Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

# Tätigkeitsbericht 2005 - 2006

# 21. Tätigkeitsbericht

# Tätigkeitsbericht 2005-2006

21. Tätigkeitsbericht

Dieser Bericht wurde am 24. April 2007 dem Präsidenten des Deutschen Bundestages, Herrn Dr. Norbert Lammert, überreicht.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Peter Schaar

# Tätigkeitsbericht 2005 und 2006 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
# – 21. Tätigkeitsbericht –

Inhaltsverzeichnis


| | | Seite |
|---|---|---|
| **1** | **Einführung** | 15 |
| **2** | **Datenschutzrechtlicher Rahmen** | 16 |
| 2.1 | Weiterentwicklung des Datenschutzrechts | 16 |
| 2.2 | Struktur der Datenschutzaufsicht auf dem Prüfstand | 17 |
| 2.3 | Das Mittelstandsentlastungsgesetz zeigt für den Datenschutz nicht den richtigen Weg auf. | 18 |
| 2.4 | Datenschutzaudit-Regelung dringend geboten | 19 |
| 2.5 | „Outsourcing“ in der Verwaltung – auch ein Problem des Datenschutzes | 20 |
| 2.6 | Zusammenarbeit mit den behördlichen Datenschutzbeauftragten | 20 |
| 2.7 | Arbeitnehmerdatenschutzgesetz | 21 |
| 2.8 | Informationsfreiheitsgesetz in Kraft | 21 |
| **3** | **Europa und Internationales** | 21 |
| 3.1 | Europäische Rechtsentwicklung | 22 |
| 3.2 | Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Europa | 22 |
| 3.2.1 | Schaffung eines Raums von Freiheit, Sicherheit und Recht | 22 |
| 3.2.2 | Vertrag von Prüm | 24 |

| | | Seite |
|---|---|---|
| 3.2.3 | Europol | 25 |
| 3.2.3.1 | Die Rechtsakte zur Änderung des Europol-Übereinkommens | 26 |
| 3.2.3.2 | Die Gemeinsame Kontrollinstanz von Europol | 27 |
| 3.2.4 | Schengen | 27 |
| 3.2.4.1 | SIS II | 28 |
| 3.2.4.2 | Kontrolle der Ausschreibungen nach Artikel 99 Abs. 2 des Schengener Durchführungsübereinkommens | 29 |
| 3.2.5 | Zollinformationssystem | 30 |
| 3.2.6 | Aufbau einer integrierten Datenbank über vermisste Personen bei Interpol | 30 |
| 3.2.7 | Zugriff der Sicherheitsbehörden auf das europäische VISA-Informationssystem (VIS) | 30 |
| 3.2.8 | Eurodac – Datenschutzkontrolle | 31 |
| 3.3 | Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie | 31 |
| 3.3.1 | Whistleblowing – Richtiger Umgang mit Insidertipps | 32 |
| 3.3.2 | Übermittlung von Flugpassagierdaten in die USA | 33 |
| 3.3.3 | Umsetzung der Richtlinie 2004/82/EG zur Übermittlung von Flugpassagierdaten | 34 |
| 3.3.4 | Europaweite Datenschutzprüfung im Krankenversicherungssektor | 34 |
| 3.3.5 | Safe Harbor | 34 |
| 3.3.6 | Binding Corporate Rules | 35 |
| 3.4 | Europäische und internationale Zusammenarbeit in Strafsachen | 35 |
| 3.5 | Internationale Datenschutzkonferenzen | 36 |
| **4** | **Technologischer Datenschutz** | 37 |
| 4.1 | Elektronische Gesundheitskarte: Das Warten geht weiter | 37 |
| 4.2 | Videoüberwachung | 39 |
| 4.2.1 | Auch Videoüberwachung braucht Sicherheit! | 40 |
| 4.2.2 | Videoüberwachung auf Bahnhöfen | 40 |
| 4.2.3 | Auch bei Videoanlagen kann die Politik ins Blickfeld geraten! | 40 |
| 4.3 | RFID (Radio Frequency Identification) | 41 |
| 4.4 | Identitätsmanagement und elektronische Signaturverfahren | 43 |
| 4.4.1 | ELSTER-Portal und StDÜV | 44 |
| 4.4.2 | Verschlüsselung nach wie vor ein wichtiges Thema! | 44 |
| 4.4.3 | Nutzung der EC-Karte zur Altersbestimmung am Zigarettenautomaten | 45 |
| 4.5 | Biometrie und Datenschutz | 45 |
| 4.5.1 | Technik | 46 |
| 4.5.2 | Automatisierte Grenzkontrolle | 46 |
| 4.5.3 | Der ePass und der neue Personalausweis | 47 |

| | | Seite |
|---|---|---|
| 4.5.4 | Symposium „Biometrie und Datenschutz – Der vermessene Mensch“ | 48 |
| 4.6 | Das JobCard-Verfahren (ELENA-Verfahren) | 48 |
| 4.7 | eGovernment – bitte nur mit Datenschutz! | 50 |
| 4.8 | Effektive Datenlöschung | 51 |
| 4.9 | IVBB – Zielpunkt für neue Angriffe | 53 |
| 4.10 | Viren, Trojaner, Phishing, Spyware, Spam und SPIT | 53 |
| 4.11 | Trusted Computing | 54 |
| 4.12 | Nano-Technologie | 55 |
| 4.13 | Zehn Thesen für eine datenschutzfreundliche Informationstechnik | 56 |
| **5** | **Innere Sicherheit** | 59 |
| 5.1 | Neue Sicherheitsarchitektur | 59 |
| 5.1.1 | Gemeinsame-Dateien-Gesetz | 60 |
| 5.1.2 | Terrorismusbekämpfungsergänzungsgesetz 2006 | 63 |
| 5.1.3 | Ermittlungstätigkeit der Sicherheitsbehörden im Internet | 64 |
| 5.1.4 | Kontrolle des Gemeinsamen Terrorismusabwehrzentrums in Berlin | 65 |
| 5.1.5 | Kooperation der Sicherheitsbehörden mit ausländischen Partnern | 66 |
| 5.2 | Bundeskriminalamt | 67 |
| 5.2.1 | Präventive Aufgaben und Befugnisse für das BKA | 67 |
| 5.2.2 | INPOL | 67 |
| 5.2.3 | Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung 2001 – gesetzgeberische Konsequenzen? | 68 |
| 5.2.4 | Verwendung erkennungsdienstlicher Daten | 69 |
| 5.2.4.1 | Verarbeitung von erkennungsdienstlichen Unterlagen der Polizeien des Bundes und der Länder beim BKA | 69 |
| 5.2.4.2 | Pilotprojekt Fast Identification | 70 |
| 5.2.5 | Fußball-Weltmeisterschaft 2006 | 71 |
| 5.2.6 | Forschungsprojekt Fotofahndung | 72 |
| 5.2.7 | Geldwäsche | 72 |
| 5.3 | Bundespolizei | 73 |
| 5.3.1 | Neues Vorgangsbearbeitungssystem (@rtus) bei der Bundespolizei | 73 |
| 5.3.2 | Datei „Gewalttäter Sport“ | 73 |
| 5.4 | Zollfahndung | 74 |
| 5.4.1 | Zollfahndungsdienstgesetz – Auswirkungen der Entscheidung des Bundesverfassungsgerichts zur präventiven Telekommunikationsüberwachung | 74 |
| 5.4.2 | INZOLL – neu | 75 |

| | | Seite |
|---|---|---|
| 5.5 | Verfassungsschutz | 76 |
| 5.5.1 | Evaluierung des Terrorismusbekämpfungsgesetzes 2002 | 76 |
| 5.5.2 | Einsatz nachrichtendienstlicher Mittel durch den Verfassungsschutz – mobile Beobachtungstruppe | 73 |
| 5.6 | MAD | 77 |
| 5.6.1 | Ausbau der Informationsverarbeitung beim MAD | 77 |
| 5.6.2 | Zusammenarbeit des MAD mit der Polizei | 77 |
| 5.7 | BND | 78 |
| 5.7.1 | Erneute Änderung des Artikel 10-Gesetzes – G 10 | 78 |
| 5.7.2 | Beobachtung von Journalisten durch den BND | 78 |
| 5.7.3 | Umbau der IT-Struktur beim BND | 79 |
| 5.7.4 | Bericht der Bundesregierung zu Auslandsaktivitäten des BND im Irak | 79 |
| 5.7.5 | Altdatenbereinigungskonzept | 80 |
| 5.7.6 | Kontrolle einer Anti-Terrorismusdatei | 80 |
| 5.7.7 | Auskunftspflicht des Bundesnachrichtendienstes (BND) | 81 |
| 5.8 | Sicherheitsüberprüfungen | 82 |
| 5.8.1 | Luftsicherheitsgesetz und Verordnung datenschutzrechtlich unzureichend | 82 |
| 5.8.2 | Personeller Sabotageschutz – Uferlos? | 82 |
| 5.8.3 | Kontrolle der Sicherheitsüberprüfungen | 83 |
| 5.8.3.1 | Bundespolizei | 83 |
| 5.8.3.2 | Nicht-öffentlicher Bereich | 84 |
| 5.8.4 | Sicherheitsüberprüfung bei diplomatischen Vertretungen der USA | 85 |
| **6** | **Rechtswesen** | 85 |
| 6.1 | Telekommunikationsüberwachung nach §§ 100a ff. StPO | 85 |
| 6.2 | Akustische Wohnraumüberwachung | 88 |
| 6.3 | Genomanalyse im Strafverfahren | 89 |
| 6.4 | Strafbarkeitslücke bei heimlicher Ortung | 90 |
| 6.5 | Verbesserung der Durchsetzung von Rechten des geistigen Eigentums – Umsetzung der IPR-Enforcement-Richtlinie | 91 |
| 6.6 | Digitales Rechtemanagement | 92 |
| 6.7 | Novellierung der Prozesskostenhilfe | 93 |
| 6.8 | Das Betreuungsbehördengesetz soll ergänzt werden | 94 |

| | | Seite |
|---|---|---|
| **7** | **Innere Verwaltung** | 94 |
| 7.1 | Ausländerrecht | 94 |
| 7.1.1 | Entwurf eines Gesetzes zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union | 94 |
| 7.1.2 | Die Integrationsgeschäftsdatei beim Bundesamt für Migration und Flüchtlinge | 95 |
| 7.1.3 | AZR: Datenerhebung zu Forschungszwecken ohne Rechtsgrundlage | 96 |
| 7.1.4 | Das Visa-Informationssystem | 96 |
| 7.1.5 | „Scheinvaterschaften“ sollen angefochten werden können | 97 |
| 7.1.6 | Vereinsrecht | 97 |
| 7.2 | Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und das Stasi-Unterlagen-Gesetz (StUG) | 97 |
| 7.2.1 | 7. Änderung des Stasi-Unterlagen-Gesetzes | 97 |
| 7.3 | Bundesmeldegesetz | 98 |
| 7.4 | Reform des Personenstandsrechts – Erleichterung der Ahnenforschung | 98 |
| 7.5 | Volkszählung 2011 – Der Countdown hat begonnen | 99 |
| 7.6 | Datenschutzgerechter Zugang von Wissenschaftlern zu statistischen Einzelangaben | 99 |
| **8** | **Finanzwesen** | 100 |
| 8.1 | Identifikationsnummer für steuerliche Zwecke (Steuer-ID) wird eingeführt | 100 |
| 8.2 | Kontenabruf durch Finanzämter und andere Behörden | 100 |
| 8.3 | Schwarzarbeitbekämpfungsgesetz – Erfahrungen in der Praxis | 105 |
| 8.4 | ELSTER-Portal und StDÜV | 103 |
| **9** | **Wirtschaft** | 104 |
| 9.1 | Profilbildung verhindern | 104 |
| 9.2 | Umsetzung von Basel II schafft eine gesetzliche Grundlage zum Ratingverfahren der Kreditinstitute | 106 |
| 9.3 | Research-Systeme der Banken zur Aufdeckung von Geldwäsche | 108 |
| 9.4 | SWIFT – Unzulässige Datenlieferung an US-Behörden | 108 |
| 9.5 | Warn- und Hinweissystem der Versicherungswirtschaft – Uniwagnis | 110 |
| 9.6 | Bundesverfassungsgericht stoppt formularmäßige Einwilligungserklärungen von Versicherungen | 111 |
| 9.7 | Datenschutz bei Rechtsanwälten | 112 |

| | | Seite |
|---|---|---|
| **10** | **Telekommunikations- und Teledienste** | 112 |
| 10.1 | Brüsseler Sündenfall – Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten | 112 |
| 10.2 | Neue Geschäftsmodelle durch Location Based Services | 113 |
| 10.3 | Anzeige der Kundennummer im Call-Center trotz Rufnummernunterdrückung | 115 |
| 10.4 | Übersendung des Einzelverbindungsnachweises per E-Mail | 115 |
| 10.5 | EVNde gut, alles gut | 116 |
| 10.6 | Datenschutz beim Abschluss von Telekommunikationsverträgen | 116 |
| 10.7 | Neue Vertriebswege und Datenschutz | 118 |
| 10.8 | Veröffentlichungen im Internet | 118 |
| 10.8.1 | Internetdatenbanken – Pranger oder Wissensdatenbank? | 118 |
| 10.8.2 | Insolvenzbekanntmachungen in Zukunft nur noch elektronisch | 119 |
| 10.9 | Das Telemediengesetz – was lange währt, ...? | 119 |
| 10.10 | Suchmaschinen: Wohl und Wehe einer hilfreichen Erfindung | 120 |
| 10.11 | Sechstes und siebtes Symposium in Bonn | 120 |
| **11** | **Postunternehmen** | 121 |
| 11.1 | Datenschutz bei der Deutschen Post AG | 121 |
| 11.2 | UPS – Verbindliche Vertragsregeln für alle Töchter in Europa (Europäisches Addendum) | 124 |
| **12** | **Verkehr** | 124 |
| 12.1 | LKW-Maut | 124 |
| 12.2 | eCall | 126 |
| 12.3 | Event Data Recorder – Der im Auto eingebaute „Große Bruder“ | 128 |
| 12.4 | Pay as You Drive – Know where You Go | 128 |
| 12.5 | Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrt-Bundesamtes (KBA) | 128 |
| 12.6 | Übermittlung von medizinischen Untersuchungsbefunden an das Luftfahrt-Bundesamt (LBA) | 129 |
| **13** | **Gesundheit und Soziales** | 129 |
| 13.1 | Gesetzliche Krankenversicherung | 129 |
| 13.1.1 | Gesundheitsreform 2006/2007 | 129 |
| 13.1.2 | Risikostruktur-Ausgleichsverordnung | 130 |

| | | Seite |
|---|---|---|
| 13.1.3 | Datenerhebung ohne gesetzliche Grundlage? – „Selbstauskunftsbögen“ der Krankenkassen | 130 |
| 13.1.4 | Qualitätssicherungs – Richtlinie Dialyse/Allgemeine Anforderungen an eine einrichtungsübergreifende Qualitätssicherung | 132 |
| 13.1.5 | Kostendämpfungsmaßnahmen bei Heil- und Hilfsmitteln – um jeden Preis? | 133 |
| 13.1.6 | „Freier Eintritt“ bei Vorlage der Krankenversichertenkarte | 133 |
| 13.1.7 | „Barmer Hausarzt- und Hausapotheken – Modell“ | 134 |
| 13.1.8 | Häusliche Krankenpflege – Was will eine gesetzliche Krankenkasse mit den medizinischen Daten ihrer Versicherten? | 134 |
| 13.1.9 | Öffentliche Ausschreibungen für Sozialleistungen | 135 |
| 13.2 | Gendiagnostikgesetz dringend erforderlich | 135 |
| 13.3 | Unfallversicherung | 136 |
| 13.3.1 | Gutachterregelung | 136 |
| 13.3.2 | Rechtsfolgen bei Missachtung der Gutachterregelung | 137 |
| 13.3.3 | Anforderung von Krankenhausentlassungsberichten durch Unfallversicherungsträger | 137 |
| 13.3.4 | Prüfdatei bei fehlerhafter Abrechnung | 138 |
| 13.4 | Rentenversicherung | 138 |
| 13.4.1 | Beratung der Deutschen Rentenversicherung Bund | 138 |
| 13.4.2 | Kontrolle einer Rehabilitationsklinik der Deutschen Rentenversicherung Bund | 138 |
| 13.5 | Arbeitsverwaltung | 139 |
| 13.5.1 | Hartz IV und Missbrauchskontrolle | 139 |
| 13.5.2 | Antragsformulare für Alg II jetzt datenschutzfreundlicher | 141 |
| 13.5.3 | Fortschritte beim Erhebungs- und Leistungssystem A2LL in Sicht | 142 |
| 13.5.4 | Datenschutzrechtliche Aufsicht für die Arbeitsgemeinschaften (ARGEn) | 142 |
| 13.5.5 | Einzelfälle | 144 |
| **14** | **Mitarbeiterdatenschutz** | 146 |
| 14.1 | Zugang von Vorgesetzten zu Personal- und Personalaktendaten | 146 |
| 14.2 | Neuordnung des Beamtenrechts in Bund und Ländern | 147 |
| 14.3 | Automatisierte Personaldatenverarbeitung | 148 |
| 14.4 | Behördeninterne Veröffentlichung von Mitarbeiterdaten | 150 |
| 14.5 | Personaldatenschutz und Verwaltungsermittlungen | 151 |

| | | Seite |
|---|---|---|
| **15** | **Deutscher Bundestag** | 151 |
| 15.1 | Online-Angebot „Öffentliche Petitionen“ | 151 |
| 15.2 | Wahrung der Vertraulichkeit von Petitionen | 152 |
| **16** | **Bundeswehr** | 152 |
| 16.1 | Das Großprojekt HERKULES | 152 |
| 16.2 | Einhaltung von Datenschutzbestimmungen durch die Kleiderkasse der Bundeswehr | 153 |
| **17** | **Auswärtige Angelegenheiten** | 153 |
| 17.1 | Urkundenüberprüfungsverfahren bei unzuverlässigem Beurkundungswesen | 153 |
| 17.2 | Vertragsloser Zustellungsverkehr | 153 |
| **18** | **Aus meiner Dienststelle** | 154 |
| 18.1 | Neuer Internetauftritt | 154 |
| 18.2 | Öffentlichkeitsarbeit | 154 |
| 18.3 | Twinning-Project Malta | 155 |
| 18.4 | Besuche ausländischer Delegationen | 155 |
| 18.5 | BfDI als Ausbildungsbehörde | 155 |
| 18.6 | Künftig mehr Präsenz in der Bundeshauptstadt | 155 |
| 18.7 | Folgen des neuen Informationsfreiheitsgesetzes für meine Dienststelle | 156 |
| **19** | **Wichtiges aus zurückliegenden Tätigkeitsberichten** | 156 |
| 1. | Fundpapierdatenbank beim Bundesverwaltungsamt | 156 |
| 2. | Zentrales Vorsorgeregister bei der Bundesnotarkammer | 156 |
| 3. | Kapitalanleger-Mustergesetz | 156 |
| 4. | Zinsinformationsverordnung (ZIV) | 157 |
| 5. | Steuerdatenabrufverordnung (StDAV) | 157 |
| 6. | Nutzung von Rentendaten durch die BA für andere Zwecke | 157 |
| 7. | Zugriff des Personalrats auf Arbeitszeitdaten | 157 |
| 8. | Neugeborenen-Screening | 157 |
| 9. | Zugriff des MAD auf PERFIS | 157 |
| 10. | Konsultationsverfahren nach Artikel 17 Abs. 2 SDÜ | 157 |
| 11. | IFOS Bund (BAköV) | 157 |
| 12. | Jugendstrafvollzug | 158 |
| 13. | Erforderliche Änderungen des Bundesverfassungsschutzgesetzes | 158 |
| 14. | Kontrollkompetenz beim BfV | 158 |

Seite

**Anlage 1**
Hinweis für die Ausschüsse des Deutschen Bundestages . . . . . 159

**Anlage 2**
Übersicht über die durchgeführten Kontrollen, Beratungen
und Informationsbesuche . . . . . 160

**Anlage 3**
Übersicht über Beanstandungen nach § 25 BDSG . . . . . 162

**Anlage 4** (zu Nr. 3.5)
27. Internationale Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre vom 14. bis 16. September 2005
Erklärung von Montreux:
„Ein universelles Recht auf den Schutz personenbezogener Daten
und der Privatsphäre unter Beachtung der Vielfalt in einer
globalisierten Welt“ . . . . . 163

**Anlage 5** (zu Nr. 3.5)
27. Internationale Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre vom 14. bis 16. September 2005
Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten
und Reisedokumenten . . . . . 165

**Anlage 6** (zu Nr. 3.5)
27. Internationale Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre vom 14. bis 16. September 2005
Resolution zur Verwendung von Personendaten für die politische
Kommunikation . . . . . 166

**Anlage 7** (zu Nr. 3.5 und Nr. 10.10)
28. Internationale Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre am 2. und 3. November 2006
Entschließung zum Datenschutz bei Suchmaschinen . . . . . 168

**Anlage 8** (zu Nr. 3.5)
28. Internationale Konferenz der Beauftragten für den Datenschutz
und den Schutz der Privatsphäre am 2. und 3. November 2006
Londoner Erklärung:
„Datenschutz vermitteln und effektiver gestalten“ . . . . . 170

**Anlage 9** (zu Nr. 3.3)
Von der Artikel 29-Gruppe im Berichtszeitraum verabschiedete Dokumente 171

**Anlage 10** (zu Nr. 4.5.3)
Entschließung zwischen der 69. und 70. Konferenz der Daten-
schutzbeauftragten des Bundes und der Länder
zur Einführung biometrischer Ausweisdokumente vom 1. Juni 2005 . . . . . 174

**Anlage 11** (zu Nr. 2.1)
Entschließung der 70. Konferenz der Datenschutzbeauftragten
des Bundes und der Länder am 27. und 28. Oktober 2005
Appell der Datenschutzbeauftragten des Bundes und der Länder:
Eine moderne Informationsgesellschaft braucht mehr Datenschutz . . . . . 175

Seite

**Anlage 12** (zu Nr. 4.7)
Entschließung zwischen der 70. und 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
Sicherheit bei eGovernment durch Nutzung des Standards OSCI . . . . . 177

**Anlage 13** (zu Nr. 4.3)
Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. Oktober 2006
Verbindliche Regelungen für den Einsatz von RFID-Technologie . . . . . 178

**Anlage 14** (zu Nr. 4.4.1, Nr. 4.7 und Nr. 8.4)
Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006
Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren . . . . . 179

**Anlage 15** (zu Nr. 4.3)
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006
Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich:
Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten! . . . . . 181

**Anlage 16** (zu Nr. 9.4)
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006
SWIFT: Datenübermittlung im SWIFT–Verfahren in die USA . . . . . 183

Organigramm der Dienststelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit . . . . . 184

**Sachregister** . . . . . 185

**Abkürzungsverzeichnis/Begriffe** . . . . . 191

**Abbildungsverzeichnis**

Abb. 1 (zu Nr. 3.2.3) So funktioniert Europol . . . . . 26

Abb. 2 (zu Nr. 4.3) RFID-Technik . . . . . 42

Abb. 3 (zu Nr. 4.3) PET-Flasche mit RFID-Chip . . . . . 43

Abb. 4 (zu Nr. 4.8) Schreddern von Datenträgern. . . . . 52

Abb. 5 (zu Nr. 4.13) Internet-Eingabemaske. . . . . 57

Abb. 6 (zu Nr. 4.13) Beispiele für Schutzprofile. . . . . 58

Abb. 7 (zu Nr. 4.13) Sicherheitseinstellungen im WLAN . . . . . 58

Abb. 8 (zu Nr. 9.4) So funktioniert SWIFT. . . . . 109

Abb. 9 (zu Nr. 12.2) Automatischer Notruf . . . . . 127

Seite

**Kasten zu Nr. 2.1**
Auszüge aus der Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005: Appell der Datenschutzbeauftragten des Bundes und der Länder: Eine moderne Informationsgesellschaft braucht mehr Datenschutz ..... 16

**Kasten zu Nr. 2.2**
Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005: Unabhängige Datenschutzkontrolle in Deutschland gewährleisten ..... 17

**Kasten zu Nr. 2.4**
Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597 ..... 19

**Kasten zu Nr. 3.2.1**
Erklärung verabschiedet von den Europäischen Datenschutzbehörden in London am 2. November 2006 ..... 24

**Kasten zu Nr. 3.2.2**
Wesentlicher Regelungsgehalt des Vertrages von Prüm ..... 25

**Kasten zu Nr. 3.2.3.1**
Auszug 19. TB Nr. 16.1 ..... 27

**Kasten a zu Nr. 3.2.4.2**
Gemeinsame Kontrollinstanz ..... 29

**Kasten b zu Nr. 3.2.4.2**
Artikel 99 Abs. 2 Schengener Durchführungsübereinkommen (SDÜ) ..... 29

**Kasten zu Nr. 3.3.1**
Forderungen der Artikel 29-Gruppe zu Whistleblowing ..... 32

**Kasten zu Nr. 3.3.2**
Anforderungen an ein neues PNR-Abkommen ..... 33

**Kasten zu Nr. 3.3.5**
Erläuterungen zu Safe Harbor ..... 35

**Kasten zu Nr. 3.5**
Abschlusskommuniqué der Londoner Konferenz ..... 37

**Kasten zu Nr. 4.1**
69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005: Entschließung zur Einführung der elektronischen Gesundheitskarte ..... 38

**Kasten zu Nr. 4.2**
§ 6b BDSG – Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen ..... 39

**Kasten zu Nr. 4.2.1**
Schutzprofil bei Videoüberwachung ..... 40

Seite

**Kasten zu Nr. 4.3**
RFID – Schutz der Persönlichkeitsrechte Betroffener . . . . . 42

**Kasten zu Nr. 4.4**
Identitätsmanagement . . . . . 43

**Kasten zu Nr. 4.4.2**
Verschlüsselung . . . . . 44

**Kasten zu Nr. 4.8**
Darauf ist zu achten: 9 Tipps zur effektiven Löschung von Daten . . . . . 52

**Kasten zu Nr. 4.11**
Das ist ein TPM (Trusted Platform Module) . . . . . 55

**Kasten zu Nr. 5.1**
Trennungsgebot . . . . . 59

**Kasten a zu Nr. 5.1.1**
Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. Oktober 2006:
Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten . . . 60

**Kasten b zu Nr. 5.1.1**
In der Antiterrordatei zu speichernde Daten . . . . . 62

**Kasten zu Nr. 5.1.2**
Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. Oktober 2006:
Das Gewicht der Freiheit beim Kampf gegen den Terrorismus . . . . . 64

**Kasten zu Nr. 5.1.4**
§ 18 BVerfSchG – Übermittlung von Informationen an die Verfassungsschutzbehörden . . . . . 66

**Kasten zu Nr. 5.2.3**
Rasterfahndung . . . . . 69

**Kasten zu Nr. 5.2.5**
Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005:
Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006 . . . . . 72

**Kasten zu Nr. 5.4.1**
Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. Oktober 2005:
Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden . . . . . 75

**Kasten a zu Nr. 6.1**
Gemeinsames Papier der Datenschutzbeauftragten des Bundes und der Länder:
Datenschutzrechtliche Forderungen für die Neuregelung verdeckter Ermittlungsmaßnahmen (§§ 100a ff. StPO) . . . . . 86

Seite

**Kasten b zu Nr. 6.1**
Gemeinsames Papier der Datenschutzbeauftragten des Bundes und der Länder:
Datenschutzrechtliche Forderungen für die Durchführung von Funkzellenabfragen . . . . . 87

**Kasten zu Nr. 6.3**
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005 zur Bundesrats-initiative mehrerer Länder zur Ausweitung der DNA-Analyse:
Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck . . . . . 89

**Kasten zu Nr. 6.5**
Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2006:
Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht . . . . . 92

**Kasten zu Nr. 8.2**
Datenschutzrechtliche Kritik . . . . . 101

**Kasten zu Nr. 8.3**
Was und wie prüft die Finanzkontrolle Schwarzarbeit . . . . . 103

**Kasten zu Nr. 9.2**
§ 10 Abs. 1 Sätze 3 bis 8 Kreditwesengesetz . . . . . 107

**Kasten zu Nr. 9.3**
Auszüge aus dem Arbeitspapier der obersten Datenschutzaufsichts-behörden der Länder und des Bundes:
Datenschutzrechtliche Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche . . . . . 108

**Kasten zu Nr. 9.5**
So funktioniert Uniwagnis . . . . . 111

**Kasten zu Nr. 10.2**
Werde ich geortet? . . . . . 115

**Kasten zu Nr. 10.10**
Forderungen an die Anbieter von Suchmaschinen . . . . . 121

**Kasten zu Nr. 11.1**
Auszug aus der Postdienste-Datenschutzverordnung;
Zustellbesonderheiten . . . . . 123

**Kasten zu Nr. 12.1**
Daten, die bei der LKW-Maut erhoben und gespeichert werden . . . . . 126

**Kasten zu Nr. 12.2**
Wie soll eCall funktionieren? . . . . . 127

**Kasten a zu Nr. 13.1.3**
Auszug: Stellungnahme der Bundesregierung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes – Bundestagsdrucksache 15/5252 – . . . . . 131

Seite

**Kasten b zu Nr. 13.1.3**
Beispiele aus mir vorliegenden „Selbstauskunftsbögen“ . . . . . 131

**Kasten zu Nr. 13.1.8**
Auszug aus der Stellungnahme der Bundesregierung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes – Bundestagsdrucksache 15/5252 – . . . . . 135

**Kasten zu Nr. 13.5.1**
Gemeinsame Erklärung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen:
Arbeitsuchende unter Generalverdacht . . . . . 140

**Kasten a zu Nr. 13.5.4**
Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 16. und 17. März 2006:
Keine kontrollfreien Räume bei der Leistung von ALG II . . . . . 143

**Kasten b zu Nr. 13.5.4**
Beschluss der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. Oktober 2006:
Datenschutzkontrollzuständigkeit für die SGB II-Arbeitsgemeinschaften . . 143

**Kasten zu Nr. 14.3**
Handlungsempfehlungen Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung:
II. Allgemeine datenschutzrechtliche Leitplanken . . . . . 149

## 1 Einführung

Seitdem das Bundesverfassungsgericht in seinem „Volkszählungsurteil“ 1983 klargestellt hat, dass es sich bei dem Datenschutz um ein Grundrecht handelt, hat sich die Informationstechnik dramatisch verändert. Die Integration von Computerchips in alle möglichen Alltagsgegenstände führt zur Registrierung unseres Verhaltens, unserer Interessen und unserer persönlichen Eigenheiten und macht sie zunehmend überwachbar. Konnte man vor 25 Jahren noch darauf hoffen, dass eine Rundumüberwachung an mangelnden Verarbeitungskapazitäten oder hohen Kosten scheitern würde, hat die begrenzende Wirkung dieser Faktoren drastisch nachgelassen. Gerade auch der Berichtszeitraum war von dieser Entwicklung geprägt. Politik, Wirtschaft und Wissenschaft sind deshalb aufgerufen, mit den technischen Möglichkeiten verantwortungsbewusst umzugehen und sich selbst zu begrenzen. Nicht alles, was irgendwie sinnvoll erscheint, darf auch realisiert werden. Stets müssen bei Entscheidungen über den Einsatz von IT-Systemen auch die Wirkungen auf das individuelle Selbstbestimmungsrecht bedacht werden.

Angesichts dieser Entwicklung müsste man eigentlich erhebliche Anstrengungen erwarten, mit denen etwa der Gesetzgeber diesen Risiken entgegenwirkt. Leider ist davon wenig zu erkennen. Statt dessen wird der mögliche Missbrauch von Informationstechnik mit immer mehr Kontrollmaßnahmen beantwortet, von denen ganz überwiegend Unverdächtige betroffen sind. So wird das Internet in der politischen Debatte bisweilen als „Schule des Terrors“ bezeichnet, um damit seine möglichst umfassende Überwachung zu begründen. Die Tatsache, dass auch Straftäter telefonieren oder E-Mails versenden, war Ausgangspunkt der Anfang 2006 auf europäischer Ebene beschlossenen Verpflichtung für die Anbieter elektronischer Dienste, sämtliche Verkehrsdaten aller Nutzer ohne konkreten Verdacht oder Anlass für mindestens sechs Monate zu speichern. Schließlich wird aus vergleichbarem Grund gefordert, dass Strafverfolgungsbehörden und Nachrichtendienste zukünftig über das Internet heimlich auf Computer zugreifen können sollen. Die Feststellung des BGH, dass solche „Online-Durchsuchungen“ ohne gesetzliche Grundlage sind, führt bei Vertretern der Sicherheitsbehörden nicht etwa zu der Frage, ob derartige Maßnahmen unverhältnismäßig in das Recht auf informationelle Selbstbestimmung eingreifen. Stattdessen wird die gesetzliche Legitimierung dieser Ermittlungsmethode gefordert.

Die Entwicklung zur Informationsgesellschaft ist unumkehrbar. Zu beeinflussen ist allerdings, ob diese Gesellschaft dauerhaft durch mehr Entfaltungschancen für den Einzelnen oder von immer weitergehender Überwachung geprägt ist. Von zentraler Bedeutung wird dabei sein, wie der Gesetzgeber von seinen Gestaltungsmöglichkeiten Gebrauch macht, ob er die Grundrechtspositionen stärkt oder ob er immer neue Grundrechtseinschränkungen legitimiert. Für äußerst bedenklich halte ich es in diesem Zusammenhang, dass im Berichtszeitraum wiederholt Einschränkungen des Datenschutzes Gesetzeskraft erlangten und es dem Bundesverfassungsgericht überlassen blieb, unverhältnismäßige Grundrechtseingriffe rückgängig zu machen.

Das Recht auf informationelle Selbstbestimmung ist eines der wichtigsten Bürgerrechte der Informationsgesellschaft. Es ist nicht zu erwarten, dass die technologisch bedingten Kontroll- und Überwachungsrisiken ohne gesetzliche Beschränkungen wirksam beherrscht werden können. Dies betrifft nicht nur das Verhältnis Staat-Bürger, sondern auch den Umgang der Wirtschaft mit personenbezogenen Daten. Der Hinweis des Bundesverfassungsgerichts, dass umfassende Persönlichkeitsprofile nicht mit dem Menschenbild des Grundgesetzes vereinbar sind, ist angesichts immer effektiverer Möglichkeiten zum Sammeln, Zusammenführen und Auswerten von Daten aktueller denn je. Umso bedenklicher ist es, dass die immer wieder angekündigte Anpassung des Datenschutzrechts an neue technologische Entwicklungen bis heute keinen Schritt vorangekommen ist, während an Gesetzgebungsvorhaben kein Mangel herrscht, die das informationelle Selbstbestimmungsrecht einschränken. Angesichts dieser bedenklichen Schieflage ist daran zu erinnern, dass die verfassungsrechtlich verankerten Grundsätze der Menschenwürde und der Verhältnismäßigkeit für eine demokratische Informationsgesellschaft von entscheidender Bedeutung sind. Daraus ergibt sich, dass es eine Rundumüberwachung genauso wenig geben darf wie eine Kontrolle des Kernbereichs der Privatsphäre.

Ich möchte auch bei diesem Bericht darauf hinweisen, dass die Tätigkeiten – auch wenn über sie in der „Ich-Form“ berichtet wird – größtenteils von meinen Mitarbeiterinnen und Mitarbeitern ausgeführt wurden. Ihnen möchte ich für ihr großes Engagement und ihre erfolgreiche Arbeit danken. Allerdings sind die Grenzen der Belastbarkeit erreicht. In den letzten Jahren hat sich allein die Zahl der Eingaben fast verdoppelt. Die Aufgabe des Bundesbeauftragten für die Informationsfreiheit ist hinzugekommen, ohne dass neue Mitarbeiter in der im Vorblatt des Gesetzentwurfs genannten Zahl hierfür bereitgestellt wurden. Es ist deswegen absehbar, dass ohne Personalverstärkung die Arbeit nicht in gleicher Intensität und Qualität fortgesetzt werden kann.

Mein Dank gilt auch den Abgeordneten aller Fraktionen des Deutschen Bundestages, die sich nachhaltig für den Datenschutz interessiert und engagiert haben, und den Vertretern von öffentlichen und privaten Stellen, für die Datenschutz eine Bedingung erfolgreichen Handelns ist.

Peter Schaar

## 2 Datenschutzrechtlicher Rahmen

### 2.1 Weiterentwicklung des Datenschutzrechts

*Die dringend erforderliche Modernisierung des Datenschutzrechts lässt weiter auf sich warten.*

Die seit vielen Jahren angekündigte und vom Deutschen Bundestag mehrfach angemahnte grundlegende Reform des Datenschutzrechts (vgl. 20. TB Nr. 2.1; 19. TB Nr. 3.3) ist auch im Berichtszeitraum nicht in Angriff genommen worden, obwohl hier ein erhebliches Potenzial für Verwaltungsmodernisierung, Entbürokratisierung und Stärkung von Bürger- und Verbraucherrechten festzustellen ist. Eine Neukonzeption des Datenschutzes, bei der das bisherige System von Verbot, Kontrolle und gegebenenfalls Sanktion durch einen integrativen Ansatz ergänzt oder sogar in Teilen ersetzt würde, der Datenschutz nicht als Einschränkung, sondern als Wettbewerbsvorteil und Mehrwert versteht, könnte einen wichtigen Beitrag zur Modernisierung von Staat und Gesellschaft leisten. Hierzu gehören die Integration des Datenschutzes in technische Systeme und Verfahren von Anfang an, datenschutzrechtliche Selbstregulierung und Selbstkontrolle und Stärkung der Schutzmöglichkeiten durch die Betroffenen selbst.

Ohne entsprechende Reformschritte wird die Lücke zwischen dem technologischen Fortschritt und dem Einsatz elektronischer Datenverarbeitung in immer neuen Lebensbereichen und den geltenden datenschutzrechtlichen Bestimmungen und dem System der datenschutzrechtlichen Kontrolle immer größer. Ich habe daher schon mehrfach darauf hingewiesen, dass eine kontinuierliche Weiterentwicklung des Datenschutzrechts und seine Anpassung an die sich rasch ändernden Verhältnisse dringend geboten ist. Sind Fehlentwicklungen einmal eingetreten, lassen sie sich nur schwer und nur mit erheblichem gesetzgeberischen Aufwand wieder korrigieren.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deswegen zu Beginn der laufenden Legislaturperiode einen Appell an die Fraktionen des Deutschen Bundestages und an die Bundesregierung gerichtet, sich verstärkt für den Schutz des Grundrechts auf informationelle Selbstbestimmung einzusetzen, und dabei die wichtigsten aktuellen Handlungsfelder aufgeführt (vgl. Kasten zu Nr. 2.1; der volle Wortlaut ist in Anlage 11 wiedergegeben).

Als erste Reformschritte sollten in Betracht gezogen werden:

- Eine Vereinfachung des geltenden Datenschutzrechts, das zur Zeit neben dem BDSG in eine Vielzahl von mehr oder weniger umfassenden Spezialregelungen zersplittert und damit für alle Beteiligten unüberschaubar geworden ist. Hier zu vereinheitlichen und zu vereinfachen wäre ein wichtiger Beitrag zur Entbürokratisierung.
- Die Schaffung eines bundeseinheitlichen Datenschutzaudits nach § 9a BDSG (s. u. Nr. 2.4) als Einstieg in einen system- und verfahrensintegrierten Datenschutz.
- Verbesserung des Schutzes und Stärkung der Rechte der betroffenen Bürgerinnen und Bürger gegen immer umfassendere Datensammlungen im nicht-öffentlichen Bereich, deren Vernetzung und Auswertung zu Lasten der Betroffenen (vgl. z. B. Nr. 9.1).

Ich hoffe, dass endlich erste Schritte für die dringend erforderliche Modernisierung des Datenschutzrechts eingeleitet werden.

Kasten zu Nr. 2.1

**Auszüge aus der Entschließung der 70. Datenschutzkonferenz vom 27./28. Oktober 2005**

**„Appell der Datenschutzbeauftragten des Bundes und der Länder:**

**Eine moderne Informationsgesellschaft braucht mehr Datenschutz**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

...

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

...

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.“

## 2.2 Struktur der Datenschutzaufsicht auf dem Prüfstand

*Die Europäische Kommission hält die Datenschutzaufsichtsbehörden in Deutschland nicht für ausreichend unabhängig und hat deswegen ein Vertragsverletzungsverfahren eingeleitet. Auch sonst kann die komplexe Struktur der Datenschutzaufsicht zu Problemen führen.*

Die Struktur der Datenschutzaufsicht in der Bundesrepublik Deutschland ist überaus komplex (vgl. 20. TB Nr. 2.3) und für die Bürgerinnen und Bürger oft undurchsichtig. Grundvoraussetzung für ihre Tätigkeit ist aber zunächst einmal ihre Unabhängigkeit von staatlicher Einflussnahme.

### Vertragsverletzungsverfahren der Europäischen Kommission

Artikel 28 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rats vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-ABl. Nr. L 281 vom 23. November 1995, S. 2 ff.) bestimmt nicht nur, dass in den Mitgliedstaaten eine oder mehrere öffentliche Stellen beauftragt werden müssen, die Anwendung der von den Mitgliedstaaten zur Umsetzung der Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen, sondern auch, dass diese Stellen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen.

Auf Grund der Beschwerde eines Bürgers hat die Europäische Kommission überprüft, ob diese Voraussetzung in der Bundesrepublik Deutschland erfüllt ist. Dabei ist sie zu dem Ergebnis gekommen, die Wahrnehmung der Datenschutzaufsicht im nicht-öffentlichen Bereich durch die Innenministerien der Länder selbst oder durch Behörden der allgemeinen Landesverwaltung entspreche nicht den Anforderungen der Richtlinie. Das gleiche gelte für die Regelungen, die die datenschutzrechtliche Kontrolle zwar den jeweiligen Landesbeauftragten für den Datenschutz übertragen, diese aber einer Fach- oder Rechtsaufsicht durch die Exekutive unterworfen hätten. Mit Schreiben vom 5. Juli 2005 hat die Europäische Kommission deswegen ein Vertragsverletzungsverfahren eingeleitet. Da ich die Rechtsauffassung der Europäischen Kommission teile, habe ich mich daraufhin an den Bundesminister des Innern gewandt und eine grundlegende Reform der Datenschutzaufsicht in Deutschland angeregt, die ein wichtiger Beitrag zur Verwaltungsvereinfachung und Kosteneinsparung und ein bedeutsamer Schritt in Richtung auf eine moderne Informationsgesellschaft sei. Auch in meiner Stellungnahme vor dem Ausschuss für Inneres und Sport des Niedersächsischen Landtages habe ich zu der Frage der „vollständigen Unabhängigkeit“ der Aufsichtsbehörden für den nicht-öffentlichen Bereich noch einmal eingehend rechtlich Stellung genommen. Die Konferenz der Datenschutzbeauftragtes des Bundes und der Länder hat auf ihrer Sitzung im Oktober 2005 in einer Entschließung zu dem Vertragsverletzungsverfahren (vgl. Kasten zu Nr. 2.2) die Rechtsauffassung der Kommission unterstützt und entsprechende Änderungen in der Aufsichtsstruktur verlangt.

Nachdem die Bundesregierung an ihrem Rechtsstandpunkt, das Deutsche Recht entspreche insoweit den europarechtlichen Anforderungen, festhält und auch Gespräche mit der Kommission ergebnislos geblieben sind, hat diese am 15. Dezember 2006 gemäß Artikel 226 Absatz 1 des Vertrags zur Gründung der Europäischen Gemeinschaft eine mit Gründen versehene Stellungnahme abgegeben, in der sie einen Verstoß gegen Artikel 28 Abs. 1 Satz 2 der Richtlinie feststellt und die Bundesrepublik Deutschland auffordert, die erforderlichen Maßnahmen zu ergreifen, um der Auffassung der Kommission binnen zwei Monaten nachzukommen. Es ist damit zu rechnen, dass die Kommission nach Ablauf dieser Frist Klage beim Europäischen Gerichtshof erheben wird.

