „Smart Cards", die elektronische Spuren hinterlassen. Wenn ein Fahrgast seine elektronische Fahrkarte benutzt, werden folgende Daten erfasst: Kartennummer, Datum, Uhrzeit und Haltestelle/Bahnsteig. Wenn der Karteninhaber seine Smart Card beim Verkehrsunternehmen registriert hat, ist die Kartennummer mit der persönlichen Identifikationsnummer sowie dem Namen und der Anschrift des Fahrgastes verbunden. So können die elektronischen Spuren der Karte einer bestimmten Person zugeordnet werden. Die Datenschutzbehörde entschied, dass solche Spuren nur 60 Tage lang gespeichert werden dürften und danach eine Identifizierung nicht mehr möglich sein sollte. Eines der untersuchten Verkehrsunternehmen legte beim Bezirksverwaltungsgericht Berufung gegen die Entscheidung der Datenschutzbehörde ein. Das Gericht hob im Januar 2009 die Entscheidung der Datenschutzbehörde auf und ließ den Fall zur Neuprüfung zu.

Im Laufe des Jahres 2007 überprüfte die Datenschutzbehörde, wie Wohngesellschaften und Wohnverbände personenbezogene Daten mit elektronischen Schlüsselsystemen verarbeiten. Der elektronische Schlüssel ist einer bestimmten Wohnung zugeordnet und hinterlässt oftmals Daten im Zugangsprotokoll über Ort und Zeit der Verwendung des Schlüssels durch den Bewohner. Die Überprüfung zeigte, dass die personenbezogenen Daten nicht korrekt verarbeitet wurden. Die Datenschutzbehörde gab Leitlinien für die Verwendung elektronischer Schlüssel durch Wohngesellschaften und Wohnverbände heraus. Die Behörde vertritt eine sehr restriktive Ansicht in Bezug auf die Verwendung der Daten zu anderen Zwecken als zur Öffnung von Türen oder zur Buchung von Waschraumzeiten. Im Juli 2008 entschied die Behörde im Fall einer Wohngesellschaft, die die Daten der elektronischen Schlüssel unter anderem verwendete, um festzustellen, wer den Waschraum genutzt hatte. Die Behörde forderte die Wohngesellschaft auf, die Zugangsprotokolle nicht mehr zu diesem Zweck zu nutzen. Beim zuständigen Verwaltungsgericht wurde Berufung gegen diese Entscheidung eingelegt. Das Gericht bestätigte jedoch die Entscheidung der Datenschutzbehörde. Die Wohngesellschaft hat im Jahr 2009 Berufung beim zuständigen Berufungsgericht eingelegt.

Im Jahr 2008 verschickte die Datenschutzbehörde einen Internet-Fragebogen an Schulen. Eine der Fragen lautete, ob und in welchem Umfang Schulen Videoüberwachung auf ihrem Gelände verwendeten. Das Ergebnis zeigte, dass das Ausmaß der Videoüberwachung verglichen mit dem Jahr 2005, in dem eine vergleichbare Untersuchung durchgeführt worden war, um 150 % zugenommen hatte. Daraufhin untersuchte die Datenschutzbehörde sieben Schulen und stellte fest, dass die Videoüberwachung von Schülern bei Tag in vielerlei Hinsicht gegen das Datenschutzgesetz verstößt. Die Untersuchungen zeigten auch, dass die Kenntnisse in Bezug auf die Datenschutzgesetze mangelhaft sind. Aus diesem Grund gab die Datenschutzbehörde eine Checkliste heraus, damit die Schulen einfacher entscheiden können, wann eine Videoüberwachung erlaubt ist. Gegen die Entscheidungen der Behörde vom 1. Oktober 2008 wurden Berufungen vor dem zuständigen Verwaltungsgericht eingelegt. Die Verfahren sind anhängig.

## C. Wichtige spezifische Themen

**Drucksachen**

Sämtliche Drucksachen der Datenschutzbehörde können auf ihrer Website kostenlos heruntergeladen werden. *Magazin Direkt* ist eine vierteljährlich erscheinende Zeitschrift mit Berichten, Nachrichten und Kommentaren im Zusammenhang mit den Interessengebieten der Datenschutzbehörde. 2008 wurden vier Ausgaben veröffentlicht.

Wie bereits im vergangenen Jahr berichtet, hat die Datenschutzbehörde von der Regierung den Auftrag erhalten, zur Entwicklung sicherer und effizienter E-Government-Dienste beizutragen. Zuvor hatte die Behörde Leitfäden für Gemeinden herausgegeben. Im Jahr 2008 wurden zwei Serien von Leitfäden erarbeitet; eine für Regierungsbehörden („*E-Government und das Datenschutzgesetz*") und eine für alle öffentlichen Behörden („*IT-Sicherheit und E-Services öffentlicher Behörden*").

Außerdem wurde ein Bericht mit dem Titel *„Die Privatsphäre im Jahr 2008"* veröffentlicht, eine umfassende Studie zu neuen Gesetzen, Vorschlägen, Entscheidungen und Techniken, die die Privatsphäre im Laufe des Jahres betrafen.

Im Jahr 2008 wurde auch ein zweiter Bericht über die Einstellung junger Menschen insbesondere im Hinblick auf das Internet veröffentlicht. Außerdem wurde der Bericht *„Junge Menschen und die Privatsphäre"* auf der 30. Internationalen Konferenz zum Thema Datenschutz in Straßburg präsentiert.

**Branchenvereinbarungen**

Im Laufe des Jahres 2008 begann die Immobilienbranche auf Initiative der Datenschutzbehörde damit, eine Branchenvereinbarung (Verhaltensregeln) zur Regelung von Videoüberwachung in Wohnungsblocks zu erarbeiten. Diese Initiative wurde wegen der zunehmenden Zahl von Beschwerden über Videoüberwachung gestartet. Die Branchenvereinbarung wird voraussichtlich im Juni 2009 abgeschlossen.

**Der nordische Workshop zur Fallbehandlung**

Im Mai 2008 veranstaltete die Datenschutzbehörde den jährlich stattfindenden *nordischen Workshop zur Fallbehandlung* mit Teilnehmern aus Dänemark, den Färöer Inseln, Finnland, Island, Norwegen und Schweden.



## Vereinigtes Königreich

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

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

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

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

### B. Bedeutende Rechtsprechung

In einem Urteil des Europäischen Gerichtshofes für Menschenrechte aus dem Jahre 2008 im Fall S. und Marper/Vereinigtes Königreich wurde beschlossen, dass die „pauschale und willkürliche" Speicherung von DNS-Zellproben und -profilen von Personen, die verdächtigt werden, eine Straftat begangen zu haben, jedoch nicht verurteilt worden sind, unverhältnismäßig ist und ein Ungleichgewicht zwischen den Rechten des Einzelnen und den Interessen des Staates zur Folge hat.

Als Reaktion auf dieses Urteil hat sich die Regierung des Vereinigten Königreichs verpflichtet, im Jahr 2009 ein Weißbuch zur Sammlung und Verwendung forensischer Daten zu veröffentlichen.

Das Marper-Urteil ist für die Datenschutzbehörde (ICO) von erheblicher Bedeutung und wird weit reichende Auswirkungen jenseits der Speicherung von DNS und Fingerabdrücken mit sich bringen, da es die maßgebliche Unterstützung für das Konzept bietet, das wir für zahlreiche Aspekte des Schutzes personenbezogener Daten anwenden.

Die ICO hat nun einen Beobachterstatus bei allen Treffen des strategischen Ausschusses für eine nationale DNS-Datenbank.

### C. Wichtige spezifische Themen

Am Europäischen Datenschutztag im Januar wurden unsere revidierten CCTV-Verhaltensregeln im Parlament vorgestellt.

Wir haben Vollstreckungsmaßnahmen gegen zahlreiche Unternehmen ergriffen, unter anderem Carphone Warehouse (CPW) und Marks & Spencer (M&S). Die Untersuchung von CPW war die Reaktion auf Beschwerden hinsichtlich der Art und Weise, wie personenbezogene Informationen gespeichert und verarbeitet wurden. Die Maßnahmen gegen M&S wurden ergriffen, nachdem ein nicht verschlüsselter Laptop mit Daten zu 26.000 Angestellten gestohlen wurde.

Wir haben 17 Organisationen strafrechtlich verfolgt, darunter ein Inkassounternehmen aus Manchester, da dieses Unternehmen Einzelpersonen und andere Unternehmen unaufgefordert mit Faxen bombardierte, sowie einen Anwalt und einen Buchhalter, da diese sich nicht als Datenkontrolleure angemeldet hatten.

Am 25. Juni wurden vier Berichte zur Behandlung personenbezogener Informationen veröffentlicht. Die ICO veröffentlichte im November ihre Antwort auf diese Berichte.

**Der Bericht zur Behandlung von Daten**
Ein Bericht über Verfahren zur Behandlung von Daten in Regierungen, verfasst vom Premierminister als Antwort auf den Verlust personenbezogener Daten von über 25 Millionen Bürgern durch die britische Zoll- und Steuerbehörde, *Her Majesty's Revenue and Customs*, (*HMRC*, im Jahr 2007). Leiter des Projekts war Sir Gus O'Donnell, Mitglied der amtierenden Regierung. Eine der Empfehlungen war, dass alle zentralen Regierungsabteilungen Bewertungen zu Auswirkungen auf die Privatsphäre durchführen sollten.

**Der Bericht über die Informationssicherheit in der HMRC**
Der Schatzkanzler beauftragte Kieran Poynter, den Vorsitzenden von PricewaterhouseCoopers, eine Untersuchung des Verlustes der personenbezogenen Daten bei der HMRC durchzuführen und einen gründlichen Bericht über die Verfahren und Systeme zur Behandlung von Daten bei der HMRC zu erstellen.

**Der unabhängige Bericht der Unabhängigen Kommission für Beschwerden gegen die Polizei (Independent Police Complaints Commission (IPCC)) über die Untersuchung des Verlustes von Daten zum Kindergeld.**
Die IPCC, die gemäß dem Polizeigesetz von 2002 zuständig ist, hat eine eigene Untersuchung der Vorfälle gestartet, die zum Verlust der Daten bei der HMRC geführt haben, um festzustellen, ob ein strafbares Verhalten oder Disziplinarvergehen seitens des HMRC-Personals vorliegen.

**Der Bericht über den Verlust personenbezogener Daten des Verteidigungsministeriums (MOD)**
Am 9. Januar 2008 wurde ein Laptop der Royal Navy mit unverschlüsselten Daten von mehr als 600.000 Personen gestohlen. Der Verteidigungsminister beauftragte Sir Edmund Burton, eine Prüfung durchzuführen, um die genauen Umstände und Vorfälle zu ermitteln, die zum Verlust der personenbezogenen Daten des Verteidigungsministeriums geführt haben, die Angemessenheit der zur Vermeidung einer Wiederholung ergriffenen Maßnahmen zu untersuchen und die Vorkehrungen des MOD bezüglich Politik, Verfahren und Verwaltung im Hinblick auf den Schutz personenbezogener Daten im Allgemeinen zu prüfen.

Der von Richard Thomas und Dr. Mark Walport im Namen des Premierministers erstellte Bericht über die gemeinsame Datennutzung wurde am 11. Juli veröffentlicht. Der Bericht sprach eine Reihe vom Empfehlungen aus, die die persönliche und organisatorische Kultur derjenigen, die Informationen erfassen, verwalten und verbreiten, verändern soll. Wir haben eine Antwort zur Beratung des Berichts eingereicht.

Im März haben wir unsere Strategie zum Datenschutz auf der Konferenz unserer Datenschutzbeauftragten in Manchester vorgestellt, und im November haben wir unseren Bericht „Privacy by Design" auf unserer Konferenz in Manchester vorgestellt. Der Bericht „Privacy by Design" legt Organisationen nahe, einfache Maßnahmen zur Verbesserung der organisatorischen und technologischen Maßnahmen zum besseren Schutz personenbezogener Informationen zu ergreifen und zielt darauf ab, Organisationen dabei zu helfen, neue Techniken im Bereich „Privacy by Design" anzunehmen. Er betont die Notwendigkeit, sicherzustellen, dass der Schutz der Privatsphäre durch Organisationen sowie ab dem Beginn der Entwicklung neuer Informationssysteme korrekt gewährleistet wird.