Kasten zu Nr. 2.2

**Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck**

**Unabhängige Datenschutzkontrolle in Deutschland gewährleisten**

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

**Auswirkungen der aktuellen Aufsichtsstruktur**

Unabhängig von der wichtigen Frage der vollständigen Unabhängigkeit der Aufsichtsbehörden für den nicht-öffentlichen Bereich, die Gegenstand des Vertragsverletzungsverfahrens ist, ergeben sich aus der sehr komplexen Struktur der Datenschutzaufsicht in Deutschland (vgl. 20. TB Nr. 2.3) weitere Schwierigkeiten. Die Vielzahl verschiedener und jeweils unabhängiger Aufsichtsbehörden hat zur Konsequenz, dass gleiche Sachverhalte und Rechtsfragen möglicherweise unterschiedlich beurteilt und gewertet werden, was im Einzelfall im nicht-öffentlichen Bereich für bundesweit operierende Unternehmen und Dienstleister zu Problemen führen kann, aber auch im öffentlichen Bereich, z. B. bei den Sicherheitsbehörden. Um diesen Schwierigkeiten zu begegnen, bemühen sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder für den öffentlichen Bereich und der sog. „Düsseldorfer Kreis“ für den nicht-öffentlichen Bereich um gegenseitige Information und Abstimmung, um zu einer möglichst einheitlichen Rechtsauffassung und Vorgehensweise zu gelangen. Dieses Verfahren ist aber sehr zeit- und arbeitsaufwendig und kann wegen der Unabhängigkeit der jeweiligen Aufsichtsbehörden nur zu einer Abstimmung, nicht aber zu bindenden Entscheidungen führen. Will z. B. ein bundesweit operierender Konzern oder ein Branchenverband eine datenschutzrechtliche Fragestellung mit der Datenschutzaufsicht verbindlich klären, kann es viele Monate dauern, bis eine abschließende Meinungsbildung im Düsseldorfer Kreis erzielt ist, die aber letztlich niemanden bindet und deswegen auch für die Unternehmen nicht die angestrebte Rechtssicherheit bringt. Hierüber wird auch in der Wirtschaft immer wieder geklagt.

Es könnte deswegen ein wichtiger Beitrag zur Verwaltungsmodernisierung und Entbürokratisierung sein, eine grundlegende Reform der Datenschutzaufsicht in Angriff zu nehmen.

## 2.3 Das Mittelstandsentlastungsgesetz zeigt für den Datenschutz nicht den richtigen Weg auf

*Das Mittelstandsentlastungsgesetz schränkt für weite Bereiche des Handwerks, des Handels und der freien Berufe die Pflicht ein, betriebliche Datenschutzbeauftragte zu bestellen, und verstößt damit gegen europäisches Recht.*

Artikel 1 des „Ersten Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft“ vom 22. August 2006 (Mittelstandsentlastungsgesetz, BGBl. I S. 1970) hat das Bundesdatenschutzgesetz (BDSG) in mehreren Punkten geändert. Die Regelungen, die im BDSG und in § 203 StGB die Möglichkeit verbessern, externe Datenschutzbeauftragte insbesondere auch bei so genannten Berufsgeheimnisträgern zu bestellen, sind uneingeschränkt zu begrüßen, nicht zuletzt auch deswegen, weil damit eine Klarstellung verbunden ist, dass das BDSG auch für Rechtsanwälte, Ärzte und andere freie Berufe gilt, die einer besonderen Schweigepflicht unterliegen.

Besonders kritisch sehe ich aber die Regelungen, die die Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter einschränken. Die beschlossenen Änderungen in §§ 4d und 4f Abs. 1 BDSG lassen sowohl die Pflicht zur Meldung von Verfahren automatisierter Verarbeitungen als auch zur Berufung eines betrieblichen Datenschutzbeauftragten bis zu einer Grenze von zehn Arbeitnehmern, die mit automatisierter Verarbeitung personenbezogener Daten beschäftigt sind, entfallen. Da nach Angaben des Statistischen Bundesamtes über 90 v.H. der deutschen Unternehmen weniger als zehn Mitarbeiter haben, sind durch die Gesetzesänderung weite Teile des Handels, des Handwerks und der freien Berufe aus der Meldepflicht herausgefallen, ohne dass stattdessen ein betrieblicher Datenschutzbeauftragter über die Einhaltung des Datenschutzes wachen würde.

Diese neue Rechtslage steht zudem nach meiner Einschätzung nicht im Einklang mit europäischem Recht, nämlich mit Artikel 18 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Amtsbl. L 281 vom 23. November 1995, S. 31). Das europäische Datenschutzrecht sieht die Meldepflicht ohne Einschränkung und „Bagatellgrenze“ zwingend vor. Ausnahmen sind nach Artikel 18 Abs. 2 der Richtlinie nur möglich, wenn entweder ein betrieblicher Datenschutzbeauftragter bestellt wird oder wenn für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorien der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung gesetzlich festgelegt sind. Diese Voraussetzungen sind im deutschen Recht nicht erfüllt. Ich halte es deshalb für europarechtlich unabdingbar, dass entweder die Meldepflicht oder ein betrieblicher Datenschutzbeauftragter verbindlich vorgesehen wird.

Es erscheint bereits fraglich, ob der bisherige § 4d Abs. 3 BDSG den europarechtlichen Anforderungen genügt hat. Die Ausweitung dieser Ausnahme steht aber mit Sicherheit nicht mehr mit der Datenschutzrichtlinie im Einklang. Die Europäische Kommission hat deswegen bereits im November 2006 gegenüber der Bundesrepublik Deutschland Bedenken geäußert und um Stellungnahme gebeten, auch zu der Frage, ob und wie die Datenschutzkontrollbehörden in Deutschland zu diesen Änderungen angehört worden sind.

Eine solche Beteiligung meiner Dienststelle hat es – entgegen der Gemeinsamen Geschäftsordnung der Bundesregierung – nicht gegeben, obwohl hier einschneidende Veränderungen des Datenschutzrechts vorgenommen worden sind. Dies bedauere ich um so mehr, als ich damit keine Möglichkeiten hatte, Alternativen vorzuschlagen und zu diskutieren, die unter Bewahrung des Prinzips der betriebsinternen Datenschutzkontrolle Unternehmen und

selbständig Tätige mit nur wenigen Mitarbeitern entlastet hätten. Hier wäre nicht nur daran zu denken gewesen, die Möglichkeit zur Bestellung externer Datenschutzbeauftragter auszubauen und rechtlich weiter abzusichern. Vielmehr wäre auch zu überlegen, ob nicht in den berufsständischen Organisationen und Verbänden, wie etwa den Handwerksinnungen, Kammern und Berufsverbänden für die jeweiligen Mitglieder betriebliche Datenschutzbeauftragte vorgesehen werden könnten, die dann kompetent und fachspezifisch die interne Datenschutzberatung und -kontrolle für ihre Mitglieder auf deren Wunsch hin durchführen.

Faktisch läuft die Gesetzesänderung auf eine Reduzierung des Datenschutzes in dem entsprechenden Bereich hinaus. Formal sind zwar nur die Meldepflicht und die Bestellpflicht für betriebliche Datenschutzbeauftragte entfallen, die rechtlichen Datenschutzanforderungen aber bestehen geblieben. Die Leitung der verantwortlichen Stelle muss nun selbst sicherstellen, was nach dem Gesetz Aufgabe des betrieblichen Datenschutzbeauftragten war, wie der während der parlamentarischen Beratung neu eingefügte § 4f Abs. 2a BDSG ausdrücklich bestimmt. Dies ist aber dann keine Entlastung, sondern eher eine zusätzliche Belastung der Verantwortlichen. Es ist deswegen zu erwarten, dass die Änderung des Gesetzes dahingehend missverstanden wird, die datenschutzrechtlichen Anforderungen seien für die betroffenen Klein- und Kleinstbetriebe reduziert worden, denn entsprechende Defizite können in der Regel durch externe Kontrolle der Aufsichtsbehörden nicht identifiziert und ggf. sanktioniert werden.

Dabei setzt aber gerade der Einsatz moderner Technologien, z. B. beim elektronischen Zahlungsverkehr, beim Einsatz von Kundenkarten und künftig von Gesundheitskarte und elektronischem Ausweis das Vertrauen der Nutzer in eine datenschutzkonforme Ausgestaltung und in die Einhaltung des Datenschutzrechts bei den entsprechenden Stellen voraus. Die Reduktion der internen Datenschutzkontrolle könnte sich deswegen im Hinblick auf Einführung und Ausbau der neuen Technologien als kontraproduktiv erweisen.

## 2.4 Datenschutzaudit – Regelung dringend geboten

*Keine Bewegung beim Auditgesetz, eine Chance für modernen Datenschutz bleibt weiter ungenutzt.*

Dass es ein bundesweit gültiges Datenschutzaudit geben soll, hatte der Deutsche Bundestag bereits im Jahre 2001 beschlossen und deswegen mit der Novelle des Bundesdatenschutzgesetzes vom 18. Mai 2001 (BGBl. I S. 904) § 9a in das BDSG eingefügt (vgl. 19. TB Nr. 3.2.1). Nur das Wie, d. h. die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter sollte noch durch ein besonderes Gesetz geregelt werden (§ 9a Satz 2 BDSG). Dabei ist es bis heute geblieben.

Über die Bedeutung des Audits für einen modernen, zukunftsorientierten Datenschutz und die Gefahr, der eingetretene Stillstand könne diesen wichtigen Ansatz entwerten, habe ich bereits mehrfach berichtet (19. TB Nr. 3.2.1; 20. TB Nr. 2.2). Obwohl der Deutsche Bundestag in seiner Entschließung zu meinem 19. Tätigkeitsbericht vom 17. Februar 2005 (Bundestagsdrucksache 15/4597; vgl. Kasten zu Nr. 2.4) mit großer Mehrheit die Bundesregierung aufgefordert hat, noch in der laufenden Legislaturperiode ein Ausführungsgesetz zu § 9a BDSG vorzulegen, gibt es bislang noch nicht einmal einen Referentenentwurf oder auch nur ein Eckpunktepapier für eine mögliche Regelung. Auch eine Initiative aus dem parlamentarischen Raum, von der ich in meinem 20. TB (a. a. O.) berichtet hatte, ist offensichtlich nicht weiterverfolgt worden.

Kasten zu Nr. 2.4

**Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597:**

„...

2. Der Deutsche Bundestag erwartet, dass die Bundesregierung noch in dieser Legislaturperiode ein Ausführungsgesetz zu § 9a des Bundesdatenschutzgesetzes vorlegt, damit dieses wichtige Element der jüngsten Novellierung nicht weiter leer läuft. Dabei ist einer möglichst unbürokratischen Lösung der Vorzug zu geben, die sich an den realen Interessen der Anbieter und Verbraucher orientiert (19. TB Nr. 3.2.1).

..."

Dieses jahrelange Zögern, ein im Grundsatz bereits vom Parlament beschlossenes Verfahren auch praktisch umzusetzen, bleibt unverständlich. Verwaltungsmodernisierung, Effizienzsteigerung, Entbürokratisierung sind heute Leitlinien des politischen und gesetzgeberischen Handelns. Das Datenschutzaudit würde sich in solche Konzepte nahtlos einfügen, weil es den Datenschutz bereits in die Konzeption von Verfahren und Produkten einbezieht und datenschutzfreundliches Verhalten wirtschaftlich belohnt. Damit könnte es zu einem wichtigen Element der Selbstregulierung und des wirksamen Verbraucherschutzes werden, ohne dass es hierfür neuer staatlicher Bürokratie bedürfte. Es gibt bereits eine Vielzahl von Modellen und Kriterien für die an ein Audit zu stellenden Anforderungen, für das Vergabeverfahren und für die Auswahl und Bestellung von Gutachtern, an die angeknüpft werden könnte, um rasch und effizient ein unbürokratisches Datenschutzaudit zu schaffen. Auch die Nachfrage in der Wirtschaft hiernach ist groß, insbesondere in den Bereichen IT und Internet. Dies belegen Erfahrungen auf Landesebene, wo es für die Verwendung in der Landesverwaltung ein solches Audit bereits gibt. Auch bei mir wird aus der Wirtschaft immer wieder nachgefragt, wann endlich mit einem Datenschutzaudit nach § 9a BDSG gerechnet werden könne.

Es fehlt also nicht am Bedarf für ein solches Audit und an Ideen und Lösungsmöglichkeiten für seine Umsetzung, sondern allein am Willen der Bundesregierung, hier einen Schritt zur Modernisierung des Datenschutzes zu tun.

## 2.5 „Outsourcing“ in der Verwaltung – auch ein Problem des Datenschutzes

*Auch in der Bundesverwaltung erledigen die einzelnen Dienststellen schon lange nicht mehr alle ihre Aufgaben selbst. Zusammenfassungen von Querschnittsaufgaben, behördenübergreifende Kooperation, gemeinsame eGovernment-Projekte und Verlagerung von Teilaufgaben auf private Unternehmen nehmen stetig zu. Sind davon personenbezogene Daten betroffen, wird dies auch zum Problem für den Datenschutz. Nicht immer hilft § 11 BDSG weiter.*

Kostendruck, Rationalisierung der Arbeitsabläufe, Effizienzsteigerung und Nutzung moderner Technologien haben zur Konsequenz, dass immer mehr Verwaltungen dazu übergehen, einen Teil ihrer bisherigen Tätigkeiten nicht mehr selbst vorzunehmen, sondern auf andere öffentliche Stellen oder auch private Anbieter zu übertragen, was häufig mit dem etwas schillernden Begriff „Outsourcing“ umschrieben wird. So werden auch in der Bundesverwaltung z. B. bereits private Callcenter beschäftigt, ganze Poststellen „privatisiert“ oder der E-Mail-Verkehr mit den Bürgerinnen und Bürgern über private Anbieter abgewickelt, ohne dass dies nach außen transparent wäre. Ist hiervon auch das Erheben und Verarbeiten personenbezogener Daten betroffen, sind solche Vorgänge auch datenschutzrechtlich relevant.

Aus Sicht des Datenschutzes unproblematisch sind in der Regel die Fälle, in denen bestimmte Aufgaben durch Gesetz oder im Wege der Organisationsgewalt der Bundesregierung oder der einzelnen Ressorts von einer Behörde auf eine andere übertragen werden, z. B. um die Bearbeitung gleich gelagerter Vorgänge auf eine Stelle zu konzentrieren. Grundsätzlich ist die Zulässigkeit der Datenverarbeitung mit der Erfüllung der zugrunde liegenden Aufgabe verbunden. Kommt es zu einer Zuständigkeitsverlagerung bei der Aufgabe, verliert die bisherige Stelle ihre Berechtigung zur entsprechenden Datenverarbeitung und die neue Stelle erwirbt sie zusammen mit der Zuständigkeit für die Aufgabe. Die entsprechenden Datenbestände bei der bisherigen Stelle sind, soweit für die künftige Aufgabenerfüllung erforderlich, nach den einschlägigen Vorschriften an die neue Stelle zu übermitteln und im Übrigen zu löschen.

Problematisch wird es, wenn einer Aufgabenverlagerung zwischen öffentlichen Stellen keine entsprechenden Organisationsakte zugrunde liegen oder private Anbieter auf vertraglicher Grundlage bestimmte Aufgaben übernehmen. Hier wird in der Regel dann auf § 11 BDSG verwiesen und der jeweilige Vorgang als Datenverarbeitung im Auftrag qualifiziert, da dann keine datenschutzrechtlich relevante Übermittlung der entsprechenden personenbezogenen Daten vorliegt und die gesetzlichen Voraussetzungen hierfür deswegen auch nicht eingehalten werden müssen. Dies führt zu einer Überstrapazierung des § 11 BDSG weit über seinen tatsächlichen Regelungsgehalt hinaus. Nach Wortlaut, Entstehungsgeschichte und Zweck regelt diese Norm nur die Fälle, in denen lediglich die (rein technische) Abwicklung der Datenverarbeitung auf einen Dritten übertragen wird, die inhaltliche Aufgabenerfüllung aber in vollem Umfang beim Auftraggeber verbleibt, der deswegen die datenschutzrechtliche Verantwortung auch weiterhin tragen soll. Immer dann, wenn neben der reinen Datenverarbeitung auch inhaltliche (Teil-)Aufgaben übertragen werden, etwa Beantwortung von Bürgeranfragen mit vorgegebenen Textbausteinen, kann § 11 BDSG allein hierfür keine rechtliche Grundlage sein, da es sich hierbei keinesfalls um eine allgemeine Rechtsgrundlage für Aufgabenübertragungen handelt. In der Fachliteratur wird deswegen zwischen zulässiger Auftragsdatenverarbeitung und nicht mehr durch § 11 BDSG gedeckter Funktionsübertragung unterschieden, in der Praxis führt dies aber zu unübersehbaren Abgrenzungsschwierigkeiten.

Deswegen hat der Arbeitskreis eGovernment der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Arbeitsgruppe unter meiner Leitung eingesetzt, die Lösungsmöglichkeiten erarbeiten soll, da Outsourcing und behördenübergreifende Projekte im Zuge der Verwaltungsmodernisierung und des eGovernment immer wichtiger werden. Konkrete Ergebnisse lagen bis Redaktionsschluss noch nicht vor. Ich werde aber im kommenden Berichtszeitraum diesen Fragen meine besondere Aufmerksamkeit widmen.

## 2.6 Zusammenarbeit mit den behördlichen Datenschutzbeauftragten

*Die behördlichen Datenschutzbeauftragten wurden bei ihrer Tätigkeit durch Beratungen und einen weiteren Erfahrungsaustausch wirkungsvoll unterstützt. Dabei wurde auch die Umsetzung des Informationsfreiheitsgesetzes erörtert.*

Die bei den Dienststellen des Bundes bestellten behördlichen Datenschutzbeauftragten habe ich bei ihrer verantwortungsvollen Aufgabe, sowohl im Interesse der Bürgerinnen und Bürger als auch der Beschäftigten auf die Einhaltung datenschutzrechtlicher Vorschriften hinzuwirken, vielfach beratend unterstützt. Dies geschah zum einen in zahlreichen Einzelfällen, in denen die behördlichen Datenschutzbeauftragten von der in § 4g Abs. 1 Satz 2 BDSG geregelten Möglichkeit Gebrauch gemacht haben, sich in Zweifelsfällen an mich als zuständige Datenschutzkontrollinstitution zu wenden. Darüber hinaus habe ich den Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden fortgesetzt, weil diese Veranstaltung eine geeignete Möglichkeit bietet, Rechtsfragen und praktische Probleme vertieft und gemeinsam zu erörtern.

Einen Schwerpunkt bildete dabei das Inkrafttreten des Informationsfreiheitsgesetzes (IFG) zum 1. Januar 2006 und dessen Auswirkungen auf die Arbeit der Datenschutzbeauftragten. Auch wenn das IFG das Amt eines behördlichen Beauftragten für Informationsfreiheit nicht vorsieht, hatten die meisten obersten Bundesbehörden da-

ran gedacht, bei der Ausführung des IFG auch die behördlichen Datenschutzbeauftragten mit Aufgaben zu betrauen. Deren Einbindung erscheint mir vor allem in den Fällen sinnvoll, in denen vom Zugang zu amtlichen Informationen bzw. von der Einsicht in Verwaltungsvorgänge personenbezogene Daten betroffen sind.

Weitere Themen waren die datenschutzrechtlichen Probleme bei der Verlagerung von Tätigkeiten auf private Unternehmen, die Videoüberwachung am Arbeitsplatz, die Auswertung des dienstlichen Telekommunikations- und E-Mail-Verkehrs und Dokumentenmanagementsysteme im Bereich der Personaldatenverarbeitung. Ein besonderer Punkt war auch die Vorstellung des von der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2005 verabschiedeten Prüfkatalogs zur Datenschutzvereinbarkeit von Gesetzen und Verordnungen, mit dessen Hilfe die Vollständigkeit datenschutzrechtlicher Regelungen in Rechtsvorschriften erreicht werden soll.

Erfreulicherweise konnte ich den Datenschutzbeauftragten eine weitere für ihr Amt bedeutsame Information mitteilen. In meinem 20. TB (Nr. 2.4) hatte ich moniert, dass die behördlichen Datenschutzbeauftragten mangels ausreichender Freistellung ihre gesetzlichen Aufgaben oft nicht optimal erfüllen können, und eine adäquate gesetzliche Freistellungsregelung gefordert. Die Bundesregierung hat inzwischen in einer Stellungnahme gegenüber dem Deutschen Bundestag ausdrücklich anerkannt, dass aus der Unterstützungspflicht nach § 4f Abs. 5 BDSG auch die Pflicht zur teilweisen oder völligen Freistellung von anderen Aufgaben folge. Dies stärkt die Datenschutzbeauftragten bei ihrer verantwortungsvollen Tätigkeit.

### 2.7 Arbeitnehmerdatenschutzgesetz

*Es fehlt weiter an konkreten Initiativen sowohl auf nationaler als auch auf europäischer Ebene, Vorschriften zum Schutz von Arbeitnehmerinnen und Arbeitnehmern zu schaffen. Aufgrund der technischen Entwicklung und der aktuellen Veränderungen in der Arbeitswelt ist dies dringender denn je.*

Obwohl auch der Deutsche Bundestag bereits mehrfach an die Bundesregierung appelliert hat, einen Gesetzentwurf zum Arbeitnehmerdatenschutz vorzulegen (vgl. 20. TB Nr. 2.5 und Nr. 10.1), hat es keine entsprechenden gesetzgeberischen Initiativen im Berichtszeitraum gegeben. Wegen fehlender klarer Regelungen sind daher Arbeitnehmer und Arbeitgeber weiterhin im Wesentlichen darauf angewiesen, sich an der lückenhaften und im Einzelfall für die Betroffenen nur schwer zu erschließenden einschlägigen Rechtsprechung zu orientieren. Gleichzeitig kommt der elektronischen Verarbeitung von Mitarbeiterdaten im Arbeitsverhältnis eine immer größere Bedeutung zu. Dies betrifft beispielsweise die Einführung und den Betrieb von Personalverwaltungs- und -informationssystemen oder auch einen möglichen Einsatz der RFID-Technik (vgl. Nr. 4.3) am Arbeitsplatz und die damit verbundenen Risiken für die Persönlichkeitsrechte der Betroffenen.

Vor diesem Hintergrund hat auch die Bundesregierung in ihrer Stellungnahme zu meinem 20. Tätigkeitsbericht anerkannt, dass Regelungen zum Arbeitnehmerdatenschutz zur Flankierung der Informations- und Kommunikationsgesellschaft notwendig sind. Diese fehlen jedoch weiterhin. Auch das geplante Gendiagnostikgesetz, welches Regelungen für genetische Untersuchungen im Zusammenhang mit Arbeitsverhältnissen beinhalten soll (vgl. Nr. 13.2), liegt noch nicht vor.

Leider haben Überlegungen auf europäischer Ebene zur Schaffung eines Gemeinschaftsrahmens zum Arbeitnehmerdatenschutz im Berichtszeitraum noch nicht zu konkreten Ergebnissen geführt. Ich appelliere daher an die Bundesregierung, sich im Interesse eines wirkungsvollen Schutzes der personenbezogenen Daten von Arbeitnehmerinnen und Arbeitnehmern auch auf europäischer Ebene für Regelungen zum Arbeitnehmerdatenschutz einzusetzen.

### 2.8 Informationsfreiheitsgesetz in Kraft

*Endlich besteht auch auf Bundesebene freier Zugang zu Informationen und Akten der Verwaltung.*

Nach vielen Jahren intensiver Diskussion (vgl. 20. TB Nr. 2.7; 19. TB Nr. 3.4) ist das „Gesetz zur Regelung des Zugangs zu Informationen des Bundes“ vom 5. September 2005 (Informationsfreiheitsgesetz – IFG; BGBl. I S. 2722) am 1. Januar 2006 in Kraft getreten. Damit haben jetzt auch auf Bundesebene die Bürgerinnen und Bürger grundsätzlich freien Zugang zu allen Informationen und Akten der öffentlichen Stellen des Bundes, soweit nicht einer der allerdings zahlreichen Ausnahmetatbestände greift. Wenn auch der Gesetzgeber bei den Ausnahmebestimmungen übervorsichtig gewesen ist und auch sonst nicht alle Regelungen optimal erscheinen, ist dieses Gesetz doch insgesamt als wichtiger Schritt zu mehr Transparenz in der Verwaltung und größerer Bürgernähe zu begrüßen. Insbesondere auch die Abgrenzung zu den datenschutzrechtlichen Belangen der Betroffenen ist gut gelungen und hat in der Praxis bislang zu keinen Problemen geführt. Mit dem Inkrafttreten des Gesetzes wurde mir auch die Aufgabe des Bundesbeauftragten für die Informationsfreiheit übertragen, was zu entsprechenden Veränderungen in meiner Dienststelle geführt hat (s. u. Nr. 18.7). Meinen ersten Tätigkeitsbericht für den Bereich Informationsfreiheit werde ich nach Ablauf des in § 12 Abs. 3 IFG i. V. m. § 26 Abs. 1 Satz 1 BDSG gesetzlich vorgegebenen Zeitrahmens Anfang 2008 vorlegen.

## 3 Europa und Internationales

*Wie kann Datenschutz in einer globalisierten Welt gewahrt bleiben?*

Elektronische Datenströme machen nicht an Staatsgrenzen halt. Zunehmender Handel, staatliche Kooperationsvorhaben und größere persönliche Mobilität tragen ebenfalls dazu bei, dass immer mehr personenbezogene Daten international übermittelt werden. Die Globalisierung des

Informationsaustauschs erfordert internationale Standards zum Datenschutz, wie die 27. Internationale Datenschutzkonferenz in Montreux 2005 festgestellt hat (vgl. Nr. 3.5). Zugleich sind die Regierungen und Parlamente gefordert, die Rechte der Bürgerinnen und Bürger in der internationalen Informationsgesellschaft zu gewährleisten. Von der Europäischen Union ist dabei zu erwarten, dass sie weiterhin ihre Vorreiterrolle in Sachen Datenschutz wahrnimmt. Die Europäische Datenschutzrichtlinie von 1995 hat Maßstäbe gesetzt, die inzwischen in vielen Teilen der Welt akzeptiert werden. Die EU sollte daran anknüpfend für die bislang ausgesparten Bereiche ebenfalls entsprechende Vorgaben definieren und nicht etwa unter der Flagge vermeintlichen „Bürokratieabbaus“ oder eines „Kriegs gegen den Terror“ den erreichten Datenschutzstandard aushöhlen. Gerade in schwierigen und von Konflikten gekennzeichneten Lagen müssen die demokratischen Gesellschaften ihre Prinzipien bewahren. Dies gilt auch für den Datenschutz.

## 3.1 Europäische Rechtsentwicklung

*Auch während der deutschen EU-Ratspräsidentschaft wird der Datenschutz ein wichtiges Thema sein.*

Im Mai 2005 haben der Bundestag und der Bundesrat jeweils mit großen Mehrheiten den Vertrag über eine Verfassung für Europa vom 29. Oktober 2004 ratifiziert. Bekanntlich ist der europäische Verfassungsprozess danach ins Stocken geraten, nachdem der Entwurf bei Volksabstimmungen in Frankreich und in den Niederlanden keine Zustimmung gefunden hatte. Die Zukunft der Europäischen Verfassung hat auch für den Datenschutz große Bedeutung, denn sie garantiert in den Artikeln I-51 und II-68 ausdrücklich das Grundrecht auf den Schutz personenbezogener Daten. Sowohl das Auskunftsrecht der Betroffenen als auch die unabhängige Datenschutzkontrolle werden auf europäischer Ebene als fundamentale Prinzipien einer freiheitlichen und demokratischen Verfassungsordnung festgeschrieben. Die zügige Fortsetzung und ein erfolgreicher Abschluss des Verfassungsprozesses ist auch deshalb von besonderer datenschutzrechtlicher Bedeutung, weil die Verfassung wichtige Anstöße auch in den Bereichen gibt, die von der europäischen Datenschutzrichtlinie bislang nicht erfasst werden. Wenn Polizei- und Strafverfolgungsbehörden intensiver zusammenarbeiten und dabei auch personenbezogene Daten ohne Rücksicht auf nationale Grenzen austauschen sollen, wie dies im Haager Programm beschlossen wurde, muss auch auf diesem Gebiet der Datenschutz europäisiert werden.

Von der deutschen Ratspräsidentschaft im ersten Halbjahr 2007 erwarte ich, dass sie auf Basis des von der Europäischen Kommission vorgelegten Entwurfs die Arbeiten an einem Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, zügig vorantreibt (s. u. Nr. 3.2.1). Ein hoher, einheitlicher Datenschutzstandard wäre Ausdruck einer an den Grundrechten der inzwischen 500 Millionen Bürgerinnen und Bürger der Europäischen Union orientierten Politik. Er wäre zugleich auch ein Signal dafür, dass der im Haager Programm niedergelegte Gedanke eines Gleichgewichts von Freiheit, Sicherheit und Recht mit Leben erfüllt wird.

In diesem Zusammenhang ist darauf hinzuweisen, dass der Datenschutz in Europa weiterhin einen Schwerpunkt meiner zukünftigen Arbeit bilden wird. So werde ich im Rahmen der Präsidentschaft im Juni 2007 in Berlin ein Symposium zu diesem Thema veranstalten.

Rumänien und Bulgarien, die schon seit einigen Jahren Datenschutzgesetze haben, sind seit 1. Januar 2007 Mitglied der Europäischen Union und werden künftig als ordentliche Mitglieder an den Sitzungen der Artikel 29-Gruppe teilnehmen. Auch in europäischen Ländern außerhalb der EU wird Datenschutz immer wichtiger. Nachdem Russland im Jahre 2005 das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (vom 28. Januar 1981, Konvention 108) ratifiziert hatte, wurde im Juli 2006 vom Präsidenten das erste Gesetz zum Schutz personenbezogener Daten unterzeichnet. Das Gesetz tritt im Februar 2007 in Kraft und lehnt sich in den Definitionen an die europäische Datenschutzrichtlinie 95/46/EG an.

## 3.2 Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Europa

### 3.2.1 Schaffung eines Raums von Freiheit, Sicherheit und Recht

*Die Intensivierung der Zusammenarbeit der Sicherheitsbehörden setzt einen gemeinsamen europaweiten Datenschutzstandard voraus.*

Am 5. November 2004 verabschiedeten die Staats- und Regierungschefs der EU-Mitgliedstaaten das Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht, das Leitlinien im Bereich der Innen- und Justizpolitik für den Zeitraum 2005 bis 2010 festlegt und eine Reihe von Maßnahmen fordert, die auch aus datenschutzrechtlicher Sicht von großer Bedeutung sind. So soll sich der Austausch strafverfolgungsrelevanter Informationen mit Wirkung vom 1. Januar 2008 nach dem Grundsatz der Verfügbarkeit richten, allerdings nur, wenn ein gemeinsamer Datenschutzstandard in den Mitgliedstaaten der EU gilt, der die Integrität und Vertraulichkeit der auf diese Weise ausgetauschten Daten sowie eine wirkungsvolle Datenschutzkontrolle gewährleistet. Die Kommission hat daraufhin im Oktober 2005 Entwürfe eines Rahmenbeschlusses über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit und eines Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, vorgelegt.

**Rahmenbeschlussvorschlag über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit**

Der Vorschlag enthält sehr weit reichende Vorgaben zum grenzüberschreitenden Informationsaustausch. Insbesondere verpflichtet er die Mitgliedstaaten, für Behörden in anderen EU-Mitgliedstaaten Informationen bereitzustellen. Zudem ist ein gegenseitiger Zugriff im automatisierten Verfahren auf Datenbanken vorgesehen. Damit geht der Rahmenbeschlussvorschlag erheblich über die Regelungen des „Prümer Vertrages“ (s. u. Nr. 3.2.2) hinaus.

Ich habe angeregt, auf den gegenseitigen Zugriff im automatisierten Verfahren zumindest bei den Fingerabdruckdaten und den DNA-Daten zu verzichten, denn ich halte es für problematisch, dass der Vorschlag alle Arten von Informationen, die in seinem Anhang aufgelistet sind, undifferenziert denselben Kriterien der Verfügbarkeit unterwirft, obwohl z. B. DNA-Daten beträchtlich sensibler sind als Daten aus Personenstandsregistern. Im Übrigen würde die Einrichtung des Online-Zugriffs auf Datenbanken in anderen Ländern die volle Anerkennung des Gegenseitigkeitsprinzips durch alle EU-Mitgliedstaaten voraussetzen, was angesichts der unterschiedlichen strafrechtlichen und strafprozessualen Regelungen nicht hinzunehmen wäre. Ein unmittelbarer Zugriff sollte daher nur auf Indexdateien zugelassen werden. Andernfalls müsste der Rahmenbeschluss zumindest eine bestimmte Relevanzschwelle enthalten. Auch in Deutschland haben die Polizeien des Bundes und der Länder nur auf solche Daten anderer Polizeibehörden unmittelbaren Zugriff, die eine bestimmte Erheblichkeitsstufe erreichen.

Der Vorschlag der EU-Kommission greift erheblich in die Rechte der Unionsbürger ein, denn es macht datenschutzrechtlich einen Unterschied, ob personenbezogene Daten nur auf nationaler Ebene oder EU-weit übermittelt werden, wobei insbesondere beim Polizei-, Straf- bzw. Strafverfahrensrecht unterschiedliche Regelungen in den EU-Mitgliedstaaten gelten. Ich halte es daher – in Übereinstimmung mit den Datenschutzaufsichtsbehörden der übrigen EU-Mitgliedstaaten und mit den Landesbeauftragten für den Datenschutz – für unabdingbar, dass die Intensivierung des grenzüberschreitenden Austausches personenbezogener Daten zwischen Polizei- und Justizbehörden in Strafsachen einen gleichermaßen hohen Datenschutzstandard in den EU-Mitgliedstaaten bezüglich der personenbezogenen Datenerhebung und -verarbeitung bei den Polizei- und Strafverfolgungsbehörden erfordert.

**Datenschutz im Bereich der sog. Dritten Säule der EU**

Ein allgemein verbindlicher hoher Datenschutzstandard im Bereich der zwischenstaatlichen Zusammenarbeit der Mitgliedstaaten in den Bereichen Polizei und Justiz existiert derzeit nicht.

Die Datenschutzrichtlinie (95/46/EG) ist nicht auf Datenverarbeitung betreffend die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich, also die 3. Säule, anwendbar. Dies hat auch der Europäische Gerichtshof mit seiner Entscheidung bestätigt, in der er die Regelungen zur Übermittlung von Fluggastdaten in die USA für nichtig erklärt hat (s. u. Nr. 3.3.2). Auch die Datenschutzkonvention 108 des Europarates von 1981 sowie die Grundsätze der Empfehlung R (87) 15 des Ministerkomitees des Europarats für die Nutzung personenbezogener Daten im Polizeibereich sind zu allgemein gehalten, um den Anforderungen eines datenschutzkonformen Informationsaustausches zwischen den EU-Staaten Rechnung zu tragen. Eine datenschutzrechtliche Regelungslücke in der 3. Säule hat auch der Europäische Rat gesehen, als er das Haager Programm verabschiedete; denn er hat nicht nur für einen grenzüberschreitenden Austausch personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen plädiert, sondern die Kommission auch aufgefordert, zugleich mit den Vorschlägen zum Informationsaustausch auch die notwendigen Regelungen zum Datenschutz zu schaffen.

Die Datenschutzbeauftragten der EU-Mitgliedstaaten haben daher den Kommissionsvorschlag eines Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, grundsätzlich begrüßt. Hierbei hat sich die Kommission entsprechend einer Forderung der Europäischen Datenschutzkonferenz an der EG-Datenschutzrichtlinie orientiert. Die Datenschutzregelungen für die 3. Säule sollen – soweit möglich – in Übereinstimmung mit dem geltenden Datenschutzniveau in der 1. Säule entwickelt werden. Ein konsistentes Datenschutzniveau in den verschiedenen Bereichen dient nicht nur dem Grundrechtsschutz der Bürgerinnen und Bürger, sondern erleichtert auch die Anwendbarkeit der entsprechenden Regelungen. Selbstverständlich werden auch nach Inkrafttreten eines Rahmenbeschlusses für den Datenschutz in der 3. Säule bestimmte bereichsspezifische Regelungen erforderlich bleiben. Diese müssen jedoch gemeinsamen grundlegenden Anforderungen entsprechen und im Hinblick auf besondere Risiken für den Schutz sensibler personenbezogener Daten zusätzliche Schutzvorkehrungen vorsehen.

Nach den bisherigen Beratungen im Rat lässt sich noch nicht vorhersagen, mit welchem Ergebnis die Verhandlungen über den Vorschlag schließen werden. Ende 2006 drängte sich der Eindruck auf, die Beratungen seien eher ins Stocken geraten. Nach meinen Informationen besteht bei einigen Regierungen der EU-Mitgliedstaaten sogar Skepsis, ob ein entsprechender Rechtsakt überhaupt notwendig ist. Zudem wird offenbar befürchtet, ein entsprechender Rahmenbeschluss errichte zusätzliche bürokratische Hürden. Diese Befürchtungen sind ohne Grund. Ein Rahmenbeschluss zum Datenschutz wirkt nicht bürokratisch, sondern trägt zur Vereinheitlichung des Verfahrens bei und fördert das beim grenzüberschreitenden Informationsaustausch erforderliche gegenseitige Vertrauen, indem er einheitliche Standards vorgibt, wie die personenbezogenen Daten durch die Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten unter Wahrung des informationellen Selbstbestimmungsrechts der Betroffenen erhoben und verarbeitet werden. Der grenzüber-

schreitende Datenaustausch würde durch einen Rahmenbeschluss zum Datenschutz erleichtert. Hindernisse für die Verwirklichung des Informationsaustausches ergeben sich vielmehr aus dem Fehlen harmonisierter Rechtsvorschriften in den EU-Mitgliedstaaten, insbesondere auf dem Gebiet des Strafrechts und des Strafverfahrensrechts. Zudem ist ein angemessener Ausgleich zu den bestehenden und künftigen Formen des Informationsaustausches zwischen den Strafverfolgungsbehörden in der Europäischen Union zu verankern, um das derzeit teilweise unausgewogene Verhältnis zwischen der Gewährleistung von Sicherheit für die EU-Bürgerinnen und -Bürger und der Wahrung ihrer Freiheitsrechte in einem „Raum der Freiheit, der Sicherheit und des Rechts“ wieder in das richtige Maß zu bringen. Die Frage nach einem angemessenen Verhältnis zwischen diesen beiden Komponenten muss auch auf europäischer Ebene befriedigend gelöst werden.

Der Rahmenbeschluss sollte daher die gesamte Informationsverarbeitung der Polizei- und Strafverfolgungsbehörden umfassen. Ziel muss ein weitgehend einheitlicher Datenschutzstandard für die polizeiliche und justizielle Informationsverarbeitung in der gesamten EU sein. Insbesondere die tragenden Grundsätze der Zweckbindung, der Datenqualität und der Erforderlichkeit sind dabei zu wahren. Auch die Rechte des Betroffenen müssen auf möglichst einheitlicher Grundlage gewährleistet sein. So muss das Recht auf Auskunft die Regel bilden und darf nicht durch zu viele Ausnahmetatbestände ausgehöhlt werden. Neben einer unabhängigen Datenschutzkontrolle in jedem Mitgliedstaat muss auch eine unabhängige Beratung des Rates durch die Vertreter der nationalen Datenschutzkontrollstellen sichergestellt werden.

Ich sehe keine Alternative zur Schaffung eines hohen und harmonisierten Datenschutzstandards in der 3. Säule der EU. Dies ist auch eine logische Konsequenz des Haager Programms. Aus Sicht des Persönlichkeitsschutzes enthält dieses Programm den Auftrag, die bei der polizeilichen und justiziellen Zusammenarbeit in Europa noch bestehende datenschutzrechtliche Regelungslücke zu schließen. Hierauf hat auch die Europäische Datenschutzkonferenz hingewiesen, zuletzt mit ihrer Londoner Erklärung vom 2. November 2006 (s. Kasten zu Nr. 3.2.1).

Ich sehe hier auch eine Herausforderung für das Europäische Parlament sowie die nationalen Volksvertretungen, auf die Regierungen der EU-Mitgliedstaaten entsprechend Einfluss zu nehmen. Es darf nicht dazu kommen, dass immer neue Datenverarbeitungsbefugnisse für die Sicherheitsbehörden mit noch tieferen Einschnitten in die Grundrechte beschlossen werden, ohne dass die Grundrechte der in der EU lebenden Bürgerinnen und Bürger mindestens in gleicher Weise gestärkt und geschützt werden. Insbesondere das Grundrecht auf Datenschutz nach Artikel 8 der Charta der Grundrechte in der EU ist zu beachten. Ich hoffe daher, dass die Beratungen des Rahmenbeschlussvorschlages unter der deutschen Ratspräsidentschaft im ersten Halbjahr 2007 zu einem erfolgreichen Abschluss gebracht werden.

Kasten zu Nr. 3.2.1

**Erklärung verabschiedet von den Europäischen Datenschutzbehörden in London am 2. November 2006**

Der Ausbau des grenzüberschreitenden Informationsaustausches und die vorbehaltlich des Grundsatzes der Verfügbarkeit erfolgende Weitergabe von in nationalen Dateien gespeicherten Daten im Rahmen der Zusammenarbeit zwischen den Polizei- und Justizbehörden auf EU-Ebene stehen im Mittelpunkt der Diskussionen in Europa. In diesem Zusammenhang haben die Europäischen Datenschutzbehörden bereits wiederholt hervorgehoben, dass angesichts der Tatsache, dass die Union verpflichtet ist, die Menschenrechte und Grundfreiheiten zu achten, Initiativen zur Verbesserung der Kriminalitätsbekämpfung in der EU, wie z. B. der Grundsatz der Verfügbarkeit, nur auf der Grundlage eines angemessenen Systems von Datenschutzmaßnahmen eingeführt werden sollten, die ein hohes und vergleichbares Datenschutzniveau gewährleisten, das den Standards der Ersten Säule entspricht.

Die Europäischen Datenschutzbehörden fordern die Mitgliedstaaten auf, die bürgerlichen Freiheiten der in der EU lebenden Bürger zu respektieren und zu stärken und ein angemessenes System von Datenschutzmaßnahmen aufzubauen, das ein hohes und vergleichbares Datenschutzniveau für die gesamte Datenverarbeitung im Bereich der Kriminalitätsbekämpfung gewährleistet.

Es gibt keine Alternative zum Aufbau eines hohen und harmonisierten Datenschutzstandards im Rahmen der Dritten Säule der EU. Dies ist eine logische Konsequenz aus dem Haager Programm, dem zu folge die Wahrung der Freiheit, der Sicherheit und des Rechts unteilbarer Bestandteil der Aufgabe der EU insgesamt ist. Einschlägige Datenschutzbestimmungen im Bereich der Kriminalitätsbekämpfung sollten so bald als möglich verabschiedet und umgesetzt werden, so dass ein angemessenes und harmonisiertes System von Datenschutzmaßnahmen geschaffen wird, die sich nicht nur auf den Datenaustausch zwischen den Mitgliedstaaten, sondern auf die gesamte Verarbeitung personenbezogener Daten im Rahmen der Kriminalitätsbekämpfung beziehen. Ein hohes Schutzniveau sollte auch für die Weitergabe von Daten an Drittstaaten und internationale Stellen gelten, die vorbehaltlich der auf der Grundlage gemeinsamer Europäischer Standards zu treffenden Feststellung eines angemessenen Datenschutzniveaus erfolgt.

Jeder andere, weniger umfassende Ansatz wäre nicht praktikabel und ungeeignet, das für eine wirksame Kooperation im Bereich der Kriminalitätsbekämpfung erforderliche Vertrauen zu schaffen.

### 3.2.2 Vertrag von Prüm

*Der Vertrag von Prüm über die grenzüberschreitende polizeiliche Zusammenarbeit ist am 27. Mai 2005 von sieben EU-Mitgliedstaaten unterzeichnet worden.*

Damit wurden die seit 2003 laufenden Verhandlungen erfolgreich abgeschlossen, die ursprünglich von den Beneluxstaaten, Österreich und Deutschland eingeleitet worden waren (vgl. 20. TB Nr. 3.3.2.3). In der Schlussphase der Verhandlungen haben sich auch Frankreich und Spanien dem Vertrag angeschlossen. Gegen Ende der Berichtsperiode haben weitere vier EU-Mitgliedstaaten ihr Interesse an einem Vertragsbeitritt bekundet, nämlich Finnland, Italien, Portugal und Slowenien. Als erste haben Österreich und Spanien, anschließend die Bundesrepublik Deutschland den Vertrag ratifiziert. Zwischen diesen Vertragsparteien ist der Vertrag am 23. November 2006 in Kraft getreten.

Anlässlich der parlamentarischen Beratungen habe ich auf einige datenschutzrechtliche Mängel in dem Vertragswerk hingewiesen, das ich im Ansatz positiv bewerte. Meine Bedenken richten sich vor allem dagegen, dass bei den Regelungen zum gegenseitigen Zugriff der Vertragsparteien auf Datenbanken der anderen Partner die Verhältnismäßigkeit nicht hinreichend beachtet wird; deshalb habe ich insbesondere beim Zugriff auf die DNA-Analyse-Dateien eine Erheblichkeitsschwelle verlangt, die den Zugriff auf die Aufklärung schwerer Straftaten begrenzt. Leider wurde dies nicht aufgegriffen. Es ist zu wünschen, dass die Anwendung des Vertrages langfristig zu einer Angleichung strafrechtlicher und strafverfahrensrechtlicher Regelungen und Methoden in den Mitgliedstaaten beiträgt.

Bevor der im Vertrag vorgesehene gestufte Informationsaustausch in Wirkbetrieb geht, bedarf es noch einer Angleichung der Informationstechnik bei den teilnehmenden Behörden und ergänzender Durchführungsvereinbarungen (Artikel 44 des Vertrages). Hierzu sind mehrere Arbeitsgruppen eingerichtet worden. Die Durchführungsvereinbarung wurde am 5. Dezember 2006 von den Vertragsparteien unterzeichnet. Leider wurden die von den Datenschutzbeauftragten der Vertragspartner im Juli 2006 in Bonn geforderten datenschutzrechtlichen Ergänzungen in der Durchführungsvereinbarung nicht berücksichtigt. Österreich und Deutschland wollten anschließend mit dem elektronischen Austausch von DNA-Daten beginnen.

Der Vertrag macht eine erhebliche Intensivierung der Zusammenarbeit der unabhängigen Datenschutzbehörden der Vertragsparteien erforderlich, die laut Vertrag die rechtliche Kontrolle der Übermittlung oder des Empfangs personenbezogener Daten haben. Hierfür sollen ihnen Protokoll- und Dokumentationsdaten zur Verfügung stehen. Nach der Vertragskonzeption ist jede Übermittlung und jeder automatisierte Abruf personenbezogener Daten durch die anfragende und die dateiführende Stelle zu protokollieren. Dies ist Kernbestandteil eines umfangreichen Kapitels zum Datenschutz (vgl. Kasten zu Nr. 3.2.2).

Über die Umsetzung des Vertrages entscheidet gemäß Artikel 43 ein Ministerkomitee. Leider wurde mein Vorschlag, vor dieser Entscheidung noch die unabhängigen Datenschutzbeauftragten zur Beurteilung der datenschutzrechtlichen Vorkehrungen anzuhören, nicht aufgegriffen. Um so wichtiger ist es, dass der Vertrag von Anfang an auch einer datenschutzrechtlichen Evaluierung unterzogen wird, um die notwendige Balance zur Sicherung der Bürgerrechte zu wahren. Hierauf werde ich mein Hauptaugenmerk richten. Sollten weitere Staaten dem Vertragswerk beitreten, stellt sich die Frage nach einer Überführung des Prümer Vertrages in das Regelwerk der Europäischen Union. Auch in diesem Zusammenhang ist auf die Bedeutung des Rahmenbeschlusses zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit verarbeitet werden, hinzuweisen (s. o. Nr. 3.2.1).

Kasten zu Nr. 3.2.2

**Wesentlicher Regelungsgehalt des Vertrages von Prüm**

Der Vertrag von Prüm dient der grenzüberschreitenden Zusammenarbeit der Vertragsparteien bei der Bekämpfung

- des Terrorismus,
- der grenzüberschreitenden Kriminalität,
- der illegalen Migration.

Zu diesen Zwecken wird der Informationsaustausch, auch personenbezogener Daten, intensiviert, u. a. durch

- gegenseitigen Zugriff auf daktyloskopische Index-Dateien im hit/no hit Verfahren,
- gegenseitigen Zugriff auf DNA-Indexdateien im hit/no hit Verfahren,
- gegenseitigen Direktzugriff auf nationale Fahrzeugregister,
- präventive Übermittlung personenbezogener Daten bei Großveranstaltungen mit grenzüberschreitendem Bezug,
- Übermittlung personenbezogener Daten zur Verhinderung terroristischer Straftaten.

Zur Wahrung der Bürgerrechte verpflichten sich die Vertragsparteien zur Einhaltung eines hohen Datenschutzstandards; dazu zählen

- einheitlicher Mindeststandard an Datenschutz,
- Zweckbindung der übermittelten Daten,
- hohe Datenqualität der übermittelten Daten,
- Dokumentation und Protokollierung der übermittelten Daten zum Zwecke der datenschutzrechtlichen Kontrolle,
- Rechte der Betroffenen, u. a. Recht auf Auskunft und Schadensersatz.

### 3.2.3 Europol

Das 1999 eingerichtete Europäische Polizeiamt, EUROPOL, soll die EU-Mitgliedstaaten bei der Bekämpfung schwerwiegender Formen der international organisierten Kriminalität unterstützen. Ziel von EUROPOL ist die Verbesserung der Zusammenarbeit der Mitgliedstaaten

bei der Verhütung und Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität. Dabei soll insbesondere der Informationsaustausch zwischen den Mitgliedstaaten durch automatisierte Informationssammlungen unterstützt werden. Inzwischen ist EUROPOL das wichtigste Instrument der europaweiten polizeilichen Zusammenarbeit. EUROPOL betreibt seit 2006 ein automatisiertes Informationssystem, in das die Daten von Mitgliedstaaten unmittelbar eingegeben werden können. Hierbei handelt es sich um Daten über Verurteilte und Beschuldigte sowie über Personen, bei denen schwerwiegende Tatsachen nach Maßgabe des nationalen Rechts die Annahme rechtfertigen, dass sie Straftaten begehen werden, für die EUROPOL zuständig ist (siehe Abbildung zu Nr. 3.2.3).

Die Einhaltung datenschutzrechtlicher Vorschriften durch EUROPOL wird von der Gemeinsamen Kontrollinstanz (GK), die mit Vertretern der Datenschutzbehörden der Mitgliedstaaten der Europäischen Union besetzt ist, kontrolliert.

### 3.2.3.1 Die Rechtsakte zur Änderung des Europol-Übereinkommens

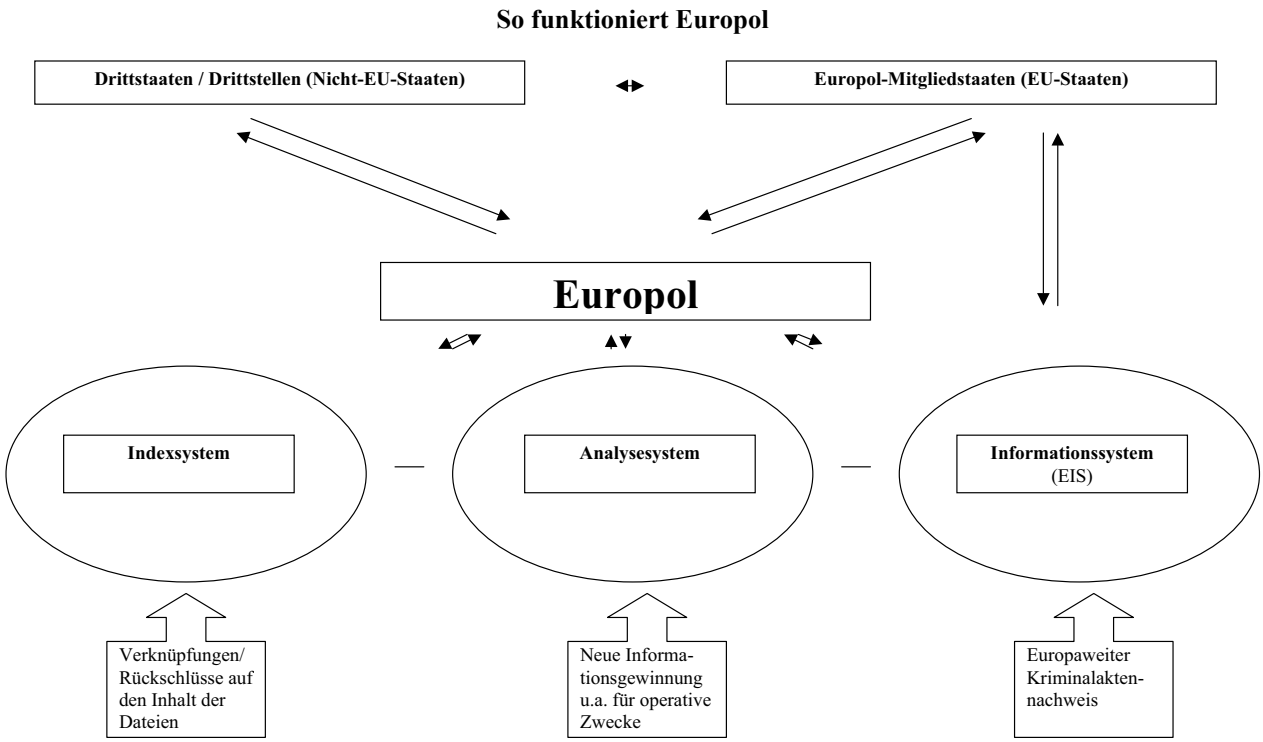
*Das Protokoll auf Vorschlag Dänemarks zur Änderung des Europol-Übereinkommens soll nunmehr im Frühjahr 2007 gemeinsam mit einem weiteren Änderungsprotokoll in Kraft treten.*

Das Schicksal der sog. Dänischen Initiative (vgl. 19. TB Nr. 16.1; s. Kasten zu Nr. 3.2.3.1), über die der Rat bereits im Dezember 2003 eine politische Grundsatzentscheidung getroffen hatte, ist ein Lehrbeispiel dafür, wie Anspruch und Wirklichkeit der polizeilichen Zusammenarbeit in Europa auseinanderklaffen. Es vergeht kein JI-Rat, auf dem nicht die zentrale Rolle von Europol bei der Bekämpfung des internationalen Terrorismus betont wird. Dies zeigt sich auch daran, dass Europol sukzessive zu einer Zentralstelle für die polizeiliche Informationsverarbeitung in der EU ausgebaut werden soll.

Im Berichtszeitraum ist das Informationssystem bei Europol (EIS)nach Artikel 7 f. der Europol-Konvention nach jahrelangen Vorbereitungen in Wirkbetrieb gegangen. Es handelt sich hierbei um einen EU-weiten Kriminalaktennachweis im Rahmen der Aufgaben gemäß Artikel 2 der Konvention. Zugriff erhalten die nationalen Zentralstellen, die nationalen Verbindungsbeamten bei Europol und besonders ermächtigte Europol-Bedienstete. Dies verschafft ihnen Kenntnis über alle laufenden Kriminalaktenvorgänge in den EU-Mitgliedstaaten mit internationalem Bezug, die noch durch weitere Falldaten ergänzt werden.

Die Unterstützungsfunktion bei der Bekämpfung der internationalen, organisierten Kriminalität soll durch Teilnahme von Europol-Bediensteten in gemeinsamen Ermittlungsteams mit nationalen Polizeibeamten ausgebaut werden. Die Ermittlungshoheit bleibt jedoch bei den nationalen Stellen. Ferner soll Europol – ähnlich wie

Abbildung 1 (zu Nr. 3.2.3)



Eurojust – umfassenden Zugriff auf das Schengener Informationssystem (vgl. Nr. 3.2.4.1), auf das Visa-Informationssystem (vgl. Nr. 3.2.7) und auf den EURODAC-Datenbestand im Rahmen seiner Zuständigkeit erhalten. Angesichts der beschränkten Kompetenzen von Europol bei der internationalen Verbrechensbekämpfung hat u. a. die GK von Europol darauf hingewiesen, dass ein solcher Direktzugriff auf Systeme, die in erster Linie Verwaltungszwecken dienen, wie das geplante VIS und EURODAC, mit dem Zweckbindungsprinzip nur schwer vereinbar ist.

Kasten zu Nr. 3.2.3.1

**Auszug 19. TB Nr. 16.1**

Drei Jahre nach Aufnahme des Wirkbetriebs bei Europol am 1. Juli 1999 zeichnet sich im Rat der Wunsch nach einer Änderung des Europol-Übereinkommens vom 26. Juli 1995 ab. Dies fand Eingang in eine Initiative des Königreichs Dänemark für einen Rechtsakt des Rates zur Erstellung eines Protokolls zur Änderung des Europol-Übereinkommens. Der Entwurf enthält zahlreiche Änderungen des Vertrages, beginnend mit einer erweiterten Zielbeschreibung von Europol (Artikel 2) bis zu einer Zusammenarbeitsregelung mit Eurojust (Artikel 42). Etliche dieser Vorschläge sind auch von datenschutzrechtlicher Relevanz. Die gemeinsame Kontrollinstanz hat am 3. Oktober 2002 eine umfassende Stellungnahme zu der dänischen Initiative abgegeben, die sowohl dem Rat als auch dem Europäischen Parlament zugänglich gemacht wurde. Unbeschadet dieser Stellungnahme, auf die im Tätigkeitsbericht der gemeinsamen Kontrollinstanz eingegangen wird, habe ich mich gegenüber der Bundesregierung ebenfalls zu dem Entwurf einer Stellungnahme der deutschen Delegation in den Ratsgremien geäußert. Dabei habe ich darauf hingewiesen, dass es bei der Fortschreibung des Europol-Übereinkommens nicht nur um die Interessen Europols und der Mitgliedsstaaten, ein effizientes Europäisches Polizeiamt und eine verbesserte Kooperation mit den Mitgliedsstaaten zu schaffen, sondern auch um den Schutz des Persönlichkeitsrechts der Betroffenen geht. Die Initiative enthält jedoch auch Vorschläge, die aus datenschutzrechtlicher Sicht zu begrüßen sind. Dazu zählen eine Änderung des Verfahrens bei der Protokollierung von Abrufen zum Zweck einer besseren Kontrolle der Zugriffe auf das Europol-Informationssystem, des Weiteren die Anwendung der datenschutzrechtlichen Grundsätze auf die Informationsverarbeitung, auch soweit diese in Akten erfolgt. Hingegen sind aus datenschutzrechtlicher Sicht erweiterte Zugriffsrecht auf die in Artikel 10 geregelten vertraulichen Analysedateien bei Europol kritisch zu sehen. Bei Redaktionsschluss hatte der Rat noch keine abschließende Entscheidung über die dänische Initiative getroffen. Auch die Stellungnahme des Europäischen Parlaments zu dem Projekt lag zu diesem Zeitpunkt noch nicht vor.

#### 3.2.3.2 Die Gemeinsame Kontrollinstanz von Europol

Die GK Europol (vgl. 18. TB Nr. 11.11) nimmt ihre Kontroll- und Beratungsfunktion gegenüber Europol zunehmend proaktiv wahr. So wurden drei Kontrollbesuche in der Europol-Zentrale durchgeführt, u. a. zur Kontrolle des neuen Informationssystems (EIS). Mit Europol bzw. dessen Verwaltungsrat wurden intensive Verhandlungen über Modifizierungen beim Erlass von Errichtungsanordnungen (Artikel 12) und zu der Problematik des Informationsaustausches zwischen Europol und Drittstaaten geführt, insbesondere wenn in Drittstaaten kein angemessenes Datenschutzniveau besteht, wie dies Artikel 18 der Konvention für den Austausch personenbezogener Daten vorschreibt. Dieser Schutzmechanismus ist jedoch wesentlich für die Wahrung der Freiheitsrechte.

Gegen Ende des Berichtszeitraums hat die GK Europol den Vorentwurf eines Ratsbeschlusses zu Europol erhalten, der im Falle seiner Annahme die Europol-Konvention als Rechtsgrundlage ablösen soll. Man erhofft sich davon ein flexibleres Rechtsinstrument, das im Zuge von Veränderungen leichter vom Rat geändert werden kann; auf nationaler Ebene müssen gegenwärtig die nationalen Parlamente zustimmen. Aus meiner Sicht wird darauf zu achten sein, dass Europol nicht durch Änderung der Rechtsgrundlage der Kontrolle des jeweiligen nationalen Gesetzgebers entgleitet; dies umso mehr, als das Europäische Parlament für Rechtsmaterien im Bereich der sog. Dritten Säule der EU nicht originär zuständig ist und die Rechtsprechung des EuGH grundsätzlich nicht für Rechtsgebiete gilt, die nicht vergemeinschaftet sind. Insbesondere das Europäische Parlament hat sich aber bisher als Garant der Bürgerrechte in der EU erwiesen.

Am 17. Oktober 2006 wurde auf Initiative der GK von Europol in Brüssel ein Symposium veranstaltet, um die Herausforderungen des Datenschutzes für Europol zu erörtern. Teilnehmer waren u. a. hochrangige Vertreter des Europäischen Parlaments, der Kommission, des Rates und unabhängige Experten. Auf der Tagung wurde die Bedeutung von Europol ebenso wie die Notwendigkeit der europaweiten Kriminalitätsbekämpfung unter ausreichender Wahrung der Grundrechte jedes Einzelnen erneut bekräftigt.

Sobald die o. g. Initiative der Kommission dem Rat zugeleitet ist, wird sich die GK Europol mit dem Dokument befassen und eine datenschutzrechtlich ausgewogene Stellungnahme erstellen.

### 3.2.4 Schengen

Heute ist es für uns selbstverständlich, mit dem Auto oder mit dem Zug von Deutschland nach Frankreich oder Italien zu reisen, ohne unterwegs an Grenzen kontrolliert zu werden. Für viele verbindet sich die Reisefreiheit in Europa mit dem Begriff „Schengen“. Das Wort steht in erster Linie für eine im gleichnamigen luxemburgischen Städtchen 1990 geschlossene Vereinbarung, das Schengener Durchführungsübereinkommen (SDÜ), mit dem der Wegfall der Binnengrenzen vereinbart wurde. Gleichzei-

tig wurde der Aufbau eines gemeinsamen Informationssystems (SIS) beschlossen, um die grenzüberschreitende Fahndung nach Personen und Sachen in den „Schengen-Staaten“ zu ermöglichen. Die Weiterentwicklung von SIS und die Nutzung der gespeicherten Daten werfen immer wieder datenschutzrechtliche Fragen auf.

#### 3.2.4.1 SIS II

*Das bisherige Schengener Informationssystem soll durch ein erweitertes System abgelöst werden. Die Rechtsgrundlagen dafür sind im Dezember 2006 vom JI-Rat und vom Europäischen Parlament verabschiedet worden.*

Das seit 1995 betriebene Schengener Informationssystem soll im Hinblick auf die Erweiterung der Europäischen Union und in Folge des technischen Fortschritts zu einem Schengener Informationssystem der zweiten Generation (SIS II) erweitert werden (20. TB Nr. 3.3.2.1). Wegen neuer Funktionalitäten und eines erweiterten Datenkranzes bedarf es hierzu neuer Rechtsgrundlagen.

Die Kommission legte am 31. Mai 2005 folgende Vorschläge hierfür vor:

- Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)
  - KOM (2005) 230 endg.
- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystem der zweiten Generation (SIS II)
  - KOM (2005) 236 endg.
- Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II)
  - KOM (2005) 237 endg.

Diese Vorschläge sollen die bisher für das SIS maßgeblichen Rechtsgrundlagen (Artikel 92 bis 118 SDÜ) ersetzen. Getrennte Rechtsgrundlagen sind notwendig, weil die Ausschreibungen im SIS teils der Dritten Säule (polizeiliche und justizielle Zusammenarbeit in Strafsachen), teils aber auch der Ersten Säule (Titel IV des EG-Vertrages) zuzurechnen sind. Nach den Vorschlägen soll die Grundkonzeption des SIS im wesentlichen beibehalten werden. Allerdings wird es in Zukunft nicht mehr von den Mitgliedstaaten betrieben. Das sog. Betriebsmanagement soll bis auf weiteres der KOM übertragen werden, bevor es auf eine Agentur übergeht. Die datenschutzrechtliche Verantwortung für die Ausschreibungen soll bei den Mitgliedstaaten bleiben.

Zur Vorbereitung der Beratungen im Rat und im Europäischen Parlament hat die Gemeinsame Kontrollinstanz von Schengen am 6. Oktober 2005 eine datenschutzrechtliche Stellungnahme abgegeben, ebenso der EDPS und die Artikel 29-Gruppe.

Die GK Schengen hat in ihrer Stellungnahme zwar begrüßt, dass den datenschutzrechtlichen Anforderungen in den Vorschlägen ein hoher Stellenwert eingeräumt wird, gleichwohl aber grundlegende Bedenken vorgebracht:

- Es sei zu befürchten, dass das SIS in Zukunft zu erweiterten Zwecken genutzt und zu einem umfassenden polizeilichen Informationssystem ausgebaut werde. Dies müsse jedoch mit den entsprechenden Änderungen der rechtlichen Schutzvorkehrungen einhergehen.
- Aus den Vorschlägen gehe die datenschutzrechtliche Verantwortung nicht eindeutig hervor. Dies sei jedoch für die Kontrolle der im System verarbeiteten Daten wichtig.
- Der dritte Problembereich betrifft die datenschutzrechtliche Überwachung des SIS II. Die bisher der Gemeinsamen Kontrollinstanz obliegenden Aufgaben der Beratung, Kontrolle und Koordinierung seien im Vorschlag nicht mehr enthalten. Dieser stelle zudem verstärkt auf die Kontrolle der Datenverarbeitung auf zentraler Ebene ab, die jedoch minimal sei. Die Überwachung der im SIS II verarbeiteten personenbezogenen Daten werde weiterhin in die Zuständigkeit der nationalen Datenschutzbeauftragten fallen. Deshalb bedürfe es weiterhin der Koordinierung.

Die Beratungen in den Europäischen Organen über die Rechtsakte waren überschattet von immer neuen Problemen bei der Ausschreibung und Entwicklung des SIS II-Projekts und zogen sich bis zum Herbst 2006 hin. Daneben galt es, viele technisch-organisatorische Probleme zu lösen. Rechtlich umstritten blieb bis zum Schluss zwischen EP und Rat u. a. noch die Frage, ob den Nachrichtendiensten ein Zugriff auf bestimmte Ausschreibungen im SIS eingeräumt werden solle. Hiergegen hatte ich mich im Hinblick auf die mangelnde Transparenz bei den Diensten und deren nicht-polizeiliche Aufgabenerfüllung im Vorfeld strikt ausgesprochen. Aufgrund des Widerspruchs des Europäischen Parlaments gegen diese Öffnung des SIS hat der Rat diesen Punkt fallen lassen, so dass der Weg für die Verabschiedung der Rechtsakte auf der Basis des Kompromissvorschlages des EP frei war. Damit sind jedoch nur die rechtlichen Grundlagen geklärt. Zu den ungeklärten Fragen zählte bis zuletzt auch die Aufnahme biometrischer Merkmale, d. h. von Fingerabdrucken, in das System. Hier einigte man sich darauf, diese Merkmale vorerst nur zur Verifizierung zu verwenden.

Technisch kann dieses Projekt, das als Ausgleich für den Wegfall der Grenzkontrollen mit den neuen Mitgliedstaaten unabdingbar ist, nach derzeitigem Stand frühestens im Verlauf des Jahres 2008 zwischen den alten Vertragsparteien in Wirkbetrieb gehen, für die neuen Mitgliedstaaten soll der Anschluss noch später realisiert werden. Da dies europapolitisch kaum vertretbar wäre, hat sich der Rat im Dezember 2006 auf ein SIS one 4All (SIS I+ für Alle) verständigt, das heißt eine Erweiterung des bisherigen SIS I+ auf die neuen Beitrittsländer ab Juli 2007, jedoch

ohne die neuen Funktionalitäten im SIS II. Sollte sich der Betrieb des SIS I+ bei den Beitrittsländern bewähren, könnte im Zeitraum Dezember 2007 bis März 2008 der Wegfall der Kontrollen an den Binnengrenzen zwischen alten und neuen EU-Staaten erfolgen. Parallel dazu wird die Entwicklung des SIS II vorangetrieben.

Bis dahin bedarf es noch einiger datenschutzrechtlicher „Flankierung“, bevor die neuen Funktionalitäten (u. a. die Verknüpfung der Ausschreibungen), erweiterte Datenkataloge (u. a. biometrische Merkmale, wie Lichtbilder und Fingerabdrucke) und erweiterte Zugriffsrechte (Europol, Eurojust) in Betrieb gehen. Ich werde – zusammen mit meinen Kollegen in den anderen Mitgliedstaaten – darauf hinwirken, dass mit dem neuen SIS II die Balance zwischen polizeilichen Fahndungserfordernissen und den Bürgerrechten gewahrt bleibt.

### 3.2.4.2 Kontrolle der Ausschreibungen nach Artikel 99 Abs. 2 des Schengener Durchführungsübereinkommens

*Die Gemeinsame Kontrollinstanz (GK) nach Artikel 115 des Schengener Durchführungsübereinkommens (SDÜ) (siehe Kasten a zu Nr. 3.2.4.2) hat in einer gemeinsamen Aktion in allen Schengen-Vertragsstaaten das Verfahren der Ausschreibungen zur verdeckten Registrierung kontrolliert.*

Kasten a zu Nr. 3.2.4.2

**Gemeinsame Kontrollinstanz**

Für die datenschutzrechtliche Kontrolle des SIS, insbesondere im Hinblick auf den Zentralcomputer in Straßburg, ist gemäß Artikel 115 SDÜ eine gemeinsame Kontrollinstanz (GK) zuständig, die sich aus je zwei Vertretern der nationalen Kontrollinstanzen zusammensetzt. Nach Inbetriebnahme des SIS am 26. März 1995 hat sich die GK am 17. Mai 1995 konstituiert. Die deutsche Delegation in dem Gremium besteht aus einem Vertreter meiner Dienststelle und dem Hessischen Landesbeauftragten für den Datenschutz für den Bereich der Länder.

Neben der Überwachung der technischen Unterstützungseinheit in Straßburg koordiniert die GK auch Kontrollen auf nationaler Ebene im Zusammenhang mit dem SIS. Sie ist ferner zuständig für Fragen der Anwendung und Auslegung im Zusammenhang mit dem SIS sowie für die Erarbeitung von Lösungsvorschlägen zu gemeinsamen Problemstellungen.

Die GK verfügt seit dem Jahr 2000 über ein eigenes Sekretariat, das beim Rat der EU angebunden ist. Das Sekretariat ist auch für die Betreuung der gemeinsamen Kontrollinstanz von Europol (s. u. Nr. 3.2.3.2) und der gemeinsamen Aufsichtsbehörde nach Artikel 18 des ZIS-Übereinkommens (s. u. Nr. 3.2.5) zuständig.

Diese Kontrolle wurde durchgeführt, weil die Anzahl der Ausschreibungen nach Artikel 99 Abs. 2 SDÜ (siehe Kasten b zu Nr. 3.2.4.2) in den Vertragsstaaten erheblich voneinander abweicht. So wurde das Ausschreibungsverfahren in einigen Vertragsstaaten überhaupt nicht genutzt, während andere Staaten über 10 000 Ausschreibungen veranlasst hatten.

Kasten b zu Nr. 3.2.4.2

**Artikel 99 Abs. 2 Schengener Durchführungsübereinkommen (SDÜ)**

(2) Eine Ausschreibung dieser Art ist zulässig zur Strafverfolgung und zur Abwehr von Gefahren für die öffentliche Sicherheit, wenn

a) konkrete Anhaltspunkte dafür vorliegen, dass der Betroffene in erheblichem Umfang außergewöhnlich schwere Straftaten plant oder begeht, oder

b) die Gesamtbeurteilung des Betroffenen, insbesondere aufgrund der bisher von ihm begangenen Straftaten, erwarten lässt, dass er auch künftig außergewöhnlich schwere Straftaten begehen wird.

Für die Bundesrepublik Deutschland wurden 1 104 Ausschreibungen vorgenommen. Da diese meistens von den einzelnen Bundesländern veranlasst waren, habe ich auch meine Länderkolleginnen und -kollegen in die Prüfung einbezogen. Bei den Kontrollbesuchen in meinem Zuständigkeitsbereich (BKA, Bundespolizei), wo nur 15 Ausschreibungen vorlagen, habe ich keine Mängel bei der Ausschreibungspraxis feststellen können. Die Entscheidungen über Ausschreibungen im Bundesbereich wurden also sehr verantwortungsbewusst herbeigeführt.

Mit einer Übersicht aller mitgeteilten Prüfungsergebnisse der Länder habe ich die LfD über die wesentlichen Ergebnisse der Kontrollen informiert, ebenso die GK im Frühsommer 2006 über die zu diesem Zeitpunkt vorliegenden Kontrollergebnisse. Die GK hat einen Bericht über die in den Vertragsstaaten durchgeführten Kontrollen zu Artikel 99 erstellt und hierzu Empfehlungen ausgesprochen, die von der GK Schengen am 18. Oktober 2006 gebilligt wurden.

Im Wesentlichen sind dies:

– Festlegung der Verfahrensweise durch die zuständigen Behörden, um eine Vereinheitlichung der Gründe für eine Ausschreibung in den einzelnen Schengen-Staaten zu erreichen.

– Die nationalen Behörden, die für die Ausschreibungen nach Artikel 99 SDÜ verantwortlich sind, sollen die Ausschreibungen regelmäßig überprüfen.

– Die nationalen Datenschutzbehörden und die GK sollten mehr in die Entwicklung eines gemeinsamen Kontrollmodells investieren, das für die Überprüfung der Ausschreibungen im SIS verwendet werden soll.

– Die für die Ausschreibungen zuständigen Behörden sollen formale und schriftliche Verfahren entwickeln,

um sicherzustellen, dass die Ausschreibungen korrekt, aktuell und rechtmäßig sind.

– Auch im Falle, dass verschiedene Behörden in den Vertragsstaaten für die Qualität der Daten verantwortlich sind, soll gewährleistet sein, dass die Daten korrekt, aktuell und rechtmäßig geführt werden und dass eine Überprüfung dieser Daten garantiert wird.

Ich werde die zuständigen Behörden auf diese Empfehlungen hinweisen. Zudem werde ich im Benehmen mit meinen Länderkollegen auch weiterhin die Ausschreibungen im Rahmen des SDÜ kontrollieren, damit insoweit ein hohes datenschutzrechtliches Niveau für die Bundesrepublik Deutschland gewährleistet bleibt.

Deutschland sollte insoweit eine Vorreiterrolle unter den Schengen-Vertragsparteien übernehmen.

### 3.2.5 Zollinformationssystem

*In den EU-Mitgliedstaaten wurde eine datenschutzrechtliche Kontrolle der Datensicherungsmaßnahmen bei der Nutzung des Zollinformationssystems (ZIS) durchgeführt. Angesichts der nur geringen Nutzung von ZIS stellt sich die Frage, ob das System weiterhin erforderlich ist.*

Das ZIS besteht aus einer zentralen Datenbank, die über Terminals von allen Mitgliedstaaten aus zugänglich ist. Die zentrale Datenbank wird von der Kommission beim Europäischen Amt für Betrugsbekämpfung (OLAF) geführt (vgl. 20. TB Nr. 3.3.3). Die gemeinsame Aufsichtsbehörde für das ZIS hatte im Sommer 2006 beschlossen, in allen EU-Mitgliedstaaten eine datenschutzrechtliche Kontrolle bei den für das ZIS zuständigen nationalen Zollbehörden durchzuführen. In Deutschland ist dies das Zollkriminalamt (ZKA). Dabei sollte überprüft werden, inwieweit die vom Europäischen Amt für Betrugsbekämpfung (OLAF) erarbeiteten Vorschläge zur Datensicherheit bei der operativen Nutzung des ZIS beachtet werden. Zudem sollte geklärt werden, aus welchen Gründen das ZIS von den Mitgliedstaaten so unterschiedlich genutzt wird.

Wie meine Kontrolle im ZKA ergab, begegnen die organisatorischen Maßnahmen bei der Nutzung des ZIS keinen durchgreifenden datenschutzrechtlichen Bedenken. Insbesondere die Verfahren zur Einräumung des lesenden und schreibenden Zugriffs auf das Informationssystem und zur Kennwortvergabe gewährleisten einen angemessenen Schutz vor unberechtigten Zugriffen.

Kritisiert habe ich, dass die Speicherfristen von Datensätzen nicht automatisiert überwacht werden, sondern mittels Aktenvermerken. Dadurch ist nicht in allen Fällen eine rechtzeitige Löschung von Daten im ZIS gewährleistet. Das ZKA hat zugesagt, künftig die Fristenverwaltung systemunterstützt durchzuführen.

Nach Mitteilung des ZKA wird das ZIS vom Zollfahndungsdienst nur wenig genutzt. Dies liege im Wesentlichen daran, dass die technische Infrastruktur des Systems zu kompliziert und nicht benutzerfreundlich sei. Hinzu komme, dass auch die von den anderen Mitgliedstaaten getätigten Ausschreibungen vielfach nicht die erforderlichen Informationen enthielten. So fehle häufig der Hinweis auf die Gründe der Ausschreibung sowie Angaben zu durchzuführenden Maßnahmen. Die wenigen verfügbaren Informationen seien daher für die Aufgabenerfüllung des Zollfahndungsdienstes nur von geringem Nutzen. Zudem würden die Ausschreibungsvoraussetzungen und -kriterien in den Mitgliedstaaten unterschiedlich ausgelegt. Das Ziel des ZIS, durch einen beschleunigten Informationsaustausch die Effizienz der Zollverwaltung zu steigern, werde damit weitestgehend verfehlt. Von OLAF werde daher eine anwenderfreundlichere webbasierte Software für das ZIS entwickelt.

Sollte das ZIS auch nach der Umstellung so wenig genutzt werden wie bisher, würde sich generell die Frage nach der Erforderlichkeit dieses Informationssystems stellen. Die Gründe für die mangelnde Akzeptanz des Systems könnten auch darin liegen, dass die Zollbehörden der EU-Mitgliedstaaten auf anderem Wege die erforderlichen Informationen austauschen. Damit wäre das ZIS überflüssig. Ich werde die Entwicklung weiter beobachten.

### 3.2.6 Aufbau einer integrierten Datenbank über vermisste Personen bei Interpol

*IKPO-Interpol plant den Aufbau einer integrierten Datenbank über vermisste Personen und unbekannte Tote. Dabei sind auch datenschutzrechtliche Aspekte zu beachten.*

Interpol prüft seit Jahren den Aufbau einer Datenbank über vermisste Personen und unbekannte Tote, um deren Schicksal aufzuklären. Durch die Tsunami-Flutkatastrophe von Dezember 2004 hat das Thema neue Aktualität gewonnen, so dass auf der Interpol-Generalversammlung im September 2005 eine Arbeitsgruppe zu diesem Thema eingesetzt wurde. Diese hat sich für ein integriertes Datenbanksystem bei Interpol ausgesprochen, in dem Angaben sowohl über vermisste Personen/unbekannte Tote als auch zur Identifizierung von unbekannten Katastrophenopfern erfasst werden sollen. Dabei soll die Datenspeicherung zentral bei Interpol erfolgen, Dateneingabe bzw. -löschung hingegen dezentral durch die Mitgliedstaaten. Ich habe keine Bedenken gegen das Konzept, wenn gewährleistet ist, dass Informationen über vermisste Personen nur unter engen Voraussetzungen für Zwecke der Verbrechensbekämpfung genutzt werden. Wegen der sensiblen Daten halte ich zudem auf nationaler Ebene den Zugang über eine zentrale Kontaktstelle für geboten.

### 3.2.7 Zugriff der Sicherheitsbehörden auf das europäische VISA-Informationssystem (VIS)

*Das geplante VISA-Informationssystem (VIS) der EG (s. u. Nr. 7.1.4) soll auch von den für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten zur Bekämpfung terroristischer und sonstiger schwerwiegender Straftaten im Wege des Direktzugriffs genutzt werden.*

Das geplante VISA-Informationssystem wird voraussichtlich eine der umfangreichsten europaweiten Daten-

sammlungen mit einer Vielzahl von Informationen über die Visa-Antragsteller und über deren Einlader. Wegen des umfangreichen Datenkatalogs einschließlich biometrischer Merkmale stieß dieses Projekt von Beginn an auf das Interesse der Strafverfolgungsbehörden in den Mitgliedstaaten. Da das VIS in erster Linie administrativen Zwecken bei der Visum-Erteilung dient, die Terrorismusbekämpfung bzw. Strafverfolgung jedoch unter Titel VI des EU-Vertrages fällt, bedarf es einer eigenständigen Rechtsgrundlage für den Zugriff der Sicherheitsbehörden. Über einen entsprechenden Vorschlag der Kommission für einen Beschluss des Rates über den Zugang der für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und von EUROPOL zum VIS für Datenabfragen zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerwiegender Straftaten vom 30. November 2005 (Rats-Dok. 15142/05) ist trotz intensiver Diskussion im Rat bis Redaktionsschluss noch nicht entschieden worden.

Der vorgesehene generelle Zugriff auf administrative Dateien aus Einreiseverfahren für Zwecke der Verbrechensbekämpfung würde dem datenschutzrechtlichen Zweckbindungsprinzip (vgl. Artikel 5 lit. b der Europaratskonvention 108) widersprechen. Danach ist eine Weiterverwendung von einmal rechtmäßig erhobenen Daten allenfalls unter klar definierten Bedingungen zulässig. Insbesondere sind solche sicherheitsbehördlichen Zugriffe auf VIS nur unter strikter Einhaltung datenschutzrechtlicher Regelungen, insbesondere einer Abwägung mit den schutzwürdigen Interessen der Betroffenen im Einzelfall, möglich. Nach dem ursprünglichen Vorschlag der Kommission sollte der Zugriff nur über zentrale Zugangsstellen erfolgen, um eine systematische bzw. routinemäßige Abfrage der Sicherheitsbehörden zu verhindern. Dies würde auch dem Grundsatz der Verhältnismäßigkeit entsprechen. Leider zeichnete sich bei den Beratungen auf Initiative der Mitgliedstaaten eine dezentrale Ausgestaltung des Zugriffs ab. Um so wichtiger ist es, dass die Daten nur zur Prävention und Aufdeckung terroristischer und sonstiger schwerwiegender Straftaten und nur im jeweiligen Einzelfall zur Verfügung gestellt werden dürfen. Ferner müssen die Suchkriterien für eine Abfrage im Einzelnen festgelegt werden, denn das VIS ist kein Informationssystem zur Verbrechensbekämpfung. Diese Einschränkungen gelten insbesondere für die Nutzung der in VIS gespeicherten biometrischen Daten. Angesichts dessen beschränkten Auftrags ist auch der umfassende Zugriff von EUROPOL kritisch zu sehen. Wichtig ist zudem eine klare Definition des Begriffs der für die innere Sicherheit zuständigen Behörden. Hierunter fallen nicht die Nachrichtendienste aufgrund ihrer vorgelagerten Aufgaben bei der Sicherheitsprävention.

Sollte der Rat dem Zugriff der Sicherheitsbehörden der Mitgliedstaaten auf das VIS zustimmen, wären klare datenschutzrechtliche Regelungen über die Weiterverwendung der aus dem VIS bezogenen Daten unverzichtbar. Der Vorschlag der Kommission sah hierfür die Anwendung der Regelungen des Rahmenbeschlusses zum Schutz personenbezogener Daten vor, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (s. o. Nr. 3.2.1). Da das Schicksal dieses Rahmenbeschlusses jedoch höchst ungewiss ist, gibt es Bestrebungen zu bereichsspezifischen Datenschutzregelungen im vorliegenden Rechtsakt selbst. Damit wäre die Gefahr einer weiteren Zersplitterung des europäischen Datenschutzrechts verbunden. Sollte gleichwohl der Datenschutz bei VIS gesondert geregelt werden, muss der bereichsspezifische Datenschutzstandard mindestens dem Niveau entsprechen, der im Prümer Vertrag vorgesehen ist (s. o. Nr. 3.2.2).

Die Verordnung über das VISA-Informationssystem der EG war bis zum Jahresende 2006 noch nicht verabschiedet.

### 3.2.8 Eurodac – Datenschutzkontrolle

*Der Europäische Datenschutzbeauftragte und die nationalen Kontrollstellen kooperieren bei der Kontrolle des Europäischen Fingerabdrucksystems Eurodac.*

Nach der Eurodac-Verordnung obliegt dem Europäischen Datenschutzbeauftragten (EDPS) die Kontrolle der zentralen Datenbank in Luxemburg. Für die Stellen, die in den einzelnen Mitgliedstaaten die Eurodac-Verordnung umsetzen, sind dagegen die nationalen Kontrollstellen zuständig. In Deutschland ist das meine Behörde. Um die Arbeit und vor allem die Kontrollschwerpunkte in allen Mitgliedstaaten zu vereinheitlichen, hat der EDPS im Berichtszeitraum zu zwei Arbeitstreffen eingeladen. Dadurch konnte der Informationsaustausch zwischen dem EDPS und den nationalen Kontrollstellen sowie zwischen den Kontrollstellen untereinander verbessert werden. So wurden die bisherigen Kontrollergebnisse der einzelnen Mitgliedstaaten vorgestellt und Maßstäbe für zukünftige Kontrollen entwickelt. Bei der Kontrolle der zentralen Datenbank in Luxemburg hat der EDPS keine datenschutzrechtlichen Verstöße festgestellt.

## 3.3 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

*Die Artikel 29-Gruppe hat sich zu einem der wichtigsten europäischen Kooperationsgremien auf dem Gebiet des Datenschutzes etabliert.*

Nach Artikel 29 der EG-Datenschutzrichtlinie 95/46/EG berät die Gruppe die Europäische Kommission und prüft die Umsetzung der Richtlinie in nationales Recht im Sinne einer einheitlichen Rechtsanwendung. Sie nimmt Stellung zum Schutzniveau sowohl in der Gemeinschaft als auch in Drittländern, erstellt Arbeitspapiere, um auf besondere datenschutzrechtliche Probleme aufmerksam zu machen und entwickelt Empfehlungen zum Schutze der Privatsphäre der Bürgerinnen und Bürger der Gemeinschaft.