Im Laufe des Jahres 2008 beantwortete der Datenschutzbeauftragte 47 Konsultationen (dieselbe Anzahl wie im Jahr 2007).

Im Laufe des Jahres 2008 legte der Datenschutzbeauftragte folgenden parlamentarischen Ausschüssen Beweise vor.

- Ausschuss Innenpolitik des Unterhauses: Bericht „Überwachungsgesellschaft?"
- Ausschuss Innenpolitik des Unterhauses: Untersuchung der „Überwachungsgesellschaft".
- Verfassungsausschuss des Oberhauses: Untersuchung zu „den Auswirkungen der Überwachung und Datenerfassung auf die Privatsphäre der Bürger und ihre Beziehung zum Staat".
- Auswahlausschuss des Oberhauses zur Europäischen Union, Unterausschuss Innenpolitik: Untersuchung des Rahmenbeschlusses zur Erfassung von Passagiernamen.
- Sonderausschuss des Oberhauses für die Europäische Union: Untersuchung von Europol.
- Ausschuss des Oberhauses für Wissenschaft und Technologie: Genomische Medizin – Folgen der Erstellung und Speicherung von Genomdaten für die Sicherheit von personenbezogenen Daten und Privatsphäre.
- Ausschuss des Unterhauses für öffentliche Gesetzesvorlagen: Stadium der Beratungen über die Verabschiedung des Gesetzes über Terrorismusbekämpfung.

Die ICO reichte überdies auch schriftliche Belege für den Thomas/Walport-Bericht zum Informationsaustausch ein und traf sich mit dem Team, das den Bericht erstellte.

Bis Ende 2008 gingen bei uns 340 Meldungen über Verstöße gegen die Sicherheitsauflagen ein, und wir hatten Leitlinien für Organisationen entwickelt, wie mit Verstößen gegen die Sicherheitsauflagen in Bezug auf personenbezogene Daten umgegangen werden muss.

# Kapitel 3
# Aktivitäten der Europäischen Union und der Gemeinschaft

## 3.1. EUROPÄISCHE KOMMISSION

*Entscheidung 2008/49/EG der Kommission vom 12. Dezember 2007 zur Umsetzung des Binnenmarktinformationssystems (IMI) im Hinblick auf den Schutz personenbezogener Daten*[24]

Die Kommission beschloss, die Entscheidung zur Umsetzung des IMI im Hinblick auf die Bestimmungen zum Schutz personenbezogener Daten zu ergänzen. Da die verschiedenen Aufgaben und Funktionen der Kommission und der Mitgliedstaaten im Hinblick auf das IMI unterschiedliche Verantwortlichkeiten und Pflichten bezüglich der Datenschutzbestimmungen mit sich bringen, definiert diese Entscheidung die jeweiligen Funktionen, Verantwortlichkeiten und Zugangsrechte gemäß den in der Stellungnahme der Artikel 29 Datenschutzgruppe genannten Vorschläge zu Fragen des Datenschutzes in Zusammenhang mit dem Binnenmarktinformationssystem (IMI).[25]

*Empfehlung der Kommission vom 2. Juli 2008 zur grenzübergreifenden Interoperabilität elektronischer Patientendatensysteme*[26]

Diese Empfehlung an die Mitgliedstaaten bietet eine Reihe von Leitlinien für die Entwicklung und den Einsatz interoperabler elektronischer Patientendatensysteme im Hinblick auf einen grenzübergreifenden Austausch von Patientendaten innerhalb der Gemeinschaft, sofern dieser Austausch einem legitimen medizinischen oder gesundheitsbezogenen Zweck dient. Solche elektronischen Patientendatensysteme sollten es Gesundheitsdienstleistern ermöglichen, zu gewährleisten, dass ein Patient durch den zeitnahen und sicheren Zugriff auf seine grundlegenden und möglicherweise lebenswichtigen gesundheitsbezogenen Informationen effektiver und effizienter behandelt wird und dass dies im Einklang mit den Grundrechten des Patienten betreffend Privatsphäre und Datenschutz erfolgt.

[24] ABl. L 13, 16.01.2008 S. 18 – 23.

[25] Stellungnahme 01911/07/EN, WP 140.

[26] ABl. L 190, 18.7.2008, S. 37–43

## 3.2. DER EUROPÄISCHE GERICHTSHOF

*Urteil des Gerichtshofes (Große Kammer) vom 29. Januar 2008 – Productores de Música de España (Promusicae) v Telefónica de España SAU (Rechtssache C-275/06)* [27]

Urteilstenor:
Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs, im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr" – „E-Commerce-Richtlinie"), Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft, Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums und Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) erfordern nicht, dass die Mitgliedstaaten in einer wie im Hauptverfahren vorliegenden Situation eine Verpflichtung zur Kommunikation personenbezogener Daten festlegen, um einen effektiven Schutz des Urheberrechts im Rahmen von Zivilverfahren zu gewährleisten. Das Recht der Gemeinschaft erfordert jedoch bei der Umsetzung dieser Richtlinien eine sorgfältige Interpretation durch die Mitgliedstaaten, so dass ein faires Gleichgewicht zwischen den verschiedenen durch die Rechtsordnung der Gemeinschaft garantierten Grundrechten gewährleistet wird. Darüber hinaus müssen die Behörden und Gerichte bei den Maßnahmen zur Umsetzung dieser Richtlinien nicht nur das jeweilige nationale Recht in Einklang mit diesen Richtlinien interpretieren, sondern auch gewährleisten, dass diese nicht auf eine Art und Weise interpretiert werden, dass sie in Konflikt mit diesen Grundrechten oder mit anderen allgemeinen Prinzipien des Rechts der Gemeinschaft stehen, wie z. B. dem Prinzip der Verhältnismäßigkeit.

[27] ABl. C 64 vom 08.03.2008, S. 9

*Urteil des Gerichtshofes (Große Kammer) vom 16. Dezember 2008 – Heinz Huber v Bundesrepublik Deutschland (Rechtssache C-524/06)*[28]

Urteilstenor:
1. Ein System zur Verarbeitung personenbezogener Daten von Unionsbürgern, die keine Staatsangehörigen des betreffenden Mitgliedstaates sind, wie das durch das Gesetz über das Ausländerzentralregister vom 2. September 1994 (geändert durch das Gesetz vom 21. Juni 2005) eingerichtete System, dessen Zweck die Bereitstellung von Unterstützung der für die Anwendung des Gesetzes über das Aufenthaltsrecht zuständigen nationalen Behörden ist, erfüllt nicht die gemäß Artikel 7(e) der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr festgelegten Anforderungen betreffend den Schutz vor Diskriminierung aufgrund der Staatsangehörigkeit, es sei denn:

- es enthält ausschließlich die Daten, die für die Anwendung des Gesetzes durch diese Behörden erforderlich sind, und
- seine zentrale Art ermöglicht eine effektivere Anwendung des Gesetzes über das Aufenthaltsrecht in Bezug auf EU-Bürger, die keine Staatsangehörigen des betreffenden Mitgliedstaates sind.

Das nationale Gericht muss entscheiden, ob diese Bedingungen im Hauptverfahren erfüllt sind.

Die Speicherung und Verarbeitung personenbezogener Daten, einschließlich individualisierter persönlicher Informationen, in einem Register wie dem Ausländerzentralregister zu statistischen Zwecken kann auf keinen Fall als gemäß Artikel 7(e) der Richtlinie 95/46 erforderlich eingestuft werden.

2. Artikel 12(1) EG muss dahingehend interpretiert werden, dass er die Umsetzung eines Systems zur Verarbeitung personenbezogener Daten von EU-Bürgern, die keine Staatsangehörigen des betreffenden Mitgliedstaates sind, durch einen Mitgliedstaat zum Zwecke der Verbrechensbekämpfung ausschließt.

[28] ABl. C 44 vom 21.02.2009, S. 5

*Urteil des erstinstanzlichen Gerichts vom 8. November 2007 – Bavarian Lager/Kommission (Rechtssache T-194/04)* [29]

Die Dritte Kammer des erstinstanzlichen Gerichts der Europäischen Gemeinschaft hob eine Entscheidung der Kommission vom 18. März 2004 auf, die den Antrag auf Einsichtnahme in das vollständige Protokoll einer Versammlung ablehnte. Das erstinstanzliche Gericht hielt dagegen, dass eine Anfrage an die Kommission der Europäischen Gemeinschaft wegen einer Einsichtnahme personenbezogener Daten in einem Bericht der Kommission nur aus Gründen der Privatsphäre und Unversehrtheit von Personen abgelehnt werden darf, wenn besagte Privatsphäre und Unversehrtheit im Allgemeinen und im Besonderen durch die Bekanntgabe unterminiert wurden; der Antragsteller muss nicht beweisen, dass die Bekanntgabe erforderlich ist. Die Kommission hat Einspruch eingelegt.

## 3.3. DER EUROPÄISCHE DATENSCHUTZBEAUFTRAGTE

*Einleitung*

Aufgabe des Europäischen Datenschutzbeauftragten (EDSB) ist es, sicherzustellen, dass die Rechte und Freiheiten von natürlichen Personen sowie insbesondere deren Privatsphäre im Hinblick auf die Verarbeitung personenbezogener Daten, von den Organen und Einrichtungen der Gemeinschaft nicht verletzt werden.

Die Hauptaktivitäten des Europäischen Datenschutzbeauftragten umfassen, wie in der Verordnung (EG) Nr. 45/2001[30] („die Verordnung") festgelegt, Folgendes:

- Überwachung und Sicherstellung der Einhaltung der Bestimmungen der Verordnung durch die Organe und Einrichtungen der Gemeinschaft bei der Verarbeitung personenbezogener Daten (Überwachung);
- Beratung der Organe und Einrichtungen der Gemeinschaft zu allen Fragen der Verarbeitung personenbezogener Daten. Dies umfasst die Beratung zu

[29] ABl. C 315 vom 22.12.2007, S.33

[30] Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr, ABl. L 8, 12.01.2001.

Gesetzesvorschlägen sowie die Überwachung neuer Entwicklungen, die Auswirkungen auf den Schutz personenbezogener Daten haben (Beratung);
- Zusammenarbeit mit nationalen Datenschutzbehörden und Aufsichtsbehörden als „dritte Säule" der EU im Hinblick auf eine Verbesserung der Einheitlichkeit des Schutzes personenbezogener Daten (Zusammenarbeit).

*Überwachung*

Die Überwachungsaufgaben reichen von der Beratung und Unterstützung der Datenschutzbeauftragten (DSB) über vorherige Überprüfung bedenklicher Verarbeitungsvorgänge bis zur Abwicklung von Anfragen, einschließlich Vor-Ort-Untersuchungen und Bearbeitung von Beschwerden usw.

**Vorherige Überprüfung** von Datenverarbeitungen war auch im Jahr 2008 der wesentliche Aspekt im Bereich Überwachung. Es wurden mehr Stellungnahmen abgegeben als in allen früheren Jahren. Der EDSB veröffentlichte über 100 Stellungnahmen zu vorherigen Überprüfungen, hauptsächlich zu folgenden Themen: Verarbeitung gesundheitsbezogener Daten, Einstellung von Personal und Auswahl von Bewerbern, Personalbewertung, Akkreditierung von Journalisten, Systeme zur Identitätsverwaltung, Zugangskontrolle und Sicherheitsüberprüfungen.

Da die meisten Organe und Einrichtungen gute Fortschritte hinsichtlich der Einhaltung der Datenschutzbestimmungen und -prinzipien machen, verlagert sich der Schwerpunkt der Überwachung hin zur Kontrolle der Umsetzung von Empfehlungen vorheriger Überprüfungen sowie der Verbesserung der Einhaltung dieser Bestimmungen und Prinzipien in Agenturen. In diesem Zusammenhang hat der EDSB seine **Prüfstrategie** weiterentwickelt und eine erste Reihe von Überprüfungen vor Ort bei verschiedenen Einrichtungen und Organen durchgeführt, um die Einhaltung in der Praxis zu bewerten.