Im Berichtszeitraum hat die Gruppe insgesamt 26 Arbeitspapiere (vgl. Anlage 9) verabschiedet, die sich erneut mit einer breiten Palette von Themen auseinandersetzen. Schwerpunkte waren dabei die Übermittlung von Flugpassagierdaten in die USA (vgl. Nr. 3.3.2), die Übermittlung von Bankkundendaten an die USA durch die belgische Industriegenossenschaft SWIFT (vgl. Nr. 9.4),

die Speicherung von Telekommunikationsdaten (vgl. Nr. 10.1) und der Datenschutz in der sog. Dritten Säule (vgl. Nr. 3.2.1). Auch datenschutzrechtliche Aspekte der elektronischen Gesundheitsakte (vgl. Nr. 4.1) und die Durchsetzung datenschutzrechtlicher Vorgaben im Krankenversicherungsbereich (vgl. Nr. 3.3.4) wurden behandelt. Zudem befasste sich die Gruppe mit dem Projekt eCall, dessen konkrete Umsetzung in Kürze beginnen soll (vgl. Nr. 12.2), und der Speicherung von personenbezogenen Daten auf RFID-Chips (vgl. Nr. 4.3).

Die Frage, wie Datenschutz effektiv gewährleistet werden kann, wenn staatliche Stellen zuvor von Wirtschaftsunternehmen im Rahmen ihrer Kundenbeziehungen erhobene personenbezogene Daten für die Strafverfolgung nutzen wollen, bildete einen weiteren Schwerpunkt der Arbeit der Gruppe. Dies betrifft etwa Daten, die bei Telematikanwendungen in Kraftfahrzeugen, beim Buchen eines Fluges oder beim Telefonieren anfallen. Als besonders problematisch hat sich dabei erwiesen, dass es bis jetzt kein gemeinschaftsrechtliches Rechtsinstrument gibt, das den Datenschutz in der Dritten Säule, also im Bereich Justiz und Strafverfolgung, regelt (s. o. Nr. 3.2.1). Aus diesem Grund hat die Gruppe wiederholt dazu aufgerufen, einen solchen Rechtsrahmen endlich zu schaffen. Auch in Zukunft wird es vordringliche Arbeit der Gemeinschaftseinrichtungen sein, sicherzustellen, dass der Datenschutz in allen Lebensbereichen angemessen Berücksichtigung findet.

Ein besonderes Augenmerk hat die Gruppe zudem auf einen stetigen Meinungsaustausch mit Vertretern der Wirtschaft und mit anderen Interessengruppen gelegt, etwa bei der öffentlichen Konsultation vor Verabschiedung des Arbeitspapiers zu RFID (WP 105, s. u. Nr. 4.3). Mit Wirtschaftsvertretern wurde auch über die Verfahrensweise beim Einsatz von verbindlichen unternehmensinternen Verhaltensregeln (sog. Binding Corporate Rules, vgl. Nr. 3.3.6) diskutiert, die die Übermittlung von personenbezogenen Daten in Länder ohne angemessenes Datenschutzniveau erheblich erleichtern soll. Bei der Erarbeitung von EU-einheitlichen BCR-Antragsformularen ist mit dem Abschluss des Abstimmungsverfahrens im Frühjahr 2007 zu rechnen. Weitere wichtige Themen waren die Verpflichtung von Unternehmen, ihre Kunden angemessen über deren Datenschutzrechte zu unterrichten (sog. Short Privacy Notices), der Schutz geistigen Eigentums und die datenschutzrechtlichen Aspekte bei Hinweisen in Unternehmen im Kampf gegen Korruption und Buchfälschung (sog. Whistleblowing, vgl. Nr. 3.3.1).

Im März des Jahres 2006 wurde ich nach Ablauf meiner ersten zweijährigen Amtszeit erneut zum Vorsitzenden der Artikel 29-Gruppe gewählt. Auch mein Vertreter, der Leiter der spanischen Datenschutzbehörde, Professor José-Louis Piñar Mañas, wurde bestätigt.

### 3.3.1 Whistleblowing – Richtiger Umgang mit Insidertipps

*Interne Verfahren zur Meldung von Missständen in Unternehmen – sog. Whistleblowing-Hotlines – müssen datenschutzkonform gestaltet werden.*

Viele Unternehmen haben Hotlines eingerichtet, über die Missstände gemeldet werden können, z. B. zur Rechnungslegung, Wirtschaftsprüfung, Korruption, Banken- und Finanzkriminalität und für spezielle Verhaltensvorgaben der Unternehmen (Ethikrichtlinien). Gründe für die Einrichtung solcher Hotlines sind – neben der Umsetzung gesetzlicher Vorgaben – auch eigene Unternehmensinteressen an der Aufdeckung rechtswidrigen Handelns und ethisch vorwerfbarer Verhaltensweisen.

In den USA sieht der sog. Sarbanes-Oxley Act vor, dass börsennotierte Unternehmen zur Meldung fragwürdiger Buchhaltungs- und Revisionspraktiken anonym nutzbare Verfahren einrichten. Diese Vorgaben waren auch von europäischen Unternehmen, die auch an den USA-Börsen gehandelt werden, bis zum Frühjahr 2006 zu erfüllen. Die Unternehmen benötigten Leitlinien zur datenschutzkonformen Umsetzung von Whistleblowing-Hotlines, um dabei nicht mit der Europäischen Datenschutzrichtlinie 95/46/EG in Konflikt zu geraten. Aus diesem Grund hat die Artikel 29-Gruppe hierzu ein Arbeitspapier veröffentlicht (WP 117 vom 1. Januar 2006).

Das Spannungsfeld zwischen dem Informanten und dem Angezeigten sollte dahingehend gelöst werden, dass der Datenschutz für beide Seiten ausreichend Beachtung findet. Die Artikel 29-Gruppe hat sich in diesem Papier zunächst auf die Bereiche Rechnungslegung, Wirtschaftsprüfung, Korruption sowie Banken- und Finanzkriminalität beschränkt und dazu Forderungen aufgestellt (s. Kasten zu Nr. 3.3.1).

Kasten zu Nr. 3.3.1

**Forderungen der Artikel 29-Gruppe zum Whistleblowing**

- Die Beschäftigten müssen über die Einführung der Hotline, ihren Zweck und Anwendungsbereich informiert werden.
- Der Anwendungsbereich und der Kreis der betroffenen Personen müssen eng begrenzt werden; eine Verwendung der Informationen für andere Zwecke ist unzulässig.
- Namentliche Meldungen sind anonymen Anzeigen vorzuziehen, wobei dem Anzeigenden Vertraulichkeit zuzusichern ist; anonyme Anzeigen sollen auf Ausnahmefälle begrenzt werden.
- Der Grundsatz der Verhältnismäßigkeit ist zu beachten, d. h. nur die für die weitere Bearbeitung notwendigen Informationen dürfen gespeichert werden.
- Die Daten sind frühestmöglich, spätestens innerhalb von zwei Monaten nach Abschluss der Untersuchung zu löschen. Eine längere Speicherung ist nur zulässig, wenn weitere rechtliche Schritte erforderlich sind.
- Die beschuldigte Person ist zu informieren, sobald kein Risiko besteht, dass Beweise vernichtet werden. Der Name des Informanten darf im Regelfall nur dann dem Angezeigten genannt werden, wenn vorsätzlich falsche Vorwürfe angezeigt wurden.

In Deutschland hat sich auch eine Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises mit der Thematik Whistleblowing auseinandergesetzt. Ein von ihr vorbereiteter Bericht wird sich mit der Beurteilung der datenschutzrechtlichen Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung bei Meldeverfahren unter Einsatz von sog. Whistleblowing-Hotlines nach den Vorschriften des BDSG befassen.

Das Papier der Artikel 29-Gruppe kann aus dem Web abgerufen werden unter http://ec.europa.eu/justice_home/fsj/privacy/index_de.htm.

### 3.3.2 Übermittlung von Flugpassagierdaten in die USA

*Auch das Interimsabkommen mit den USA zur Übermittlung von Flugpassagierdaten wirft datenschutzrechtliche Fragen auf.*

Im Mai 2004 hatte die Europäische Union mit den USA ein Abkommen zur Übermittlung von Flugpassagierdaten geschlossen, gegen das vom Europäischen Parlament beim Europäischen Gerichtshof Klage eingereicht wurde (vgl. 20. TB Nr. 22.2). Mit Urteil vom 30. Mai 2006 entschied der Europäische Gerichtshof, dass dieses Abkommen wegen fehlender Rechtsgrundlage spätestens bis Ende September 2006 zu kündigen sei. Im Oktober 2006 wurde daraufhin ein Folgeabkommen mit einer Laufzeit bis zum 30. Juli 2007 ausgehandelt. Die Artikel 29-Gruppe hatte sich zuvor gegen den Abschluss von bilateralen Abkommen ausgesprochen, um eine uneinheitliche Anwendung der europäischen Datenschutzrichtlinie und eine damit einhergehende Schwächung der Rechte der betroffenen Passagiere zu vermeiden. Den Abschluss dieses Folgeabkommens begrüße ich daher grundsätzlich, da ansonsten Passagierdaten ohne Rechtsgrundlage und ohne vertragliche Schutzvorkehrungen an das US-Heimatschutzministerium übermittelt worden wären. Bei den Verhandlungen zu dem neuen Abkommen, das in zahlreichen Details mit der vorherigen Vereinbarung identisch ist, konnte zwar erreicht werden, dass die im Jahre 2004 bei Vertragsabschluß von den USA gegebenen Zusicherungen weiterhin Bestand haben. Die von der Artikel 29-Gruppe bereits bei Abschluss des ersten PNR-Abkommens geäußerten Vorbehalte zu wesentlichen Punkten der Vereinbarung bleiben allerdings weiterhin bestehen. Dies betrifft insbesondere die Zweckbindung, die nach wie vor nicht genau definiert ist, aber auch den Umfang der zu übermittelnden Daten, die bis zu 34 Elemente umfassen können. Die Artikel 29-Gruppe hatte sich bereits in früheren Stellungnahmen dafür ausgesprochen, den Datensatz auf 19 Datenelemente zu beschränken, da diese im Kampf gegen Terrorismus und organisiertes Verbrechen für ausreichend erachtet werden.

Bis zum Jahresende 2006 ist die bereits im ursprünglichen Abkommen vereinbarte Umstellung von einem Abrufverfahren (pull) auf ein aktives Übermittlungsverfahren (push) noch immer nicht erfolgt. Nach wie vor erhalten die US-Behörden die Daten im sog. pull-Verfahren, d. h. durch Zugriff auf die Reservierungssysteme der Fluggesellschaften, und greifen damit auf den kompletten Datensatz zu, der zu jedem einzelnen Passagier vorliegt. Im Einzelfall können dies sogar mehr als 34 Datenelemente sein. Schon im Abkommen von 2004 war vorgesehen, die Übermittlung auf ein aktives „push-Verfahren“ umzustellen, um zu gewährleisten, dass sensible Daten durch Einsatz einer Filtersoftware herausgefiltert werden. Nachdem die europäischen Fluglinien mehrfach mitgeteilt hatten, dass die Voraussetzungen für eine Übermittlung der Daten im „push-Verfahren“ erfüllt sind, gibt es nunmehr keine plausiblen Gründe mehr, die Umstellung weiter zu verzögern. Die Artikel 29-Gruppe hat deshalb die Vertragsparteien wiederholt aufgefordert, sich unverzüglich für eine entsprechende Lösung einzusetzen.

Kasten zu Nr. 3.3.2

**Anforderungen an ein neues PNR-Abkommen**

Auch das Folge-Abkommen mit den USA muss einen effektiven Schutz der Grundrechte der europäischen Bürgerinnen und Bürger gewährleisten, die an Transatlantikflügen teilnehmen. Es könnte sich dabei an dem zwischen der EU und Kanada abgeschlossenen Abkommen orientieren.

- Strikte Zweckbindung der übermittelten Daten auf die Bekämpfung des internationalen Terrorismus und der schweren grenzüberschreitenden Kriminalität. Beschränkung der automatisierten Datenzugriffe auf die für die Einreisekontrollen zuständigen US-Behörden.
- Begrenzung der übermittelten Datenelemente auf die zur Identifikation der Reisenden und zur Durchführung von Einreisekontrollen im Sinne der Zweckbestimmung erforderlichen Daten. Orientierungspunkte sind dabei die von der Artikel 29-Gruppe vorgeschlagenen 19 Datenelemente und die mit Kanada vereinbarten 25 Datenelemente.
- Ausschließliche Verwendung eines aktiven Übermittlungsverfahrens (push) unter Ausfilterung sensibler personenbezogener Daten durch die Fluggesellschaften.
- Gewährleistung eines angemessenen Datenschutzstandards bei der Verarbeitung der Daten in den USA, insbesondere durch eine unabhängige Datenschutzkontrolle und gemeinsame regelmäßige Überprüfungen unter Beteiligung der europäischen Datenschutzbehörden.
- Löschung der Daten nach Ablauf einer angemessenen Speicherfrist.
- Gewährleistung der individuellen Datenschutzrechte, insb. auf Auskunft und Korrektur.
- Befristung des Abkommens und Einfügung einer Evaluierungsklausel, damit das Abkommen rechtzeitig vor Ablauf der Frist nach wissenschaftlichen Kriterien unter Einbeziehung von unabhängigen Experten auf seine Wirksamkeit und seine Einschränkung der Grundrechte hin überprüft werden kann.

Es wird Aufgabe der deutschen Ratspräsidentschaft im ersten Halbjahr 2007 sein, ein neues und langfristig geltendes PNR-Abkommen auszuhandeln, das in der Zukunft den Datenschutz angemessen berücksichtigt und die Rechte und Freiheiten der Flugpassagiere sichert.

### 3.3.3 Umsetzung der Richtlinie 2004/82/EG zur Übermittlung von Flugpassagierdaten

*Die Richtlinie 2004/82/EG des Rates über die Verpflichtung von Beförderungsunternehmen, Passagierdaten zu übermitteln, ist noch nicht in nationales Recht umgesetzt, obwohl die Frist hierzu bereits am 5. September 2006 abgelaufen ist.*

Auch in der EU sollen von Fluggesellschaften erhobene Passagierdaten genutzt werden, um den Gefahren des internationalen Terrorismus zu begegnen. Allerdings wurde die diesbezügliche Richtlinie (APl-Richtlinie – Abl. L 261/24 vom 6. August 2004, vgl. 20. TB Nr. 3.3.5) im Berichtszeitraum noch nicht in nationales Recht umgesetzt. Der vom BMI im Juli 2005 vorgelegte Gesetzentwurf erlangte keine Kabinettreife.

Die Artikel 29-Gruppe (vgl. Nr. 3.3) hat in einer Stellungnahme zu der API-Richtlinie (WP 127 vom 28. September 2006) kritisiert, dass diese zuviel Raum für abweichende Interpretation und Durchführung lasse. Sie hat die Mitgliedstaaten deshalb aufgefordert, ihren Ermessensspielraum für eine harmonisierte Umsetzung zu nutzen und dabei ein ausgewogenes Verhältnis zwischen dem Kampf gegen illegale Einwanderung und dem Recht auf Datenschutz zu wahren.

Im Herbst 2006 hat das BMI einen neuen Entwurf eines Fluggastdatengesetzes in die Ressortabstimmung eingebracht. Dieser sieht vor, die Richtlinie durch eine Ergänzung des Bundespolizeigesetzes – BPolG – umzusetzen. Obwohl dies zu begrüßen ist, stößt der Entwurf aus datenschutzrechtlichen Gründen auf erhebliche Bedenken:

- Der personelle Anwendungsbereich der Richtlinie 2004/82/EG gilt zwar für sämtliche Flugpassagiere, also auch für EU-Staatsangehörige. Damit den Regelungen des Schengener Durchführungsübereinkommens Rechnung getragen wird, sollte das Gesetz aber auf Beförderungen von Drittstaatsangehörigen über die Außengrenzen in das Bundesgebiet beschränkt werden.
- Die Liste der von den Luftverkehrsunternehmen zu übermittelnden Daten geht erheblich über den Datenkatalog in der Richtlinie hinaus. Problematisch erscheint mir insbesondere die Kopie der Lichtbildseite des Personaldokuments.
- Die übermittelten Daten sollen binnen 24 Stunden nach der Einreise des jeweiligen Flugzeuges bei der Bundespolizei gelöscht werden, sofern sie nicht zur Erfüllung einer dieser obliegenden gesetzlichen Aufgabe benötigt werden. Eine solche Öffnungsklausel, die datenschutzrechtlich eine sehr weitgehende Zweckänderungserlaubnis darstellt, erscheint mir unverhältnismäßig und auch mit dem Prinzip der Normenklarheit nicht vereinbar. Angesichts des weit gespannten Aufgabenbereichs der BPol (vgl. §§ 1 bis 13 BPolG) habe ich eine Begrenzung der Verwendung der Daten im Hinblick auf die Zielrichtung der Richtlinie, insbesondere die Einreisekontrolle zu verbessern und die illegale Einwanderung zu bekämpfen, gefordert.

Die Ressortabstimmung über den Gesetzentwurf war bei Redaktionsschluss noch nicht abgeschlossen. Ich werde darauf achten, dass dabei die datenschutzrechtlichen Belange angemessen berücksichtigt werden.

### 3.3.4 Europaweite Datenschutzprüfung im Krankenversicherungssektor

*Die erste europaweite Überprüfung bei Krankenversicherungen unterstreicht die Wichtigkeit gemeinsamen Vorgehens der nationalen Aufsichtsbehörden.*

Im März 2006 startete die Artikel 29-Gruppe eine europaweite Initiative mit dem Ziel, gemeinsam in allen europäischen Mitgliedstaaten die Anwendung und Umsetzung von datenschutzrechtlichen Bestimmungen im Krankenversicherungssektor zu überprüfen. Mit der Aktion sollten Erkenntnisse darüber gewonnen werden, wie hier personenbezogene Daten erhoben und verarbeitet werden, um daraus ggf. Schlüsse für weitere Maßnahmen ziehen zu können. Der Sektor war ausgewählt worden, weil er einen sehr großen Teil der Bevölkerung betrifft und dort bei den Versicherungsnehmern in besonderem Maße sensible Daten erhoben werden. Die Artikel 29-Gruppe hatte sich zuvor auf einen Fragenkatalog verständigt, der repräsentativen Unternehmen und Branchenverbänden zugesandt wurde. In die Vorbereitung der Aktion waren auch Vertreter des Europäischen Verbandes der Versicherungsunternehmer einbezogen worden. Von deutscher Seite wurden 5 Versicherungsunternehmen angeschrieben, die zusammen gut 50 Prozent des Marktes abdecken.

Für die Artikel 29-Gruppe ist eine solche gemeinsame koordinierte europaweite Überprüfung von großer Bedeutung. Sie zeigt, dass die Aufsichtsbehörden der EU-Mitgliedstaaten nicht nur eng zusammenarbeiten, sondern auch gemeinsam entwickelte Positionen zum Datenschutz durchsetzen können. Für die betroffenen Unternehmen hat dieses gemeinsame Vorgehen unterstrichen, dass die datenschutzrechtlichen Vorgaben im europäischen Raum einheitlich umgesetzt werden. Schließlich hat diese Aktion bei den Versicherungsnehmern das Bewusstsein für den Datenschutz gestärkt und sie über ihre Rechte aufgeklärt. Einzelergebnisse der Aktion werden im ersten Halbjahr 2007 erwartet.

### 3.3.5 Safe Harbor

*Das zwischen der EU und den USA geschlossene Safe Harbor Abkommen hat sich bewährt und soll weiter ausgebaut werden.*

Als im Jahr 2000 das Abkommen zwischen den Vereinigten Staaten und der Europäischen Union über einen „sicheren Hafen“ (vgl. Kasten zu Nr. 3.3.5) abgeschlossen wurde, wurde dies allseits als Experiment betrachtet. Inzwischen kann es als Erfolg bewertet werden. Zwei Veranstaltungen, die 2005 und 2006 gemeinsam vom US-Handelsministerium, der Europäischen Kommission und den in der Artikel 29-Gruppe zusammengeschlossenen Datenschutzbeauftragten der europäischen Staaten organisiert

wurden, bestätigen, dass Safe Harbor von einer immer größeren Zahl US-amerikanischer Unternehmen akzeptiert wird. Ende 2005 waren bereits mehr als 850 amerikanische Unternehmen beigetreten; im darauf folgenden Jahr 2006 waren es schon mehr als 1 000 Unternehmen.

Im Mittelpunkt der Veranstaltungen stand der Erfahrungsaustausch von Datenschutzbeauftragten, Unternehmen, der US-Federal Trade Commission (FTC) und Vertretern der US-Regierung über Möglichkeiten, wie der Datenschutz bei der transatlantischen Übermittlung personenbezogener Daten weiter verbessert werden kann. Besondere Aufmerksamkeit genoss die Frage, wie die Betroffenen – insbesondere Verbraucher und Arbeitnehmer – besser über ihre sich aus dem Abkommen ergebenden Rechte und Pflichten unterrichtet werden können, da die entsprechenden Möglichkeiten bislang kaum in Anspruch genommen werden.

Thematisiert wurde darüber hinaus der verstärkte Zugriff öffentlicher Stellen – insbesondere von Sicherheitsbehörden – auf Daten, die von Firmen für eigene Geschäftszwecke gespeichert werden. Die FTC und die europäischen Datenschützer planen, den Gedankenaustausch fortzusetzen und ihre Zusammenarbeit weiter zu intensivieren.

Kasten zu Nr. 3.3.5

**Erläuterungen zu Safe Harbor:**

Für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten von Amerika existiert seit November 2000 eine europäisch-amerikanische Vereinbarung, um nach den Anforderungen der europäischen Datenschutzrichtlinie 95/46/EG im Empfängerland (USA) ein angemessenes Datenschutzniveau zu gewährleisten. Rechtlicher Ausgangspunkt ist die in Kapitel IV der Datenschutzrichtlinie geregelte Übermittlung personenbezogener Daten in Drittländer. Nach Artikel 25 ist der Datentransfer in Drittstaaten strikten Grundsätzen verpflichtet, die die Richtlinie – dem Adäquanzprinzip folgend – als Angemessenheit des Datenschutzniveaus definiert (Artikel 25 Abs. 1 und 2). Nach Artikel 25 Abs. 6 kann die Europäische Kommission die Angemessenheit des Datenschutzes in einem Drittland „feststellen“, wenn dieses die in der Vorschrift näher genannten Anforderungen erfüllt. Das Arrangement des „Sicheren Hafens“ sieht vor, dass das US-Handelsministerium ein Verzeichnis derjenigen Unternehmen führt, die sich, um die Vorteile des Systems zur erhalten, öffentlich auf die Grundsätze des Safe Harbor verpflichtet haben. Wer sich auf amerikanischer Seite dem System des Safe Harbor anschließt, ist vor der Sperrung des Datenverkehrs aus Datenschutzgründen sicher, während im Gegenzug die europäischen Unternehmen wissen, an welche US-Firmen Daten übermittelt werden können, ohne dass zusätzliche Datenschutzgarantien verlangt werden müssen. Schließlich können die Unionsbürger sicher sein, dass ihre Daten vorschriftsmäßig geschützt werden.

Weitere Informationen zu Safe Harbor finden sich auf der Seite http://www.export.gov/safeharbor/.

### 3.3.6 Binding Corporate Rules

*Unternehmensinterne Regelungen zum Datenschutz (Binding Corporate Rules, BCR) stellen ein wichtiges Instrument als Grundlage für die Datenübermittlung in Drittstaaten dar.*

Der internationale Datenverkehr weitet sich immer mehr aus. Deshalb werden schon seit längerem verbindliche unternehmensinterne Regelungen als Schutzgarantie beim Drittland-Transfer diskutiert. Auf der Grundlage derartiger BCR können ausnahmsweise Übermittlungen personenbezogener Daten an Drittstaaten ohne angemessenes Datenschutzniveau genehmigt werden (Artikel 26 der Europäischen Datenschutzrichtlinie 95/46/EG). Aus diesem Grund hat sich die Artikel 29-Gruppe unter meinem Vorsitz im Berichtszeitraum mehrfach mit diesem Thema beschäftigt.

Im Jahre 2005 wurden zwei Arbeitspapiere erstellt, die europaweit von den Datenschutzbehörden als Hilfsmittel genutzt werden können. Zum einen wurde eine Muster-Checkliste für Anträge auf Genehmigung von Datenübermittlungen in Drittstaaten erstellt (WP 108 vom 14. April 2005). Den Unternehmen wird darin erläutert, welche Unterlagen in der Regel hierfür bei der zuständigen Datenschutz-Aufsichtsbehörde vorzulegen sind. In einem weiteren Arbeitspapier wurde ein Verfahren zur Kooperation innerhalb Europas zur Anerkennung von BCR festgelegt (WP 107 vom 14. April 2005).

Da die Verfahrensweise sich in der Praxis als kompliziert und zeitaufwendig erwiesen hat, hat die Artikel 29-Gruppe Empfehlungen für ein Standardantragsverfahren erarbeitet, um ein vereinfachtes Verfahren wie bei den Standardvertragsklauseln zu erreichen (WP 133 vom 10. Januar 2007).

## 3.4 Europäische und internationale Zusammenarbeit in Strafsachen

*Zahlreiche Maßnahmen sollen die europäische und internationale Zusammenarbeit in Strafsachen verbessern. Die Rechte des Einzelnen dürfen dabei jedoch nicht in den Hintergrund treten.*

Ein wichtiges Thema war auch in diesem Berichtszeitraum der Informationsaustausch zwischen den Strafregistern (vgl. 20. TB Nr. 7.9.2). Das von Deutschland, Frankreich, Spanien und Belgien verfolgte Pilotprojekt zur Verbesserung des Informationsaustauschs über strafrechtliche Verurteilungen auf elektronischer Basis hat Anfang April 2006 den Echtbetrieb aufgenommen. Ich habe dieses sog. „Strafregistervernetzungsprojekt“ begleitet und keine datenschutzrechtlichen Einwände gegen seine Ausgestaltung erhoben. Es werden die gleichen Informationen zwischen den nationalen Strafregistern ausgetauscht, die bislang auf dem Papierwege übermittelt wurden, also Strafnachrichten über Verurteilungen von Staatsangehörigen an deren Heimatstaaten sowie – auf Ersuchen eines anderen Staates – Auskünfte aus dem Strafregister. Neu

ist die Möglichkeit der elektronischen Übermittlung, die im „Trans-European Services for Telematics between Administrations (TESTA)"-Netz (vgl. 19. TB Nr. 8.8) mit ausreichenden IT-Sicherheitsmaßnahmen erfolgt; ein direkter Online-Zugriff auf die ausländischen Register ist nicht möglich. Ich halte eine solche Vernetzung der bestehenden nationalen Strafregister unter dem Aspekt der Datensparsamkeit und mit Blick auf die Rechte des Einzelnen in jedem Fall für vorzugswürdig gegenüber der Schaffung eines zentralen europäischen Strafregisters oder der von der Kommission in einem Weißbuch (KOM (2005) 10 endg.) vorgeschlagenen Einrichtung einer Art Vorbestraftenkartei als Indexdatei auf europäischer Ebene.

Des Weiteren hat die Europäische Kommission einen Vorschlag für einen Rahmenbeschluss des Rates über die Durchführung und den Inhalt des Austausches von Informationen aus dem Strafregister zwischen den Mitgliedstaaten vorgelegt (KOM (2005) 690 endg.; Ratsdok. 5463/06). Datenschutzrechtlich bedenklich ist hier insbesondere die vorgesehene Zweckänderungsvorschrift, nach der personenbezogene Daten, die dem ersuchenden Staat übermittelt wurden, von diesem nicht nur für die Zwecke, für die sie erbeten wurden, sondern auch zur Gefahrenabwehr und sogar zur Gefahrenvorsorge verwendet werden dürfen. Dies ist insbesondere deshalb problematisch, weil damit der Zeitpunkt der Datenverwendung in einen Bereich vorverlagert würde, der mit einem hohen Prognoserisiko behaftet ist. Hinzu kommt, dass die vorgeschlagene Verwendungsregelung zeitlich nicht begrenzt ist, so dass Angaben, die im Strafregister des ersuchenden Mitgliedstaates bereits getilgt oder zu tilgen sind, in größerem Umfang zum Nachteil des Betroffenen verwendet werden dürften, als es nach innerstaatlichem Recht (§§ 51, 52 Bundeszentralregistergesetz) zulässig wäre. Ich habe meine Bedenken dem BMJ mitgeteilt und gebeten, diese für die Bundesregierung in die Beratungen im Rat einzubringen. Ich werde die weitere Entwicklung aufmerksam verfolgen.

Noch immer nicht verabschiedet wurden die bereits im 20. TB (Nr. 7.9.2) dargestellten Rahmenbeschlussvorschläge über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafverfahren (KOM (2003) 688 endg.; Ratsdok. 15221/02) sowie über bestimmte Verfahrensrechte in Strafverfahren in der Europäischen Union (KOM (2004) 328 endg.; Ratsdok. 9318/04).

Neues zu berichten gibt es dagegen vom Europäischen Haftbefehl (vgl. 20. TB Nr. 7.9.2). Das BVerfG hat mit Urteil vom 18. Juli 2005 (Az.: 2 BvR 2236/04) das deutsche „Gesetz zur Umsetzung des Rahmenbeschlusses über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten der Europäischen Union" vom 21. Juli 2004 (BGBl. I S. 1748) für verfassungswidrig und damit nichtig erklärt, da es die Umsetzungsspielräume, die der Rahmenbeschluss den Mitgliedstaaten belässt, nicht so grundrechtsschonend wie möglich ausfüllte. Ich begrüße die Entscheidung, da sie eine grundsätzliche Stärkung des Verfassungsrechts bei der Umsetzung von Rahmenbeschlüssen bedeutet, die auch für andere Maßnahmen im Bereich der „Dritten Säule" zu beachten ist. Die erforderliche Neufassung des Europäischen Haftbefehlsgesetzes ist am 2. August 2006 in Kraft getreten (Gesetz vom 20. Juli 2006, BGBl. I S. 1721).

In Kraft getreten ist außerdem das Gesetz zur Umsetzung des Übereinkommens vom 29. Mai 2000 über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union (Gesetz vom 22. Juli 2005, BGBl. I S. 2189). Datenschutzrechtlich problematisch war hier die Umsetzung der Regelung des Übereinkommens zu den sog. Spontanmitteilungen, d.h. personenbezogenen Auskünften aus strafprozessualen Ermittlungen, die Gerichte und Staatsanwaltschaften anderen Staaten auch ohne Ersuchen erteilen dürfen. Hier ist der deutsche Gesetzgeber über das umzusetzende Übereinkommen hinausgegangen, indem er Spontanmitteilungen nicht nur EU-weit, sondern weltweit ermöglicht hat (§ 61a des Gesetzes über die Internationale Rechtshilfe in Strafsachen). Der ursprüngliche Gesetzentwurf enthielt allerdings keine hinreichenden Regelungen zum Ausschluss der Datenübermittlung, wenn im Empfängerstaat kein angemessenes Datenschutzniveau gewährleistet ist. Dies hatte ich sowohl gegenüber dem BMJ als auch gegenüber dem Rechtsausschuss des Deutschen Bundestages bemängelt. Im Rahmen der Beratungen im Rechtsausschuss konnte ich auf datenschutzrechtliche Verbesserungen hinwirken. Insbesondere ist das Vorhandensein eines angemessenen Datenschutzniveaus im Empfängerstaat nunmehr zumindest als schutzwürdiges Interesse des Betroffenen, das zu einem Ausschluss der Datenübermittlung führen kann, zu berücksichtigen.

## 3.5 Internationale Datenschutzkonferenzen

*Die Internationale Datenschutzkonferenz hat im Berichtszeitraum zwei Mal getagt und wichtige Entschließungen verabschiedet.*

Die 27. Internationale Konferenz der Datenschutzbeauftragten fand unter dem Titel „Der Schutz von Personendaten und der Privatsphäre in einer globalisierten Welt: ein universelles Recht unter Achtung der Verschiedenheiten" vom 14. bis 16. September 2005 in Montreux (Schweiz) statt. Etwa 50 unabhängige Datenschutzbehörden, Staaten, die noch kein unabhängiges Organ zur Datenschutzkontrolle haben, darunter die USA, internationale Organisationen, Wissenschaft und Industrie entsandten Vertreter.

Mit ihrer „Erklärung von Montreux" stellte die Konferenz fest, dass trotz der zunehmenden internationalen Geltung des Datenschutzes immer noch die weit überwiegende Mehrheit der Länder, darunter so bedeutende Länder wie Russland, China und Indien, keinen gesetzlichen Datenschutz haben (in Russland wurde allerdings inzwischen

ein Datenschutzgesetz verabschiedet – siehe Nr. 3.1). In einer Welt der globalisierten Datenverarbeitung in Netzen sei jedoch ein globaler Datenschutz dringend notwendig. Sie appellieren an die Vereinten Nationen, ein internationales Abkommen zum Datenschutz in Angriff zu nehmen. (s. Anlage 4).

Ferner erarbeitete die Konferenz eine Entschließung zur Einführung biometrischer Merkmale in Pässen. Die Datenschutzbeauftragten fordern hier wirksame technische Schutzmaßnahmen, eine strikte Zweckbindung und die Begrenzung der Nutzung der Biometriepässe auf die Verifikation der Identität der Passinhaber (s. Anlage 5).

Die Konferenz beschloss weiterhin Grundsätze zur „politischen Kommunikation“, d. h. zur Verwendung personenbezogener Daten im politischen Wettbewerb, vor allem im Wahlkampf (s. Anlage 6).

Bei der 28. Internationalen Datenschutzkonferenz, die vom 2. bis 3. November 2006 in London stattfand, standen die Gefahren einer Überwachungsgesellschaft im Mittelpunkt. Vertreter von 58 unabhängigen Datenschutzbehörden aus mehr als 40 Staaten aus aller Welt sowie Mitarbeiter von internationalen Organisationen und Repräsentanten aus Wirtschaft und Wissenschaft nahmen daran teil.

Der britische Datenschutzbeauftragte Richard Thomas legte eine Studie vor, die sich mit dem Thema Überwachungsgesellschaft heute und in der Zukunft beschäftigt. Die Studie zeigt, dass immer effektivere technische Überwachungsmöglichkeiten und ihr Einsatz im privaten wie im öffentlichen Sektor zusammen mit immer weiter gehenden Befugnissen der Sicherheitsbehörden weltweit den Weg in die Überwachungsgesellschaft ebnen. Nach Auffassung der Konferenz stellt die Reaktion der demokratischen Staaten auf die terroristischen Anschläge der letzten Jahre eine der größten Herausforderungen für den Datenschutz dar. Die für den Fortbestand demokratischer Verhältnisse unverzichtbare Balance zwischen Sicherheit und Freiheitsrechten gerate in Gefahr, wenn sich die Gesellschaften immer stärker in Richtung Überwachung entwickeln. (Die deutsche Kurzfassung und der englischsprachige Text der gesamten Studie sind aus dem Web abrufbar unter http://www.privacyconference2006.co.uk/index.asp? PageID=10).

Die Konferenz verabschiedete zudem eine Entschließung zum „Datenschutz bei Suchmaschinen“, in der auf die Gefahren für Persönlichkeitsrechte hingewiesen wird, die mit der verstärkten Nutzung von Rechercheinstrumenten im Internet ausgehen (s. Anlage 7).

In ihrem Abschlusskommuniqué wies die Londoner Konferenz darauf hin, dass der Datenschutz einen neuen Anschub braucht, um die Rechte der Bürgerinnen und Bürger in der Informationsgesellschaft zu gewährleisten (s. Kasten zu Nr. 3.5).

Kasten zu Nr. 3.5

**Abschlusskommuniqué der Londoner Konferenz**

- Für die Gesellschaft ist der Schutz der personenbezogenen Daten ihrer Bürger unerlässlich. Er steht auf gleicher Ebene wie die Presse- und die Bewegungsfreiheit. Datenschutz ist möglicherweise genauso kostbar wie die Luft, die wir atmen. Beide sind unsichtbar, aber ihr Verlust ist dennoch mit katastrophalen Folgen verbunden.
- Datenschutzbeauftragte sollten eine neue Kommunikationsstrategie entwickeln, um Öffentlichkeit und maßgebliche Interessenvertreter auf ihre Rechte und deren Bedeutung aufmerksam zu machen. Datenschutzbeauftragte sollten wirkungsvolle langfristige Kampagnen zur Stärkung des Bewusstseins ins Leben rufen und die Effektivität dieser Maßnahmen messen.
- Datenschutzbeauftragte sollten ihre eigenen Aktivitäten besser vermitteln und Datenschutz konkreter machen. Nur wenn diese Aktivitäten für die Bevölkerung insgesamt bedeutsam, zugänglich und relevant sind, wird es ihnen möglich sein, die öffentliche Meinung mit der nötigen Überzeugung zu beeinflussen und von Entscheidungsträgern gehört zu werden.
- Datenschutzbeauftragte sollten ihre Effizienz und Effektivität beurteilen und – sofern nötig – ihre Arbeitsweise entsprechend anpassen. Sie sollten mit ausreichenden Befugnissen und Mitteln ausgestattet werden und diese einzelfallbezogen und pragmatisch einsetzen. Sie sollten sich auf gravierende mögliche Beeinträchtigungen und Hauptrisiken konzentrieren, denen der Einzelne ausgesetzt ist.

(Vollständiger Text der Londoner Erklärung s. Anlage 8)

## 4 Technologischer Datenschutz

### 4.1 Elektronische Gesundheitskarte: Das Warten geht weiter

*Die elektronische Gesundheitskarte lässt weiter auf sich warten. Bei diesem wichtigen Projekt geht aber zu Recht Gründlichkeit vor Schnelligkeit.*

Die elektronische Gesundheitskarte sollte laut Gesetz bis spätestens zum 1. Januar 2006 die heutige Krankenversichertenkarte ablösen. Das Vorhaben betrifft rund 80 Millionen Versicherte, 260 Krankenversicherungen, 2 200 Krankenhäuser, 21 000 Apotheken und 188 000 Ärzte. Es handelt sich damit um das größte IT-Projekt in Deutschland und übersteigt in seinem Umfang die damit oft verglichene Einführung des Lkw-Mautsystems bei weitem.

In der Diskussion über die Einführung der elektronischen Gesundheitskarte wird vielfach die Gefahr des „gläsernen Patienten“ heraufbeschworen. Gesundheitsdaten, die zu den besonders schützenswerten personenbezogenen Daten nach dem Bundesdatenschutzgesetz gehören, befin-

den sich künftig in einer für die Versicherten unüberschaubaren virtuellen Welt. Die Telematikinfrastruktur im Gesundheitswesen soll die technischen Voraussetzungen dafür bieten, dass die behandelnden Ärzte und Apotheker im Rahmen ihrer jeweiligen Tätigkeit über die erforderlichen aktuellen medizinischen Informationen der Patienten verfügen können. Die angestrebte verbesserte medizinische Versorgung der Patienten darf aber nicht mit einem Verlust an Datenschutz einhergehen. Die gesetzlichen Grundlagen für die elektronische Gesundheitskarte enthalten deshalb in den §§ 291 ff. SGB V (vgl. 20. TB Nr. 21.1) detaillierte Zugriffsregelungen. Der Zugriff auf die Karte wird erst durch eine PIN des Versicherten und einen Heilberufsausweis des Arztes bzw. Apothekers ermöglicht. Das Zugriffskonzept ist technisch so konzipiert, dass das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt (vgl. hierzu auch die Entschließung der Datenschutzbeauftragten des Bundes und der Länder, Kasten zu Nr. 4.1). Auch die Grundprinzipien der Datenvermeidung und Datensparsamkeit werden eingehalten. Die neue Karte führt nicht zur Erhebung neuer medizinischer Daten, sondern soll lediglich einen verlagerten Zugriff auf die erhobenen Daten ermöglichen.

Die Karte soll schrittweise eingeführt werden. Sie enthält bereits in ihrer Einführungsphase zum Schutz gegen Missbrauch ein Lichtbild des Versicherten und eine einheitliche Versichertennummer, die auch bei einem Kassenwechsel beibehalten wird. In einer nächsten Stufe werden Rezepte von Ärzten und Notfalldaten auf der Karte gespeichert. In den letzten Stufen soll die Karte dann Zugang zu Daten über bisher verordnete Arzneimittel, elektronischen Arztbriefen und Patientenakten gewähren. Die einzige Pflichtanwendung ist das elektronische Rezept. Alle anderen medizinischen Daten dürfen nur mit ausdrücklicher Einwilligung des Versicherten gespeichert werden.

Verantwortlich für die grundlegenden Entscheidungen zur Einführung, Pflege und Weiterentwicklung der elektronischen Gesundheitskarte ist die „Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH“, kurz gematik genannt, die im Januar 2005 von den Spitzenorganisationen der Selbstverwaltung im Gesundheitswesen gegründet wurde. Das BMG erließ Ende 2005 die „Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte“ (BGBl. I S. 3128 ff.), die inzwischen mit der Änderungsverordnung vom 2. Oktober 2006 (BGBl. I S. 2189 ff.) fortgeschrieben wurde. Wesentliche Inhalte sind die Festlegung der Testziele, Testkomponenten und die zu testenden Anwendungen. In insgesamt vier Teststufen sollen die technischen Komponenten und deren Zusammenspiel geprüft werden. Nach dem Abschluss der Labortests bei der gematik und Tests in Musterumgebungen wurden inzwischen Feldtests mit 10 000 Versicherten begonnen. Die Feldtests sollen in der abschließenden weiteren Testphase auf 100 000 Teilnehmer ausgeweitet werden. Durch die Änderungsverordnung wird der erste Testabschnitt (Einsatz der elektronischen Gesundheitskarte im offline-Verfahren) um die Anwendungen „elektronisches Rezept“ und „Notfalldatensatz“ erweitert. Ich begrüße es, dass dabei auch meine Anregung berücksichtigt wurde, solche organisatorische und technische Verfahren, mit Hilfe derer Versicherte ihre Rechte wie z. B. Einsichtnahme und Löschung der Daten wahrnehmen können, in die Tests einzubeziehen.

Kasten zu Nr. 4.1

**69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005 in Kiel**

**Entschließung zur Einführung der elektronischen Gesundheitskarte**

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend auf Grund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

Im Dezember 2006 starteten in Flensburg und in Sachsen die ersten Feldtests mit bis zu 10 000 Versicherten; in den nächsten Monaten werden Tests in fünf weiteren Bundesländern anlaufen. Die Handhabung der Karte und die Prozesse in der Praxis müssen erprobt werden, um Rückschlüsse auf die Akzeptanz bei Versicherten und Leistungserbringern ziehen zu können. Der Gesetzgeber hat klare Vorgaben zum Schutz der Gesundheitsdaten formuliert, die sich jetzt im täglichen Umgang bewähren müssen. Deshalb kommt diesen Tests, in denen die Versicherten erstmals ihre eigenen Gesundheitsdaten mit der neuen Karte bei Ärzten, Apotheken und Krankenhäusern offenbaren, besondere Bedeutung zu. Die Patienten werden die Gesundheitskarte nur akzeptieren, wenn sie sicher sind, dass Datenschutz und Arztgeheimnis gewahrt bleiben. Der Erfolg der neuen Gesundheitskarte hängt wesentlich davon ab, dass alle datenschutzrechtlichen Fragen auch in der Praxis sicher gelöst werden. Vor diesem Hintergrund begrüße ich die sorgfältigen Vorbereitungsarbeiten seitens der gematik und des BMG und begleite gemeinsam mit den Landesdatenschutzbeauftragten die Tests sehr aufmerksam.

## 4.2 Videoüberwachung

Videoüberwachung ist ein fester Bestandteil unseres Lebens geworden. Sie ist in vielen Teilen allgegenwärtig – auf Bahnhöfen, in Geschäftsstraßen, während des Einkaufens in Geschäften und an sozialen Brennpunkten der Städte.