Die Anzahl der insgesamt eingereichten **Beschwerden** erhöhte sich auch im Jahr 2008 wieder. Zwar gab es weniger zulässige Beschwerden, diese waren jedoch insgesamt komplexer. Die zulässigen Fälle betrafen insbesondere Fragen zum Zugriff auf Daten, zur Verarbeitung sensibler Daten, zum Recht auf Berichtigung und zur Informationspflicht.

Es wurde auch weiterhin in Bezug auf **Verwaltungsmaßnahmen** beraten, die die Organe und Einrichtungen der Gemeinschaft in Bezug auf die Verarbeitung personenbezogener Daten in Betracht zogen. Es ergab sich eine Vielzahl von schwierigen Fragen, wie etwa die der Übertragung medizinischer Akten an nationale Gerichte, des Zugriffs auf öffentliche Dokumente, die personenbezogene Daten enthalten, der Umsetzung der Bestimmungen der Verordnung (EG) Nr. 45/2001 sowie der vom Europäischen Bürgerbeauftragten bearbeiteten Beschwerden.

Der Europäische Datenschutzbeauftragte arbeitete weiter an den **Videoüberwachungsrichtlinien** als praktische Anleitung für Organe und Einrichtungen zur Einhaltung der Datenschutzvorschriften beim Einsatz von Videoüberwachungssystemen.

*Beratung*

Der EDSB hat seine Beratungsfunktion weiter ausgebaut und Stellungnahmen zu einer steigenden Anzahl von Gesetzesvorschlägen abgegeben. Er hat den Umfang seiner Interventionen auf ein breiteres Spektrum von Politikbereichen sowie auf alle Phasen des Gesetzgebungsprozesses ausgeweitet.

Im Jahr 2008 gab der EDSB 14 Stellungnahmen zu vorgeschlagenen EU-Gesetzen und Initiativen ab. Die meisten betrafen Fragen zu den Bereichen **Freiheit, Sicherheit und Gerechtigkeit**. Eine wichtige Entwicklung in diesem Bereich war die Verabschiedung der **Rahmenentscheidung zum Datenschutz** im Bereich der Zusammenarbeit von Polizei und Justiz bei Strafsachen. Bei den Verhandlungen schenkte der EDSB diesem Gesetz große Beachtung und gab drei Stellungnahmen sowie Kommentare zu diesem Thema ab.

Auch dem Vorschlag zur Änderung der Verordnung über den **öffentlichen Zugriff auf Dokumente** von EU-Einrichtungen sowie der Überprüfung der Richtlinie über Privatsphäre und elektronische Kommunikation („**ePrivacy"-Richtlinie**) schenkte der EDSB besondere

Aufmerksamkeit. Fragen zu **Fluggastdatensätzen** (PNR) wurden im Rahmen der Beratungstätigkeiten des EDSB ebenfalls häufig gestellt, insbesondere im Hinblick auf die Nachbereitung des entsprechenden PNR-Vorschlags der EU.

Ein wesentlicher Schwerpunktbereich für den ESDB war der **Austausch von Informationen**. Er gab Stellungnahmen zu Systemen zum Informationsaustausch ab, die im Zusammenhang mit dem Binnenmarktinformationssystem (IMI), Eurojust, der Straßenverkehrssicherheit, dem Schutz von Kindern bei der Nutzung des Internets, dem Europäischen Strafregisterinformationssystem (ECRIS), der hochrangigen Kontaktgruppe EU-USA für den Informationsaustausch und der Europäischen Strategie für den elektronischen Rechtsverkehr vorgeschlagen wurden. Vorläufige Kommentare wurden auch zum EU-Grenzschutzpaket der Kommission abgegeben. Die Stellungnahmen des EDSB betonten die Notwendigkeit der sorgfältigen Prüfung eines solchen Austauschs von Informationen sowie die Integration spezifischer Sicherheitsmaßnahmen bezüglich des Datenschutzes.

Auch der Einsatz **neuer Technologien** wurde zu verschiedenen Anlässen (z. B. ECRIS oder die Europäischen Strategie für den elektronischen Rechtsverkehr) angesprochen. Der EDSB forderte wiederholt, Datenschutzfragen so früh wie möglich zu berücksichtigen („Privacy-by-Design"). Er betonte außerdem, dass die Technologien nicht nur zum Austausch von Informationen, sondern auch zur Förderung der Rechte der betreffenden Personen eingesetzt werden sollten.

Ein weiteres wichtiges Thema war die **Qualität von Daten**. Ein hohes Maß an Datenkorrektheit ist erforderlich, um Unklarheiten hinsichtlich des Inhalts der verarbeiteten Informationen zu vermeiden. Die Korrektheit muss regelmäßig und ordnungsgemäß überprüft werden. Darüber hinaus bedeutet ein hohes Maß an Datenqualität nicht nur eine Grundgarantie für das Datensubjekt, sondern ermöglicht denen, die die Daten verarbeiten, auch eine effiziente Nutzung.

Es wurde eine Reihe von Perspektiven für künftige Änderungen festgestellt, die dem EDSB als Agenda wesentlicher **Prioritäten** dienen sollen. Hierzu gehören neue technologische Trends, die Bedenken hinsichtlich Datenschutz und Privatsphäre mit sich bringen wie z. B. die Entwicklung so genannter Cloud Computing-Systeme[31] und DNS-Sequenzierungstechnologien.

Hinsichtlich neuer Entwicklungen in den Bereichen **Politik und Gesetzgebung** umfassen die wesentlichen Themen, auf die der EDSB einen besonderen Schwerpunkt legen möchte, unter anderem Folgendes:

- Überlegungen zu weiteren Verbesserungen der **Rahmenentscheidung zum Datenschutz** zur Verbesserung des durch das neue Instrument der dritten Säule gewährten Schutzes;
- **die Zukunft der Datenschutzrichtlinie**;
- das Mehrjahresprogramm der Kommission im Bereich Freiheit, Sicherheit und Gerechtigkeit – mit dem Titel „**Stockholm-Programm**";
- **wichtige Trends im Gesetzesvollzug** sowie legislative Aktivitäten zur Bekämpfung des Terrorismus und des organisierten Verbrechens;
- Revision der Verordnung über den **öffentlichen Zugang zu Dokumenten**;
- neue Initiativen zur Verbesserung der **grenzüberschreitenden medizinischen Versorgung** in Kombination mit dem Einsatz von Informationstechnologien.

*Zusammenarbeit*

Die wesentliche Plattform für die Zusammenarbeit zwischen den Datenschutzbehörden in Europa ist die **Artikel 29 Datenschutzgruppe**. Der Europäische Datenschutzbeauftragte nimmt an den Aktivitäten der Datenschutzgruppe teil, die eine zentrale Rolle bei der einheitlichen Anwendung der Datenschutzrichtlinie spielt.

Der EDSB und die Arbeitsgruppe haben zusammengearbeitet, um eine gute Synergie zu einer Reihe von Themen zu erreichen. Der Schwerpunkt lag hierbei auf der Umsetzung der Datenschutzrichtlinie sowie auf Herausforderungen durch die Nutzung neuer Technologien. Der EDSB unterstützte außerdem Initiativen zur Erleichterung internationaler Datenflüsse.

[31] Cloud Computing bezeichnet die Nutzung internetbasierter („Cloud") Computertechnologien für eine Vielzahl von Diensten. Hierbei werden dynamisch skalierbare und oftmals virtualisierte Ressourcen als Dienst über das Internet bereitgestellt.

Die Arbeitsgruppe hat Stellungnahmen zu Gesetzesentwürfen angenommen, die in einigen Fällen auch Thema der Stellungnahmen des EDSB waren (z. B. Überprüfung der „e-Privacy"-Richtlinie). Während die Stellungnahme des EDSB im Gesetzgebungsprozess der EU verpflichtend ist, so sind auch Beiträge der Arbeitsgruppe sehr nützlich, insbesondere da sie eventuell von einem nationalen Standpunkt aus auf besondere Punkte eingehen. Aus diesem Grund begrüßt der EDSB diese Beiträge, die mit seinen eigenen Stellungnahmen konform gingen.

Eine der wichtigsten Aufgaben des Europäischen Datenschutzbeauftragten in Bezug auf die Zusammenarbeit betrifft **Eurodac**, für deren Verantwortung hinsichtlich der Überwachung des Datenschutzes die nationalen Datenschutzbehörden und der Europäische Datenschutzbeauftragte zeichnen. Der Koordinierungsausschuss zur Eurodac-Überwachung – der sich aus den Datenschutzbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten zusammensetzt – trat im Jahr 2008 zwei Mal zusammen. Der Schwerpunkt lag hierbei auf der Umsetzung des vom Ausschuss im Dezember 2007 verabschiedeten Arbeitsprogramms. Innerhalb des Arbeitsprogramms wurden die folgenden drei Themen zur genaueren Überprüfung und Berichterstattung ausgewählt: Information der Datensubjekte, Kinder und Eurodac sowie DubliNet[32]. Gleichzeitig wurde auch dem Rahmen, innerhalb dessen der Ausschuss tätig ist, Aufmerksamkeit geschenkt: Die Europäische Kommission hat eine Überprüfung der Dublin- und Eurodac-Verordnungen im allgemeinen Rahmen von Asylmaßnahmen durchgeführt.

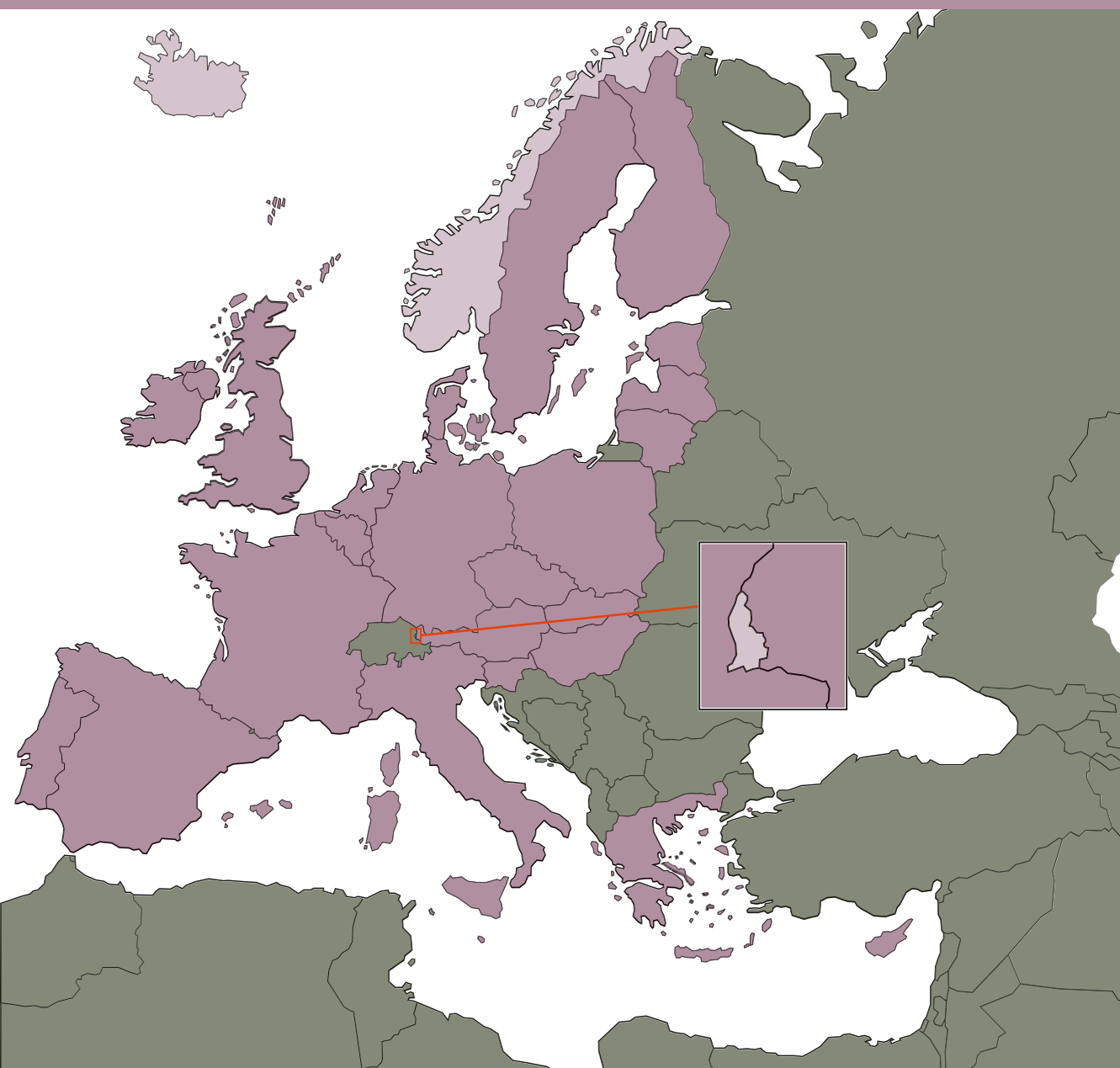
Die Notwendigkeit einer engen Zusammenarbeit zwischen den EDSB und anderen Datenschutzbehörden zu **Fragen der dritten Säule** – des Bereichs der Zusammenarbeit zwischen Polizei und Justiz – ist in den vergangenen Jahren aufgrund der steigenden Zahl von Initiativen betreffend Erfassung und Austausch personenbezogener Daten auf europäischer und internationaler Ebene offensichtlich geworden.

Der EDSB ist bemüht, ein hohes und einheitliches Maß an Datenschutz bei der Arbeit der im Rahmen der dritten Säule der EU eingerichteten Kontrollinstanzen der Datenschutzbehörden (Gemeinsame Kontrollinstanz von Schengen, Europol, Eurojust und das Zollinformationssystem) zu gewährleisten. Darüber hinaus arbeitet der EDSB durch eine aktive Teilnahme an Treffen der Arbeitsgruppe Polizei und Justiz mit nationalen Datenschutzbehörden zusammen.

Der Zusammenarbeit in anderen **internationalen Foren,** wie z. B. der Internationalen Konferenz für Beauftragte für den Schutz von Daten und Privatsphäre in Straßburg und der „London-Initiative" zur Sensibilisierung für Datenschutz und dessen effektiverer wurde auch weiterhin Beachtung geschenkt. Nach ähnlichen Veranstaltungen in den Jahren 2005 und 2007 wird ein dritter Workshop zum Thema Datenschutz in internationalen Organisationen derzeit in Erwägung gezogen.

[32] DubliNet ist ein sicheres elektronisches Übermittlungsnetz zwischen den nationalen Behörden, die Asylanträge bearbeiten. Ein „Treffer" im Eurodac-System löst normalerweise einen Austausch von Daten über den Asylbewerber aus. Dieser Austausch erfolgt über DubliNet.

# Kapitel 4
# Die wichtigsten Entwicklungen im Europäischen Wirtschaftsraum



# Island

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

Im Jahr 2008 wurde eine Reihe von Rechtsakten und Verwaltungsvorschriften im Zusammenhang mit dem Datenschutz erlassen, die die Richtlinie 95/46/EG (jedoch nicht die Richtlinie 2002/58/EG) betrafen. Die wichtigsten davon waren die Folgenden:

1. Gesetz Nr. 88/2008 über Strafverfahren. – Dieses Gesetz enthält eine Reihe von Bestimmungen zur Privatsphäre von Personen, insbesondere Angeklagten, beispielsweise aber auch von Zeugen. Hierzu gehören die Bestimmungen von Artikel 16 betreffend den Zugang zu Gerichtsdokumenten. Artikel 16 bietet nicht nur dem Angeklagten und seinem Anwalt dieses Recht, sondern auch der Öffentlichkeit. Sowohl die Aussagen des Klägers als auch des Angeklagten sind der Öffentlichkeit zugänglich. Teile dieser Dokumente mit Informationen zu privaten, finanziellen oder wirtschaftlichen Angaben sind jedoch unter Verschluss zu halten, da ein solches Maß an Geheimhaltung als fair und angemessen gilt, es sei denn, die betreffende Partei willigt in die Offenlegung dieser Informationen ein. Urteile und sonstige gerichtliche Entscheidungen sind der Öffentlichkeit auf Antrag offen zu legen. In einigen Fällen sind bestimmte Informationen jedoch aus diesen Dokumenten zu löschen, z. B. dann, wenn private Interessen die Löschung wegen besonderer Umständer erfordern. Gemäß Artikel 17 sind Urteile und gerichtliche Entscheidungen nicht nur auf Antrag offen zu legen. Die Gerichte können diese beispielsweise auch auf ihren Websites veröffentlichen, müssen dann jedoch Bestimmungen zur Löschung von Daten einhalten, die nicht veröffentlicht werden dürfen.

2. Gesetz Nr. 97/2008 zur Änderung des Medizinproduktegesetzes Nr. 93/1994. – Im Jahr 2003 wurden neue Bestimmungen in das Gesetz Nr. 93/1994 eingefügt; vgl. Gesetz Nr. 89/2003 über eine zentrale Arzneiverordnungsdatenbank, die der nationalen Gesundheitsverwaltung untersteht. Die Bestimmungen zu dieser Datenbank sind in Artikel 27 des Gesetzes Nr. 93/1994 festgelegt. Gemäß diesen Bestimmungen hat die nationale Gesundheitsverwaltung Zugang zur Datenbank, um suchtfördernde bzw. narkotische medizinische Produkte, die von Ärzten ausgestellten Rezepte sowie die Entwicklung bei medizinischen Produkten überwachen zu können. Wenn bestimmte Kriterien erfüllt sind, kann auch der isländischen Arzneimittelkontrollbehörde und der Krankenversicherungsanstalt Zugang gewährt werden. Ursprünglich sollten Daten, mithilfe derer Personen identifiziert werden könnten, drei Jahre nach ihrem Eintrag in die Datenbank gelöscht werden. Das Gesetz Nr. 97/2008 verlängerte diesen Zeitraum jedoch auf 30 Jahre.

3. Gesetz Nr. 112/2008 zur Krankenversicherung. – Gemäß diesem Gesetz wurde eine neue öffentliche Anstalt eingerichtet, die Krankenversicherungsanstalt. Diese Anstalt hat die Aufgabe, mit Gesundheitseinrichtungen und unabhängigen Gesundheitsdienstleistern über Zahlungen aus öffentlichen Gesundheitsfonds zu verhandeln. Gemäß Artikel 46 des Gesetzes sind Mediziner, die für die Speicherung von Patientendaten verantwortlich sind, verpflichtet, der Krankenversicherungsanstalt Zugang zu den Daten und Dokumenten zu gewähren, die für die Erledigung der Aufgaben der Anstalt erforderlich sind. Angestellte der Anstalt dürfen die Patientenakten nur in den Räumlichkeiten lesen, in denen sie aufbewahrt werden. Ferner dürfen sie auch nur die Teile lesen, die zur Verwaltung von Krankenversicherungsverträgen erforderlich sind.

4. Gesetz Nr. 142/2008 zur Untersuchung der Ereignisse und der Gründe für den Niedergang der isländischen Banken im Jahr 2008 sowie damit in Zusammenhang stehender Ereignisse. – Das Gesetz bildet die Grundlage für die Einrichtung eines Sonderuntersuchungsausschusses unter der Federführung des isländischen Parlaments. Der Ausschuss soll die Finanzkrise in Island, die im Herbst 2008 begann, untersuchen und über die Schlussfolgerungen der Untersuchungen Bericht erstatten. Der Ausschuss soll dem Generalstaatsanwalt gemäß Artikel 14 des Gesetzes jeden Verdacht kriminellen Verhaltens melden. Darüber hinaus soll der Ausschuss den Leiter der Institution sowie das zuständige Ministerium informieren, wenn es wahrscheinlich ist, dass ein Beschäftigter im öffentlichen Dienst eine Amtspflichtverletzung begangen hat. Gemäß Paragraph 1, Artikel 6 des Gesetzes sind

alle Personen, Institutionen und juristische Personen verpflichtet, dem Untersuchungsausschuss alle geforderten Informationen, Dokumente und Erklärungen zur Verfügung zu stellen.

Die Mitglieder des Ausschusses sowie die Personen, die bei den Untersuchungen mitarbeiten, sind gemäß Paragraph 3, Artikel 4 des Gesetzes verpflichtet, Stillschweigen hinsichtlich vom Ausschuss erhaltener vertraulicher Informationen zu wahren. Der Ausschuss kann den Arbeitsgruppen und Fachberatern jedoch gegebenenfalls auch Informationen und Dokumente zur Verfügung stellen. Außerdem kann der Ausschuss gegebenenfalls Informationen zum gegenseitigen Informationsaustausch sowie zur Zusammenarbeit mit Parteien im Ausland liefern, die an Untersuchungen beteiligt sind, die mit denen des Ausschusses vergleichbar sind. Die Partei, die Informationen erhält, ist ebenfalls zu Stillschweigen verpflichtet. Gemäß Paragraph 4, Artikel 4 schließen die oben genannten Bestimmungen jedoch nicht die Veröffentlichung von Informationen durch den Ausschuss aus, wenn der Ausschuss dies zur Begründung seiner Schlussfolgerungen für erforderlich hält. Dies gilt auch dann, wenn die Informationen ansonsten als vertraulich einzustufen wären. Informationen zu persönlichen Angaben der betreffenden Personen, unter anderem beispielsweise Angaben zur finanziellen Situation, dürfen nur dann veröffentlicht werden, wenn das öffentliche Interesse an der Offenlegung schwerer wiegt als die persönlichen Interessen der betreffenden Person.

Gemäß Paragraph 2, Artikel 17 des Gesetzes gelten die Bestimmungen der Artikel 18–21 des Datenschutzgesetzes Nr. 77/2000, d. h. die Bestimmungen betreffend Zugangsrechte und dem Datensubjekt bereitzustellende Informationen, nicht für die Aktivitäten des Ausschusses. Nichtsdestotrotz sollen die Personen, die der Ausschuss untersucht, gemäß Paragraph 3, Artikel 17 nach Abschluss der Untersuchungen die Rechte der zuvor genannten Bestimmungen des Datenschutzgesetzes genießen, wenn in ihrem Fall kein Strafverfahren eingeleitet wurde. Für das Recht auf Zugang gelten in diesen Fällen die Bestimmungen des betreffenden Verfahrensrechts.

5. Gesetz Nr. 160/2008 über ein Service- und Wissenszentrum für Blinde und Sehbehinderte. – Gemäß Artikel 6 des Gesetzes soll das Service- und Wissenszentrum ein Register aller Blinden und Sehbehinderten führen, um so die diesen Menschen angebotenen Dienstleistungen zu verbessern und die Qualität der Dienstleistungen zu garantieren, die Bereitstellung der Dienstleistungen zu überwachen sowie statistische und wissenschaftliche Forschungen durchzuführen. Die diesbezügliche Verarbeitung personenbezogener Daten soll im Einklang mit dem Datenschutzgesetz erfolgen.

6. Gesetz Nr. 164/2008 zur Änderung des Einkommensteuergesetzes Nr. 90/2003. – Mit Artikel 6 des Gesetzes wurde eine neue Bestimmung für das Einkommensteuergesetz eingeführt, die besagt, dass Banken und andere Kreditinstitute, die Depots führen, auf eigene Initiative hin den nationalen Steuerbeauftragten am Jahresende über Depotzinsen und Geldbeträge in diesen Depots informieren sollen.