Videokameras sind die wohl sichtbarste Form allgegenwärtiger Überwachung. Ganze Innenstadtbereiche werden bereits durch private und öffentliche Stellen videoüberwacht: Ob auf Flughäfen, in Bahnhöfen, Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken, überall müssen Bürgerinnen und Bürger damit rechnen, ins Blickfeld von Videosystemen zu geraten.

Die Videotechnik entwickelt sich rasant und bietet immer neue Einsatzmöglichkeiten. Während bis vor kurzem Videokameras groß und daher auffällig waren, sind mittlerweile überwiegend kleine und unauffällige Geräte im Einsatz. Noch vor wenigen Jahren waren Videosysteme allein schon wegen ihrer Größe und auffälligen Form kaum zu übersehen. Insbesondere Geschäfte setzten auf den Abschreckungseffekt der Videoüberwachung. Dies ging bisweilen sogar soweit, dass an Stelle von echten Kamerasystemen Attrappen eingesetzt wurden. Heute sind derartige Bemühungen kaum mehr notwendig. Der allgemeine Preisverfall elektronischer Systeme hat vor der Videotechnik nicht Halt gemacht. Dementsprechend würde sich der Aufwand nur minimal reduzieren, falls man an Stelle funktionsfähiger Videokameras Videoattrappen einsetzen würde. Zudem kommen inzwischen – vor allem für die Überwachung von großen Räumen, etwa Bahnhöfen – so genannte „Dome-Kameras“ zum Einsatz. Dabei handelt es sich um voll schwenkbare Kameras, die eine starke Zoomfunktion haben und noch auf hundert Meter Details erkennen lassen. Da sie in ihrer äußerlichen Gestalt Deckenlampen ähneln, weil sie unter Glaskuppeln verborgen sind, werden sie kaum als Kameras erkannt.

Es gibt eine Vielzahl von gesetzlichen Regelungen, die sich mit der Zulässigkeit der Videoaufzeichnung befassen, u. a. die Polizeigesetze der Länder, das Versammlungsrecht und das BDSG. In dessen § 6b ist die „Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung)“ geregelt (s. Kasten zu Nr. 4.2). Diese Vorschrift bindet aus datenschutzrechtlicher Sicht die Zulässigkeit der Videoüberwachung an feste Voraussetzungen. Was viele Anwender aber nicht bedenken, ist die Tatsache, dass die erhobenen Daten, soweit darauf Personen erkennbar sind, auch unter die anderen Regelungen des BDSG fallen. Zum Tragen kommen dann die technisch-organisatorischen Regelungen gem. § 9 nebst Anlage sowie die Vorschriften zur Löschung der Daten gemäß § 3 Abs. 4 Ziffer 5.

Kasten zu Nr. 4.2

**§ 6b BDSG**

**Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen**

Die Beobachtung öffentlich zugänglicher Räume mit optischelektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(1) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(2) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(3) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(4) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

### 4.2.1 Auch Videoüberwachung braucht Sicherheit!

*Ein Schutzprofil für Videoüberwachungsanlagen unterstützt deren datenschutzgerechten Einsatz.*

Die in der Vergangenheit von mir durchgeführten Kontrollen zeigten, dass nicht alle Videoanlagen, die heute im Einsatz sind, diese Forderungen an die Technik erfüllen können. Vor diesem Hintergrund war es aus Sicht des Datenschutzes längst überfällig, die technisch-organisatorischen Anforderungen an Videoanlagen festzulegen.

Die Auflistung dieser Forderungen in Form einer Checkliste reicht aufgrund der in der Vergangenheit gewonnenen Erfahrung nicht aus. Deshalb wurde zur Beschreibung der technisch-organisatorischen Anforderungen auf die Möglichkeiten der Common Criteria (CC, ein Prüfrahmen für IT-Sicherheit) zurückgegriffen und die Anforderungen an die Verarbeitung von personenbeziehbaren Daten in Videoanlagen in Form eines Schutzprofils (Protection Profiles) beschrieben. Das Konzept soll besonders IT-Anwender, Hersteller und Datenschutzbeauftragte bei der Entwicklung und dem Betrieb von Videoüberwachungsanlagen unterstützen.

Das Schutzprofil stellt einen Katalog von Anforderungen auf, die aufgrund der datenschutzrechtlichen Anforderungen vorhanden sein müssen und in einem Zertifizierungsverfahren geprüft werden können (vgl. Kasten zu Nr. 4.2.1). Ferner können die Anforderung zur Revision und Prüfung, ob eine Installation datenschutzgerecht vorgenommen wurde, verwendet werden. Das Schutzprofil wurde durch das BSI zertifiziert und kann von meiner Homepage herunter geladen werden.

Kasten zu Nr. 4.2.1

Das Schutzprofil fordert zur Unterstützung eines gesetzeskonformen Umganges mit den Bilddaten einen Mindestsatz an Sicherheitsfunktionalität, diese sind:

- Gewährleistung der Löschung von Bilddaten (individueller Löschungsanspruch) mit erzwungener Begründung;
- Gewährleistung, dass die Bilddaten nach der jeweils zulässigen Speicherdauer automatisch gelöscht werden (Sollen Bilddaten über die vorgegebene Speicherdauer hinaus aufbewahrt werden, müssen diese zuvor aus der Videoüberwachungsanlage heraus exportiert werden);
- Zugriffsregelung auf Bilddaten;
- Gewährleistung, dass ein Export von Bilddaten immer begründet werden muss und ausschließlich von Beobachter und Administrator vorzunehmen ist;
- Protokollierung der Auswerte-, Lösch- und Konfigurierungsaktionen;
- Gewährleistung, dass Bilddaten ordnungsgemäß verarbeitet werden;
- Sicherstellung der Integrität, Authentizität und Vertraulichkeit der empfangenen Bilddaten

Das vollständige Schutzprofil kann aus dem Internet abgerufen werden unter www.bfdi.bund.de

### 4.2.2 Videoüberwachung auf Bahnhöfen

*Die Bundespolizei nutzt zur Erfüllung ihrer Aufgaben auf Bahnanlagen die Videotechnik der Deutschen Bahn AG. Hierzu wurde im Jahr 2006 zwischen der DB AG und der BPol ein Nutzungsvertrag geschlossen.*

Die Deutsche Bahn AG setzt auf ihren Bahnhöfen Videotechnik ein, um bei Störungen kurzfristig eingreifen zu können. Die dabei eingesetzte Videotechnik wird, wie bereits im 20. TB dargestellt (Nr. 5.3.6), auch von der für die Sicherung des Bahnbetriebs zuständigen Bundespolizei genutzt. Mit dem Abschluss des Nutzungsvertrags ist die BPol meiner Forderung, eine Rechtsgrundlage zu schaffen, die den Anforderungen des § 11 BDSG Rechnung trägt, nachgekommen.

Die Bombenfunde in Zügen am Dortmunder und Koblenzer Hauptbahnhof im Sommer 2006 sowie der schnelle Fahndungserfolg der Polizei bei der Tätersuche führten zu Forderungen nach einem Ausbau der Videoüberwachung auf Bahnhöfen und den Einbau solcher Anlagen auch in den Zügen. Ich begegne diesen Forderungen mit Zurückhaltung, da bei der Videoüberwachung ohne unmittelbaren Anlass eine Vielzahl von Personen beobachtet und deren Bilddaten aufgezeichnet werden. Der Einsatz und der daraus resultierende Nutzen für die öffentliche Sicherheit müssen in einem angemessenen Verhältnis zu den Freiheitsrechten stehen, d. h. auch hier muss der Grundsatz der Verhältnismäßigkeit gewahrt sein. Bei den Aufzeichnungen muss eine schnelle Auswertung sichergestellt sein, damit gegenwärtigen Gefahren tatsächlich begegnet werden kann. Die Videoüberwachung muss sich auf gefährdete Bereiche beschränken. Schließlich ist zu gewährleisten, dass die Aufzeichnungen nicht in falsche Hände geraten und nur für gesetzlich zugelassene Zwecke verwendet werden. Nach dem mir vorliegenden Konzept werden diese Anforderungen weitgehend erfüllt.

Ich werde auch künftig Wert darauf legen, dass selbst bei einem verstärkten Einsatz der Videotechnik, aber auch bei Einführung neuerer Techniken, wie z. B. Gesichtserkennungsverfahren (Nr. 5.2.6), die Balance zwischen den Bürgerrechten und den Belangen der öffentlichen Sicherheit gewahrt bleibt. Eine lückenlose, flächendeckende Videoüberwachung darf es auch in Zukunft nicht geben; sie wäre unverhältnismäßig und würde das soziale Verhalten der Bürger unvertretbar beeinflussen.

### 4.2.3 Auch bei Videoanlagen kann die Politik ins Blickfeld geraten!

*Mit Blick auf die Videoüberwachung habe ich in meinem Zuständigkeitsbereich zwei Kontrollen vorgenommen. Die Erkenntnisse waren auch maßgeblich für die Erstellung eines Schutzprofils.*

Der zunehmende Einsatz der Videotechnik hat mich veranlasst, eine Reihe von Videoüberwachungssystemen im Hinblick auf die Einhaltung der datenschutzrechtlichen Vorgaben in § 6b Abs. 2 BDSG (vgl. Kasten zu Nr. 4.2) zu überprüfen.

Der Deutsche Bundestag betreibt auf seinen Liegenschaften in Berlin Videokameras (insgesamt 397), deren Signale in einer Überwachungszentrale zusammenlaufen.

Jede Kamera ist individuell eingestellt und wird über die Überwachungszentrale individuell angesteuert. Die Bilddaten werden dort abgerufen und zu Kontrollzwecken eingesehen, jedoch nicht aus dem Überwachungssystem an andere Stellen übertragen. An vielen Gebäuden sind die Kameras sichtbar angebracht, am Reichstagsgebäude sind sie allerdings aufgrund von Denkmalschutzauflagen nur nach einiger Suche erkennbar. Grundsätzlich wurden die Anforderungen nach § 6b BDSG erfüllt. Gleichwohl habe ich im Rahmen einer Kontrolle Probleme bei dem Aufnahmebereich und der Sichtbarkeit festgestellt. Nach dem BDSG ist die Videoüberwachung kenntlich zu machen (§ 6b Abs. 2 BDSG). Dieser Verpflichtung kommt der Deutsche Bundestag – abhängig vom Standort der Kamera – in verschiedener Weise nach, beispielsweise in Form von Hinweistafeln. Bedenken hatte ich jedoch, wenn – wie z. B. im Bereich „Unter den Linden“ – die Kameras so ausgerichtet waren, dass Teile des öffentlich zugänglichen Raumes aufgenommen wurden, beispielsweise die Außenbewirtschaftung eines Restaurants. Die Kontrolle einer Kamera ergab, dass jeder Gast im Außenbereich dieses Restaurants erkannt werden konnte. Auf meine Anregung veranlasste die Verwaltung des Deutschen Bundestages daraufhin, diese Kamera erst abends zu aktivieren, wenn der Innenraum des Restaurants nicht mehr einsehbar ist. Problematisiert habe ich auch die Form der Hinweise auf diese Videoüberwachungsanlage. Hierzu gibt es ein vom DIN festgelegtes Piktogramm (DIN-Norm 33450), das auch international verstanden wird. Die bisher angebrachten schriftlichen Hinweise allein in deutscher Sprache erfüllen dagegen diese Forderung nicht, zumal gerade dieser Bereich sehr stark von ausländischen Besuchern frequentiert wird. In Zukunft wird der Deutsche Bundestag Piktogramme nach der DIN-Norm verwenden.

### 4.3 RFID (Radio Frequency Identification)

*Computerchips werden immer kleiner und kompakter. Informationstechnik wird mittlerweile in einer Dimension verwendet, in der sie kaum noch vom Menschen wahrnehmbar ist. Der RFID-Technologie kommt dabei eine Schlüsselrolle zu.*

RFID-Chips bilden eine Schlüsselkomponente bei der Computerisierung unseres Alltags. Von dieser Technologie gehen ganz neue Gefahren aus. Nicht nur deshalb, weil sie für den Betroffenen weitgehend unsichtbar ist, sondern auch, weil sie uns ein Stück weit kontrollierbar macht. Die RFID-Chips werden nämlich bereits heute nicht nur vereinzelt bei der Warenauszeichnung verwendet, auch öffentliche Stellen bedienen sich dieser Technologie. So enthalten zum Beispiel die neuen so genannten ePässe RFID-Chips, auf denen seit November 2005 die digitalisierten Gesichtsbilder und einige Grunddaten gespeichert und per Funk ausgelesen werden können (vgl. 20. TB Nr. 6.2) oder sie werden zur Fälschungssicherung und somit zur Unterbindung des Schwarzhandels von Tickets, wie etwa zur WM 2006 (vgl. 20. TB Nr. 5.3.7) eingesetzt. In einem gewissen Umfang ist dieses Verfahren gegen Missbrauch gesichert; doch besteht bei RFID-Chips die Gefahr, dass sie unbemerkt vom Träger ausgelesen oder sogar verändert werden können.

Eine flächendeckende Einführung birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. Die weltweit eindeutigen RFID-Kennungen – ähnlich einer Seriennummer – verschiedenster Gegenstände können sowohl untereinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise besteht die Möglichkeit, detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile zu erstellen.

Bereits heute sind die Unternehmen zur Information der Verbraucher verpflichtet, wenn mit Hilfe von RFID-Chips personenbezogene Daten verarbeitet werden. Die Informationspflicht betrifft sowohl die Chips selbst als auch die Kennzeichnung von Lese-/Schreibgeräten. Fraglich ist allerdings, wann und wie die Betroffenen informiert werden. Im Sinne eines effektiven Datenschutzes sollte die Transparenz möglichst frühzeitig, also bereits auf dem Produkt und an den Verkaufsregalen erfolgen, und nicht erst, wenn die Daten des Kunden durch ein Kassensystem erfasst werden.

Darüber hinaus muss der Verbraucher die Möglichkeit haben, den Speicherinhalt der RFID-Chips auszulesen. Bei RFID-Chips, die zur Kennzeichnung von Produkten und Verpackungen verwendet werden, muss der Lese-/Schreib-Mechanismus durch den Kunden kontrollierbar sein und ggf. deaktiviert werden können.

Auch auf europäischer und internationaler Ebene werden die Risiken von RFID gesehen. In mehreren Workshops der EU-Kommission in 2006 wurden Potential und Gefahren der RFID-Technologie, Standards, Interoperabilität, internationale Funkfrequenzzuweisung und die Zukunft der RFID-Technologie bewertet (http://www.rfidconsultation.eu). In einer Befragung wurde mit deutlicher Mehrheit die Auffassung vertreten, dass Funketiketten Vorteile bringen können, dies jedoch nicht auf Kosten der Privatsphäre gehen dürfe.

RFID war auch ein Schwerpunktthema der 72. Datenschutzkonferenz des Bundes und der Länder sowie der Konferenz der obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, die jeweils eine Entschließung hierzu gefasst haben (vgl. Anlagen 13 und 15). Wesentlicher Inhalt der beiden Entschließungen ist, dass die Wirtschaft für den schnellen und effektiven Schutz der Verbraucherinteressen verbindliche Regelungen für den Einsatz von RFID-Chips aufstellen und diesen auch nachkommen soll.

Die Selbstverpflichtung muss für alle Marktteilnehmer gelten und verbindlich sein. Bloße Absichtserklärungen sind nicht ausreichend. Wenn die Hersteller und der Handel nicht zu einer Selbstverpflichtung kommen, muss der Gesetzgeber die Rechte der Verbraucher bei der Anwendung der RFID-Technologie schützen. Ebenso halte ich die Einhaltung bestimmter Rahmenbedingungen (siehe Kasten zu Nr. 4.3) für zwingend notwendig.

Zum Thema „Datenschutzgerechter Einsatz von RFID“ hat der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder auch eine Orientierungshilfe erarbeitet, die sich mit datenschutzrechtlichen Fragestellungen zur RFID-Technologie auseinandersetzt. Die Orientierungshilfe ist auf meiner Internetseite (http://www.bfdi.bund.de) als Download eingestellt.

Kasten zu Nr. 4.3

Für den Schutz der Persönlichkeitsrechte Betroffener sind folgende Forderungen zu berücksichtigen:

– Transparenz

  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Chips informiert werden.

– Kennzeichnungspflicht

  Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

– Keine heimliche Profilbildung

  Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

– Vermeidung der unbefugten Kenntnisnahme

  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

– Deaktivierung

  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Chips dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Chips gespeichert wurden.

Abbildung 2 (zu Nr. 4.3)

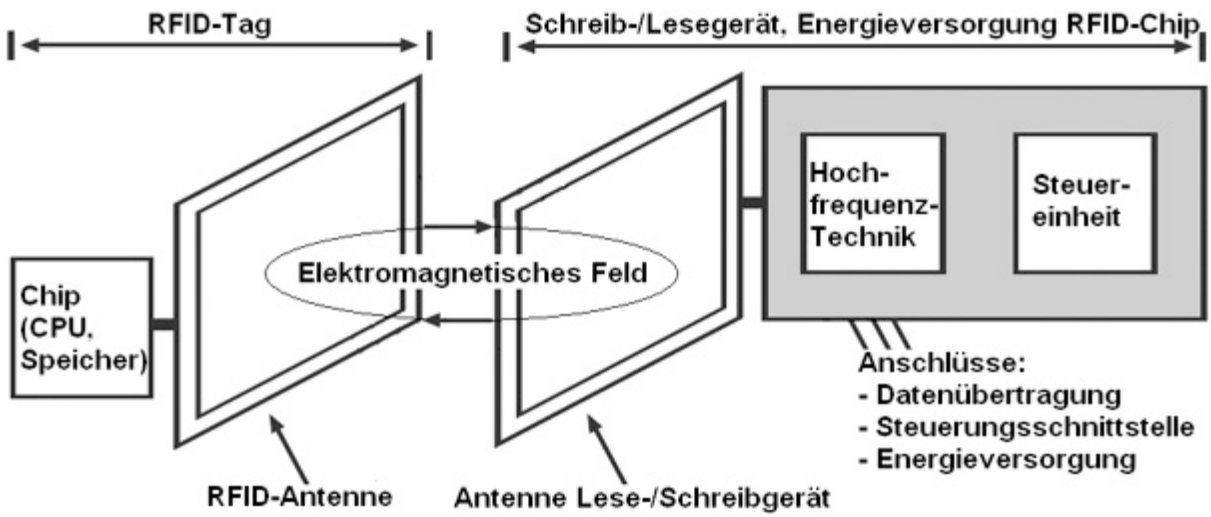


Abbildung 3 (zu Nr. 4.3)

## 4.4 Identitätsmanagement und elektronische Signaturverfahren

*Identitätsmanagement und Signaturverfahren sind für den Datenschutz in der Informationsgesellschaft von zunehmender Bedeutung.*

Die Frage, wie bei elektronischen Diensten die Identität der Beteiligten festgestellt werden kann und welche Daten dabei offenbart werden, gewinnt weiter an Bedeutung. Sie betrifft sowohl die Kommunikation zwischen den Bürgerinnen und Bürgern mit staatlichen Stellen als auch kommerzielle Transaktionen. Datenschutzfreundliche Lösungen müssen einerseits die eindeutige Authentifizierung sicherstellen und andererseits gewährleisten, dass dabei möglichst wenig personenbezogene Daten preisgegeben werden (vgl. auch 20. TB Nr. 4.1.1). Schließlich ist darauf zu achten, dass die „informationelle Gewaltenteilung“ bestehen bleibt, also die Trennung zwischen den von verschiedenen Verwaltungsbereichen für unterschiedliche Zwecke erhobenen Daten.

In letzter Zeit hat die Zahl so genannter „Identitätsdiebstähle“ deutlich zugenommen. Davon betroffen sind insbesondere elektronische Bankdienstleistungen, bei denen massenweise der Versuch unternommen wird, durch „Phishing“-Attacken Zugangsdaten (Benutzerkennung, Passwörter, PIN) und Transaktionsnummern (TAN) zu erschleichen. Sind die Daten erst einmal in die falschen Hände gelangt, dauert es häufig nur noch Minuten oder Stunden, bis das Konto leer geräumt ist.

Vor diesem Hintergrund begrüße ich es, dass sich die Bundesregierung im Rahmen ihrer „eCard-Strategie“ auch der Frage einer sicheren Authentifizierung im Internet stellen will. Neben der Datensicherheit muss dabei allerdings auch der Datenschutz gewährleistet bleiben. So muss jeweils hinterfragt werden, ob eine namentliche Identifizierung des Betroffenen für die Wahrnehmung eines bestimmten Dienstes wirklich erforderlich ist. Ähnlich wie bei der Anfang 2007 eingeführten Altersfeststellung an Zigarettenautomaten (vgl. Nr. 4.4.3) muss es auch im Internet weiterhin möglich sein, die Berechtigung zur Teilnahme an einem Verfahren oder zur Inanspruchnahme bestimmter Leistungen und Dienste nachzuweisen, ohne dass dabei der Name und die Adresse des Betroffenen registriert werden.

Eine sichere Authentifizierung ist nicht nur seitens der Nutzer erforderlich, sondern auch seitens der Stellen, die elektronische Dienste anbieten. Phishing-Attacken bedienen sich zum Beispiel in vielen Fällen gefälschter Web-Sites, bei denen den Nutzern vorgegaukelt wird, sie seien mit einer Bank oder mit einer Behörde verbunden. Deshalb müssen sowohl öffentliche Stellen als auch Unternehmen dafür sorgen, dass die Nutzer die Echtheit ihres Online-Angebots überprüfen können. Die entsprechenden Verfahren stehen seit längerer Zeit zur Verfügung; sie müssen allerdings auch eingesetzt werden, was immer noch in vielen Fällen nicht geschieht.

Ein gutes Identitätsmanagement setzt auch einen bewussten Umgang der Nutzerinnen und Nutzer mit den elektronischen Diensten und ihre Vorsicht bei der Offenbarung persönlicher Daten voraus. Die Anbieter müssen die erforderlichen Informationen über einen sicheren Umgang mit ihren Diensten zur Verfügung stellen. Außerdem müssen Sie ihnen reinen Wein über die Folgen von unachtsamem Umgang mit ihren Daten und über unvermeidliche Restrisiken einschenken. Nur so kann das erforderliche Vertrauen in die Zuverlässigkeit von Online-Angeboten gewonnen und erhalten werden (s. auch Kasten zu Nr. 4.4).

Kasten zu Nr. 4.4

**Identitätsmanagement** bezeichnet den zielgerichteten und bewussten Umgang mit Identität, Anonymität und Pseudonymität. Es wird hier verstanden als die Verwaltung von Benutzerdaten, die einzelnen Personen zugeordnet sind. Datenschutzrechtlich bedeutsam ist vor allem die Zuordnung mehrerer Rollen zu einer Person. Das Identitätsmanagement verhindert damit die Möglichkeit einer Profilbildung über mehrere Lebensbereiche hinweg, z. B. als Kunde, Versicherter, Patient und Arbeitnehmer. Durch die Einführung umfassender elektronischer Verfahren wie ELENA (s. u. Nr. 4.6), der Gesundheitskarte (s. o. Nr. 4.1) und des ePasses (s. u. Nr. 4.5.3) ist ein geeignetes Identitätsmanagement in den Mittelpunkt von datenschutzrechtlichen Anforderungen an die Technik gerückt.

**Elektronische Signaturen** sichern elektronische Dokumente, insbesondere ihre Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente.

Zwischen Computersystemen werden **Authentisierungsverfahren** eingesetzt, um die Identität der Systeme – gegebenenfalls auch diejenige des Nutzers dieser Systeme – nachzuweisen.

Beide Verfahren nutzen in der Regel die asymmetrische Verschlüsselung. Gleichwohl unterscheiden sie sich. Dies muss bei der Planung als auch beim Einsatz in Verwaltungsverfahren berücksichtigt werden. Die qualifizierte elektronische Signatur ist durch Gesetz mit Rechtsfolgen verknüpft. Die eingesetzten Verfahren werden ständig durch das BSI auf ihre Sicherheit, Robustheit und Gültigkeit geprüft und überwacht. Reine Authentisierungsverfahren (z. B. die Verwendung von Passwörtern oder biometrischen Merkmalen) liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente, nicht jedoch hinsichtlich der Echtheit und Integrität bestimmter Daten oder Dokumente. Diese Verfahren werden beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System benutzt. Daher dürfen an die Authentizität und Integrität der auf diesen Systemen verarbeiteten Daten nicht die gleichen Rechtsfolgen (siehe hierzu Nr. 8.4) geknüpft werden wie an eine qualifizierte elektronische Signatur. Die Unterscheidung dieser beiden Bereiche ist für die technische Entwicklung eines Verfahrens und seiner Anwendung wichtig und sollte gerade aus datenschutzrechtlicher Sicht beachtet werden.

### 4.4.1 ELSTER-Portal und StDÜV

In der Steuerverwaltung zeigte sich die Bereitschaft, auf den ursprünglich vorgesehenen Einsatz der qualifizierten elektronischen Signatur zu verzichten, vor allem bei der Änderung der Steuerdatenübermittlungsverordnung (StDÜV) und dem Betrieb des ELSTER-Portals. Mit diesem lässt sich eine Vielzahl steuerlicher Vorgänge (z. B. Abgabe einer Steuererklärung) vom privaten Computer aus erledigen (s. https://www.elsteronline.de/eportal/). Mit einem Verzicht auf die qualifizierte elektronische Signatur wird jedoch das Sicherheitsniveau der jeweiligen Anwendung bei der elektronischen Übermittlung von Dokumenten gesenkt. Um dem entgegen zu treten, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 11. Oktober 2006 eine Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren gefasst (vgl. Anlage 14).

Durch Änderungen des § 87a Abs. 6 Abgabenordnung und der StDÜV wurde für die Finanzverwaltung der Einsatz „anderer sicherer Verfahren“ als die qualifizierte elektronische Signatur zugelassen (s. u. Nr. 8.4). Derzeit gibt es keine anderen Verfahren, die ein vergleichbares Sicherheitsniveau wie die qualifizierte elektronische Signatur bieten. Im Gesetzgebungsverfahren habe ich deshalb darauf gedrungen, dass aus Sicherheitsgründen andere Authentisierungsverfahren nur neben der qualifizierten elektronischen Signatur verwendet werden dürfen. Auch wenn, wie bei der Nutzung des ELSTER-Portals, die Verwendung einer qualifizierten elektronischen Signatur nicht zwingend erforderlich ist, appelliere ich an die Nutzer, sie dennoch im eigenen Interesse einzusetzen, wenn Dokumente mit persönlichen Daten über das Internet versendet werden sollen.

### 4.4.2 Verschlüsselung nach wie vor ein wichtiges Thema!

*Vertrauliche Daten müssen gegen unberechtigte Einsichtnahme geschützt werden. Verfahren zur Datenverschlüsselung werden in der Verwaltung viel zu selten eingesetzt.*

Auch und gerade in der Informationsgesellschaft muss darauf geachtet werden, dass vertrauliche Informationen gegenüber unberechtigten Zugriffen und Manipulationen geschützt werden. Mit dem Übergang zu elektronischen Formen der Datenspeicherung und -übermittlung gewinnt die Frage zunehmend an Brisanz, wie die Vertraulichkeit digitaler Informationen gewahrt werden kann. Selbst umfangreichste Datenbestände, zu denen ein unberechtigter Zugang besteht, können in kürzester Zeit kopiert oder elektronisch weitergeleitet werden. Das damit verbundene Risiko ist immens. Soweit es sich um personenbezogene Daten handelt, verpflichten die datenschutzrechtlichen Regelungen die verantwortlichen Stellen zu Maßnahmen, mit denen die unberechtigte Kenntnisnahme und Veränderung verhindert werden kann. Von zentraler Bedeutung sind dabei Methoden zur sicheren Verschlüsselung der Daten.

Leider musste ich bei Beratungen und Kontrollen immer wieder feststellen, dass nur in wenigen Fällen entsprechende Verfahren eingesetzt werden. So musste ich zum Beispiel darauf hinweisen, dass insbesondere sensible Daten (z. B. Personal- und Sozialdaten, Daten über den Gesundheitszustand) in besonderer Weise geschützt werden müssen. Häufig wird mir das Argument entgegengehalten, die Verschlüsselung sei mit unzumutbarem Aufwand und mit zusätzlichen Kosten verbunden. Hierzu ist festzustellen, dass inzwischen effektive Verschlüsselungsverfahren zur Verfügung stehen, die sich verhältnismäßig einfach einsetzen lassen (siehe Kasten zu Nr. 4.4.2). Außerdem sollte nicht außer Acht bleiben, dass der Datenmissbrauch ein erhebliches materielles Schadenspotenzial aufweist und tief greifende Verletzungen des Rechts auf informationelle Selbstbestimmung zur Folge haben kann.

Kasten zu Nr. 4.4.2

Mit der Verschlüsselung werden ein klar lesbarer Text oder auch Informationen anderer Art, wie Ton- oder Bildaufzeichnungen, mit Hilfe eines Verschlüsselungsverfahrens (Kryptoverfahrens) in eine nicht mehr les-

bare Darstellung, das heißt nicht einfach interpretierbare Zeichenfolge, umgewandelt. Entscheidend für die Verschlüsselung ist die Verwendung eines Schlüssels zur Ver- oder Entschlüsselung der Information. Was sich in der Theorie für einen Laien kompliziert anhört, gestaltet sich in der Praxis recht einfach: Das Ver- und Entschlüsseln wird dort von den unterschiedlichsten Krypto-Programmen vorgenommen. Heute gängige Verschlüsselungsverfahren wie AES, IDEA und RSA sind auch für den Laien nutzbar, ohne dass besondere Fachkenntnisse hinsichtlich der eingesetzten Kryptoverfahren notwendig sind. Zur einfachen Dateiverschlüsselung stellt das Bundesamt für Sicherheit in der Informationstechnik das Programm Chiasmus zur Verfügung. Dies ist eine Verschlüsselungssoftware für Windows-PCs und wird für den Bereich der Öffentlichen Verwaltung und der geheimschutzbetreuten Wirtschaft abgegeben. Das Programm ist einfach zu bedienen und kann auch von Laien benutzt werden.

Auf die Verschlüsselung muss zum besseren Schutz von personenbezogenen Daten vermehrt zurückgegriffen werden, dafür werde ich mich einsetzen.

### 4.4.3 Nutzung der EC-Karte zur Altersbestimmung am Zigarettenautomaten

Nach dem am 1. April 2003 in Kraft getretenen neuen Jugendschutzgesetz gilt für Tabakwaren ein Verkaufsverbot an Jugendliche unter 16 Jahren. Diese Vorgabe musste bis zum 1. Januar 2007 an allen öffentlichen Zigarettenautomaten umgesetzt sein. Seit dem Jahreswechsel kann nur noch derjenige Zigaretten an Automaten ziehen, der einen Altersnachweis erbringt. Dazu benötigt man eine ec-Karte mit Chip. Darauf muss ein Jugendschutzmerkmal gespeichert sein, das Auskunft über die Altersberechtigung des Käufers gibt. Volljährige Karteninhaber erhalten einen sog. Legitimationsvermerk, dem der Automat entnehmen kann, dass die betreffende Person nicht vom Schutzbereich des Jugendschutzgesetzes erfasst ist. Dieser Vermerk ist ohne Geburtsdatum und daher nicht personenbeziehbar. Bei minderjährigen Karteninhabern erhält der Vermerk das verschlüsselte Datum, an dem der Karteninhaber volljährig wird. Von diesem Datum aus kann das Lesegerät des Zigarettenautomaten zurückrechnen und überprüfen, ob der Inhaber der Karte zum aktuellen Zeitpunkt bereits 16 Jahre alt ist. Davon abhängig wird ihm der Zugang zu dem Automaten eröffnet oder verweigert. Für die Aufbringung des Datums auf den Geldkartenchip der ec-Karte ist eine Einwilligung der Eltern der Minderjährigen erforderlich. Der Zigarettenautomat selber registriert keinerlei Informationen über den Käufer.

Dieses Verfahren ist in der vorgesehenen Form datenschutzrechtlich nicht zu beanstanden. Es könnte sogar beispielhaft sein für elektronische Identifizierungsverfahren, wie z. B. den digitalen Dienstausweis, den elektronischen Pass oder den eFührerschein (vgl. Nr. 4.4 u. 4.5.3). Die Datenschutzaufsichtsbehörden werden den praktischen Einsatz der Altersverifikation weiterhin im Auge behalten.

## 4.5 Biometrie und Datenschutz

*Biometrie wird in immer stärkerem Maße zur Personenerkennung eingesetzt. Dies betrifft sowohl den öffentlichen, als auch den nicht-öffentlichen Bereich.*

Behörden und Unternehmen setzten biometrische Verfahren in immer größerem Umfang ein, um Personen zu identifizieren und um ihre Identität zu verifizieren. Ich habe mich deshalb bereits seit längerer Zeit mit den datenschutzrechtlichen Fragen auseinandergesetzt, die bei der Verwendung biometrischer Merkmale zu lösen sind (vgl. z. B. 19. TB, Nr. 1.1.1 und 20. TB Nr. 4.2.2). Der Einsatz von Biometrie ist datenschutzrechtlich nur zu verantworten, wenn die entsprechenden Verfahren eine hinreichende Erkennungssicherheit aufweisen, der Missbrauch der Daten durch technisch-organisatorische Maßnahmen ausgeschlossen wird und das Gesamtverfahren den Prinzipien der Verhältnismäßigkeit und Zweckbindung entspricht. Von besonderer Bedeutung ist in diesem Zusammenhang auch, dass die Betroffenen Kenntnis von der Tatsache und vom Zweck von Verfahren erhalten, bei denen ihre biometrischen Daten ausgewertet werden.

Auf Bundesebene wurden im Berichtszeitraum verschiedene biometrische Verfahren auf ihre Tauglichkeit getestet. Vom Bundesamt für die Sicherheit in der Informationstechnik wurde im Auftrag des Bundesministeriums des Innern eine Studie BioP II durchgeführt, die die Prüfung der Fingerabdruck-, Iris- und Gesichtserkennung auf ihre Erkennungsleistung und Überwindungssicherheit zum Gegenstand hatte. Ziel der Studie war es, die Leistungsfähigkeit von seinerzeit verfügbaren biometrischen Verifikationssystemen für eine Verwendung im Zusammenhang mit Personaldokumenten zu untersuchen. Leider wurden mir die vollständigen Ergebnisse des Forschungsprojekts BioP II im Herbst 2005 erst nach hartnäckigem Nachfragen vom zuständigen Bundesministerium des Innern zur Verfügung gestellt. Zudem wurden Teile des Ergebnisberichts als Verschlusssache gekennzeichnet, so dass eine öffentliche Diskussion darüber nicht möglich war. Eine solche Diskussion wäre besonders notwendig gewesen, weil die Ergebnisse zeigen, dass bei der Gesichts- und Fingerabdruckerkennung noch erhebliche Schwächen vorhanden waren. Des weiteren wurden Nutzbarkeitsstudien vom Bundeskriminalamt (Gesichtserkennung im Projekt Fotofahndung am Mainzer Hauptbahnhof, s. u. Nr. 5.2.6) und von der Bundespolizei (Automatisierte Grenzkontrolle am Frankfurter Flughafen, s. u. Nr. 4.5.2) durchgeführt. Ich habe diese Projekte datenschutzrechtlich begleitet.

Neben den hoheitlichen Anwendungen werden biometrische Verfahren für die Prüfung der Identität bei Zugangsberechtigungsprüfungen (i. d. R. Fingerabdruck, Gesichts- und Iriserkennung), bei Bezahlsystemen und der Verifikation von Passagieren (i. d. R. Fingerabdruck) eingesetzt. Bei den Bezahlsystemen werden sowohl die biometrischen Merkmale wie auch die übrigen Kundendaten

(z. B. Bankinformationen) in Datenbanken gespeichert. Hier sind angemessene Datenschutz- und IT-Sicherheitsvorkehrungen zum Schutz der Daten zu treffen. Grundsätzlich gilt für den Einsatz biometrischer Erkennungssysteme, dass sie im Regelfall einwilligungsbedürftig sind. Ob bei Betriebsvereinbarungen die Zustimmung über die Mitarbeitervertretung ausreichend ist, ist im jeweiligen Einzelfall zu klären. In jedem Fall müssen die Anwender über das technische Verfahren, die verfolgten Zwecke, die Datenschutzbestimmungen und über die Risiken der Anwendung aufgeklärt werden.

Hohe Erkennungsraten sind derzeit überwiegend nur unter Laborbedingungen zu erreichen. Eine hundertprozentige Erkennungssicherheit wird es bei biometrischen Systemen auch in Zukunft nicht geben. Biometrische Massenanwendungen können den Komfort und die Bequemlichkeit für den Nutzer allerdings verbessern. Sicherheit und der Datenschutz müssen dabei aber Schritt halten. Dies kann nur durch zusätzliche technische und organisatorische Maßnahmen erreicht werden.

### 4.5.1 Technik

Biometrie hält Einzug in viele Bereiche unseres Lebens. Von der Kontrolle im Reiseverkehr bis hin zur Identifikation beim Bezahlsystem im Supermarkt. Ob die Technik dabei eine sichere Identifizierung gewährleistet, wie häufig versprochen wird, bleibt zweifelhaft. Bezogen auf Fingerabdruck- und Gesichtserkennung sind allerdings Fortschritte bei der Überwindungssicherheit und der Erkennungsleistung zu verzeichnen. So ist bei den auf dem Markt erhältlichen Fingerabdrucksystemen die Erkennungsleistung (bei einer entsprechenden Merkmalsausprägung der zu verifizierenden Person) als gut zu bewerten. Der große Schwachpunkt ist jedoch die Überwindbarkeit der Lesegeräte. Es ist nach wie vor relativ einfach, an den Fingerabdruck einer anderen Person zu gelangen und mit der Kopie des Fingerabdrucks einen Identitätsbetrug zu begehen. Die Kopie des Fingers kann bereits mit einfachen Mitteln hergestellt werden (Stichwort: „Silikonfinger“). Selbst Erkennungssysteme mit einer so genannten „Lebenderkennung“ bieten nur einen bedingten Schutz. Derzeit werden für die Lebenderkennung verschiedene Systeme, z. B. Ultraschall Fingerabdruckmessverfahren oder Messungen, bei denen die Feuchtigkeit (Schweiß) mit in die Erkennung einbezogen wird, getestet. Diese Systeme versprechen eine höhere Sicherheit gegen Manipulation. Ob derartige Fingerabdrucklesegeräte auch bei Massenanwendungen zum Einsatz kommen werden, bleibt angesichts der höheren Kosten abzuwarten.

Bei der Gesichtserkennung wird derzeit überwiegend zweidimensionale Messtechnik eingesetzt, d. h. es wird zum Vergleich der Gesichtsdaten jeweils ein Bild (Foto) erzeugt, und bestimmte Gesichtsmerkmale aus den vorliegenden Bildinformationen werden miteinander verglichen. Die Erkennungsleistung dieses Verfahrens ist von vielen äußeren Störfaktoren abhängig und daher – wenn diese Störfaktoren nicht gering gehalten werden können – eher als nicht sicher zu bewerten. Auf die Fehlerrate wirken sich insbesondere die Qualität des Referenzbildes, die Beleuchtung und die Kopfhaltung, aber auch Alterungsprozess und chirurgische Veränderung der Person aus. Eine erhebliche Verbesserung der Erkennungsleistung wird von der Einführung der dreidimensionalen Gesichtserkennung erwartet. Hierbei wird von dem Gesicht ein 3D-Model (Relief) aufgenommen. Der Vergleichsprozess erfolgt auf Basis der umgerechneten Gesichtscharakteristika. Bei der 3D-Methode werden Störeinflüsse wie Kopfhaltung, Beleuchtungsprobleme, ungünstiger Kamerawinkel, Entfernung der Kamera zum aufgenommenen Gesicht oder Kopfrotation minimiert, da der Rechner die aktuell aufgenommenen Daten auf den Basisdatensatz zurückrechnet und dann den Vergleich vornimmt. Eine Einsatzmöglichkeit der 3D-Technologie ist die Identifizierung von Personen bei der Zutrittskontrolle und die Videoüberwachung von Industrieanlagen oder Flughäfen. Auch wird im Rahmen der Kriminalitätsbekämpfung über Einsatzszenarien nachgedacht, bei denen jedoch erhebliche datenschutzrechtliche Fragen offen sind.

Die Europäische Union (EU) hat ein Projekt in Auftrag gegeben, das auf die eindeutige Identifikation von Personen mit Hilfe dreidimensionaler Gesichtserkennung zielt. Das Vorhaben trägt den Namen „3Dface“ und soll bis Ende März 2009 laufen. Ziel ist es, mit Hilfe der 3D-Technologie Flughäfen sicherer zu machen, Grenzkontrollen zu automatisieren und die Abfertigung von Passagieren zu beschleunigen. Zu diesem Zweck wird die 3D-Gesichtserkennung auch mit Oberflächen- und Texturbestimmung verknüpft. Ein umfassendes Projekt, in dem nicht nur Fragen der Betriebs- und Fälschungssicherheit, sondern auch Probleme des Persönlichkeitsschutzes untersucht werden.

### 4.5.2 Automatisierte Grenzkontrolle

Das von der Bundespolizei betriebene Pilotprojekt zur automatisierten und biometriegestützten Grenzkontrolle auf Iriserkennungsbasis am Flughafen Frankfurt/Main, über das ich in meinem 20. TB (Nr. 5.3.5) berichtet hatte, wurde mehrfach verlängert und soll nach Mitteilung des BMI nun im August 2007 beendet werden.

In diesem Zusammenhang habe ich darauf hingewiesen, dass ich der Speicherung der von den Teilnehmern erhobenen personenbezogenen Daten sowie der Merkmale ihrer Augeniris in einer von der Bundespolizei geführten Datenbank nur im Hinblick auf den Testcharakter des Verfahrens zugestimmt hatte. Gemäß § 4 Abs. 4 Passgesetz bzw. § 1 Abs. 5 des Gesetzes über Personalausweise ist das Speichern biometrischer Merkmale in einer zentralen Datei unzulässig. Im Hinblick auf die von der Bundesregierung getroffenen Festlegungen, Gesichtsbild und Fingerabdrücke als biometrische Merkmale in den elektronischen Reisepass aufzunehmen, stellt sich allerdings die Frage, welchen Sinn die Fortsetzung des Pilotverfahrens am Flughafen Frankfurt/Main noch hat. Von dem Projektbericht, der nun hoffentlich im Jahr 2007 vorliegen wird, erhoffe ich mir jedenfalls belastbare Erkenntnisse über die Geeignetheit der Iris zur Verifizierung von Personenidentitäten, insbesondere Angaben über die Falsch-

erkennungen und die zu Unrecht zurückgewiesenen Personen, die sich einer verschärften Kontrolle unterziehen mussten.

### 4.5.3 Der ePass und der neue Personalausweis

*Die Ausstattung von Pässen und Personalausweisen mit elektronischen Chips wirft erhebliche datenschutzrechtliche Fragen auf.*

Aufgrund der Ratsverordnung 2252/2004 vom 13. Dezember 2004, in die Reisepässe der EU-Bürger einen RFID-Chip zu integrieren, in dem neben den bisher im Reisepass vorhandenen Daten – einschließlich eines digitalisierten Lichtbildes – auch Fingerabdrücke aufzunehmen sind, werden seit dem 1. November 2005 die sog. ePässe ausgegeben. Kurz vor Ende des Berichtszeitraumes hat das BMI einen Entwurf zur Änderung des Passgesetzes vorgelegt, der vorsieht, ab dem 1. November 2007 auch Fingerabdrücke in den Reisepass aufzunehmen. Außerdem plant die Bundesregierung die Einführung des biometriegestützten Personalausweises ab 2008.

Über die EU-Pass-Verordnung hatte ich bereits in meinem letzten Tätigkeitsbericht (20. TB Nr. 6.2.1) berichtet. In ihrer Entschließung zur „Einführung biometrischer Ausweisdokumente“ vom 1. Juni 2005 (vgl. Anlage 10) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder das Eintreten des Europäischen Parlamentes für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten, ausdrücklich begrüßt und unterstützt. Gleichzeitig hat die Konferenz festgestellt, dass mit der Einführung biometrischer Merkmale Risiken für den Datenschutz verbunden sind. Die Anregung für ein Moratorium bei der Einführung der biometrischen Merkmale in Ausweisdokumente hat die Bundesregierung zu meinem Bedauern nicht berücksichtigt und zum 1. November 2005 – wiederum ohne ausreichende Beteiligung des Parlaments – durch die „Zweite Verordnung zur Änderung passrechtlicher Vorschriften“ vom 8. August 2005 (BGBl. I S. 2306) die Einführung des sog. ePasses zum 1. November 2005 beschlossen.

Das BMI war der Auffassung, dass es wegen der europarechtlichen Vorgaben durch die Verordnung 2252/2004 für die Einführung eines im Reisepass integrierten RFID-Chips (zu RFID-Chips vgl. Nr. 4.3), in dem die schon im bisherigen Pass aufgedruckten Daten – einschließlich des Passbildes – gespeichert werden sollten, keiner Änderung des Passgesetzes bedurfte. Dem habe ich widersprochen. Einerseits ist in § 4 Abs. 4 Satz 1 PassG unmissverständlich geregelt, dass „die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung ... durch Bundesgesetz“ geregelt werden. Andererseits ging die Änderung des Passwesens über die digitale Speicherung der bereits im herkömmlichen Reisepass gedruckt enthaltenen Informationen hinaus. So wurde in § 3 der neuen Passmusterverordnung die Art des Passbildes nicht unerheblich verändert. Zudem stellte der Übergang zum digitalen, automatisiert auswertbaren Passbild einen Qualitätssprung mit erheblichen datenschutzrechtlichen Auswirkungen dar, der einer gesetzlichen Normierung bedurft hätte. Immerhin war das BMI der Ansicht, dass die Einführung von Fingerabdrücken in den Reisepass nicht unmittelbar aus der Verordnung 2252/2004 herleitbar ist, sondern dass es hierzu der Befassung des Deutschen Bundestages durch eine Änderung des Passgesetzes bedurfte. Wenige Tage vor Ende des Berichtszeitraumes hat das Bundeskabinett einen entsprechenden Gesetzentwurf beschlossen.

Zu meinem großen Bedauern ist durch die Verordnung 2252/2004 dem Bundestag die grundlegende Entscheidung darüber entzogen worden, ob Fingerabdrücke überhaupt in die Reisepässe der deutschen Staatsbürger aufgenommen werden sollen. Eine öffentliche Auseinandersetzung über die Sinnhaftigkeit dieser Regelung hat praktisch nicht stattgefunden. Zwingend vorgeschrieben durch Vorgaben der Internationalen Zivil-Luftfahrt-Organisation (ICAO – International Civil Aviation Organization) ist dieses Merkmal nicht. So war in dem Vorschlag für die Verordnung 2252/2004 – in der Fassung wie sie dem Europäischen Parlament vorgelegt worden war – auch nur die fakultative Aufnahme von Fingerabdrücken vorgesehen. Angesichts vieler Zugangssysteme, die auf der Nutzung von Fingerabdruckdaten basieren, halte ich es für möglich, dass hier die Risiken den angestrebten Zusatznutzen für die Sicherheit bei weitem überwiegen.

Ich verkenne nicht das Bemühen der Bundesregierung, durch technische Maßnahmen den Schutz der Daten weitgehend sicherzustellen. Zweifel bleiben, ob dies gelingen wird. Das für die erste Version des ePass genutzte Authentifizierungsverfahren „Basic Access Control“ ist schon einigen Angriffsversuchen ausgesetzt gewesen. In der Presse fanden sich nicht nur Berichte über das Kopieren des RFID-Chips, sondern auch darüber, dass sich Angreifer Zugang zu den Passdaten verschafft hätten. Ob die vorgesehenen Sicherungssysteme (z. B. das Authentifizierungsverfahren „Extended Access Control“), die die Fingerabdruckdaten im RFID-Chip vor Missbrauch schützen sollen, ausreichend sind, werde ich sorgfältig beobachten.

Die Bundesregierung plant, biometrische Merkmale auch in den Personalausweis aufzunehmen. Dies wird in erster Linie damit begründet, dass der Personalausweis innerhalb der EU als Reisedokument diene. Es ist beabsichtigt, die gleichen biometrischen Merkmale wie im ePass, in einem in den Personalausweis zu integrierenden RFID-Chip zu speichern. Außerdem wird erwogen, im Personalausweis ein digitales Zertifikat nach dem Signaturgesetz vorzusehen, das vom Bürger aktiviert werden kann und ihm die Möglichkeit eröffnet, etwa über das Internet, digital zu signieren (Bürgerkartenfunktion).

Gegen die Aufnahme weiterer biometrischer Daten in den Personalausweis bestehen die gleichen Bedenken wie

hinsichtlich der Einführung dieser Merkmale in den Reisepass, die noch dadurch verstärkt werden, dass praktisch jeder Erwachsene seinen Personalausweis – anders als den Reisepass – ständig mit sich führt. Im Hinblick darauf, dass für die Aufnahme der Fingerabdrücke in den Personalausweis keine europarechtlichen Vorgaben bestehen, rege ich an, auf die Aufnahme dieses Merkmals in den elektronischen Personalausweis zu verzichten.

Neu in dem Entwurf ist sowohl im Passgesetz als auch im Personalausweisgesetz eine Regelung, die es den Polizei- und Ordnungsbehörden erlauben soll, aus den bei den Kommunen geführten Pass- und Personalausweisregistern automatisiert Lichtbilder im Rahmen der Verfolgung von Verkehrsordnungswidrigkeiten zu übermitteln. Zwar bestehen keine durchgreifenden datenschutzrechtlichen Bedenken dagegen, unter Einhaltung datensicherheitsrechtlicher Vorgaben, im Einzelfall Lichtbilddaten automatisiert an die Polizei- und Ordnungsbehörden zu übermitteln. Allerdings wurde in der Begründung nicht nachvollziehbar vorgetragen, warum es hierfür eines automatisierten Abrufverfahrens bedarf. Nach der ursprünglichen Begründung dieser Regelung bleibt die Übermittlung von Lichtbildern aus dem Pass- bzw. dem Personalausweisregister nur ultima ratio, d. h. sie darf nur erfolgen, wenn „die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können oder nach der Art der Aufgabe, zu der die Daten erforderlich sind, von einer solchen Datenerhebung abgesehen werden muss“. Insoweit scheint es sich hierbei nicht um ein Massenphänomen zu handeln, das einen Online-Zugriff der Ordnungswidrigkeiten- und Polizeibehörden auf das Pass- bzw. Personalausweisregister rechtfertigen würde. Hinzu kommt, dass zwar keine bundesweite Datei mit biometrischen Merkmalen durch das Änderungsgesetz errichtet wird. Gefahren für das informationelle Selbstbestimmungsrecht können aber auch von vernetzten Datenbanken ausgehen, die in funktionaler Hinsicht zentralen Dateien entsprechen. Gerade der geplante Online-Abruf von Lichtbildern aus dem Personalausweis- bzw. dem Passregister würde eine Vernetzung der beteiligten Stellen erfordert, worauf selbst die neue Begründung im Passgesetz hinweist. Ich habe daher angeregt, auf die geplanten Regelungen zu verzichten.

### 4.5.4 Symposium „Biometrie und Datenschutz – Der vermessene Mensch“

*Unter diesem Titel stand ein Symposium, in dem die Nutzung biometrischer Merkmale nicht nur aus rechtlicher und technischer Sicht, sondern auch im Hinblick auf gesellschaftliche Aspekte beleuchtet wurde.*

Um die öffentliche Diskussion zu einer immer umfassenderen Nutzung von biometrischen Merkmalen zu fördern, hatte ich für den 27. Juni 2006 zu einem Symposium in der Berliner Staatsbibliothek eingeladen. Es handelte sich hierbei um das zweite Symposium zu wichtigen datenschutzpolitischen Themen in meiner Amtszeit und ist in Fortsetzung des Symposiums „Staatliche Eingriffsbefugnisse auf dem Prüfstand“ am 8. November 2004 zu sehen (vgl. 20. TB Nr. 7.1.3). Die Universitätsprofessoren Peter Strasser (Graz), Christoph Busch (Darmstadt) und Alexander Roßnagel (Kassel) führten in die gesellschaftlichen, technischen und rechtlichen Aspekte der Benutzung biometrischer Merkmale ein. Anschließend fand eine Podiumsdiskussion mit Rechts- und Innenpolitikern der Fraktionen des Deutschen Bundestages statt: Für die CDU/CSU-Fraktion Herr Dr. Hans Peter Uhl, für die FDP-Fraktion Frau Gisela Piltz, für die Fraktion BÜNDNIS 90/DIE GRÜNEN Frau Silke Stokar von Neuforn und für die Fraktion DIE LINKE Frau Petra Pau. Die Veranstaltung fand mit rund 150 Gästen aus Politik, Wissenschaft, Verwaltung und privater Wirtschaft statt. Alle Beteiligten wiesen – nicht nur wegen der aktuell eingeführten biometrischen Merkmale in Personaldokumenten (siehe hierzu Nr. 4.5.3) – auf die weitreichende Bedeutung der Biometrie auf das gesellschaftliche Leben hin und waren sich über die Notwendigkeit einig, dass Technologie-Entwickler, Systembetreiber, Datenschützer und Verbrauchervertreter im Dialog bleiben und sicherstellen, dass zukünftige Technologien datenschutzkonform ausgestaltet werden.

Über das Symposium wurde ein Tagungsband erstellt, der über meine Behörde bezogen, aber auch auf meiner Homepage abgerufen werden kann.

## 4.6 Das JobCard-Verfahren (ELENA-Verfahren)

*Aus dem JobCard-Verfahren ist aus sprachlichen Gründen das ELENA-Verfahren geworden. Die mit dem Verfahren verbundenen datenschutzrechtlichen Fragen haben sich dadurch nicht verändert.*

Mit dem JobCard-Verfahren (neuerdings und im folgenden ELENA genannt, ELENA steht für **El**ektronischer **E**inkommens**na**chweis und soll der elektronischen Bereitstellung von Einkommensnachweisen in 16 sozialrechtlichen Verfahren sowie in Prozesskostenhilfeverfahren und beim Versorgungsausgleich dienen), über das ich in meinen beiden letzten Tätigkeitsberichten (19. TB Nr. 23.2.2; 20. TB Nr. 15.2) berichtet habe, soll eine der größten Datensammlungen mit personenbezogenen Daten in Deutschland entstehen und ist auch deshalb von besonderer datenschutzrechtlicher Brisanz. Das BMWi hat inzwischen einen Entwurf eines Gesetzes zur Einführung des Elektronischen Einkommensnachweises vorgelegt, dem insgesamt drei JobCard-Projekte zugrunde liegen und an dem ich von Anfang an beteiligt war. Im Laufe des Projektes JobCard II wurden auch die Landesbeauftragten für den Datenschutz in die Diskussion einbezogen.

Das Projekt JobCard besteht aus folgenden drei Einzelprojekten:

JobCard I — untersuchte die Praktikabilität des Abrufs von Daten aus der Arbeitsbescheinigung nach § 312 SGB II aus einer Datenbank mit Hilfe eines Signaturkartenverfahrens; das Projekt wurde 2004 abgeschlossen.

JobCard II — überträgt die Ergebnisse des Projektes JobCard I auf Einkommensbescheinigungen aus dem gesamten Sozialrecht sowie zwei

Einkommensbescheinigungen aus dem Bereich des Zivilprozessrechts (Prozesskostenhilfe, Versorgungsausgleich); der Abschlussbericht mit Stand vom 31. Dezember 2005 wurde dem BMWi vorgelegt.

JobCard III wurde im Frühjahr 2006 begonnen, womit auch Entgeltersatzleistungen (Arbeitslosengeld I, Krankengeld, Kindergeld, Unterhaltsvorschuss usw. ) einbezogen werden sollen.

Der vom BMWi vorgelegte Referentenentwurf basiert im Wesentlichen auf den Ergebnissen des Abschlussberichtes zum Projekt JobCard II. Der elektronische Abruf von Daten zu Entgeltersatzleistungen soll erst später durch die Ergänzung der entsprechenden gesetzlichen Regelungen einbezogen werden.

ELENA soll nach Erwartung des BMWi die Unternehmen entlasten. Die ca. drei Millionen Arbeitgeber in Deutschland stellen jährlich etwa 60 Millionen Einkommensbescheinigungen in Papierform aus, mit denen die Bürger gegenüber Behörden oder Gerichten die Voraussetzungen für eine bestimmte Leistung nachweisen können. Unter Vermeidung von Medienbrüchen sollen die Arbeitgeber künftig einen multifunktionalen Verdienstdatensatz, der u. a. die Rentenversicherungsnummer enthält, an eine Zentrale Speicherstelle (ZSS) übermitteln. Die Übermittlung erfolgt unter Anwendung des sog. DEÜV-Verfahrens nach der Datenerfassungs- und -übermittlungsverordnung. Seit dem 1. Januar 2006 sind die Arbeitgeber ohnehin gesetzlich verpflichtet, diese Meldungen elektronisch abzugeben. Der Arbeitgeber soll die Daten für Einkommensbescheinigungen seiner Mitarbeiter nicht mehr selbst speichern müssen. Anschließend fragt die ZSS bei der sog. Registratur Fachverfahren (RFV) an, ob zu der mitgelieferten Rentenversicherungsnummer eine Signaturkarte im ELENA-Verfahren angemeldet ist, die eine weltweit eindeutige Zertifizierungsidentitätsnummer (ZID) enthält. Ist dies der Fall, werden die Daten in der ZSS verschlüsselt unter dem Ordnungskriterium der ZID gespeichert. Ist zu der Rentenversicherungsnummer noch keine Signaturkarte zum Verfahren angemeldet, vergibt die RFV eine Übergangsnummer (UID), die den Konventionen der ZID entspricht. Die Daten werden in diesem Fall in der ZSS unter dieser UID in der Datenbank gespeichert. Aufgabe der RFV ist im Wesentlichen die Verwaltung der ZID und der UID sowie die Verbindung zur identifizierenden Rentenversicherungsnummer.

Soweit ein Bürger künftig einen Einkommensnachweis benötigt, soll er seine Identität mittels einer Signaturkarte mit qualifiziertem elektronischen Zertifikat (§ 7 SigG) nachweisen. Diese Signaturkarte wäre im ELENA-Verfahren unter seiner Rentenversicherungsnummer anzumelden. Mit Hilfe der auf der Signaturkarte gespeicherten ZID und des für den zuständigen Sachbearbeiter vergebenen elektronischen Zertifikats können dann die erforderlichen Einkommensdaten in der ZSS abgerufen werden.

Nach Inbetriebnahme des ELENA-Verfahrens würde der Arbeitgeber nicht mehr erfahren, dass sein Mitarbeiter bzw. sein ehemaliger Mitarbeiter eine Sozialleistung oder Prozesskostenhilfe beantragt hat. Dabei soll künftig sicher gestellt werden, dass nur die gesetzlich vorgesehenen Einkommensdaten von den Sozialbehörden erhoben werden. Zudem könnten die Daten nicht mehr durch Eingabe- oder Übertragungsfehler verfälscht werden. Schließlich wird angestrebt, dass die erforderlichen Daten in Sozialverwaltungsverfahren zugunsten des Antragstellers zeitnah vorliegen.

Bei der Entwicklung des ELENA-Verfahrens haben sich einige schwerwiegende datenschutzrechtliche Probleme ergeben. Besonders hervorzuheben ist, dass in der ZSS einkommensrelevante Daten der ca. 35 bis 40 Millionen abhängig Beschäftigten gespeichert werden sollen, bei denen in der Regel noch nicht feststeht, ob die Daten im Einzelfall tatsächlich gebraucht werden. Verfassungsrechtlich ist eine solche Datenbank nur zulässig, wenn zum Zeitpunkt der Speicherung deren Zweck bestimmt ist und wirksame technische, organisatorische und rechtliche Sicherungen gegen Zweckänderungen und Datenmissbrauch gewährleistet sind. So muss die Verwendung der Daten durch eine strikte gesetzliche Zweckbindungsregelung abgesichert werden. Da das Grundrecht auf Datenschutz durch die Ausgestaltung des Verfahrens effektiv geschützt werden muss, habe ich sehr frühzeitig umfassende technisch-organisatorische Sicherungen eingefordert. Deshalb müssen die Daten bei der ZSS unter der Zertifizierungsnummer der Signaturkarte des Betroffenen verschlüsselt gespeichert werden; es ist gesetzlich und technisch sicherzustellen, dass die Daten nur mit dessen Signaturkarte und mit der Signatur einer Sozialbehörde abrufbar sind. Dabei habe ich besonderen Wert auf die durchgängige Einhaltung des sog. „Zwei-Karten-Prinzips“ (besser: „Zwei-Signaturen-Prinzip“) gelegt, das sicherstellt, dass die Daten nur von der berechtigten Stelle und grundsätzlich nur nach Vorlage der Signaturkarte des betroffenen Teilnehmers abgerufen werden können.

Verfassungsrechtlich zulässig bleibt die Speicherung personenbezogener Daten nur so lange, wie dies für die Erreichbarkeit des Zwecks erforderlich ist. Im ELENA-Verfahren wurde unter meiner Mitwirkung daher ein differenziertes Konzept zur Löschung der jeweils nicht mehr erforderlichen personenbezogenen Daten entwickelt. Die von der ZSS gespeicherten Daten müssen unverzüglich gelöscht werden, wenn sie für kein vom ELENA-Verfahren unterstütztes Verwaltungs- oder gerichtliches Verfahren mehr erforderlich sind.

Gegen die ursprünglich vorgesehene Nutzung der Rentenversicherungsnummer als Ordnungskriterium habe ich mich frühzeitig gewandt (vgl. 19. TB Nr. 23.2.2). Ihre Nutzung würde u. a. die Gefahr der Erstellung von Persönlichkeitsprofilen in sich bergen, da die Bescheinigungsdaten über die Rentenversicherungsnummer abgerufen und mit weiteren Daten des betroffenen Bürgers zusammengeführt werden könnten. Nach der Rechtsprechung des BVerfG ist die Erschließung eines Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal unzulässig (vgl. BVerfGE 65

S. 1, [53]). Aufgrund meiner Intervention wurde daher die verfassungsrechtlich unzulässige Verwendung der Rentenversicherungsnummer zugunsten der ZID aufgegeben. Zu berücksichtigen war dabei, dass dem Arbeitgeber, der die Daten an die Zentrale Speicherstelle übermittelt, die ZID nicht bekannt ist. Da er für die Meldung an die Rentenversicherung die Rentenversicherungsnummer kennt, war es zwingend erforderlich, die Rentenversicherungsnummer erst im Verfahren mit der ZID zu verbinden, um die Daten in der ZSS unter der ZID verschlüsselt zu speichern. Diese Verbindung geschieht in der Registratur Fachverfahren. So wird auch sichergestellt, dass ein Abruf der Daten nur mit der Mitwirkung des betroffenen Teilnehmers möglich ist, da dieser hierzu die Signaturkarte mit der ZID vorlegen muss. Ein Abruf der Daten unter Nutzung der in vielen Bereichen bekannten Rentenversicherungsnummer würde damit technisch ausgeschlossen. Zudem hat der Teilnehmer die Möglichkeit, mehrere Signaturkarten registrieren zu lassen, wodurch sich die Verknüpfungsmöglichkeiten weiter verringern dürften.

Da ein von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder angeregtes Gutachten des BSI zum Ergebnis kommt, dass eine Ende-zu Ende-Verschlüsselung der Daten nicht praktikabel ist, insbesondere weil dann etwa im Falle des Verlustes der Signaturkarte sämtliche Daten des Betroffenen nicht mehr verfügbar wären, hat sich das BMWi dazu entschlossen, die Daten in einem symmetrischen Verfahren zu verschlüsseln. Dies würde es theoretisch ermöglichen, auf die Daten auch ohne Vorliegen der Signaturkarte des Betroffenen zuzugreifen. Deshalb muss beim weiteren Gesetzgebungsverfahren besonderer Wert darauf gelegt werden, dass die für die Erschließung der verschlüsselten Daten erforderlichen Schlüssel sicher von einer unabhängigen Stelle verwaltet werden, für die ein gesetzlicher Beschlagnahmeschutz besteht.

## 4.7 eGovernment – bitte nur mit Datenschutz!

*Das sog. eGovernment zieht immer weiter in die tägliche Verwaltungspraxis ein. Diese Entwicklung ist zu begrüßen, solange Datenschutz und Datensicherheit gewährleistet sind.*

Der zunehmende Einsatz von elektronischen Kommunikations- und Verarbeitungsformen auch in der Verwaltung ist schon lange ein Thema (vgl. etwa 19. TB Nr. 1.5 und Nr. 4.7) und wird allgemein als eGovernment bezeichnet. Darunter fallen aber ganz unterschiedliche Bereiche. Die elektronische Kommunikation zwischen Verwaltung und Bürger oder zwischen verschiedenen Verwaltungen anstelle von Brief oder Fax ist etwas anderes als die Umstellung der verwaltungsinternen Verfahrensabläufe auf elektronische Abwicklung und Speicherung. Wieder anders zu beurteilen ist die verwaltungsübergreifende Vernetzung verschiedener Dateien mit online-Zugriffsberechtigungen oder die Entwicklung von Gemeinschaftsprojekten verschiedener Stellen zur Effizienzsteigerung der Verwaltung insgesamt. Jedes einzelne Projekt ist deswegen daraufhin zu prüfen, ob es den Anforderungen gerecht wird, die sich jeweils aus dem informationellen Selbstbestimmungsrecht der Betroffenen ergeben. Vielfach wird allerdings nur Fragen der Datensicherheit nachgegangen, die inhaltlichen Anforderungen des Datenschutzes werden aber vernachlässigt. Datenschutzrechtlich sind die folgenden Punkte von Bedeutung:

- Datenvermeidung und Datensparsamkeit (z. B. Pseudonymisierung);
- sichere Transaktionen über das öffentliche Netz;
- Transparenz der Verfahren (Datenschutzinformationen, elektronische Auskunft, Berichtigung, Löschung);
- Beachtung der Zweckbindung und anderer datenschutzrechtlicher Vorschriften sowie
- datenschutzgerechte Gestaltung der Internetangebote (nur zulässige Daten ins Internet, rechtzeitige Löschung von Verbindungsdaten, Anbieterkennzeichnung, Reduzierung von Cookies, Anonymität von Statistiken).

Im Berichtszeitraum habe ich verschiedene eGovernment-Projekte begleitet, aber auch allgemein die mit eGovernment verbundenen datenschutzrechtlichen Fragestellungen aufgegriffen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen eigenen Arbeitskreis eGovernment eingesetzt, der gemeinsame Lösungsansätze entwickelt, da eGovernment-Projekte länderübergreifend entwickelt werden und häufig auch die Bundesverwaltung einbeziehen. Außerdem hat sie die Entschließungen

- „Sicherheit bei eGovernment durch Nutzung des Standards OSCI“ (Anlage 12) und
- „Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren“ (Anlage 14)

gefasst.

**Elektronische Akte beim Bundesamt für den Zivildienst (BAZ)**

Die Verdrängung des Papiers durch den Einsatz elektronischer Systeme für die Dokumentenverwaltung schreitet voran und hat auch das Bundesamt für den Zivildienst erreicht. Das BAZ, das zum Geschäftsbereich des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) gehört, befindet sich in einem umfassenden Modernisierungsprozess. Das Projekt e-Akte ist dabei ein wesentliches Element. Die Anträge auf Anerkennung als Kriegsdienstverweigerer gehen zunächst bei den Kreiswehrersatzämtern (KWEÄ) ein. Diese übermitteln sie an das BAZ. Hier werden sie abschließend bearbeitet. Bislang geschah dies in Papierform. Die KWEÄ führen die Personalakten der Wehrpflichtigen aber bereits weitgehend elektronisch. Sofern ein Wehrpflichtiger einen Antrag auf Anerkennung als Kriegsdienstverweigerer stellt, werden die Akten von den KWEÄ ausgedruckt und dem BAZ per Post zur Bearbeitung zugeleitet. Dieser Medienbruch soll zukünftig vermieden werden.

Bereits in 2002 entschied sich das BMFSFJ u. a. für die Einführung der e-Akte, mit der die Arbeitsabläufe effizi-

enter und die Kosten für die Aktenlagerung sowie die Bearbeitungszeiten reduziert werden sollen. Ein weiteres Ziel ist die deutliche Erhöhung der Qualität von Auskünften durch den Zugriff auf den aktuellen elektronischen Datenbestand. Nach Vorgabe des BMFSFJ wird die e-Akte in mehreren Stufen eingeführt. Die erste Stufe umfasst u. a. die Einführung der elektronischen Personalakte (s. u. Nr. 14.2 und 14.3). Hierzu gehören insbesondere der elektronische Akten- und Datenaustausch mit den KWEÄ, die automatisierte Aktenverteilung im Bereich der Anerkennung und die elektronische Wiedervorlage im Bereich der Betreuung der Zivildienstpflichtigen.

Der Pilotbetrieb hierzu mit zunächst ca. 30 Mitarbeitern hat begonnen. Grundlegende datenschutzrechtliche Bedenken gegen den Einsatz der e-Akte habe ich nicht, da bewährte datenschutzrechtliche Standards wie Zugriffsberechtigungskonzepte und Protokollierungen Anwendung finden. Ich habe jedoch auf einige Punkte aufmerksam gemacht, die die Benutzung des Systems aus datenschutzrechtlicher Sicht noch verbessern können, wie z. B. die Einrichtung einer elektronischen Poststelle, für die ich ein Konzept entwickelt habe. Die weitere Entwicklung werde ich begleiten.

**eGovernment bei den Sicherheitsbehörden**

Auch im Bereich der Inneren Sicherheit sind im Berichtszeitraum wichtige Projekte der elektronischen Datenverarbeitung umgesetzt worden. So ist über das neue Vorgangsbearbeitungssystem (Artus) bei der Bundespolizei (s. u. Nr. 5.3.1), den Ausbau der elektronischen Informationsverarbeitung beim MAD (s. u. Nr. 5.6.1) und den Umbau der IT-Struktur beim BND (s. u. Nr. 5.7.3) zu berichten.

## 4.8 Effektive Datenlöschung

*Wird bei Disketten, Festplatten, USB- oder Flash-Speicherbausteinen nur die Löschfunktion des Betriebssystems genutzt, können persönliche Daten leicht wiederhergestellt werden. Für diese Speichermedien können daher nur spezielle Löschprogramme empfohlen werden. Ansonsten können bei Verkauf oder Aussonderung gebrauchter Geräte vermeintlich gelöschte Daten von Unbefugten leicht rekonstruiert werden.*

**Datenlöschung bei USB-Sticks und Speicherkarten**

Die Verwendung mobiler Speichermedien, wie USB-Sticks und Speicherkarten ist sehr verbreitet; vielfach ersetzen sie die bisher dazu verwendeten Medien wie Diskette, CD und DVD. Als mobile Speichermedien sollen hier Datenspeicher betrachtet werden, die ohne Stromversorgung betrieben werden, wieder beschreibbar sind, ohne Aufwand transportiert werden können und betriebssystemunabhängig sind. Nach Jahren sorglosen Einsatzes solcher Speicher, weise ich mit Nachdruck auf die damit verbundenen Sicherheitsrisiken hin:

1. Die Benutzer gehen fälschlicherweise davon aus, dass das Löschen der Daten auf einem mobilen Speichermedium endgültig sei, und Daten nicht mehr lesbar seien, wenn sie auf dem Speichermedium gelöscht wurden.
2. Ein sorgloser Umgang mit diesen Speichermedien kann leicht zur Verbreitung von Schadprogrammen (Viren, Trojaner) führen.
3. Auch der mit dem USB-Stick verbundene Rechner kann zur Gefahr werden, wenn der gesamte USB-Speicher – und damit auch die vermeintlich gelöschten Daten – auf den Host kopiert werden und nicht nur einzelne ausgesuchte Dateien. Betroffen wäre in diesem Fall der gesamte Speicherbereich des USB-Speichermediums. Ein entsprechendes (kostenloses) Programm steht hierzu im Internet zur Verfügung (USBDumper).

Vor dem Hintergrund des sehr verbreiteten Einsatzes solcher Medien, habe ich die Fachhochschule Bonn-Rhein-Sieg gebeten, das Löschen auf mobilen Speichermedien unter Windows und Linux zu untersuchen. Die Ergebnisse der Projektarbeit bestätigen, dass einfach gelöschte Daten in der Regel wiederherstellbar sind; aber je nach Betriebssystem unterschiedliche Methoden existieren, um Daten so zu löschen, dass sie nicht wiederherstellbar sind. Der gesamte Bericht steht auf meiner Internetseite zum Abruf zur Verfügung. Die Ergebnisse sind aus datenschutzrechtlicher Sicht ernüchternd. Sie zeigen, dass der Einsatz solcher Medien geeignete Löschtools voraussetzt. Besonders brisant ist die unvollkommene Löschung der Daten bei Verkauf der Geräte in Online-Börsen. Beim Verkauf von Digital-Kameras, Camcordern, digitalen Diktiergräten, Handys und anderen Geräten, die mit solchen Speicherkarten arbeiten, könnten so persönliche Daten ohne Wissen des Betroffenen ungewollt an Dritte übermittelt werden – sofern vorher nicht richtig gelöscht wurde. Dies musste auch jener Bürger erfahren, der sich Hilfe suchend an mich gewandt hatte, weil er beim Verkauf seiner gebrauchten Digitalkamera über eine Online-Börse die privaten Bilder nicht mit der gebotenen Sicherheit auf der Speicherkarte gelöscht hatte.

**Umgang mit gebrauchten und ausgesonderten Festplatten**

Jeder Computerbenutzer kennt die Situation: Nicht mehr benötigte Dateien sollen gelöscht werden. Mancher denkt sich, ein Druck auf die Löschtaste oder ein einfacher Löschbefehl im Explorer genügt. Dies mag für den Alltagsgebrauch angemessen erscheinen. Wenn es sich aber um sensible Daten handelt, ist diese einfache Löschmethode bei weitem nicht ausreichend. Vielen Computerbenutzern ist nicht bekannt, dass dabei lediglich die Einträge im Dateiverzeichnis des jeweiligen Datenträgers entfernt werden, und selbst dies geschieht nicht vollständig. Wenn ein Computer mit einer Festplatte verkauft wird, ist es dem Käufer in vielen Fällen ohne weiteres möglich, den vermeintlich gelöschten früheren Inhalt zu rekonstruieren. Die Folge davon ist, dass die Daten Dritten unbefugt zur Kenntnis gelangen und unter Umständen missbraucht werden. Auch bei vielen Löschprogrammen werden die Dateninhalte nicht tatsächlich gelöscht, sondern es wird nur die Verknüpfung im „Inhaltsverzeichnis“ auf dem Datenträger (Festplatte, Disketten, Speicherkarten, USB-Stick, etc.) gelöscht. Da die Daten weiterhin

Abbildung 4 (zu Nr. 4.8)

vorhanden sind, können sie beim Verkauf, bei einer Reparatur oder bei der Aussonderung des Gerätes von Unbefugten ausgelesen werden. Für sensible Daten gibt es nur wenige Möglichkeiten der sicheren Vernichtung. Hierbei empfehle ich aus Sicherheitsgründen die Hardware-Lösungen.

**Software-Lösungen:**

Das BSI beschreibt im IT Grundschutz-Handbuch das Löschen von Datenträgern (http://www.bsi.de/gshb/deutsch/m/m02167.htm) und bietet für Bundes-, Landes- und Kommunalverwaltungen das Festplatten-Löschprogramm VS-Clean Version 2.1 kostenlos an. VS-Clean wurde vom BSI zum sicheren Wiederaufbereiten magnetischer Datenträger nach behördlichen Richtlinien entwickelt (die Spezifikation der Software, die Bezugsquelle und der Preis für Privat-Personen ist unter http://www.bsi.de/produkte/vsclean/index.htm einzusehen).

Des Weiteren werden zum Löschen von Datenträger verschiedene Programme auf dem freien Markt angeboten.

Software-Lösungen reichen aber nachweislich nicht, um die Daten von der Festplatte nachhaltig und vor allem gründlich zu löschen.

**Hardware-Lösungen:**

Als sichere Löschung kommt die Datenträgervernichtung durch Entmagnetisieren (Degausser-Technik), Ausglühen oder Schreddern in entsprechend gesicherten Vernichtungsanlagen bei einer zertifizierten Recycling-Firma in Frage.

Beim professionellen Löschen mit einem Entmagnetisierer (Degausser) wird der Datenträger mehreren Magnetfeldern von sich ändernder Polarität und allmählich abnehmender Stärke ausgesetzt. Selbst bei diesem gründlichen Verfahren gibt es aber immer noch die Gefahr von Restmagnetisierungen und damit der Datenrückgewinnung.

Das „Ausglühen“ der Datenträger in einer Verbrennungsanlage ist eine sichere Löschmöglichkeit. Beim Ausglühen verliert die Kobalt-Nickel-Legierung, deren Schmelzpunkt bei 700°C liegt, ihre magnetischen Eigenschaften. Damit sind die Daten irreversibel gelöscht.

Beim „Schreddern“ werden die Datenträger mechanisch zermalen. Dann ist eine Reproduktion der Daten nur unter erheblichen Aufwand möglich. Nach dem Verbrennen des Schreddergutes ist der Datenträger endgültig gelöscht. Ich empfehle die Vernichtung von sensiblen Datenträgern unter Aufsicht des Auftraggebers durchführen zu lassen, was bei verschiedenen Recycling-Firmen angeboten wird.

Bei einer professionellen Datenträgervernichtung werden in einem Zertifikat Typ, Hersteller, Modell und Seriennummer bei der endgültigen Vernichtung des Datenträgers dokumentiert.

Auch bei neuer Hardware sind „Garantiefälle“ zu beachten: Vorbeugend sollte beim Kauf von IT-Gerät im Kaufvertrag ein Passus wie „Keep Your Harddrive“ enthalten sein. Dann kann man – evtl. gegen eine geringe Gebühr – im Gewährleistungsfall kostenlosen Ersatz ohne Rückgabe der defekten Festplatte erhalten.

Eine Bemerkung zum Schluss: Festplatten und andere Datenträger mit sensiblen Daten befinden sich auch in weiteren Geräten wie Netzwerkdruckern, Digicams, Faxgeräten, Diktiergeräten und Kopierern. Auch hier ist also Vorsicht angebracht.

Kasten zu Nr. 4.8

**Darauf ist zu achten: 9 Tipps zur effektiven Löschung von Daten**

1. Sicheres Löschen erfordert technisch-organisatorische Maßnahmen in allen Phasen der Verarbeitung, insbesondere bei Veräußerung, Vermietung, Aussonderung, Rückgabe, Reparatur und Wartung von Datenträgern.
2. Die Maßnahmen sind durch konkrete Handlungsanweisungen zu untersetzen. Diese Anweisungen müssen den Schutzbedarf der zu löschenden Daten ebenso berücksichtigen wie den Aufwand und die Kosten für eine mögliche Datenwiederherstellung.
3. Schutzwürdige Daten (§ 3 Abs. 9 BDSG) sind in verschlüsselter Form zu speichern.
4. Das einmalige, komplette Überschreiben mit Zufallszahlen sollte beim Löschen von Daten jeder Art praktiziert werden. Mehrmaliges Überschreiben ist beim Löschen personenbezogener Daten mittlerer und höherer Schutzstufen erforderlich. Hierbei können spezielle Softwarewerkzeuge zum Einsatz kommen.
5. Soll ein noch intakter Datenträger verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger zu löschen.
6. Das selektive Löschen einzelner Dateien durch Überschreiben ist nur dann geeignet, wenn sichergestellt ist, dass keine Kopien der in diesen Dateien

enthaltenen Daten an anderen Orten abgelegt wurden.

7. Das Löschen durch Überschreiben ist durch geeignete und geprüfte Softwarewerkzeuge vorzunehmen und stichprobenartig zu kontrollieren.
8. Defekte Datenträger, deren Daten nicht mehr mit Softwarewerkzeugen überschrieben werden können, sind durch mechanische oder thermische Zerstörung (Disketten, DD, DVD, Festplatten) bzw. durch magnetische Durchflutung (Disketten) unbrauchbar zu machen.
9. Müssen Datenträger ohne sicheres Löschen der Daten aus der Hand gegeben werden (z. B. Reparatur, Rückgabe an den Hersteller in der Garantiezeit), ist in Abhängigkeit von der Sensibilität der Daten durch vertragliche Regelungen zu verhindern, dass unerwünschte Informationsflüsse stattfinden oder von Angreifern ausgenutzt werden. Ggf. sind Schadensersatzansprüche zu vereinbaren oder es ist auf Garantieansprüche zu verzichten.

## 4.9 IVBB – Zielpunkt für neue Angriffe

*Der Informationsverbund Berlin-Bund (IVBB) wird gezielt aus dem Internet angegriffen, um an vertrauliche Informationen zu kommen.*

Der IVBB ist in hohem Maße Angriffen durch Schadsoftware ausgesetzt und wird mit unerwünschten E-Mail (SPAM) „überflutet". Die Abwehrmaßnahmen der Firewall des IVBB können nur bei bekannten Angriffen und bekannter Schadsoftware greifen. Derzeit liegt das E-Mail-Aufkommen in einem normalen Monat im IVBB bei ca. 20 Mio. E-Mails. Davon sind ca. 80 Prozent unerwünscht, Tendenz steigend. Zur Absicherung der regierungsinternen Kommunikation hat der IVBB daher den E-Mail-Verkehr zwischen den IVBB-Teilnehmern untereinander und den E-Mail-Verkehr von bzw. zu externen Teilnehmern vollständig getrennt. Dadurch sollen interne Engpässe vermieden und SPAM besser zurückgehalten werden.

Die Zahl der gezielten Angriffe auf das Regierungsnetz ist ebenfalls steigend. Stichproben belegen, dass gezielte Angriffe auf vertrauliche Informationen (Datendiebstahl) von außen versucht werden. Untersuchungen des BSI haben zudem ergeben, das diese Angriffe teilweise mit hohem technischen Know-how durchgeführt werden. Zwar soll ein Virenschutzkonzept nach dem Stand der Technik diese Angriffe verhindern. Gleichwohl verbleibt eine Sicherheitslücke, da individuelle Spionageprogramme von Virenschutzprogrammen und andere Maßnahmen häufig erst nach einiger Zeit entscheidend und wirksam bekämpft werden können.

Zur Minimierung dieser Gefahren werden die Sicherheitsmaßnahmen gegen Spam und Denial-of-Service-Angriffe kontinuierlich weiterentwickelt. Dabei sollen Angriffe auf Informationen erkennbar gemacht werden, um gezielte Gegenmaßnahmen einleiten und die Teilnehmer des IVBB wirksam schützen zu können. Wesentliche Elemente der Abwehrstrategie sind die Aufzeichnung und Analyse bestimmter Logdaten und die Auswertung infizierter E-Mails, die vom Virenschutz abgefangen wurden.

Bei allen Gegenmaßnahmen muss der Schutz der Vertraulichkeit der übermittelten Informationen und der Datenschutz der Nutzerinnen und Nutzer des IVBB gewährleistet bleiben. So dokumentieren Logdateien das Nutzungsverhalten und geben Auskunft über die jeweiligen Kommunikationspartner und unterliegen insofern dem Fernmeldegeheimnis. Andererseits verkenne ich nicht die Risiken, denen auch personenbezogene und sonstige Informationen durch Hacking-Angriffe ausgesetzt sind.

Ich habe deshalb der Analyse von Protokolldaten des IVBB unter der Voraussetzung zugestimmt, dass die erweiterte Analyse von Protokolldaten auf 6 Monate befristet wird, sich auf bestimmte teilnehmende Stellen beschränkt und erst nach entsprechender Information der Nutzer erfolgt. Ferner habe ich darauf gedrungen, dass in der Regel anonymisierte oder zumindest pseudonymisierte Daten verwendet werden und nur in Ausnahmefällen der vollständige Personenbezug ermittelt wird, wenn dies für die Aufklärung eines Angriffs bzw. einer stattgefundenen Sicherheitsbeeinträchtigung unabdingbar ist und nach Abschluss der erweiterten Protokollierung mir und den IVBB-Teilnehmern über die Ergebnisse berichtet wird.

## 4.10 Viren, Trojaner, Phishing, Spyware, Spam und SPIT

*Der elektronischen Werbeflut – oft mit Schadsoftware versehen – Herr zu werden, stellt sowohl Privatpersonen als auch Betreiber größerer Netzwerke und Software-Entwickler vor neue Herausforderungen.*

Im Mai 2004 wurde ein E-Mail-Server im Regierungsnetz IVBB (Informationsverbund Berlin-Bonn) durch Werbemails in die Knie gezwungen (vgl. 20. TB Nr. 13.8). Nicht zuletzt wegen dieser erheblichen Störung, hat der Betreiber mittlerweile eine leistungsfähige Anti-Spam-Lösung etabliert. Untersuchungen ergaben, dass bei Rechnern, die ohne Schutzvorrichtungen mit dem Internet verbunden waren, bereits nach der ersten Sekunde Angriffe registriert wurden und nach wenigen Monaten sich mehr als 10 000 verschiedene Schadprogramme auf den, auch Honeypots genannten, Systemen befanden. Dabei kommt es durch Schadprogramme (Viren, Trojaner, Würmer) nicht nur zu Identitätsdiebstahl und Löschung von Daten oder Programmen. Der eigene PC kann durch Schadprogramme über eine „Steuerungssoftware" auch Teil eines Bot-Netzes werden. Dadurch sind dann über den eigenen Rechner – unbemerkt für den Anwender – ferngesteuerte Angriffe im Internet möglich. Schätzungen gehen davon aus, das über 50 000 PCs täglich in diesen Bot-Netzen von außen kontrolliert werden.

Elektronischer Werbemüll („Spam") und die damit eingeschleusten Schadprogramme haben erhebliche Auswirkungen auf den Datenschutz und können große materielle Schäden verursachen. So ist es möglich, dass mittels Schadsoftware Festplatten durchsucht, deren Inhalte ma-

nipuliert und sogar Hardwarekomponenten unbrauchbar gemacht werden. Auf diese Weise können Angreifer Kenntnis von sensiblen persönlichen Daten erlangen, ohne dass der Besitzer eines ausgespähten Rechners dies bemerkt.

In den letzten Jahren hat der Betrug durch Phishing, der auf das Ausspähen von vertraulichen Zugangsdaten für Onlinebanking oder Bezahlsysteme, Versandhäuser, Internet-Auktionshäuser, webbasierte Onlineberatungen oder Kontaktportale abzielt, stärker an Bedeutung gewonnen. Hersteller von Internetanwendungen etablieren deshalb mittlerweile entsprechende Schutzmaßnahmen in ihrer Software.

Bereits heute erhält man als Telefonkunde manchen unerwünschten Werbeanruf. Da die Internettelefonie, Voice over IP (VoIP) deutlich preiswerter und leichter automatisierbar ist, wird befürchtet, dass bei VoIP-Anschlüssen die Anzahl belästigender Werbeanrufe deutlich zunimmt. Diese werden auch als „Spam over Internet Telephony" (SPIT) bezeichnet. Allerdings sind die Überlegungen, wie dies abgewehrt werden kann, noch zu keinem befriedigenden Ergebnis gekommen.