7. Vorschriften betreffend die Verpflichtung zur Meldung bzw. zur Einholung einer Genehmigung für die Verarbeitung personenbezogener Daten, Nr. 712/2004. – Diese von der Datenschutzbehörde (DSB) im Einklang mit dem Datenschutzgesetz, Artikel 31 und 33, verabschiedeten Vorschriften ersetzen die Vorschrift Nr. 698/2004. Die wichtigste Änderung besteht darin, dass für die Verarbeitung personenbezogener Daten in der Genforschung keine Genehmigung mehr eingeholt werden muss, sofern die Datensubjekte in die Verarbeitung eingewilligt haben. Die Verarbeitung ist der DSB jedoch zu melden. Wie nachstehend unter Punkt 8 beschrieben, hat die DSB Vorschriften zur Verarbeitung personenbezogener Daten in der Genforschung verabschiedet.

8. Vorschrift Nr. 1100/2008 über die Verarbeitung personenbezogener Daten in der Genforschung. – Wie zuvor unter Punkt 7 beschrieben, muss für die Verarbeitung personenbezogener Daten in der Genforschung keine Genehmigung mehr eingeholt werden, wenn die Datensubjekte in die Verarbeitung eingewilligt haben. Die Bestimmungen von Vorschrift 1100/2008 sind stets einzuhalten. Diese Bestimmungen haben die Bestimmungen betreffend die Genehmigungen für individuelle Forschungsprojekte ersetzt. Gemäß diesen Bestimmungen müssen für die Einwilligung eines Datensubjektes bestimmte Anforderungen

erfüllt sein. So muss beispielsweise darüber informiert werden, wann die Daten gelöscht oder ob sie dauerhaft zu Forschungszwecken gespeichert werden, ob geplant ist, Verwandte zu kontaktieren, um sie um ihre Teilnahme am Forschungsprojekt zu bitten und ob das Datensubjekt Informationen über sein Erbbild (Genotyp) erhält, sofern dies gewünscht wird. Diese Vorschriften umfassen auch Bestimmungen, die beispielsweise die Verschlüsselung personenbezogener Daten betreffen, damit niemand, der Gendaten verarbeitet, Zugang zu Daten erhält, über die eine Person identifiziert werden könnte,< und damit diejenigen, die die Genforschung durchführen, der DSB die Verarbeitung personenbezogener Daten jedes Forschungsprojektes melden und ihr eine Beschreibung der Sicherheitsmaßnahmen bei den betreffenden Forschungen zur Verfügung stellen. Werden dieselben Sicherheitsmaßnahmen bei mehr als einem Forschungsprojekt verwendet, so ist eine gemeinsame Beschreibung für all diese Projekte ausreichend.

## B. Bedeutende Rechtsprechung

Am 3. Oktober 2008 fällt der Oberste Gerichtshof Islands ein Urteil zur Befugnis des nationalen Steuerbeauftragten, finanzielle Daten von Personen anzufordern. Der Steuerbeauftragte hatte Daten von Kreditkartenunternehmen zu allen Transaktionen von Kreditkarten angefordert, die im Ausland im Auftrag gegeben und belastet wurden, da die gesamte Belastungssumme einen bestimmten Betrag überschritten hatte. Die Anforderung erfolgte auf der Grundlage von Artikel 94 des Einkommensteuergesetzes Nr. 90/2003, der besagt, dass jeder verpflichtet ist, den Steuerbehörden alle erforderlichen Informationen und Dokumente zu Verfügung zu stellen, die die Behörden anfordern.

Ein Kreditkartenunternehmen weigerte sich, die angeforderten Informationen zur Verfügung zu stellen. Gemäß Artikel 94 des oben genannten Gesetzes beantragte der nationale Steuerbeauftragte eine richterliche Entscheidung hinsichtlich der Verpflichtung des Unternehmens, die Informationen zur Verfügung zu stellen. Das Bezirksgericht von Reykjavik kam zu dem Schluss, dass das Unternehmen hierzu verpflichtet sei. Das Unternehmen legte beim Obersten Gerichtshof Berufung gegen diese Entscheidung ein. Das Gericht stellte unter anderem fest, dass die Aufforderung des nationalen Steuerbeauftragten zur Bereitstellung der Informationen nicht die Grenzen der Unterabsätze 2 und 3 von Paragraph 1, Artikel 7 des Datenschutzgesetzes überschritt. Diese Absätze besagen, dass personenbezogene Daten zu speziellen, ausdrücklichen und relevanten Zwecken einzuholen sind und für keine sonstigen Zwecke weiterverarbeitet werden und dass besagte personenbezogene Daten angemessen, relevant und im Hinblick auf den Zweck der Verarbeitung nicht unverhältnismäßig sein dürfen. Dementsprechend kam der Oberste Gerichtshof zu dem Schluss, dass das betreffende Unternehmen verpflichtet war, die vom nationalen Steuerbeauftragten angeforderten Informationen zur Verfügung zu stellen.

## C. Wichtige spezifische Themen

Wie in den zuvor aufgeführten Entwicklungen in der Gesetzgebung im Jahr 2008 beschrieben, wurde das Medizinproduktegesetz Nr. 93/1994 dahingehend geändert, dass der Speicherzeitraum personenbezogener Daten in der zentralen Arzneiverordnungsdatenbank von drei auf 30 Jahre verlängert wurde. Dies war eine der wichtigsten Fragen zum Thema Datenschutz im Jahr 2008. Die DSB gab eine Stellungnahme zur Gesetzesvorlage der vorgeschlagenen Änderung des Gesetzes ab, in der sie die Verlängerung des Speicherzeitraums als unverhältnismäßig bezeichnete.

Ein weiteres wichtiges Thema war die Verabschiedung der Vorschrift Nr. 1100/2008 der DSB über die Verarbeitung personenbezogener Daten in der Genforschung, vgl. die Diskussionen über diese Vorschriften in der Beschreibung der Entwicklungen in der Gesetzgebung im Jahr 2008.

Am 6. Oktober 2008 gab die DSB eine Stellungnahme für den isländischen Arbeitgeberverband zur Frage ab, ob die Verarbeitung personenbezogener Daten durch ein Unternehmen im Hinblick auf einen Resozialisierungsplan legal ist. Nach diesem Plan würde eine des Diebstahls oder des versuchten Diebstahls von Waren verdächtigte Person nicht von der Polizei angezeigt, wenn sie dem betreffenden Unternehmen einen bestimmten Geldbetrag zahlt. Die betreffende Person würde diesbezüglich eine Vereinbarung unterschreiben, mit der sie in die Eintragung ihrer personenbezogenen Daten

in eine von einem bestimmten Sicherheitsunternehmen gepflegte Datenbank einwilligt.
Die DSB war der Ansicht, dass es unsicher sei, ob Vereinbarungen mit Einzelpersonen hinsichtlich dieses Resozialisierungsplans legal sind. Darüber hinaus würde dies bedeuten, dass private Unternehmen Funktionen des Staates ausüben würden, d. h. über die Strafe für einen Rechtsverstoß entscheiden. Daher hielt es die DSB für fraglich, ob die Verarbeitung personenbezogener Daten im Rahmen des Resozialisierungsplans als rechtmäßig eingestuft werden kann. Dementsprechend wurde der Plan nicht umgesetzt.

## Liechtenstein

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

Eine der Aufgaben des Datenschutzbeauftragten (DSB) ist es, zu gesetzlichen Vorlagen und Erlassen, die für den Datenschutz erheblich sind, Stellung zu nehmen und die Übereinstimmung mit den Bestimmungen der Richtlinie 95/46/EG zu überprüfen. Im Jahr 2008 gab der DSB zu 20 Gesetzesvorhaben eine Stellungnahme ab. Hervorzuheben, da von besonderer datenschutzrechtlicher Relevanz, sind hierbei die zwei Teilrevisionen des liechtensteinischen Datenschutzgesetzes (DSG) und eine Sammelvorlage zur Bearbeitung von besonders schützenswerten Daten, auf die im Folgenden näher eingegangen werden soll:

Die *erste Teilrevision des DSG* war in Zusammenhang mit einem Beitritt zu Schengen und Dublin zu sehen, in dessen Rahmen auch ein Fokus auf dem Datenschutz liegt. Diese Gesetzesänderung betraf daher vor allem die Struktur und Organisation der Stabsstelle für Datenschutz (SDS). Bis dato war die SDS in die Landesverwaltung Liechtensteins eingebettet und dem Ressort Justiz unterstellt und wurde demzufolge eher als eine Amtsstelle, denn als eine unabhängige Institution wahrgenommen. Unter Berücksichtigung der Datenschutzrichtlinie 95/46/EG erfüllte die SDS damit nicht die Voraussetzung an eine „völlig unabhängige Kontrollstelle".[33] Diese völlige Unabhängigkeit bedeutet, dass die Institution des DSB institutionell, personell und finanziell vollständig selbstständig sein muss. Insofern war eine Anpassung des DSG erforderlich, um auf die Evaluation zu Schengen/Dublin bestmöglich vorbereitet zu sein. Die diesbezüglichen Abänderungen des DSG sehen vor, dass die SDS neu als Datenschutzstelle (DSS) bezeichnet werden wird und in völliger Unabhängigkeit dem Landtag zugeteilt ist. Der DSB wird nicht mehr von der Regierung bestellt, sondern vom Landtag gewählt. Der DSB erhält die personelle und finanzielle Unabhängigkeit und ein eigenes Beschwerderecht. Diese sehr bedeutenden Gesetzesneuerungen konnten zum 1.1.2009 in Kraft treten.

In einer *zweiten Teilrevision des DSG* wurde eine Umsetzung der Bestimmungen des Zusatzprotokolls zum Datenschutzabkommen des Europarates zusammen mit einer textnäheren Umsetzung der Datenschutzrichtlinie angegangen. Neben kleineren redaktionellen Änderungen, die sich vor allem auf Grund der gesammelten Erfahrungen in den letzten fünf Jahren ergeben hatten, sollen datenschutzrechtliche Zertifizierungsverfahren neu eingeführt werden. Danach kann für betriebliche Abläufe und Organisationsstrukturen, aber auch für informationstechnische Produkte die Auszeichnung durch ein noch zu gründendes Datenschutzqualitätszeichen verliehen werden. Letztere führen zu einer Stärkung der Selbstverantwortung der Inhaber der Datensammlungen und werden sicherlich dazu beitragen, den Datenschutz zu fördern. Dieses Ziel verfolgt auch die Anpassung der Vorschriften zum Datentransfer ins Ausland an die Richtlinie 95/46/EG. Die bislang bestehende Meldepflicht von bestimmten Datenbekanntgaben ins Ausland soll einer generellen Sorgfaltspflicht der Inhaber der Datensammlungen weichen. Neu vorgesehen ist auch die Aufnahme einer gesetzlichen Grundlage für die Videoüberwachung im öffentlichen Raum, nachdem die Datenschutzkommission in ihrer Entscheidung von April 2008 die Schaffung einer solchen dringend empfohlen hatte.[34] Die Zulässigkeit einer Videoüberwachung im öffentlichen Raum bedarf sodann der vorherigen Bewilligung durch die Datenschutzstelle. Diese Teilrevision wird am 01. Juli 2009 in Kraft treten.

Nach *Artikel 44 Absatz 3 DSG* lief bereits am 31. Juli 2007 die Übergangsfrist ab, wonach ab diesem Datum keine Datensammlungen und Persönlichkeitsprofile mehr bearbeitet werden dürfen, ohne dass eine explizite Rechtsgrundlage gegeben ist. Der Schaffung der noch ausstehenden und erforderlichen gesetzlichen Grundlagen zur Bearbeitung von besonders schützenswerten Personendaten wurde nunmehr in einer *Sammelvorlage* nachkommen.

[33] Vgl. Artikel 28 der Richtlinie 95/46/EG („complete independence").

[34] Vgl. unten, B.