Umso wichtiger ist es, dass sich die Betreiber und Nutzer von Computern, die mit dem Internet verbunden sind, dieser Gefahren bewusst sind und zumindest die verfügbaren Schutzmechanismen aktivieren. Neben den bereits erwähnten Sicherheitseinstellungen in der Anwendungssoftware sollten Virenscanner mit aktuellen Virensignaturen und Firewalls verwendet werden. Auch wenn sich hierdurch keine 100-prozentige Sicherheit erreichen lässt, werden so die Daten deutlich besser geschützt.

2005 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) – verantwortlich für die Sicherheit des IVBB – eine umfassende Publikation „Antispam-Strategien" mit dem Untertitel: „Unerwünschte E-Mails erkennen und abwehren." veröffentlicht (http://www.bsi.de/literat/studien/antispam/antispam.pdf).

Auch der Gesetzgeber ist nicht untätig geblieben und will mit dem Telemediengesetz klare gesetzliche Begrenzungen und Sanktionen für die Versendung elektronischer Werbung definieren (s. u. Nr. 10.9).

## 4.11 Trusted Computing

*Bringt Trusted Computing (TC) mehr Sicherheit oder mehr Kontrolle? Führt die vom Datenschutz gewünschte Anonymisierung von Kommunikationsvorgängen zu mehr Sicherheit?*

Trusted Computing Systeme (Personalcomputer, Mobiltelefone usw.) sollen die IT-Sicherheit durch einen zusätzlichen Sicherheitschip, den Trusted Platform Module (TPM), erhöhen. Der TPM (s. Kasten zu Nr. 4.11) ermittelt dazu mittels kryptographischer Verfahren die Integrität sowohl der Software-/Datenstrukturen als auch der Hardware und speichert diese Werte sicher und nachprüfbar bis zur nächsten Prüfung (z. B. bis zum nächsten Rechnerstart) ab. Hierzu wird die Spezifikation der Schnittstellen des TPM durch die Trusted Computing Group (TCG), eine internationale industriebetriebene Standardisierungs-Organisation entwickelt. Dabei sind TPM nicht mehr nur auf dem Mainboard eines Personalcomputers zu finden; sie sollen künftig auch andere Geräte, etwa Mobiltelefone, sicherer machen. Problematisch können TPM-Systeme deshalb sein, weil sie Informationen über die installierte Hard- und Software an Internet-Server übermitteln und damit die Konfiguration der IT-Systeme für Dritte kontrollierbar machen. Dies ist nicht nur datenschutzrechtlich problematisch. Wenn die Informationen in die falschen Hände geraten, könnten sie auch für den Angriff auf IT-Systeme (Hacking) missbraucht werden. Erfreulich ist, dass Anregungen zur Verbesserung des Datenschutzes berücksichtigt wurden, etwa die von der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. März 2003 gefasste Entschließung oder das von der Artikel 29-Gruppe der Europäischen Datenschutzbeauftragten angenommene Arbeitspapier vom 23. Januar 2004 (WP 86). So wurden insbesondere auch Möglichkeiten zur anonymen Kommunikation geschaffen.

Zu begrüßen sind auch Überlegungen der TCG, durch eine Testsuite die korrekte Arbeitsweise des TPM zu prüfen. Untersuchungen der Universität Bochum in 2006 ergaben, dass nicht alle am Markt angebotenen TPM vollständig der Spezifikation folgen.

Durch eine richtige Anwendung könnten viele Sicherheitsprobleme von Systemen deutlich abgemildert bzw. gelöst werden. Europa setzt und fördert offene Standards: So sollen z. B. mit der Entwicklung von OpenTC nur kritische Teile eines Personalcomputers sicher gemacht werden, ohne das gesamte System zu kontrollieren. Hierdurch könnten sich Vorteile durch einen sparsamen Umgang mit Nutzerdaten ergeben.

Datenschutzprobleme sind besonders bei sog. Digital Rights Management-Anwendungen (DRM, s. u. Nr. 6.6) und bei der Benutzertransparenz evident: So ist bei der Weiterentwicklung sicherzustellen, dass

– Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über ihre IT-Systeme bewahren; insbesondere dürfen Zugriffe und Äderungen nur nach vorheriger Information und Einwilligung erfolgen,

– die Nutzung von IT für den Zugriff auf eigene Dokumente und freie Informationen im Internet auch weiterhin ohne Einschränkung oder Kontrolle möglich ist, das bedeutet, ohne dass Dritte davon Kenntnis erhalten oder Nutzungsprofile anlegen können und

– alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind.

Die nach Gesprächen inzwischen erzielten Fortschritte sind zu begrüßen. Den Dialog mit Bundesregierung und TCG werde ich fortsetzen, um dem Datenschutz weiterhin Nachdruck zu verleihen.

Kasten zu Nr. 4.11

**Das ist ein TPM**

Ein Trusted Platform Module (TPM) ist ein fest eingebauter Chip, der hinsichtlich seiner Funktionen und Sicherheitsanforderungen weitgehend einer Smartcard entspricht. Praktisch alle großen PC-Hersteller stellen PC-Systeme mit TPM her. Ein TPM stellt maßgeblich vier Funktionen bereit:

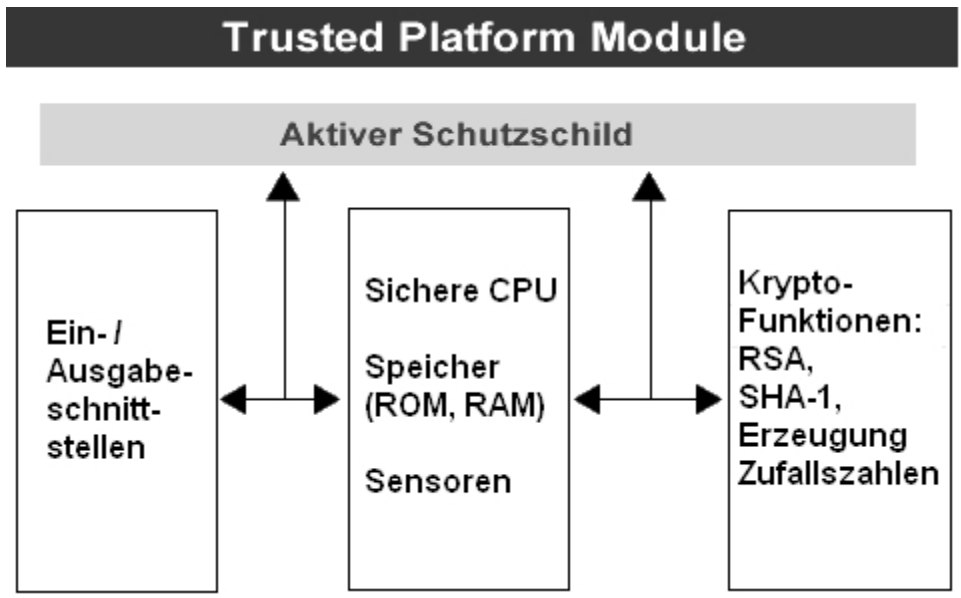
– Authentifizierung der Plattform (Attestation) – Die Authentifizierung des Systems gegenüber Dritten erfolgt über eine Plattform-Signatur und über Attestation Identity Keys, das sind im TPM nur für diesen Zweck erzeugte öffentliche Schlüssel.

– Versiegelung von Daten und Programmen – Dazu werden die zu speichernden Daten/Programme mit einem Konfigurations-Hash signiert. Zugriff ist dann nur noch bei unverändertem Hashwert möglich.

– Sichere Speicherung von Schlüsseln – Auch außerhalb des TPM können Schlüssel gespeichert werden. Dazu wird ein Schlüssel-Baum auf der Festplatte mit einem Key aus dem TPM verschlüsselt. Somit ist die Anzahl der sicher gespeicherten Schlüssel nahezu unbegrenzt.

– Sicherer Zufallsgenerator – Durch eine hardwareseitige Lösung ist die Erzeugung sicherer Zufallszahlen garantiert, sie sind zur Generierung der Schlüssel notwendig.

Weitere Komponenten schützen die Schlüssel und alle kryptographischen Prozesse im TPM.




## 4.12 Nano-Technologie

*Schaltkreise aus Hybridenchips, also aus biologischen und halbleitenden Komponenten, werden bereits erprobt, medizinische Produkte in Nano-Röhren eingebaut und Nano-Partikel gezielt mit bestimmten Eigenschaften oder Markierungen hergestellt. Für den Datenschutz ergeben sich durch diese Technologie neue Fragen und Forderungen.*

Die Nano-Technologie befasst sich mit atomaren oder molekularen Strukturen, also in der Größe eines Nanometer (nm) bis zur Größe von maximal 100 nm. Dabei entspricht ein nm, dem Milliardstel eines Meters. Zum Vergleich: Bei der Fertigung von Mikroprozessoren werden heute Strukturengrößen von 60 nm bis 90 nm verwendet; das menschliche Haar hat etwa einen Durchmesser von 50 000 nm. Für Strukturen kleiner als 50 nm gelten andere physikalische Gesetze, da hier die Quanteneffekte dominierend werden. Allerdings sind viele zur Manipulation von einzelnen Atomen oder Molekülen erforderliche Verfahren heute noch nicht für eine Nutzung in größerem Umfang brauchbar.

Studien zu Zukunftstechnologien gehen von einer Konvergenz zwischen den Bereichen Nano-Technologie, Biologie und Informatik in den nächsten 10 Jahren aus. So sind z. B. winzige autonome Systeme vorstellbar, die biologische Prozesse steuern oder Informationen über

Nano-Strukturen weiterleiten, was von Bedeutung für die Medizin, etwa den gezielten Transport von Medikamenten wäre.

Für den Schutz des Persönlichkeitsrechts sind neue Gefahren durch Produkte der Nano-Technologie vorstellbar:

– Winzige Partikel können Personen kennzeichnen. Durch die gezielte Freisetzung so gekennzeichneter Partikel ließe sich etwa feststellen, wer sich wann an einem bestimmten Ort aufgehalten hat. Dieser Staub wäre dann an der Kleidung, am oder im Körper dieser Personen nachweisbar.

– Viel weiter gehen – heute noch theoretische – Überlegungen, autonome informationstechnische Systeme mit biologischen oder physikalischen Sensoren und mikromechanische Systemen so zusammen zu bauen, dass ein autonomes System – in der Größe weniger Nanometer – entsteht (Smart Dust). Dieser Staub könnte leicht verteilt werden. In den positiven Szenarien könnte er Wetterdaten übermitteln, vor chemischen Produkten oder Waffen warnen. Smart Dust könnte aber auch Personen „erkennen“ oder „beobachten“ und anschließend Daten über diese Personen gezielt an andere Systeme weiterleiten.

Meine Kollegen bei der französischen Datenschutzbehörde (http://www.cnil.fr/) haben eine Studie erstellt und im Internet veröffentlicht, die auch auf die ethischen Aspekte einer Nano-Biologie eingeht.

Ich werde die weitere Entwicklung der Nano-Technologie im Auge behalten.

## 4.13 Zehn Thesen für eine datenschutzfreundliche Informationstechnik

*Anlässlich des am 18. Dezember 2006 stattgefundenen IT-Gipfels der Bundesregierung habe ich Forderungen für eine datenschutzfreundliche Informationstechnik aufgestellt. Zu meinem Bedauern sind praktisch keine Verbraucher- und Datenschützer zu dieser für die Bundesregierung und die Ausrichtung der Informationstechnik in Deutschland sehr wichtigen Veranstaltung eingeladen worden.*

Bei allem Nutzen bringt die Informationstechnik auch Risiken für den Schutz persönlicher Daten mit sich, die durch die frühzeitige Einbeziehung von Datenschutzanforderungen minimiert werden könnten. Ich halte es für unverzichtbar, die Bedingungen und die Folgen der Informationstechnik offen zu diskutieren, dabei auch ihre Risiken auszuloten und Strategien zu ihrer Vermeidung zu entwickeln. Neben wirtschaftlichen und technologischen Aspekten müssen auch die sozialen und rechtlichen Konsequenzen berücksichtigt werden, die sich aus dem zunehmenden IT-Einsatz ergeben. Die teilweise negativen Folgen lassen sich nicht allein durch gesetzliche Ver- oder Gebote verhindern. Bereits bei der Konzeption von IT-Systemen sollten verstärkt Vorkehrungen getroffen werden, die das Recht auf informationelle Selbstbestimmung gewährleisten. Zugleich kann sich Datenschutz auch wirtschaftlich auszahlen. Im Mittelpunkt muss aber bei all diesen Fragen künftiger IT-Ausrichtung der Mensch stehen: Als Bürger, als Kunde und als Betroffener. Sein Recht auf Selbstbestimmung muss in einer immer stärker durch Informationstechnik geprägten Umwelt gewahrt und gestärkt werden. Meine Forderungen zur Ausgestaltung von neuer Informationstechnik aus Datenschutzsicht habe ich anlässlich des von der Bundesregierung im Dezember 2006 durchgeführten „IT-Gipfels“ zusammengefasst.

### Zehn Thesen für eine datenschutzfreundliche Informationstechnik

#### 1 Informationstechnik transparent gestalten

Die Entwickler und Anwender von Informationssystemen müssen dafür sorgen, dass ihre Auswirkungen für den Einzelnen und für die Gesellschaft nachvollziehbar sind. Nur wenn die Betroffenen wissen, welche Konsequenzen neue technische Hilfsmittel haben, können sie souverän damit umgehen. Transparenz schafft zugleich Vertrauen in neue IT-Vorhaben und Technologien. Umfassende Aufklärung, Beratung und Information tragen dazu bei, dass datenschutzfreundliche Technologien sich auf dem Markt durchsetzen können. Das gesetzlich bereits seit langem vorgeschriebene Auskunftsrecht des Betroffenen über die gespeicherten personenbezogenen Daten sollte weiterentwickelt werden und generell auch die Herkunft der Daten umfassen und auch dann greifen, wenn die Daten nur temporär zusammengeführt und zur individuellen Bewertung verwendet werden (Scoring). Soweit IT-Systeme mit dem Zweck der späteren Personalisierung betrieben werden (etwa bei RFID-Chips im Handel), sollten die Betroffenen frühzeitig auf ihre Verwendung hingewiesen werden. Ferner sollten technische Systeme so konzipiert werden, dass sie den Nutzern signalisieren, wenn sie aktiviert werden, damit eine heimliche Datenerhebung vermieden wird. Die Anbieter von elektronischen Produkten und Dienstleistungen müssen die Nutzer darüber informieren, wie sie durch ihr Verhalten Datenschutzgefahren vermeiden können und welche Restrisiken jeweils bestehen. Schließlich sollten die für die Verarbeitung verantwortlichen Stellen dazu verpflichtet werden, die Betroffenen über Datenschutzverstöße zu informieren, wie dies bereits in den meisten US-Bundesstaaten vorgeschrieben ist.

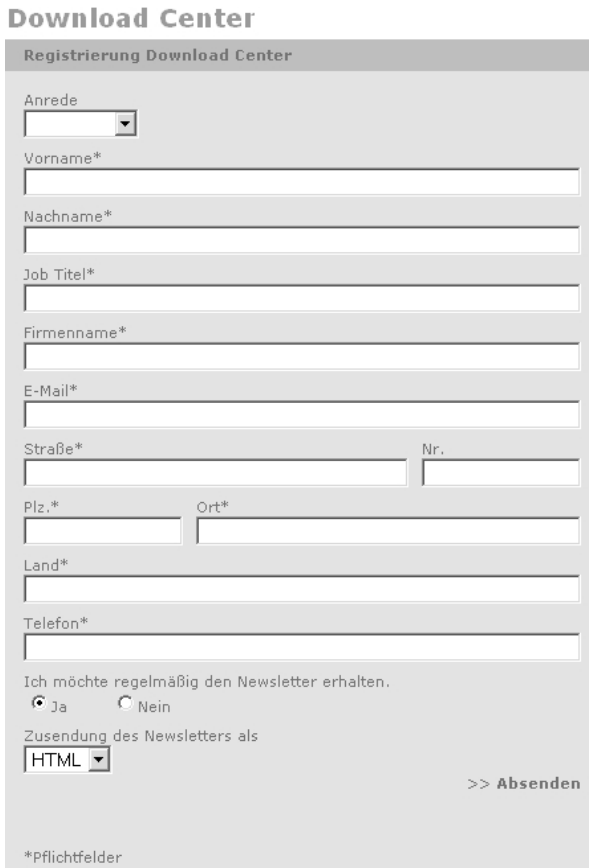
#### 2 Entscheidungsfreiheit des Betroffenen stärken

IT-gestützte Verfahren müssen so ausgestaltet werden, dass sie den Nutzerinnen und Nutzern umfassende Wahlrechte hinsichtlich des Umgangs mit ihren Daten bieten. Gegebenenfalls sollte die Möglichkeit erhalten bleiben, private und öffentliche Dienstleistungen auch ohne Nutzung elektronischer Systeme in Anspruch zu nehmen. Die Erhebung von Daten sollte so weit wie möglich an die informierte Einwilligung der Betroffenen gebunden werden. Der Zugriff auf sensible Daten (etwa medizinische Angaben) sollte grundsätzlich nur mit Zustimmung der Betroffenen möglich sein. Echte Freiwilligkeit ist nur dann gegeben, wenn es wirkliche Alternativen gibt. So sollten z. B. bei kommerziellen Diensten verschiedene

Abbildung 5 zu Nr. 4.13

**Beispiel 1:**

Immer noch werden für Informationsbestellung oder kostenlose Downloads viel zu viele Daten abgefragt.




Bezahlmöglichkeiten angeboten werden, etwa auch datenschutzfreundliche Prepaid-Lösungen. Im Handel verwendete RFID-Chips müssen vom Nutzer deaktivierbar sein, ohne die Funktionalität des Produkts zu beeinträchtigen. Die Betroffenen müssen darüber informiert werden, welche Konsequenzen sich aus ihren Entscheidungen ergeben. Schließlich muss der Einzelne grundsätzlich die Möglichkeit haben, seine Entscheidung nachträglich zu korrigieren und Einwilligungen zu widerrufen.

### 3 Datenschutzanforderungen frühzeitig berücksichtigen

Datenschutz sollte bereits in das System-Design der IT eingebunden werden. Nachträglich aufgepfropfter Datenschutz ist oftmals schlechter und teurer. Deshalb sollte es eine Selbstverständlichkeit sein, dass Konzepte von IT-Verfahren und Geräten möglichen Gefährdungen des Datenschutzes Rechnung tragen. Je sensibler der Anwendungsbereich und die Daten, desto höher sind auch die Anforderungen an Schutzvorkehrungen gegen einen Missbrauch. Die Gewährleistung dieser Anforderungen darf nicht allein dem Anwender überlassen bleiben, sondern sie muss auch durch die Hersteller ermöglicht werden. Nur wenn das Produkt bzw. IT-Verfahren einen datenschutzkonformen Betrieb ermöglicht (etwa durch Zugriffsschutz-, Protokollierungs- und Verschlüsselungsfunktionen), können es die Anwender datenschutzgerecht verwenden.

### 4 Datenvermeidung und Datensparsamkeit

Datenvermeidung und Datensparsamkeit sind Grundprinzipien eines zeitgemäßen Datenschutzes. Verfahren müssen so ausgestaltet werden, dass möglichst wenig personenbezogene Daten erfasst werden. Dieser Grundsatz muss bereits bei der Gestaltung der Technik und ihrer Einsatzbedingungen berücksichtigt werden. Dies gilt vor allem für Prozess- und Verkehrsdaten, die beim Betrieb von IT-Systemen beiläufig anfallen und denen beim Übergang zum Ubiquitous Computing zunehmende Bedeutung zukommt. Diese Daten sollten auf ein Mindestmaß beschränkt und so früh wie möglich gelöscht werden. Elektronische Dienste sollten so gestaltet werden, dass auch hierbei so wenig wie möglich personenbezogene Daten verarbeitet werden. Hierzu können anonyme Nutzungsmöglichkeiten einen wichtigen Beitrag leisten. Soweit eine Individualisierung von Dienstleistungen, Statistiken und wissenschaftlichen Forschungsvorhaben erforderlich ist, sollten soweit wie möglich Pseudonyme verwendet werden. Die in § 3a des Bundesdatenschutzgesetzes enthaltenen Vorgaben Datenvermeidung und Datensparsamkeit müssen mit Leben gefüllt werden.

### 5 Nachprüfbarer Datenschutz

Sowohl Anwender als auch Betroffene müssen prüfen können, ob ein Produkt, eine Dienstleistung oder ein Verfahren datenschutzgerecht ist. Um datenschutzkonforme Lösungen zu erhalten, muss die mit der Umsetzung vertraute Institution den Rahmen vorgeben und nicht der Technik „hinterherlaufen“. Schutzprofile, in denen die Anforderungen des Datenschutzes technikspezifisch konkretisiert werden, können den Grundstein für datenschutzgerechte Lösungen bieten. Soweit Schutzprofile auf einer internationalen Norm basieren, können sie die Gültigkeit der Anforderungen über Grenzen hinweg sicherstellen und einen Wettbewerbsvorteil auf dem internationalen Markt bringen. Datenschutzfreundliche Verfahren können durch Auditverfahren zertifiziert werden. Um die Qualität der Auditierung zu gewährleisten, sollten die qualitativen Anforderungen und das Verfahren zur Vergabe von Datenschutzgütesiegeln – wie im Bundesdatenschutzgesetz vorgesehen – gesetzlich vorgegeben werden. Datenschutzgütesiegel können es den Verbrauchern erleichtern, aus der Vielzahl der Angebote solche auszusuchen, bei denen sie sicher sein können, dass mit ihren Daten sorgfältig umgegangen wird.

### 6 Voreingestellte Sicherheit

Viele Sicherheits- und Datenschutzprobleme bei IT-Produkten sind auf unsichere Grundeinstellungen der Systeme zurückzuführen. So werden Netzwerke häufig ohne Verschlüsselungsfunktion ausgeliefert und dem Normalanwender ist es nur unter Schwierigkeiten oder überhaupt

nicht möglich, einen sicheren Betrieb zu gewährleisten. Damit wird dem Datenmissbrach durch Hacking, Abhörmaßnahmen und Datenmanipulation Vorschub geleistet. Die Hersteller und die für den Betrieb der Systeme verantwortlichen Unternehmen, Forschungseinrichtungen und Hochschulen müssen für sichere Grundeinstellungen sorgen. Verständliche Benutzungshinweise und einfach zu bedienende Hard- und Software müssen es den Anwendern ermöglichen, bei den Produkten eine angemessene Datenschutzstufe einzustellen. Beim professionellen Einsatz von IT muss Datenschutzrisiken durch geeignete Sicherheitskonzepte begegnet werden, bei denen der jeweilige Schutzbedarf der Daten berücksichtigt wird. Es muss gewährleistet sein, dass insbesondere sensible Daten stets angemessen geschützt werden.

A b b i l d u n g 6 zu Nr. 4.13

**Beispiel 2:**

Schutzprofile können eine geeignete Grundlage für die Prüfung von IT-Sicherheit und Datenschutz bilden. Beispiele für vom BSI registrierte Schutzprofile:

| **Titel** |
|---|
| Schutzprofil für USB-Datenträger |
| Protection Profile for a Identity Manager |
| BAROC Smart Card Protection Profile |
| Protection Profile – electronic Health Card (eHC) |
| Protection Profile Secure Module Card (SMC) |
| Protection Profile Professional Health Card (PP-HPC) |
| Protection Profile for Machine Readable Travel Document with ICAO Application, Basic Access Control |
| Protection Profile Biometric Verification Mechanisms |
| Schutzprofil - Benutzerbestimmbare Informationsflusskontrolle (SU/MU) Protection Profile - Discretionary Information Flow Control (SU/MU) |

## 7 Vertraulichkeit der Kommunikation stärken

Das Vertrauen in den Schutz der Privatsphäre und die Vertraulichkeit von Kommunikationsvorgängen ist eine wichtige Grundlage für den Erfolg elektronischer Dienste. Das traditionelle Fernmeldegeheimnis schützt lediglich die Nachrichtenübermittlung mittels Telekommunikationseinrichtungen. Im Zeitalter des Internet, in denen neben die Individualkommunikation vielfältige andere Formen der elektronischen Kommunikation treten, muss das Fernmeldegeheimnis zu einem umfassenden Mediennutzungsgeheimnis ausgebaut werden. Nur wenn der einzelne sicher sein kann, dass sein individuelles Nutzungsverhalten weder durch private noch durch öffentliche Stellen überwacht wird, wird er sich im virtuellen Raum frei bewegen. Neben politischen Entscheidungen und rechtlichen Regelungen zur Weiterentwicklung des Kommunikationsgeheimnisses müssen sichere Konzepte und Produkte der Kommunikationstechnik dazu beitragen, dass die Vertraulichkeit gewahrt wird. Hierzu gehören auch Möglichkeiten zur verschlüsselten Datenübertragung und zur anonymen bzw. pseudonymen Nutzung elektronischer Dienste.

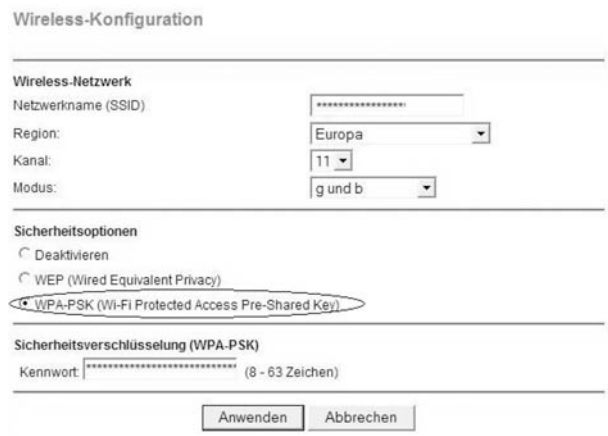
## 8 Datenschutz-Werkzeuge

In einer zunehmend technisch geprägten Umwelt lässt sich die Komplexität von IT-Systemen und elektronischen Dienstleistungen für den Einzelnen immer schwerer beherrschen. Deshalb sollten den Nutzern einfach zu bedienende Instrumente an die Hand gegeben werden, mit denen sie ihre Daten wirksam schützen und den Umgang mit ihnen kontrollieren können. Derartige Werkzeuge – etwa zur Verwendung von Pseudonymen, zur Erzeugung von sicheren Passworten, zum Auslesen des Inhalts von persönlichen Datenspeichern und zur automatischen Bewertung des Datenschutz-Niveaus – müssen entwickelt und kostengünstig bereitgestellt werden. Hierbei können auch Programme zum Identitätsmanagement hilfreich sein, die den Betroffenen dabei unterstützen, selbst darüber zu entscheiden, wem gegenüber er welche persönlichen Daten offenbart. Solche Werkzeuge können einen wichtigen Beitrag zu einem wirksamen Datenselbstschutz leisten.

A b b i l d u n g 7 zu Nr. 4.13

**Beispiel 3:**

Sicherheitseinstellungen müssen als Standardeinstellung konfiguriert sein. Besonders bei nicht kontrollierbaren Netzen wie z. B. WLAN:




## 9 Keine Persönlichkeitsprofile

Vielfältig sind heute die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten: So werden Cookies oder Web Bugs verwendet, um das Nutzungsverhalten von Internetnutzern zu registrieren. In Mobiltelefonen werden fortlaufend Lokalisierungsdaten erzeugt und zunehmend durch Location Based Services ausgewertet. Im Handel erfolgt eine individuelle Registrierung des Kaufverhaltens mittels Verbindung von Produkt- und Käuferdaten. Verkehrsdaten der Telekommunikation geben Auskunft darüber, wer wann mit wem telefoniert hat. Die RFID-Technik erlaubt das heimliche Auslesen von Daten mittels Funk. Beim Geomarketing werden Wohn- und Aufenthaltsorte mit allen möglichen Sekundärinformationen verknüpft, vom Durchschnittseinkommen über das Alter bis zur Kaufkraft. Die Zusammenführung dieser Daten zu Profilen birgt erhebliche Gefahren für das informationelle Selbstbestimmungsrecht. Diesen Gefahren

muss wirksam begegnet werden. Die Verantwortlichen haben dafür zu sorgen, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile – wenn überhaupt – nur mit Wissen und Zustimmung der Betroffenen erstellt werden, sich auf konkret definierte Sachverhalte und Zwecke beschränken und unter Kontrolle der Betroffenen bleiben. Umfassende Persönlichkeitsprofile, in denen alle möglichen privaten und öffentlichen Daten zusammengeführt werden, darf es auch und gerade unter den Bedingungen einer immer leistungsfähigeren Informationstechnik nicht geben.

### 10 Informationelle Selbstbegrenzung von Staat und Wirtschaft

Die Informationstechnik bietet das Potenzial einer Totalüberwachung. Politik und Wirtschaft sind deshalb aufgerufen, mit diesen Möglichkeiten verantwortungsbewusst umzugehen und sich selbst zu begrenzen. Nicht alles, was irgendwie sinnvoll erscheint, darf auch realisiert werden. Stets müssen bei Entscheidungen über den Einsatz von IT-Systemen auch die Wirkungen auf das individuelle Selbstbestimmungsrecht bedacht werden. Die Grundsätze der Menschenwürde und der Verhältnismäßigkeit sind verfassungsrechtlich verankert. Ihre Beachtung ist für eine demokratische Informationsgesellschaft von entscheidender Bedeutung. Daraus ergibt sich, dass es eine Rundumüberwachung genauso wenig geben darf wie eine Kontrolle des Kernbereichs der Privatsphäre. Diese Grundsätze sind nicht nur bei der Erhebung von Daten bedeutsam, sondern auch bei ihrer weiteren Nutzung. Insbesondere Daten, die bei der Verwendung von IT-Systemen automatisch generiert werden, können vielfältig miteinander verknüpft werden. Eine Mehrfachnutzung von Daten mag wirtschaftlich oder auch politisch sinnvoll erscheinen. Zweckänderungen bedürfen jedoch auch unter veränderten technologischen Bedingungen grundsätzlich der Zustimmung des Betroffenen oder einer ausdrücklichen gesetzlichen Erlaubnis. IT-Systeme müssen so gestaltet werden, dass die Zusammenführung für unterschiedliche Zwecke gespeicherter Datenbestände nur unter klar definierten und kontrollierten Bedingungen erfolgen kann.

## 5 Innere Sicherheit

### 5.1 Neue Sicherheitsarchitektur

*Bei der Weiterentwicklung der Sicherheitsinfrastruktur von Bund und Ländern müssen die verfassungsrechtlichen Vorgaben berücksichtigt werden.*

Die Weiterentwicklung der Sicherheitsinfrastruktur, d. h. der Organisation von Polizeibehörden und Nachrichtendiensten und ihre Zusammenarbeit, bilden eines der zentralen Projekte der Bundesregierung im Bereich der Inneren Sicherheit. Im Koalitionsvertrag von 2005 wird in diesem Zusammenhang auch angekündigt zu „überprüfen, inwieweit rechtliche Regelungen etwa des Datenschutzes einer effektiven Bekämpfung des Terrorismus entgegenstehen“. In der Berichtsperiode wurden dementsprechend zwei wesentliche Gesetzgebungsvorhaben auf den Weg gebracht, die den Sicherheitsbehörden neue Datenverarbeitungsbefugnisse einräumen, das Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz – Bundestagsdrucksache 16/2950 – s. u. Nr. 5.1.1) und das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (Terrorismusbekämpfungsergänzungsgesetz – Bundestagsdrucksache 16/2921 – s. u. Nr. 5.1.2). Beide Gesetzentwürfe hat der Deutsche Bundestag am 1. Dezember 2006 verabschiedet.

Wie in meinem 20. Tätigkeitsbericht ausgeführt (Nr. 5.1.1), müssen bei der Intensivierung der Zusammenarbeit zwischen Polizei und Nachrichtendiensten die Vorgaben des Grundgesetzes beachtet werden. Zu beachten ist insbesondere das verfassungsrechtliche Trennungsgebot (vgl. Kasten zu Nr. 5.1), das die informationelle Zusammenarbeit von Polizei und Nachrichtendiensten begrenzt, um zu verhindern, dass die organisatorische Trennung von Polizei und Geheimdiensten durch wechselseitige Unterstützungs- und Hilfsmaßnahmen unterlaufen wird.

Diese Auswirkung des Trennungsgebots hat auch der Verfassungsgerichtshof des Freistaates Sachsen in seinem Urteil vom 21. Juli 2005 (Az.: Vf. 67-II-04) hervorgehoben. Danach ist das Gebot der organisatorischen Trennung unvollständig, wenn es nicht zugleich eine Abgrenzung der Aufgaben von Polizei und Geheimdiensten beinhaltet. Nur so könne vermieden werden, dass die Nachrichtendienste im Rahmen ihrer Aufgabenerfüllung unter Einsatz nachrichtendienstlicher Mittel gewonnene Daten an die Polizei übermitteln und auf dieser Datengrundlage polizeiliche Maßnahmen auch in den Fällen angeordnet werden, in denen diese Daten durch polizeiliche Maßnahmen nicht hätten erhoben werden dürfen. Andernfalls könnten rechtsstaatlich ausgeformte Handlungsschwellen für den Einsatz polizeilicher Mittel unterlaufen werden. Das Trennungsgebot verhindert somit nicht die insbesondere zur Terrorismusbekämpfung notwendige Zusammenarbeit von Sicherheitsbehörden, setzt ihr allerdings Grenzen, die auch vom Gesetzgeber zu beachten sind.

Kasten zu Nr. 5.1

**Trennungsgebot**

Das Trennungsgebot von Polizei und Nachrichtendiensten beruht auf dem Schreiben der Militärgouverneure an den Parlamentarischen Rat über die Polizei-Befugnisse der Bundesregierung vom 14. April 1949. Punkt 2 dieses Polizeibriefs regelt: „Der Bundesregierung wird auch gestattet, eine Stelle zur Sammlung und Verbreitung von Auskünften über umstürzlerische, gegen die Bundesregierung gerichtete Tätigkeiten einzurichten. Diese Stelle soll keine Polizeibefugnis haben.“ Aufgrund dieser Vorgabe bestimmt beispielsweise § 8 Abs. 3 des Bundesverfassungsschutzgesetzes: „Polizeiliche Befugnisse oder Weisungsbefugnisse stehen dem Bundesamt für Verfassungsschutz nicht zu; es darf die Polizei auch nicht im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.“

Inhaltliche Ausgestaltung/Rechtsfolgen des Trennungsgebots:

1. Organisationsrechtlich

   Organisatorische Trennung von Geheimdiensten und polizeilichen Dienststellen.

2. Materiell-rechtlich

   Wahrung der rechtlichen Grenzen der den Polizeien und Nachrichtendiensten zugewiesenen spezifischen Aufgaben und Befugnisse.

3. Informationell

   Begrenzung der informationellen Zusammenarbeit von Polizei und Geheimdiensten, um zu verhindern, dass die organisatorische Trennung dieser Sicherheitsbehörden durch wechselseitige Unterstützungs- und Hilfsmaßnahmen unterlaufen wird.

Dieses Trennungsgebot hat Verfassungsrang. Es ist zudem in mehreren Landesverfassungen explizit verankert.

### 5.1.1 Gemeinsame-Dateien-Gesetz

*Ob das Gemeinsame-Dateien-Gesetz im Einklang mit dem Gebot der Trennung von Polizei und Nachrichtendiensten steht, bleibt verfassungsrechtlich zweifelhaft.*

Mit dem vom Deutschen Bundestag am 1. Dezember 2006 verabschiedeten Gesetz zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz – Bundestagsdrucksache 16/2950) wurden erstmals die rechtlichen Grundlagen für die Errichtung einer gemeinsamen Antiterrordatei sowie anlassbezogener gemeinsamer Projektdateien von Polizeibehörden und Nachrichtendiensten geschaffen. Eine informationelle Kooperation dieser Art war bisher nicht zulässig. Meine verfassungs- und datenschutzrechtlichen Bedenken, insbesondere zur Gestaltung einer gemeinsamen Antiterrordatei beim Bundeskriminalamt, wurden in dem Gesetzgebungsverfahren im Wesentlichen nicht ausgeräumt.

Mit der Antiterrordatei wird ein im Online-Verbund nutzbarer Datenbestand geschaffen, in dem die Erkenntnisse von Polizeien und Nachrichtendiensten im Bereich der Terrorismusbekämpfung zusammengeführt werden (vgl. Artikel 1 des Gemeinsame-Dateien-Gesetzes: „Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Antiterrordateigesetz – ATDG)“). Erfasst werden bei den Polizeien und Nachrichtendiensten vorhandene – auch vage – Informationen zu Ziel- und Randpersonen (mutmaßlichen Unterstützern, Kontaktpersonen etc.) aus dem Bereich des internationalen Terrorismus und des ihn unterstützenden Extremismus mit Bezug zum Inland.

Ich verkenne nicht die Bedrohung durch den internationalen Terrorismus, mit der der Gesetzentwurf begründet wird. In ihrer Entschließung zur Antiterrordatei vom 27. Oktober 2006 hat die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder dies zum Ausdruck gebracht und zugleich betont, dass jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot von Polizei und Nachrichtendiensten (vgl. Nr. 5.1) entsprechen müsse (s. Kasten a zu Nr. 5.1.1).

Kasten a zu Nr. 5.1.1

**Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg**

**Verfassungsrechtliche Grundsätze bei Antiterrordatei-Gesetz beachten**

Mit dem Entwurf eines Gesetzes zur Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten des Bundes und der Länder (Gemeinsame-Dateien-Gesetz, Bundestagsdrucksache 16/2950) – verschärft durch Forderungen aus dem Bundesrat – sollen in der Bundesrepublik Deutschland erstmals die rechtlichen Grundlagen für die Errichtung gemeinsamer Dateien von Polizeibehörden und Nachrichtendiensten geschaffen werden. Von besonderer Bedeutung ist die beim Bundeskriminalamt zur Aufklärung und Bekämpfung des internationalen Terrorismus einzurichtende Antiterrordatei, in welcher umfangreiches Datenmaterial der beteiligten Sicherheitsbehörden zusammengeführt werden soll.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verkennt nicht die zur Begründung des Gesetzentwurfs geltend gemachte hohe Bedrohung durch den internationalen Terrorismus und die Notwendigkeit zur Optimierung des Informationsaustauschs. Jede Intensivierung der informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten muss jedoch den verfassungsrechtlichen Vorgaben, insbesondere dem Recht auf informationelle Selbstbestimmung, dem Grundsatz der Verhältnismäßigkeit und dem – in einigen Landesverfassungen ausdrücklich genannten – Trennungsgebot zwischen Polizei und Nachrichtendiensten entsprechen. Der vorliegende Entwurf zur Antiterrordatei enthält schwerwiegende verfassungs- und datenschutzrechtliche Risiken.

Insbesondere den folgenden brisanten Aspekten wird im Rahmen der anstehenden parlamentarischen Beratungen besondere Beachtung zu schenken sein:

- Die Anti-Terror-Datei sieht gravierende Erweiterungen des Datenaustauschs vor. Deshalb ist zumindest eine weitergehende Präzisierung der zu erfassenden Personen erforderlich. Insoweit ist insbesondere zu berücksichtigen, dass die Nachrichtendienste in der Antiterrordatei auch Personen erfassen, bei denen nur auf weichen Informationen beruhende tatsächliche Anhaltspunkte für eine Zuordnung zum internationalen Terrorismus bestehen. Diese Anhaltspunkte können auf legalem Verhalten beruhen, mit der Folge, dass auch unbescholtene Personen in der Antiterrordatei erfasst werden und deren Daten allen zugriffsberechtigten Behörden zur Verfügung stehen. Dass im Bereich der Vorfeldermittlungen ein besonders hohes Risiko einer Fehlprognose besteht, ist auch bereits verfassungsgerichtlich festgestellt.
- Die Definition der in der Datei zu erfassenden sog. Kontaktpersonen muss präzisiert werden und der Kreis der Betroffenen ist einzuschränken. Dies gilt insbesondere für solche Kontaktpersonen, gegen die keinerlei belastende Erkenntnisse vorliegen. Es muss sichergestellt werden, dass nicht bereits unverdächtige soziale Kontakte zu einer Erfassung von Personen aus dem Umfeld Verdächtigter führen.
- Die Aufnahme besonderer Bemerkungen, ergänzender Hinweise und Bewertungen in Freitextform eröffnet den am Verbund teilnehmenden Behörden die Möglichkeit, eine Vielzahl, auch weicher personenbezogener Informationen (z. B. nicht überprüfte Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Datei zu erfassen. Deshalb sollte darauf verzichtet werden.
- In diesem Zusammenhang ist auch der Zugriff von Polizeibehörden auf Vorfelderkenntnisse der Nachrichtendienste im Hinblick auf das Trennungsgebot kritisch zu hinterfragen. Besonders bedenklich erscheint dabei die Zulassung von Ausnahmen vom verfassungsrechtlichen Trennungsgebot in den sog. Eilfällen, in welchen den beteiligten Behörden ein unmittelbarer Online-Zugriff auf alle Daten gestattet wird.
- Die zugriffsberechtigten Sicherheitsbehörden sind nicht klar genug bezeichnet. Aufgrund der Speicherung auch höchst sensibler personenbezogener Vorfelddaten muss der Gesetzgeber aus rechtsstaatlichen Gründen selbst festlegen, welche Stellen zugriffsberechtigt sein sollen.
- Im Übrigen sind auch die bereits jetzt erkennbaren Tendenzen zu einer Erweiterung der Antiterrordatei über die Terrorismusbekämpfung hinaus nicht akzeptabel. Dies gilt insbesondere für die im Gesetzentwurf vorgesehene Nutzung der Datei im Rahmen der Strafverfolgung. Es darf nicht zu einer immer niedrigeren Eingriffsschwelle kommen.

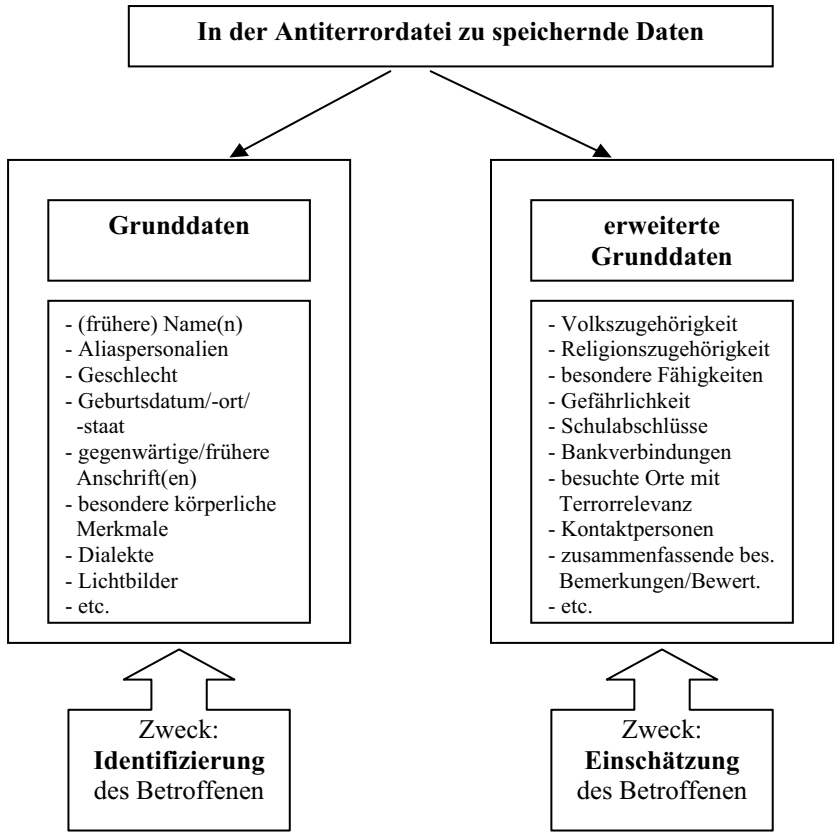
In Bezug auf die Antiterrordatei bleiben schwerwiegende verfassungs- und datenschutzrechtliche Risiken, insbesondere für diejenigen Regelungen, die erst im Nachgang zum Beschluss der Sonderkonferenz der Innenminister des Bundes und der Länder (IMK) vom 4. September 2006 in den Gesetzentwurf aufgenommen worden sind.