## B. Bedeutende Rechtsprechung

Die *Entscheidung der Datenschutzkommission des Fürstentums Liechtenstein (DSK) vom 07. April 2008* zur Videoüberwachung in der Fussgängerzone in Vaduz stellt einen Grundsatzentscheid dar, der verfassungsrechtliche Anforderungen an den Staat zum Eingriff in die Privatsphäre wiedergibt.[35]

**Zum Sachverhalt:**
Auf Beschluss des Gemeinderates vom 29. August 2006 installierte die Gemeinde Vaduz Videokameras zur Überwachung der Fussgängerzone. Es fand rund um die Uhr eine flächendeckende Videoüberwachung durch 16 Kameras statt. In Bezug auf die gesetzliche Grundlage stützte sich die Gemeinde Vaduz hierbei auf Artikel 52 Absatz 4 Gemeindegesetz.[36]

Auf Grund einer bei der SDS eingegangenen Beschwerde[37] hatte der DSB 2007 an die Gemeinde die Empfehlung abgegeben, die Videoüberwachung in der Fussgängerzone zu reduzieren, da nicht von einem verhältnismässigen Eingriff in die Privatsphäre ausgegangen werden könne. Ausserdem sei zu bezweifeln, dass Artikel 52 Absatz 4 Gemeindegesetz eine hinreichend bestimmte Gesetzesgrundlage darstelle. Da die Gemeinde der Empfehlung nicht Folge leistete, legte der DSB die Angelegenheit der DSK zur Entscheidung vor.

**Zu den Entscheidungsgründen:**
Die flächendeckende Videoüberwachung der Fussgängerzone bewirkt einen erheblichen Eingriff in die grundrechtlich geschützten Rechte auf Privatsphäre[38] und persönliche Freiheit[39] des einzelnen Passanten. Die flächendeckende Videoüberwachung eines öffentlichen Raums stellt schon deshalb einen erheblichen Eingriff in die Grundrechte der Privatsphäre und der persönlichen Freiheit dar, weil sie als Eingriff mit grosser Streubreite anzusehen ist, der verdachtsunabhängig alle Personen betrifft, die den überwachten Bereich betreten, ohne dass diese in einer Beziehung zu einem konkreten Fehlverhalten stehen bzw. den Eingriff durch ihr Verhalten veranlasst haben.[40]

Die Einschränkung eines Grundrechts ist nach Auffassung der DSK nur möglich, wenn sie auf einer gesetzlich Grundlage beruht, im öffentlichen Interesse liegt, verhältnismässig ist und den Kerngehalt des geschützten Rechtsguts nicht völlig aushöhlt; diese Grundsätze gelten allein schon auf Grund der Europäischen Menschenrechtskonvention.

Die Generalklausel des Artikel 52 Absatz 4 Gemeindegesetz als gesetzliche Grundlage wird von der DSK dementsprechend als nicht ausreichend empfunden, da eine flächendeckende Videoüberwachung eines öffentlichen Raumes einen Eingriff von erheblichem Gewicht in die Privatsphäre und das Grundrecht der persönlichen Freiheit darstellt und als solcher einer speziellen gesetzlichen Ermächtigung bedarf. Je grösser also die Intensität des Eingriffs ist, umso klarer müssen die Voraussetzungen dafür geregelt sein. Die DSK empfiehlt daher in ihrer Entscheidung die Schaffung einer spezialgesetzlichen Ermächtigung zur Videoüberwachung, da eine solche im Fürstentum Liechtenstein bisher nicht besteht und die Videoüberwachung eine immer grössere Rolle spielt.[41]

Das von der Gemeinde verfolgte öffentliche Interesse, für Ruhe, Sicherheit und Ordnung zu sorgen und konkrete Straftaten, wie beispielsweise Vandalismus und Sachbeschädigungen zu verhindern, sei zwar unbestritten. Dem Verhältnismässigkeitsprinzip[42] aber liegt der Gedanke zugrunde, dass ein Eingriff in ein Freiheitsrecht nicht weiter gehen darf, als das öffentliche Interesse es erfordert. Die staatliche Massnahme muss geeignet sein, um den im öffentlichen Interesse verfolgten Zweck herbeizuführen. Die Massnahme muss im Hinblick auf den angestrebten Zweck zudem erforderlich sein, d. h. sie hat zu unterbleiben, wenn eine gleich geeignete, aber mildere Massnahme für den angestrebten

[35] Die vollständige Entscheidung kann abgerufen werden unter: http://www.llv.li/entscheidung_der_datenschutzkommission_zur_videoueberwachung_in_der_fussgaengerzone_in__vaduz.pdf.

[36] Artikel 52 Absatz 4 Gemeindegesetz besagt: „Er [der Gemeindevorsteher] steht der örtlichen Polizei vor und sorgt für Ruhe, Sicherheit und Ordnung. Er trifft die dazu nötigen Anordnungen und verhängt aufgrund gesetzlicher und ortspolizeilicher Vorschriften Bussen."

[37] Vgl. Jahresbericht 2007.

[38] Artikel 32 Absatz 1 der liechtensteinischen Landesverfassung.

[39] Artikel 8 EMRK

[40] Vgl. Entscheidung des deutschen Bundesverfassungsgerichts vom 23.02.2007, Az. 1 BvR 2368/06.

[41] Vgl. oben, zu A. zur zweiten Teilrevision des DSG.

[42] Vgl. Artikel 4 DSG.

Erfolg ausreichen würde. Der Eingriff darf in sachlicher, räumlicher und zeitlicher Beziehung nicht über das Notwendige hinausgehen.

Neben den Grundsätzen der Geeignetheit und der Erforderlichkeit muss eine Massnahme zumutbar sein, d. h. sie muss ein vernünftiges Verhältnis zwischen angestrebtem Ziel oder Zweck und Freiheitseingriff wahren.

Um die Verhältnismässigkeit überprüfen zu können, hatte der DSB schon im Vorfeld diverse Fragen an die Gemeinde Vaduz gerichtet. So ersuchte er um Auskunft, ob weniger weit gehende Massnahmen überprüft worden seien, ob der angestrebte Zweck nicht durch den gezielten, punktuellen Einsatz von Kameras auf bestimmte „Hot Spots" erreicht werden könne, zu wie vielen Schadensfällen es vor und nach Installierung der Videoüberwachung in der Fussgängerzone gekommen sei und in wie vielen Fällen die Videoaufzeichnung zur Aufklärung eines Sachverhalts gedient und zur Identifizierung des Täters beigetragen habe, usw. Diese Fragen konnten jedoch auch im Verfahren vor der DSK von der Gemeinde nur unzureichend beantwortet werden.

Die Datenschutzkommission bestätigt in ihrer Entscheidung daher die Empfehlung des Datenschutzbeauftragten, wonach die flächendeckende und durchgehende Überwachung entsprechend räumlich und/oder zeitlich auf das notwendige Mass zu reduzieren ist. Die spezielle Frage ist also, ob eine 24 Stunden Überwachung an 7 Tagen in der Woche wirklich notwendig ist oder ob die Überwachung nicht auf bestimmte Tage sowie bestimmte Zeiten reduziert werden kann. Ausserdem ist zu überprüfen, ob nicht die gezielte punktuelle Überwachung bestimmter, im öffentlichen Interesse stehender Objekte ausreicht.

## C. Wichtige spezifische Themen

Neben den intensiven Vorbereitungen zum Beitritt Liechtensteins zu den Abkommen von Schengen und Dublin lag ein weiterer Schwerpunkt der Arbeit der SDS im Telekommunikations- und Arbeitsbereich. Bei letzterem ging es oftmals um eine Überwachung des Arbeitsnehmers am Arbeitsplatz und um den Umgang mit E-Mail und Internet am Arbeitsplatz. Erstmals seit dem Inkrafttreten des indirekten Auskunftsrecht nach Artikel 34h Polizeigesetz[43] hatte der DSB auf Anträge hin konkret zu überprüfen, ob Personendaten der Antragsteller im Zusammenhang mit dem Staatsschutz oder mit Ermittlungen zur vorbeugenden Bekämpfung von Straftaten von der Landespolizei bearbeitet werden und wenn ja, ob die Bearbeitung rechtmässig ist.

Im Berichtsjahr konnte ein grosses Informationsbedürfnis hinsichtlich der Zulässigkeit von Datenbekanntgaben in den unterschiedlichsten Zusammenhängen vermerkt werden. Als Beispiele können an dieser Stelle genannt werden: Veröffentlichung von Rufnamen Verstorbener (Stichwort postmortaler Persönlichkeitsschutz); Zulässigkeit einer Datenbekanntgabe ins Ausland; Veröffentlichung von Noten im Internet; Datenbekanntgabe nach einer Entbindung vom Versicherungsgeheimnis; Bekanntgabe von Adressen von Bürgern durch Gemeinden.

Zur Information der Öffentlichkeit wird vor allem die Internetseite der SDS genutzt, auf der laufend über aktuelle und/oder wichtige Themen informiert wird. Die Wichtigkeit der Internetseite als Informationsmedium zeigt sich an der stetig ansteigenden Zahl der Besucher: Die Anzahl von Zugriffen auf die Internetseite während des Berichtsjahres betrug 234 646 (8 355 unterschiedliche Besucher). Damit hat sich die Anzahl der Zugriffe im Vergleich zum Vorjahr mehr als vervierfacht.[44]

Die wichtigsten Themen für das Berichtsjahr waren: Meldepflicht von Datentransfers ins Ausland, Schutz der Daten von Kindern, Entschliessungen der 30. Internationalen Datenschutzkonferenz, soziale Netzwerke sowie die Pressemitteilungen zum 2. Europäischen Datenschutztag. Über die Internetseite sind neben aktuellen Themen auch Anleitungen für die

[43] Artikel 34h Absatz 1 Polizeigesetz besagt: „Jede Person kann bei der Datenschutzstelle verlangen, dass diese prüfe, ob bei der Landespolizei rechtmässig Daten im Rahmen des Staatsschutzes (Artikel 2 Absatz 2) oder zur vorbeugenden Bekämpfung von Straftaten (Artikel 2 Absatz 1 Buchstabe d) über sie bearbeitet werden. Die Datenschutzstelle teilt der Gesuch stellenden Person in einer stets gleich lautenden Antwort mit, dass in Bezug auf sie entweder keine Daten unrechtmässig bearbeitet werden oder dass sie bei Vorhandensein allfälliger Fehler in der Datenbearbeitung eine Empfehlung zu deren Behebung verfügt habe." Die Bestimmung ist 2007 in Kraft getreten, vgl. Jahresbericht 2007.

[44] Im Jahr 2007 betrug die Anzahl der Zugriffe noch 54 679 bei 7 158 unterschiedlichen Besuchern.

Auslegung und Anwendbarkeit des Datenschutzgesetzes abzurufen, die so genannten Richtlinien. Im Jahr 2008 wurden die *Richtlinien über die Rechte der betroffenen Personen* grundlegend überarbeitet und aktualisiert sowie die *Richtlinien über den Umgang mit unerwünschter Werbung, insbesondere Spam* herausgegeben. Ausserdem wurden die *Richtlinien zur Bearbeitung von Personendaten im privaten Bereich* erarbeitet. Anlässlich des 2. Europäischen Datenschutztages hat der DSB die letztgenannten Richtlinien als Broschüre herausgegeben und diese einem Grossteil der international tätigen Unternehmen, Versicherungen und Inkassounternehmen in Liechtenstein überreicht. Gleichzeitig wurde ein Fragebogen übermittelt, um einerseits zu eruieren, wie die Unternehmen mit dem Thema Datenschutz umgehen, und um andererseits die Zusammenarbeit zu intensivieren.

## Norwegen

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

Im Mai 2008 verabschiedete das norwegische Parlament (*Storting*) Änderungen am Gesetz über Ablagesysteme für Patientendaten zur Verhinderung von Zugriffen auf Patientenakten. Gemäß Abschnitt 13a des Gesetzes über Ablagesysteme für Patientendaten „ist es nach diesem Gesetz verboten, gesundheitsbezogene Daten zu lesen, zu suchen, anderweitig zu verwenden oder zu besitzen, sofern die Gesundheitsversorgung des Patienten oder die Verwaltung dieser Versorgung dies nicht erfordert bzw. sofern dies nicht nach anderen Gesetzen oder Verordnungen ausdrücklich gestattet ist". Verstöße gegen diese Bestimmungen führen zu Geldstrafen oder Gefängnisstrafen von bis zu drei Monaten. Die Vorschriften sind in Kraft und werden von der Datenschutzbehörde umgesetzt.

Im Dezember 2008 verabschiedete das Parlament zahlreiche Änderungen des Datenschutzgesetzes. In Abschnitt 3 des Gesetzes wurde eine neue Bestimmung zur Befugnis der Anordnung von Bestimmungen integriert. Diese Änderung war erforderlich, um die rechtliche Befugnis für geplante Regulierungen betreffend den Zugriff auf E-Mails von Angestellten bereitzustellen.

Gleichzeitig wurde die Datenschutzbehörde durch eine Änderung von Abschnitt 46 des Gesetzes befugt, Geldstrafen für die Nichteinhaltung von Bestimmungen des Datenschutzgesetzes zu verhängen. Die Datenschutzbehörde war bereits befugt, Geldbußen für Verstöße gegen das Gesetz zu verhängen. Eine Geldstrafe für die Nichteinhaltung würde dann verhängt werden, wenn der Verstoß in der Vergangenheit erfolgt wäre.

Außerdem wurde der neue Abschnitt 47a verabschiedet. Dieser Abschnitt ermöglicht es der Datenschutzbehörde, das nationale Inkassobüro mit der Eintreibung dieser Geldstrafen für die Nichteinhaltung sowie sonstiger von der Behörde verhängter Geldbußen zu beauftragen. Die Datenschutzbehörde hat ihre Befugnis zur Verhängung von Geldbußen bisher nicht genutzt, da die für die Eintreibung dieser Geldbußen erforderlichen Ressourcen nicht zur Verfügung standen.

Die rechtlichen Änderungen traten am 1. Januar 2009 in Kraft.

Im Juni 2008 verabschiedete das Parlament Änderungen des Gesetzes über das Schengener Informationssystem (SIS-Gesetz). Grund hierfür war die Verabschiedung zweier Verordnungen durch den Rat der EU im Dezember 2006 sowie eine Entscheidung vom Juni 2007, die gemeinsam die rechtliche Befugnis für die zweite Generation des Schengener Informationssystem (SIS II) umfassen. Diese Rechtsakte wurden durch entsprechende Änderungen des SIS-Gesetzes in norwegisches Recht umgesetzt. Außerdem wurden einige Änderungen aufgrund von Beobachtungen verabschiedet, die im Rahmen der Nachbereitung der EU-Schengen-Bewertung von Norwegen in den Jahren 2005 und 2006 gemacht wurden. Schließlich waren auch weitere Änderungen erforderlich, da Norwegen beschlossen hat, nach Start des zentralen SIS II direkte Suchen durchzuführen. Als Folge dieser Änderung ist die Datenschutzbehörde verpflichtet, auf Anfrage eines Datensubjektes zu überprüfen, ob dessen Daten im SIS korrekt sind, ob die Vorschriften für den Zugriff auf die Daten eingehalten wurden und ob die Informationen gemäß dem SIS-Gesetz registriert und verwendet wurden. Wurden die Informationen von einer anderen Vertragspartei des Übereinkommens eingegeben, so muss diese Überprüfung in Zusammenarbeit mit der Aufsichtsbehörde der betreffenden Partei erfolgen. Diese Änderungen sind noch nicht in Kraft getreten.

Die Inkraftsetzung des neuen Gesetzes über die Informationsfreiheit mit seinen zugehörigen Verordnungen (im Juni 2007 verabschiedet), die am 1. Juli 2008 erfolgen sollte, wurde auf den 1. Januar 2009 verschoben. Das neue Gesetz wurde im Jahresbericht 2007 erwähnt. Aus den neuen Bestimmungen ergibt sich, dass öffentliche Behörden, die E-Mail-Aufzeichnungen führen, diese unmittelbar nach Abschluss des betreffenden öffentlichen Informationssystems im Internet veröffentlichen müssen. Namen von Personen können in diesem System nur 12 Monate lang gesucht werden. Zusätzlich erlaubt das Gesetz auch die Veröffentlichung von Dokumenten zu öffentlichen Fällen im Internet. Aus den Verordnungen

ergibt sich jedoch, dass bestimmte Daten niemals im Internet veröffentlicht werden dürfen. Dies gilt für vertrauliche Informationen, sensible personenbezogene Daten, nationale Identifikationsnummern, persönliche Identifikationsnummern und Nummern mit ähnlichen Funktionen sowie für Informationen zum Gehalt oder sonstigen Vergütungen natürlicher Personen, mit Ausnahme von Informationen zu Gehältern und Vergütungen von leitenden Angestellten im öffentlichen Bereich sowie von leitenden Angestellten oder Vorstandsmitgliedern unabhängiger juristischer Personen.

Das Parlament hat ein neues Gesundheitsforschungsgesetz verabschiedet. Dieses Gesetz wurde im Jahresbericht 2007 erwähnt. Weitere Einzelheiten sind diesem Bericht zu entnehmen. Für die Inkraftsetzung wurde noch kein Termin festgelegt.

## B. Bedeutende Rechtsprechung

Keine nennenswerte.

## C. Wichtige spezifische Themen

**Unklare Verteilung von Verantwortung und unzureichende interne Kontrolle**
Gemäß dem Datenschutzgesetz liegt die Verantwortung für die Verarbeitung personenbezogener Daten bei einem Datenkontrolleur. Im Jahr 2008 durchgeführte Aufsichtsmaßnahmen deckten jedoch bezüglich einer Reihe von Datenbanken und Registern mit personenbezogenen Daten eine unklare Verteilung dieser Verantwortung auf. Die Überprüfungen zeigten außerdem, dass die internen Kontrollroutinen oftmals unzureichend waren und dass Datenverarbeiter eingesetzt wurden, die keine angemessene Vereinbarung unterschrieben hatten.

**Zunehmender Datenaustausch zwischen Datenbanken schwächt den Datenschutz**
Bei einer zunehmenden Anzahl von Behörden ist der Trend zu erkennen, personenbezogene Daten mit anderen Regierungsdiensten und -behörden auszutauschen oder Zugriff auf diese Daten zu haben. Ziel ist oftmals die Steigerung der prozeduralen Effizienz. Im Jahr 2008 wurde dies besonders in den Bereichen Justiz und Gesundheit sowie im Hinblick auf das vorgeschlagene neue Gesetz für ein Bevölkerungsregister deutlich.

Im Bereich Justiz werden methodisch Systeme entwickelt, um einen größeren Datenaustausch zwischen Datenbanken zu ermöglichen. Nach Ansicht der Datenschutzbehörde erfordert diese Entwicklung strenge Anforderungen zur rechtlichen Regelung von Polizeiregistern. Der Datenschutzbehörde ist bewusst, dass das Justizministerium im Jahr 2008 an Gesetzesentwürfen gearbeitet hat. Die Behörde hat spezifische Vorschläge für ihrer Meinung nach erforderliche Änderungen des neuen Gesetzes über das Polizeiregister ausgesprochen, so beispielsweise die Verbesserung der Grundgarantien wie z. B. angemessene Löschung/Sortierung von Daten, Zugangskontrolle und Geheimhaltungspflicht.

**Zunehmende Verwendung von Überwachungskamera-Attrappen**
Die Datenschutzbehörde wird immer öfter von Menschen kontaktiert, die der Meinung sind, dass ihre Privatsphäre durch Überwachungskameras verletzt wird. Diese Kameras erweisen sich bei genauer Untersuchung jedoch als Attrappen. Die Verwendung solcher Attrappen bringt grundsätzliche Probleme mit sich. In vielen Fällen werden die Kameraattrappen so positioniert, dass sie eine unrechtmäßige Überwachung dargestellt hätten, wenn sie echt gewesen wären.

Auch wenn keine tatsächliche Überwachung erfolgt, so ist das Gefühl, überwacht zu werden, dennoch real. Im schlimmsten Fall können Plastikkameras erheblich beeinträchtigen, wie eine Person ihren Alltag wahrnimmt. Da jedoch tatsächlich keine personenbezogenen Daten verarbeitet werden, fällt die Verwendung solcher Kameraattrappen nicht in den Geltungsbereich des Datenschutzgesetzes.

# Kapitel 5
# Mitglieder und Beobachter der Artikel 29 Datenschutzgruppe

# MITGLIEDER DER ARTIKEL 29 DATENSCHUTZGRUPPE IM JAHR 2008

| **Österreich** | **Belgien** |
|---|---|
| Frau Waltraut Kotschy<br>Österreichische Datenschutzkommission<br>Ballhausplatz 1 - AT - 1014 Wien<br>Tel: +43 1 531 15 / 2525<br>Fax: +43 1 531 15 / 2690<br>E-Mail: dsk@dsk.gv.at<br>Website: http://www.dsk.gv.at/ | Herr Willem Debeuckelaere<br>Kommission für den Schutz des Privatlebens<br>(Commission de la protection de la vie privée/<br>Commissie voor de bescherming van de persoonlijke levenssfeer)<br>Rue Haute, 139 - BE - 1000 Bruxelles<br>Tel: +32(0)2/213.85.40<br>Fax : +32(0)2/213.85.65<br>E-Mail: commission@privacycommission.be<br>Website: http://www.privacycommission.be/ |
| **Bulgarien** | **Zypern** |
| Herr Krassimir Dimitrov<br>Kommission zum Schutz personenbezogener Daten<br>(Комисия за защита на личните данни)<br>1 Dondukov - BG - 1000 Sofia<br>Tel: +359 2 915 3501<br>Fax: +359 2 915 3525<br>E-Mail: kzld@government.bg<br>kzld@cpdp.bg<br>Website: http://www.cdpd.bg | Frau Goulla Frangou<br>Beauftragte für den Schutz personenbezogener Daten (Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>1, Iasonos str.<br>Athanasia Court, 2nd floor - CY - 1082 Nicosia<br>(P.O. Box 23378 - CY - 1682 Nicosia)<br>Tel: +357 22 818 456<br>Fax: +357 22 304 565<br>E-Mail: commissioner@dataprotection.gov.cy<br>Website: http://www.dataprotection.gov.cy |
| **Tschechische Republik** | **Dänemark** |
| Herr Igor Nemec<br>Amt für den Schutz personenbezogener Daten<br>(Úřad pro ochranu osobních údajů)<br>Pplk. Sochora 27 - CZ - 170 00 Praha 7<br>Tel: +420 234 665 111<br>Fax: +420 234 665 501<br>E-Mail: posta@uoou.cz<br>Website: http://www.uoou.cz/ | Frau Janni Christoffersen<br>Dänische Datenschutzbehörde (Datatilsynet)<br>Borgergade 28, 5th floor - DK - 1300 Koebenhavn K<br>Tel: +45 3319 3200<br>Fax: +45 3319 3218<br>E-Mail: dt@datatilsynet.dk<br>Website: http://www.datatilsynet.dk |

| **Estland** | **Finnland** |
|---|---|
| Herr Urmas Kukk<br>Herr Viljar Peep<br>Estnische Datenschutzbehörde<br>(Andmekaitse Inspektsioon)<br>Väike - Ameerika 19 - EE - 10129 Tallinn<br>Tel: +372 6274 135<br>Fax: +372 6274 137<br>E-Mail: info@dp.gov.ee<br>Website: http://www.dp.gov.ee | Herr Reijo Aarnio<br>Büro des Datenschutzombudsmannes<br>(Tietosuojavaltuutetun toimisto)<br>Albertinkatu 25 A, 3rd floor - FI - 00181 Helsinki<br>(P.O. Box 315)<br>Tel: +358 10 36 166700<br>Fax: +358 10 36 166735<br>E-Mail: tietosuoja@om.fi<br>Website: http://www.tietosuoja.fi |
| **Frankreich** | **Deutschland** |
| Herr Alex Türk<br>Vorsitzender der Nationalen Kommission der Informatik und der Freiheiten<br>(Commission Nationale de l'Informatique et des Libertés - CNIL)<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tel: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br><br>Herr Georges de La Loyère<br>Nationale Kommission der Informatik und der Freiheiten<br>(Commission Nationale de l'Informatique et des Libertés - CNIL)<br>Rue Vivienne, 8 -CS 30223 FR - 75083 Paris Cedex 02<br>Tel: +33 1 53 73 22 22<br>Fax: +33 1 53 73 22 00<br>E-Mail: laloyere@cnil.fr<br>Website: http://www.cnil.fr | Herr Peter Schaar<br>Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit<br>Husarenstraße 30 - DE -53117 Bonn<br>Tel: +49 (0)1888 7799-0<br>Fax: +49 (0)1888 7799-550<br>E-Mail: poststelle@bfdi.bund.de<br>Website: http://www.bfdi.bund.de<br><br>Herr Alexander Dix<br>(Vertreter der Bundesländer)<br>Berliner Beauftragter für Datenschutz und Informationsfreiheit<br>An der Urania 4-10 – DE – 10787 Berlin<br>Tel: +49 30 13 889 0<br>Fax: +49 30 215 50 50<br>E-Mail: mailbox@datenschutz-berlin.de<br>Website: http://www.datenschutz-berlin.de |

| **Griechenland** | **Ungarn** |
|---|---|
| Herr Christos Yeraris<br>Griechische Datenschutzbehörde<br>(Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)<br>Kifisias Strasse 1-3<br>GR - 115 23 Athen Tel: +30 210 6475608<br>Fax: +30 210 6475789<br>E-Mail: christosyeraris@dpa.gr<br>Website: http://www.dpa.gr | Herr András Jóri<br>Datenschutzbeauftragter<br>(Adatvédelmi Biztos)<br>Nador u. 22 - HU - 1051 Budapest<br>Tel: +36 1 475 7186<br>Fax: +36 1 269 3541<br>E-Mail: adatved@obh.hu<br>Website: http://abiweb.obh.hu/abi/ |
| **Irland** | **Italien** |
| Herr Billy Hawkes<br>Datenschutzbeauftragter<br>(An Coimisinéir Cosanta Sonraí)<br>Canal House, Station Rd, Portarlington, IE -Co.Laois<br>Tel: +353 57 868 4800<br>Fax:+353 57 868 4757<br>E-Mail: info@dataprotection.ie<br>Website: http://www.dataprotection.ie | Herr Francesco Pizzetti<br>Italienische Datenschutzbehörde<br>(Garante per la protezione dei dati personali)<br>Piazza di Monte Citorio, 121 - IT - 00186 Roma<br>Tel: +39 06.69677.1<br>Fax: +39 06.69677.785<br>E-Mail: garante@garanteprivacy.it,<br>f.pizzetti@garanteprivacy.it<br>Website: http://www.garanteprivacy.it |
| **Lettland** | **Litauen** |
| Frau Signe Plumina<br>Lettische Datenaufsichtsbehörde (Datu valsts inspekcija)<br>Blaumana str. 11/13 – 15, Riga, LV-1011, Latvia<br>Tel: +371 6722 31 31<br>Fax: +371 6722 35 56<br>E-Mail: signe.plumina@dvi.gov.lv,<br>info@dvi.gov.lv<br>Website: http://www.dvi.gov.lv | Herr Algirdas Kunčinas<br>Staatliche Datenschutzbehörde (Valstybinė duomenų apsaugos inspekcija)<br>A.Juozapaviciaus str. 6 / Slucko str. 2,<br>LT-01102 Vilnius<br>Tel: +370 5 279 14 45<br>Fax: + 370 5 261 94 94<br>E-Mail: ada@ada.lt<br>Website: http://www.ada.lt |

| **Luxemburg** | **Malta** |
|---|---|
| Herr Gérard Lommel<br>Nationale Kommission für den Datenschutz<br>(Commission nationale pour la Protection des Données - CNPD)<br>41, avenue de la Gare - L - 1611 Luxembourg<br>Tel: +352 26 10 60 -1<br>Fax: +352 26 10 60 – 29<br>E-Mail: info@cnpd.lu<br>Website: http://www.cnpd.lu | Herr Joseph Ebejer<br>Datenschutzbeauftragter<br>Datenschutzbehörde<br>(Office of the Data Protection Commissioner)<br>2, Airways House<br>High Street<br>Sliema SLM 1549<br>MALTA<br>Tel: +356 2328 7100<br>Fax: +356 23287198<br>E-Mail: joseph.ebejer@gov.mtWebsite: http://www.dataprotection.gov.mt |
| **Niederlande** | **Polen** |
| Herr Jacob Kohnstamm<br>Niederländische Datenschutzbehörde<br>(College Bescherming Persoonsgegevens - CBP)<br>Juliana van Stolberglaan 4-10, P.O Box 93374<br>2509 AJ Den Haag<br>Tel: +31 70 8888500<br>Fax: +31 70 8888501<br>E-Mail: info@cbpweb.nl<br>Website: http:// www.cbpweb.nl<br>http://www.mijnprivacy.nl | Herr Michał Serzycki<br>Generalinspektor für den Schutz personenbezogener Daten (Generalny Inspektor Ochrony Danych Osobowych)<br>ul. Stawki 2 - PL - 00193 Warsaw<br>Tel: +48 22 860 70 86<br>Fax: +48 22 860 70 90<br>E-Mail: Sekretariat@giodo.gov.pl<br>Website: http://www.giodo.gov.pl |
| **Portugal** | **Rumänien** |
| Herr Luís Novais Lingnau da Silveira<br>Datenschutzbehörde (Comissão Nacional de Protecção de Dados - CNPD)<br>Rua de São Bento, 148, 3º<br>PT - 1 200-821 Lisboa<br>Tel: +351 21 392 84 00<br>Fax: +351 21 397 68 32<br>E-Mail: geral@cnpd.pt<br>Website: http://www.cnpd.pt | Frau Georgeta Basarabescu<br>Nationale Aufsichtsbehörde für die Verarbeitung personenbezogener Daten (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal)<br>Olari Street no. 32, Sector 2, RO - Bucharest<br>Tel: +40 21 252 5599<br>Fax: +40 21 252 5757<br>E-Mail: georgeta.basarabescu@dataprotection.ro<br>international@dataprotection.ro<br>Website: www.dataprotection.ro |

| **Slowakei** | **Slowenien** |
|---|---|
| Herr Gyula Veszelei<br>Behörde zum Schutz personenbezogener Daten der Slowakischen Republik (Úrad na ochranu osobných údajov Slovenskej republiky)<br>Odborárske námestie 3 - SK - 81760 Bratislava 15<br>Tel: +421 2 5023 9418<br>Fax: +421 2 5023 9441<br>E-Mail: statny.dozor@pdp.gov.sk<br>Website: http://www.dataprotection.gov.sk | Frau Natasa Pirc Musar<br>Datenschutzbeauftragte (Informacijski pooblaščenec)<br>Vosnjakova 1, SI - 1000 Ljubljana<br>Tel: +386 1 230 97 30<br>Fax: +386 1 230 97 78<br>E-Mail: gp.ip@ip-rs.si<br>Website: http://www.ip-rs.si |
| **Spanien** | **Schweden** |
| Herr Artemi Rallo Lombarte<br>Spanische Datenschutzbehörde<br>(Agencia Española de Protección de Datos)<br>C/ Jorge Juan, 6<br>ES - 28001 Madrid<br>Tel: +34 91 399 6219/20<br>Fax: + +34 91 445 56 99<br>E-Mail: director@agpd.es<br>Website: http://www.agpd.es | Herr Göran Gräslund<br>Datenschutzbehörde (Datainspektionen)<br>Fleminggatan, 14<br>(Box 8114) - SE - 104 20 Stockholm<br>Tel: +46 8 657 61 57<br>Fax: +46 8 652 86 52<br>E-Mail: datainspektionen@datainspektionen.se,<br>goran.graslund@datainspektionen.se<br>Website: http://www.datainspektionen.se |
| **Vereinigtes Königreich** | **European Data Protection Supervisor** |
| Herr Richard Thomas<br>Datenschutzbehörde<br>(Information Commissioner's Office)<br>Wycliffe House<br>Water Lane, Wilmslow SK9 5AF GB<br>Tel: +44 1625 545700Fax: +44 1625 524510<br>E-Mail: Fuellen Sie bitte das Online-Kontaktformular auf unserer Website aus<br>Website: http://www.ico.gov.uk | Herr Peter Hustinx<br>Europäischer Datenschutzbeauftragter (EDPS)<br>(European Data Protection Supervisor – EDPS)<br>Postal address: 60, rue Wiertz, BE - 1047 Brussels<br>Office: rue Montoyer, 63, BE - 1047 Brussels<br>Tel: +32 2 283 1900<br>Fax: +32 2 283 1950<br>E-Mail: edps@edps.europa.eu<br>Website: http://www.edps.europa.eu |

## BEOBACHTER DER ARTIKEL 29 DATENSCHUTZGRUPPE IM JAHR 2008

| **Island** | **Norwegen** |
|---|---|
| Frau Sigrun Johannesdottir<br>Datenschutzbehörde<br>(Persónuvernd)<br>Raudararstigur 10 - IS - 105 Reykjavik<br>Tel: +354 510 9600<br>Fax: +354 510 9606<br>E-Mail: postur@personuvernd.is<br>Website: http://www.personuvernd.is | Herr Georg Apenes<br>Datenschutzbehörde (Datatilsynet)<br>P.O.Box 8177 Dep - NO - 0034 Oslo<br>Tel: +47 22 396900<br>Fax: +47 22 422350<br>E-Mail: postkasse@datatilsynet.no<br>Website: http://www.datatilsynet.no |
| **Liechtenstein** | **Republik Kroatien** |
| Herr Philipp Mittelberger<br>Datenschutzbeauftragter<br>Datenschutzstelle (DSS)<br>Kirchstrasse 8, Postfach 684 –FL -9490 Vaduz<br>Tel: +423 236 6090<br>Fax: +423 236 6099<br>E-Mail: info@dss.llv.li<br>Website: http://www.dss.llv.li | Herr Franjo LACKO<br>Direktor<br>Kroatische Datenschutzaufsichtsbehörde<br>(Agencija za zaštitu osobnih podataka - AZOP)<br>Republike Austrije 25, 10000 Zagreb<br>Tel. +385 1 4609 000<br>Fax +385 1 4609 099<br>E-Mail: azop@azop.hr or info@azop.hr<br>website: http://www.azop.hr/default.asp |
| **die ehemalige jugoslawische Republik Mazedonien** | |
| Frau Marijana Marusic<br>Datenschutzdirektion<br>(ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ)<br>Samoilova 10, 1000 Skopje, RM<br>Tel: +389 2 3244 760<br>Fax: +389 2 3244 766<br>Website: www.dzlp.mk, info@dzlp.gov.mk | |

**Sekretariat der Artikel 29 Datenschutzgruppe**

Frau Niovi Ringou
Geschäftsführende Referatsleiterin
Referat Datenschutz
Generaldirektion Justiz, Freiheit und Sicherheit
Europäische Kommission
Büro: LX46 1/02 - BE - 1049 Brussels
Tel: +32 2 295 12 87
Fax: +32 2 299 8094
E-Mail: Niovi.Ringou@ec.europa.eu
Website: http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm

NE-AC-10-002-DE-C
10.2758/21561

EUROPÄISCHE
KOMMISSION

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

- zu Fragen des Datenschutzes in der Gemeinschaft gegenüber der Kommission in Form von Sachverständigenbeiträgen der Mitgliedstaaten Stellung zu nehmen;
- die einheitliche Anwendung der allgemeinen Grundsätze der Richtlinie in allen Mitgliedstaaten durch die Zusammenarbeit der Aufsichtsbehörden für den Datenschutz zu fördern;
- die Kommission hinsichtlich aller Gemeinschaftsmaßnahmen zu beraten, die sich auf die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten auswirken;
- gegenüber der Allgemeinheit und insbesondere gegenüber den Organen den Gemeinschaft Empfehlungen zu Angelegenheiten auszusprechen, die den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Gemeinschaft betreffen.

ISBN 978-92-79-13760-0