Entgegen meinem Petitum (vgl. 20. TB Nr. 5.1.1) ist die Antiterrordatei keine reine Indexdatei zum leichteren Auffinden von Aktenfundstellen. Die beteiligten Stellen haben neben Grunddaten auch sog. erweiterte Grunddaten zu speichern (s. Kasten b zu Nr. 5.1.1). Bei jeder Anfrage erfolgt eine Recherche in den Grunddaten und erweiterten Grunddaten. Allerdings sind die erweiterten Grunddaten für die anfragende Behörde grundsätzlich nicht sofort sichtbar. Erst auf Nachfrage werden sie von der speichernden Stelle nach den für sie geltenden Rechtsvorschriften übermittelt.

In den gesetzlich definierten Eilfällen sind aber auch die erweiterten Grunddaten für jede anfragende Behörde sofort und ohne Zustimmung der für diese Daten verantwortlichen Stelle sichtbar und dürfen für weitere Zwecke – beispielsweise zur Einleitung operativer Maßnahmen gegen einen Betroffenen – verwendet werden. In derartigen Fällen kann die Polizei – u. U. ausschließlich gestützt auf weiche, d. h. gänzlich ungesicherte, Erkenntnisse der Nachrichtendienste – polizeiliche (Zwangs-)Maßnahmen gegen einen Betroffenen ergreifen. Dies kann auch vollkommen unbescholtene Personen treffen, weil die Geheimdienste bereits weit im Vorfeld der Gefahrenabwehr tätig werden. Aufgrund ihrer spezifischen gesetzlichen Aufgaben- und Befugniszuweisung dürfen die Dienste auch Daten von sich rechtmäßig verhaltenden, unbescholtenen Personen erfassen, sofern tatsächliche Anhaltspunkte für eine vermeintliche Zuordnung dieser Personen etwa zum Umfeld des internationalen Terrorismus bestehen. Für das Vorliegen tatsächlicher Anhaltspunkte genügen bereits in gewissem Umfang verdichtete Umstände als Tatsachenbasis. Diese Umstände können mehrdeutig sein; sie können bei weiterer Entwicklung in eine Gefahrenlage münden, aber auch Teil eines – auch zukünftig – vollkommen legalen Verhaltens eines Betroffenen sein. Diese hohe Unsicherheit in Bezug auf die Bedeutung einzelner Verhaltsumstände im Vorfeldbereich hat das Bundesverfassungsgericht in seiner Entscheidung vom 27. Juli 2005 zum niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (vgl. 1 BvR 668/04, Rdn. 121) betont.

Für die Nachrichtendienste resultieren hieraus, insbesondere bei der Erfassung sog. Kontakt- und Begleitpersonen, erhebliche Probleme, zulässige von unzulässigen Datenspeicherungen abzugrenzen. So ist es schwierig, Kontaktpersonen, d.h. Personen im Umfeld bzw. Randbereich einer Zielperson, von Personen abzugrenzen, die mit einer Zielperson nur in einem sozial üblichen, d. h. z. B. beruflichen, familiären, freundschaftlichen oder nur gelegentlichen oder flüchtigen Kontakt stehen (Freunde,

Kasten b zu Nr. 5.1.1




Verwandte, Bekannte, Nachbarn, Kollegen oder sonstige Dritte, etwa Anwälte, Geistliche, Journalisten etc.).

Da die Nachrichtendienste auch die Daten von Kontaktpersonen in der Antiterrordatei speichern müssen, können die beteiligten Polizeibehörden von diesen Daten Kenntnis erlangen, obwohl sie diese nach ihren Befugnissen nicht erheben dürften.

Ich habe dies im Rahmen der Gesetzesberatungen kritisiert und auch in der vom Innenausschuss des Deutschen Bundestages am 6. November 2006 durchgeführten öffentlichen Sachverständigenanhörung zur Antiterrordatei darauf hingewiesen, dass dies die vom Bundesverfassungsgericht vorgegebenen Beschränkungen überschreitet. Nach der Entscheidung des Bundesverfassungsgerichts vom 25. April 2001 zum hamburgischen Gesetz über die Datenverarbeitung der Polizei (1 BvR 1104/92) ist der Begriff der Kontakt- und Begleitperson im Polizeirecht „restriktiv auszulegen“ (a.a.O., Rdn. 54). „Vorausgesetzt sind konkrete Tatsachen für einen objektiven Tatbezug und damit für eine Einbeziehung in den Handlungskomplex der Straftatenbegehung, insbesondere eine Verwicklung in den Hintergrund oder das Umfeld der Straftaten“ (a. a. O.). Demnach darf die Polizei – anders als die Nachrichtendienste – keine Kontaktpersonendaten nur aufgrund von tatsächlichen Anhaltspunkten erheben. Durch die Verpflichtung der Nachrichtendienste zur generellen Speicherung auch von nur auf tatsächlichen Anhaltspunkten beruhenden Kontaktpersonendaten in der Antiterrordatei, was der Polizei eine Kenntnisnahme ermöglicht, wird diese verfassungsgerichtlich vorgegebene Datenerhebungsschwelle nicht gewahrt.

Meine Kritik ist von anderen Sachverständigen in der Anhörung des Innenausschusses des Deutschen Bundestages geteilt worden. Dies gilt auch für folgende Kritikpunkte: Auf Drängen der Innenminister der Länder wurde der Kreis der an der Antiterrordatei beteiligten Behörden über die zentralen Sicherheitsbehörden des Bundes und der Länder hinaus erheblich erweitert. Teilnahmeberechtigt sind nunmehr auch weitere Polizeivollzugsbehörden der Länder (nach fachkundiger Schätzung sind dies mehrere hundert Behörden in der Bundesrepublik Deutschland), sofern die gesetzlichen Voraussetzungen vorliegen. Diese Ausweitung halte ich weder für sachgerecht noch für verhältnismäßig.

Verfassungs- und datenschutzrechtlich kritisch ist auch die Speicherung von zusammenfassenden besonderen Bemerkungen, ergänzenden Hinweisen und Bewertungen zu Grunddaten und erweiterten Grunddaten in der Antiterrordatei. Die Speicherung entsprechender Freitexte eröffnet den teilnehmenden Behörden die Möglichkeit, eine Vielzahl auch weicher personenbezogener Daten (z. B. nicht überprüfte bzw. überprüfbare Hinweise oder Vermutungen) ohne Bindung an hinreichend konkrete Festlegungen des Gesetzgebers in der Antiterrordatei zu erfassen.

Aufgrund der Kritik hat der Gesetzgeber die Regelungen zur Antiterrordatei im Wesentlichen in den folgenden Punkten nachgebessert:

- Eine Erweiterung des Kreises der teilnahmeberechtigten Behörden auf weitere Polizeivollzugsbehörden der Länder ist nunmehr abhängig vom Benehmen des Bundesministeriums des Innern.
- Die im Gesetz enthaltene Definition der „Kontaktpersonen“ wurde dahingehend begrenzt, dass ein nur flüchtiger oder zufälliger Kontakt mit einer Zielperson nicht ausreicht.
- Die Möglichkeit für eine beschränkte bzw. verdeckte Speicherung besteht nunmehr nicht mehr nur im Falle besonderer Geheimhaltungsinteressen, sondern auch, wenn besondere schutzwürdige Interessen des Betroffenen dies ausnahmsweise erfordern.

Diese Nachbesserungen sind datenschutzrechtlich zu begrüßen. Dies gilt ebenfalls für die – meinem Petitum folgende – gesetzliche Verpflichtung zur Evaluierung des Gemeinsame-Dateien-Gesetzes unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist. Kritisch zu bewerten ist jedoch die im Zuge der Nachbesserungen vorgenommene Verlängerung der ursprünglich auf fünf Jahre befristeten Geltungsdauer des Gesetzes auf zehn Jahre.

### 5.1.2 Terrorismusbekämpfungsergänzungsgesetz 2006

*Entgegen verfassungs- und datenschutzrechtlicher Bedenken werden die Befugnisse der Nachrichtendienste durch das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes erneut erheblich erweitert.*

Am 1. Dezember 2006 hat der Deutsche Bundestag das Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes (TBEG – Bundestagsdrucksache 16/2921) verabschiedet, mit dem die Bundesregierung die Konsequenzen aus dem vom Bundesinnenministerium erstellten Evaluierungsbericht zum Terrorismusbekämpfungsgesetz (TBG – s. u. Nr. 5.5.1) zieht. Nach Artikel 22 Abs. 1 TBG waren die durch das TBG im Jahr 2002 neu geschaffenen Befugnisse der Sicherheitsbehörden vor Ablauf der Geltungsdauer dieses Gesetzes (10. Januar 2007) zu evaluieren (vgl. 20. TB Nr. 5.5.4).

Die Bundesregierung hat ihren Gesetzentwurf damit begründet, dass sich die durch das TBG neu geschaffenen Befugnisse bewährt hätten und fortgelten müssten. Zudem seien weitere Verbesserungen bei der Terrorismusbekämpfung notwendig. Dies habe die Evaluierung ergeben. Diese Auffassung der Bundesregierung teile ich nicht (s. u. Nr. 5.5.1).

Bei der am 6. November 2006 vom Innenausschuss des Deutschen Bundestages durchgeführten öffentlichen Sachverständigenanhörung habe ich verfassungs- und datenschutzrechtliche Bedenken insbesondere gegen die folgenden Regelungen geltend gemacht:

- Artikel 1 Nr. 2 (§ 8a Bundesverfassungsschutzgesetz – BVerfSchG (neu))

  Gegenüber dem geltenden Recht (§ 8 Abs. 5 ff. BVerfSchG) werden die materiellen Voraussetzungen und Verfahrenssicherungen der Auskunftsbefugnisse erheblich abgesenkt. Zukünftig können alle Nachrichtendienste des Bundes (Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD) und selbst der für Auslandsangelegenheiten zuständige Bundesnachrichtendienst (BND) unter wesentlich erleichterten Voraussetzungen umfängliche Auskünfte bei Kreditinstituten, Finanzdienstleistern, Luftverkehrsgesellschaften, Post- und Telekommunikationsunternehmen etc. einholen. Betroffen hiervon sind auch Personen, bei denen nur ein vager Verdacht besteht, eine Person im Umfeld des Terrorismus zu unterstützen. Unter Verweis auf die Plenardebatte und die Beratungen des Innenausschusses des Deutschen Bundestages zum TBG habe ich darauf hingewiesen, dass mit allen Auskunftsbefugnissen „schwerwiegende Eingriffsmöglichkeiten in Bürgerrechte“ (Bundestagsdrucksache 15/4694, Seite 4) verbunden sind. So können durch Auskünfte von Luftverkehrsgesellschaften partielle Bewegungsprofile erstellt und aufgrund der Auskünfte von Kreditinstituten sämtliche Finanztransaktionen eines Betroffenen unter Angabe der jeweiligen Transaktionspartner und -zwecke erschlossen werden. Bereits die bloße Anfrage eines Nachrichtendienstes kann zudem zur Stigmatisierung des Betroffenen bei der um Auskunft ersuchten Stelle, z. B. einer Bank, führen und damit erhebliche Nachteile bis hin zur Auflösung der Vertragsbeziehung zur Folge haben.
- Artikel 1 Nr. 4 Buchst. b (§ 17 Abs. 3 BVerfSchG (neu))

  Durch diese Neuregelung soll dem BfV, MAD und BND die Befugnis zur eigenständigen Ausschreibung von Personen und Sachen im nationalen polizeilichen Informationssystem (INPOL) sowie im Schengener Informationssystem (SIS) gewährt werden. Nach geltendem Recht (vgl. § 11 Abs. 2 BKAG) sind Nachrichtendienste auf INPOL nicht zugriffsberechtigt – weder lesend noch schreibend. Gegen eine Befugnis der Nachrichtendienste zur Ausschreibung in INPOL habe ich im Hinblick auf das verfassungsrechtliche Trennungsgebot (s. o. Nr. 5.1) weiterhin erhebliche Bedenken.
- Artikel 3 Nr. 2 (§ 4a MADG (neu)); Artikel 4 Nr. 2 (§ 2a BNDG (neu))

  Im Gegensatz zum geltenden Recht (vgl. § 10 Abs. 3 MADG, § 2 Abs. 1a BNDG) sollen die in § 8a BVerfSchG – neu – geregelten Auskunftsbefugnisse des BfV inhaltsgleich auf den MAD und BND übertragen werden. Die Erforderlichkeit dieser erheblichen Befugniserweiterung von MAD und BND hat die Bundesregierung in dem von ihr vorgelegten Evaluierungsbericht (s. u. Nr. 5.5.1) nicht überzeugend dargelegt.

Aufgrund der Sachverständigenanhörung hat der Gesetzgeber den Entwurf des TBEG teilweise nachgebessert. Wie von mir gefordert, müssen Betroffene zur Wahrung ihrer Rechtsschutzmöglichkeiten nun auch über Auskunftsersuchen informiert werden, die an Luftverkehrsgesellschaften gerichtet worden sind.

Auf die datenschutzrechtlichen Defizite des TBEG-Entwurfs haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 26./27. Oktober 2006 hingewiesen (s. Kasten zu Nr. 5.1.2).

Kasten zu Nr. 5.1.2

**Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg**

**Das Gewicht der Freiheit beim Kampf gegen den Terrorismus**

Seit dem 11. September 2001 wandelt sich der Staat immer mehr zu einem Präventionsstaat, der sich nicht darauf beschränkt, Straftaten zu verfolgen und konkrete Gefahren abzuwehren. Der Staat verlagert seine Aktivitäten zunehmend in das Vorfeld der Gefahrenabwehr. Sicherheitsbehörden gehen der abstrakten Möglichkeit von noch nicht einmal geplanten Taten nach. Immer mehr Daten werden auf Vorrat gesammelt und damit eine Vielzahl unverdächtiger Menschen erfasst. Auch unbescholtene Bürgerinnen und Bürger werden als Risikofaktoren behandelt, ohne dass diese dafür Anlass gegeben haben. Dieses neue Verständnis von innerer Sicherheit führt zu gravierenden Einschränkungen der Freiheitsrechte. Beispiele sind die von der Europäischen Union beschlossene Speicherung der Telekommunikationsverkehrsdaten oder die im Jahr 2002 verfassungswidrig durchgeführten Rasterfahndungen.

In diesem Zusammenhang ist auch der „Entwurf eines Gesetzes zur Ergänzung des Terrorismusbekämpfungsgesetzes“ kritisch zu bewerten. Die ursprünglich zur Terrorismusbekämpfung geschaffenen Befugnisse werden immer weiter ausgedehnt und nicht mehr nur auf Terrorverdächtige beschränkt.

Bei allen Gesetzen und Maßnahmen zur Terrorbekämpfung stellt sich die Frage nach deren Eignung und Verhältnismäßigkeit. Mehr Überwachung führt nicht automatisch zu mehr Sicherheit, aber stets zu weniger Freiheit. Es gibt keine absolute Sicherheit.

Die verfassungsrechtlich notwendige wissenschaftliche Evaluation der bisherigen Vorschriften zur Terrorismusbekämpfung durch eine unabhängige Stelle fehlt bislang. Der „Bericht der Bundesregierung zu den Auswirkungen des Terrorismusbekämpfungsgesetzes“ ist keine vollwertige Evaluation der bisherigen Vorschriften. Damit steht sowohl die Notwendigkeit einer Verlängerung als auch die Erforderlichkeit der Schaffung neuer Befugnisse in Zweifel.

Zunehmende Befugnisse verlangen nach zusätzlichen Kontrollen. Daher ist es unerlässlich, einen angemessenen Ausgleich zwischen den Befugnissen der Sicherheitsbehörden und den Kompetenzen der Kontrollorgane zu schaffen. Insbesondere müssen die Handlungsmöglichkeiten der parlamentarischen Kontrollorgane entsprechend ausgestaltet sein.

### 5.1.3 Ermittlungstätigkeit der Sicherheitsbehörden im Internet

*Seit 1998 führt das BKA anlassunabhängige Recherchen im Internet durch. Wegen der aktuellen Bedrohung durch den internationalen Terrorismus sollen diese Ermittlungen bis hin zur Möglichkeit der sog. „Online-Durchsuchung“ von Computern ausgeweitet werden.*

Durch Beschluss der Ständigen Konferenz der Innenminister und -senatoren der Länder (IMK) ist im November 1998 das BKA als zentrale Stelle für das gesamte Bundesgebiet mit der Durchführung anlassunabhängiger Recherchen im Internet und der Weiterleitung daraus gewonnener Erkenntnisse an die zuständigen Strafverfolgungsbehörden beauftragt worden (vgl. 18. TB Nr. 11.8.). Die Ermittlungstätigkeit der Sicherheitsbehörden soll nun erheblich erweitert werden. So sollen die Ergebnisse der mittlerweile auch in einigen LKA eingerichteten Recherchedienststellen in einer beim BKA geführten Indexdatei gebündelt werden. Weiter beabsichtigt das BMI, Anfang des Jahres 2007 ein gemeinsames Internetzentrum in Berlin zu errichten, in dem Vertreter von BKA, BfV, BND, MAD und des Generalbundesanwalts im Rahmen der Bekämpfung des islamistischen Terrorismus gemeinsam Informationen durch Beobachtung einschlägiger Websites beschaffen und auswerten sollen.

Zudem werden im Rahmen eines Projekts beim BKA die technischen Voraussetzungen für die Durchführung sog. „Online-Durchsuchungen“ entwickelt. Hierunter wird die Suche nach verfahrensrelevanten Inhalten auf Datenträgern verstanden, die sich nicht im direkten physikalischen Zugriff der Strafverfolgungsbehörden befinden, sondern nur verdeckt über Kommunikationsnetze mittels spezieller Computerprogramme erreichbar sind.

Gegen eine anlassunabhängige Recherche des BKA und anderer Sicherheitsbehörden im Internet bestehen keine grundlegenden datenschutzrechtlichen Bedenken, soweit dabei in frei zugänglichen, aber gleichwohl einschlägigen Bereichen des Internets „gesurft“ wird. Inwieweit auch das gemeinsame Internetzentrum unter diesen Bedingungen tätig wird und ob bei der Zusammenarbeit zwischen Polizei und Nachrichtendiensten die geltenden Übermittlungsregelungen beachtet werden, bedarf noch der Überprüfung.

Eine gänzlich andere Qualität erhält die Internet-Recherche jedoch, wenn sie in Form der heimlichen „Online-Durchsuchung“ von Computern durchgeführt wird. Nach Mitteilung der Bundesregierung wird die „Online-Durchsuchung“ derzeit nur zu repressiven Zwecken praktiziert. Grundlage hierfür sollen die strafprozessualen Vorschriften über die Durchsuchung gemäß §§ 102 ff. StPO bilden. Da die Durchsuchung jedoch eine offene Maßnahme ist, die in Anwesenheit des Betroffenen, von Zeugen oder Dritten durchgeführt wird, halte ich es nicht für vertretbar, die genannten Regelungen der StPO als Rechtsgrundlage hierfür heranzuziehen. Erst jüngst hat der Bundesgerichtshof mit Beschluss vom 31. Januar 2007 (Az.: StB 18/06) entschieden, dass für die verdeckte Online-Durchsuchung in der StPO keine Rechtsgrundlage besteht.

Zur Verhütung von Straftaten und damit zu präventiven Zwecken ist die „Online-Durchsuchung“ nach geltendem Recht weder für die Polizeibehörden des Bundes noch für

die Nachrichtendienste des Bundes zulässig. Die bis jetzt vorliegenden Gesetzentwürfe der Bundesregierung über Regelungen im Sicherheitsbereich enthalten auch keine entsprechenden Vorschläge. Allerdings ist eine entsprechende Änderung des nordrhein-westfälischen Verfassungsschutzgesetzes erfolgt, die nach Auffassung der nordrhein-westfälischen Landesbeauftragten für Datenschutz und Informationsfreiheit in „Widerspruch zu den klaren Vorgaben des Bundesverfassungsgerichts“ steht, insbesondere weil bei Online-Durchsuchungen der Schutz des Kernbereichs der Privatsphäre nicht gewährleistet werden kann.

Ich teile diese Kritik. Online-Durchsuchungen von Computern greifen unverhältnismäßig tief in das Recht auf informationelle Selbstbestimmung der davon betroffenen Internet-Nutzer ein. Durch die Maßnahme werden auch private Inhalte des Computers erfasst (etwa Arztrechnungen oder Tagebücher), ohne dass der Kernbereich privater Lebensgestaltung dabei entsprechend geschützt ist. Wie bei allen verdeckten Erhebungsmaßnahmen wird auch bei der „Online-Durchsuchung“ der Betroffene in der Regel von der Maßnahme nicht unterrichtet, was seine Rechtsschutzmöglichkeiten stark einschränkt.

Außerdem würden Online-Durchsuchungen das Vertrauen in die Sicherheit des Internet erheblich beschädigen. Ganz praktisch stellt sich nämlich die Frage, wie Online-Durchsuchungen durchgeführt werden sollen. Bisher wurden Nutzer und Hersteller von Computerprogrammen gewarnt, wenn staatliche Stellen – etwa das Bundesamt für die Sicherheit in der Informationstechnik – Sicherheitslücken festgestellt hatten und es wurden ihnen Wege zu deren Behebung aufgezeigt. Sollen etwa in Zukunft derartige Warnungen unterbleiben, weil staatlichen Stellen ansonsten das Eindringen in Computer über das Internet erschwert würde? Oder sollen die Hersteller zukünftig „Hintertüren“ in ihre Software einbauen, die Online-Durchsuchungen ermöglichen? Schließlich müsste auch die Frage beantwortet werden, wie Hacker und Spione daran gehindert werden sollen, die für Sicherheitsbehörden eingebauten bzw. offen gelassenen verdeckten Zugangsmöglichkeiten zu nutzen, um in Privatcomputer einzudringen.

Angesichts der verfassungsrechtlichen Bedenken und der aus meiner Sicht unlösbaren praktischen Fragen rege ich an, das Projekt Online-Durchsuchungen nicht länger zu verfolgen.

Ich werde die Ermittlungstätigkeit der Sicherheitsbehörden im Internet weiterhin aufmerksam beobachten.

### 5.1.4 Kontrolle des Gemeinsamen Terrorismusabwehrzentrums in Berlin

*Die Kontrolle des Gemeinsamen Terrorismusabwehrzentrums hat schwerwiegende datenschutzrechtliche Mängel offenbart.*

Das im Dezember 2004 neu errichtete Gemeinsame Terrorismusabwehrzentrum (GTAZ) ist ein wichtiger Baustein der neuen Sicherheitsarchitektur der Bundesregierung (vgl. 20. TB Nr. 5.1.1). In diesem Zentrum arbeiten alle für die Terrorismusbekämpfung relevanten Sicherheitsbehörden des Bundes und der Länder (Bundeskriminalamt, Bundesamt für Verfassungsschutz, Bundesnachrichtendienst, Kriminal- und Verfassungsschutzämter der Länder, Bundespolizei, Zollkriminalamt, Militärischer Abschirmdienst und Generalbundesanwalt, zusammen.

Im Oktober 2005 habe ich einen Beratungs- und Kontrollbesuch im GTAZ durchgeführt und dabei festgestellt, dass das Bundeskriminalamt (BKA) eine Vielzahl personenbezogener Daten ohne Rechtsgrundlage an das Bundesamt für Verfassungsschutz (BfV) übermittelt hat. Diese Daten waren weder zur Terrorismusbekämpfung noch zur sonstigen Aufgabenerfüllung des BfV erforderlich. Hierauf hatte das BfV das BKA nach Erhalt der Daten hingewiesen, aber entgegen der gesetzlichen Verpflichtung die in Papierform erhaltenen Unterlagen nicht zur weiteren Verwendung gesperrt. Meinem Petitum folgend hat das BfV dies im Kontrolltermin umgehend nachgeholt. Insoweit habe ich deswegen von einer Beanstandung abgesehen.

Dagegen habe ich die rechtswidrige Datenübermittlung des BKA an das BfV nach § 25 BDSG beanstandet. Wie das BKA mitteilte, handelte es sich bei den übermittelten Daten im Wesentlichen um Informationen, die das BKA von den Landeskriminalämtern (LKÄ) erhalten hat. Das BKA sei dabei im Vertrauen auf eine ordnungsgemäße Selektion dieser Informationen durch die LKÄ davon ausgegangen, die Daten seien für den polizeilichen Staatsschutz und zur Terrorismusbekämpfung erforderlich gewesen. Dementsprechend habe keine Notwendigkeit zur eigenständigen Prüfung bestanden. Im übrigen vertritt das BKA die Auffassung, dass für diese Datenübermittlungen des BKA an das BfV im Rahmen des GTAZ § 18 Abs. 3 Bundesverfassungsschutzgesetz (BVerfSchG) Anwendung finde und die Datenübermittlungen demnach auf ein Übermittlungsersuchen des BfV gestützt worden seien.

Dieser Rechtsauffassung habe ich widersprochen und darauf hingewiesen, ein „Ersuchen“ im Sinne des § 18 Abs. 3 BVerfSchG könne nur in einem konkreten Einzelfall, d.h. unter Berücksichtigung der spezifischen Einzelfallumstände, erfolgen. Da im Rahmen der GTAZ-Kooperation eine umfassende Zusammenarbeit, d. h. ein genereller, standardisierter Datenaustausch zwischen BKA und BfV zur Terrorismusabwehr stattfindet, kann dieser Datenaustausch nicht auf § 18 Abs. 3 BVerfSchG als Rechtsgrundlage gestützt werden. Weil das BKA die Pflicht zur Datenübermittlung im Rahmen des GTAZ hat, ist § 18 Abs. 1 BVerfSchG die für die Datenübermittlung einschlägige Rechtsgrundlage. Demnach hätte das BKA das Vorliegen der Übermittlungsvoraussetzungen prüfen müssen.

Entsprechendes gilt auch für Datenübermittlungen der Bundespolizei an das BfV. Diesen datenschutzrechtlichen Verstoß habe ich ebenfalls nach § 25 BDSG beanstandet.

Gegenstand des Beratungs- und Kontrollbesuchs war auch die Übermittlung personenbezogener Daten an so genannte Drittstaaten, d. h. an Staaten außerhalb der Europäischen Union. Gemäß § 14 Abs. 7 Satz 7 BKAG muss eine Datenübermittlung durch das BKA unterblei-

ben, wenn durch sie schutzwürdige Interessen des Betroffenen beeinträchtigt werden, insbesondere, wenn im Empfängerstaat ein angemessener Datenschutzstandard nicht gewährleistet ist. Entsprechendes gilt auch für die Bundespolizei (vgl. § 3 Abs. 3 Satz 2 des Gesetzes über die Bundespolizei).

Die Klärung, ob bzw. inwieweit diesen gesetzlichen Restriktionen hinreichend entsprochen worden ist, dauerte bei Redaktionsschluss noch an.

Kasten zu Nr. 5.1.4

**§ 18 BVerfSchG – Übermittlung von Informationen an die Verfassungsschutzbehörden**

Absatz 1:

Die Behörde des Bundes, der bundesunmittelbaren juristischen Personen des öffentlichen Rechts, die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleistungsbefugnis, die Polizeien, die Behörden des Zollfahndungsdienstes sowie andere Zolldienststellen, soweit diese Aufgaben nach dem Bundesgrenzschutzgesetz wahrnehmen, unterrichten von sich aus das Bundesamt für Verfassungsschutz oder die Verfassungsschutzbehörde des Landes über die ihnen bekannt gewordenen Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht oder Bestrebungen im Geltungsbereich dieses Gesetzes erkennen lassen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Abs. 1 Nr. 1, 3 und 4 genannten Schutzgüter gerichtet sind. Über Satz 1 hinausgehende Unterrichtungspflichten nach dem Gesetz über den Militärischen Abschirmdienst oder dem Gesetz über den Bundesnachrichtendienst bleiben unberührt. Auf die Übermittlung von Informationen zwischen Behörden desselben Bundeslandes findet Satz 1 keine Anwendung.

...

Absatz 3:

Das Bundesamt für Verfassungsschutz darf zur Erfüllung seiner Aufgaben die Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, die Polizeien sowie andere Behörden um Übermittlung der zur Erfüllung seiner Aufgaben erforderlichen Information einschließlich personenbezogener Daten ersuchen wenn sie nicht aus allgemein zugänglichen Quellen oder nur mit übermäßigem Aufwand oder nur durch eine den Betroffenen stärker belastende Maßnahme erhoben werden können. Unter den gleichen Voraussetzungen dürfen Verfassungsschutzbehörden der Länder

1. Behörden des Bundes und der bundesunmittelbaren juristischen Personen des öffentlichen Rechts,
2. Staatsanwaltschaften und, vorbehaltlich der staatsanwaltschaftlichen Sachleitungsbefugnis, Polizeien des Bundes und anderer Länder um die Übermittlung solcher Informationen ersuchen.

### 5.1.5 Kooperation der Sicherheitsbehörden mit ausländischen Partnern

*Bei der Übermittlung personenbezogener Daten an ausländische Behörden sind die verfassungsrechtlichen und gesetzlichen Grenzen strikt zu beachten.*

Vor dem Hintergrund in der Öffentlichkeit diskutierter Fälle habe ich mit den Sicherheitsbehörden intensiv erörtert (vgl. Nr. 5.1.4), wie weit die informationelle Kooperation mit ausländischen Partnern zulässig ist. Datenschutzrechtlich problematisch ist insbesondere die Übermittlung personenbezogener Daten an Behörden in Staaten, die über kein angemessenes Datenschutzniveau verfügen. Das Bundeskriminalamt, die Bundespolizei und die Behörden des Zollfahndungsdienstes dürfen hier grundsätzlich keine personenbezogenen Daten weitergeben. Insoweit sind die Vorgaben des Gesetzgebers eindeutig (vgl. § 14 Abs. 7 Satz 7 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG), § 33 Abs. 3 Satz 2 des Gesetzes über die Bundespolizei (Bundespolizeigesetz – BPolG) und § 34 Abs. 4 Satz 5 des Gesetzes über das Zollkriminalamt und die Zollfahndungsämter (Zollfahndungsdienstgesetz – ZFdG)). Maßgeblich zur Beurteilung derartiger Datenübermittlungen des Bundesamtes für Verfassungsschutz (BfV) ist § 19 Abs. 3 Satz 2 des Bundesverfassungsschutzgesetzes (BVerfSchG). Diese Regelung findet auf den MAD und BND entsprechende Anwendung. Eine Übermittlung personenbezogener Daten muss demnach unterbleiben, wenn überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Insoweit ist die Regelung wortidentisch mit den vorstehend genannten Regelungen des BKAG, BPolG und des ZFdG. Im Gegensatz zu diesen Vorschriften enthält § 19 Abs. 3 Satz 2 BVerfSchG jedoch nicht den Hinweis, dies sei insbesondere dann der Fall, wenn im Empfängerland ein angemessener Datenschutzstandard nicht gewährleistet sei. Folglich besteht nach Auffassung der Nachrichtendienste keine Pflicht, die Angemessenheit des Datenschutzniveaus im Empfängerland abstrakt zu bewerten. Ausreichend sei vielmehr, die schutzwürdigen Interessen des Betroffenen im Einzelfall hinreichend zu berücksichtigen.

Ich habe die Nachrichtendienste darauf hingewiesen, dass bei einer einzelfallbezogenen, fundierten und umfassenden Prüfung die Interessenabwägung unter Einbeziehung aller im jeweiligen Einzelfall relevanten Aspekte durchgeführt werden muss und zu Kontrollzwecken zu dokumentieren ist.

Zudem ist uneingeschränkt zu gewährleisten, dass die Vorgaben des BKAG, BPolG und des ZFdG durch die intensivere Zusammenarbeit der Sicherheitsbehörden, z. B. durch die Errichtung gemeinsamer Dateien (vgl. Nr. 5.1.1), nicht ausgehöhlt bzw. umgangen werden.

Die Diskussion mit den Sicherheitsbehörden dauert an.

## 5.2 Bundeskriminalamt

### 5.2.1 Präventive Aufgaben und Befugnisse für das BKA

*Durch die Föderalismusreform hat der Bund die Gesetzgebungskompetenz für die Abwehr des internationalen Terrorismus durch das BKA erhalten (Artikel 73 Abs. 1 Nr. 9a GG).*

Das Grundgesetz hatte ursprünglich auf eine Zuweisung polizeilicher Aufgaben an den Bund verzichtet, um nach den Erfahrungen mit der Nazi-Diktatur das erneute Entstehen einer mächtigen Zentralpolizei zu vermeiden. Im Hinblick auf die Bedrohung durch den internationalen Terrorismus wurde dem Bund im Rahmen der Föderalismusreform allerdings die alleinige Gesetzgebungskompetenz zur Abwehr der Gefahren des internationalen Terrorismus zugebilligt (BGBl. I 2006, S. 2034). Die neue Bundeskompetenz zur Regelung präventiver Befugnisse des BKA soll der besonderen Bedrohungslage Rechnung tragen: Nicht in allen Fällen, in denen z. B. Hinweise zum internationalen Terrorismus aus dem Ausland kommen, sei eine örtliche Zuständigkeit einer deutschen Polizeibehörde erkennbar, eine Sachaufklärung aber gleichwohl veranlasst. Das BKA soll dementsprechend nur in den Fällen Aufgaben und Befugnisse zur Abwehr des internationalen Terrorismus erhalten, in denen eine länderübergreifende Gefahr vorliegt, die Zuständigkeit einer Landespolizeibehörde nicht erkennbar ist oder die oberste Landesbehörde um eine Übernahme ersucht. Im Herbst 2006 wurden im Ressortkreis erste Überlegungen für eine Normierung präventiver Aufgaben und Befugnisse für das BKA im BKA-Gesetz bekannt.

Aus Sicht des Datenschutzes sind in diesem Zusammenhang klare Aufgaben- und Befugnisabgrenzungen zwischen dem BKA und den weiteren Polizeien des Bundes und der Länder wichtig, damit es nicht zu Doppelzuständigkeiten und damit zu mehrfachen Eingriffen in das Persönlichkeitsrecht Betroffener wegen identischer Sachverhalte kommt.

Die dem BKA für die Gefahrenabwehr gegen den internationalen Terrorismus eingeräumten Befugnisse müssen zudem erforderlich und verhältnismäßig sein. Dabei ist zu berücksichtigen, dass das BKA im Hinblick auf seine subsidiäre Zuständigkeit auch in Zukunft nur in wenigen Fällen zur Abwehr von Gefahren des internationalen Terrorismus tätig werden wird. Vielfach dürften zudem ausreichende Erkenntnisse für die Annahme eines hinreichenden Tatverdachts im Sinne von § 152 Abs. 2 StPO vorliegen, so dass in diesen Fällen das BKA die betreffenden Maßnahmen nach der StPO ergreifen könnte. Insbesondere gilt dies im Bereich der Organisationsdelikte wie den §§ 129a, 129b StGB, bei denen die Tatbestandsmäßigkeit bereits in einem frühen Stadium erfüllt ist.

Ich werde im Gesetzgebungsverfahren darauf dringen, dass die Vorgaben des Bundesverfassungsgerichts, die es in seinen Entscheidungen zur akustischen Wohnraumüberwachung (s. o. Nr. 6.2; 20. TB Nr. 5.1.2), zur präventiven Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz (vgl. 20. TB Nr. 5.4.3) und nach dem niedersächsischen Polizeigesetz (s. u. Nr. 5.4.1) sowie zur präventiv-polizeilichen Rasterfahndung (s. o. Nr. 5.2.3) aufgestellt hat, bei der Ausgestaltung entsprechender Eingriffsbefugnisse für das BKA beachtet werden. Zudem halte ich es für geboten, die Erforderlichkeit und Geeignetheit der dem BKA für die Gefahrenabwehr eingeräumten Befugnisse nach einer bestimmten Zeit zu evaluieren und eine entsprechende Evaluierungspflicht in den Gesetzestext aufzunehmen, zumal die Aufgabenerweiterung für das BKA nicht in der Gefahrenabwehr im engeren Sinne, sondern in der Straftatenverhütung liegen wird.

### 5.2.2 INPOL

*Der Ausbau des Informationssystems der Polizeien des Bundes und der Länder (INPOL-neu) war wegen der Fußball-WM 2006 vorläufig ausgesetzt worden. Die Beratungen über die konzeptionelle Weiterentwicklung des Systems wurden inzwischen wieder aufgenommen.*

Der Ausbau des im August 2003 unter der Bezeichnung „INPOL-neu“ in Wirkbetrieb gegangenen Informationssystems der Polizeien des Bundes und der Länder (vgl. 20. TB Nr. 5.2.3) ist wegen der Fußball-WM 2006 (s. u. Nr. 5.2.5) zunächst vorläufig abgeschlossen worden. Die Polizeien des Bundes und der Länder wollten zur Gewährleistung der Sicherheit dieses Großereignisses auf ein konsolidiertes polizeiliches Informationssystem zurückgreifen können.

Beim Ausbau von INPOL sind u. a. die im Vorgängersystem betriebenen Arbeits- und Recherchedateien in das neue INPOL-Fall-System überführt worden. Die in diesem Rahmen geführten Falldateien basieren auf einer gemeinsamen Datenstruktur. Sie setzen sich aus einzelnen Objekten zusammen (z. B. „Sachen“, „Personen“, „Ereignis“), an die jeweils auch Bilder oder importierte Textdateien – wie z. B. Vernehmungsprotokolle – angehängt werden können. Alle Informationsobjekte einer Datei lassen sich zudem über beliebige Beziehungen verknüpfen und erlauben eine entsprechende Auswertung der dabei gewonnenen Erkenntnisse.

Datenschutzrechtlich brisant ist vor allem die Möglichkeit, in den Dateianhängen und in den Objektdatensätzen Freitexte zu speichern, die anhand frei wählbarer Suchbegriffe recherchierbar sind.

Vor diesem Hintergrund habe ich die Sorge, dass bei INPOL-Fall-Anwendungen die Freitexte für die polizeiliche Sachbearbeitung im Vordergrund stehen werden, wohingegen den durch die jeweilige Errichtungsanordnung bezeichneten Datenfeldern kaum noch eine eigenständige Bedeutung zukommt. Damit würde die Errichtungsanordnung, die den Inhalt einer Datei festlegen soll, in großen Teilen die ihr zugewiesene Funktion einer „organisatorischen und verfahrensrechtlichen Vorkehrung verlieren, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegen wirken“ soll (BVerfGE 65, 1, 44). Zudem habe ich erhebliche Zweifel, ob dies mit der Regelung des § 34 Abs. 1 Satz 1 BKA-Gesetz vereinbar ist. Beim Anhörungsverfahren zu den Falldateien habe ich daher dafür

plädiert sicherzustellen, dass Dokumentenanhänge nur Daten zu Personen enthalten, zu denen nach Maßgabe des BKA-Gesetzes ein Personendatensatz angelegt wurde und anderweitige personenbezogene Daten ggf. aus den Anhängen zu entfernen sind. Dieser Anregung ist das BMI gefolgt. Zudem dürfen nun Lichtbilder nur zu Beschuldigten, Verdächtigen und „sonstigen Personen“ im Sinne von § 8 Abs. 5 BKA-Gesetz in den Fall-Dateien erfasst werden. Meine Bedenken gegen die weiterhin unübersichtliche, z. T. kumulative Möglichkeit von Freitextfeldern zu den einzelnen Datenfeldern bestehen dagegen unverändert fort.

Mit Ende der Fußball-WM 2006 sind die Beratungen zur konzeptionellen Weiterentwicklung von INPOL-neu in den zuständigen Gremien der IMK wieder aufgenommen worden. Vertreter von BKA und LKÄ erörtern die fachlichen und technischen Anforderungen, die INPOL künftig erfüllen soll. Auf meine Bitte um rechtzeitige Beteiligung der AG „INPOL“ der Datenschutzbeauftragten des Bundes und der Länder hat das BKA zugesagt, diese regelmäßig zweimal im Jahr über die technischen Aspekte der weiteren Entwicklung von INPOL-neu zu unterrichten. Zudem sollen weiterhin die Beratungsunterlagen zur Verfügung gestellt werden. Zu dem noch wichtigeren Aspekt der künftigen fachlichen Anforderungen an INPOL liegt mir dagegen noch kein Vorschlag für eine Einbeziehung der AG „INPOL“ in die Beratungen der zuständigen IMK-Gremien vor.

Sofern die Bundesregierung bzw. die Landesregierungen an einer datenschutzrechtlichen Begleitung der weiteren Konzeption von INPOL-neu durch die Datenschutzbeauftragten des Bundes und der Länder interessiert sind, muss für meine Kollegen in den Ländern bzw. für mich die Möglichkeit bestehen, die datenschutzrechtlichen Aspekte dieser Weiterentwicklung frühzeitig zu bewerten. In wie weit im Hinblick auf die Komplexität des polizeilichen Informationssystems INPOL-neu und dessen Weiterentwicklung das künftige Beteiligungsverfahren geeignet ist, die datenschutzrechtliche Beratungsaufgabe sachgerecht zu erfüllen, bleibt abzuwarten.

### 5.2.3 Entscheidung des Bundesverfassungsgerichts zur Rasterfahndung 2001 – gesetzgeberische Konsequenzen?

*Das Bundesverfassungsgericht hat die nach dem 11. September 2001 durchgeführte Rasterfahndung beanstandet. Die Entscheidung hat auch Bedeutung für die Ausgestaltung anderer präventiv-polizeilicher Eingriffsmaßnahmen.*

Der Beschluss vom 4. April 2006 (1 BvR 518/02) betrifft die Durchführung einer Rasterfahndung aus Anlass der Terroranschläge vom 11. September 2001 (vgl. 20. TB Nr. 5.2.1) nach dem nordrhein-westfälischen Polizeigesetz. Dem Gericht zufolge sind bei einer präventiv-polizeilichen Rasterfahndung begrenzende Anforderungen an die Wahrscheinlichkeit des Gefahreneintritts sowie an die Nähe des Betroffenen zur abzuwehrenden Bedrohung zu stellen. Der Gesetzgeber dürfe den Eingriff erst von der Schwelle einer hinreichend konkreten Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person vorsehen. Im vorliegenden Fall sei der Kläger in seinem Recht auf informationelle Selbstbestimmung verletzt worden, weil die Rasterfahndung auf einer den verfassungsrechtlichen Grundsätzen widersprechenden weiten Auslegung des Begriffs der „gegenwärtigen Gefahr“ angeordnet und durchgeführt worden sei. Eine Rasterfahndung im Vorfeld einer konkreten Gefahr sei verfassungsrechtlich nicht zulässig. Schließlich betont das Gericht die grundrechtssichernde Bedeutung des Richtervorbehalts und der nachträglichen Benachrichtigung der von einer Rasterfahndung betroffenen Personen.

Der Beschluss hat Auswirkung auf die Ausgestaltung der präventiv-polizeilichen Rasterfahndung in den Ländern und beim Bund: Bei den Gesetzen, die auf das Vorliegen einer Gefahr als Anknüpfungspunkt für die Durchführung einer Rasterfahndung bisher gänzlich verzichten, besteht entsprechender gesetzgeberischer Handlungsbedarf. Regelungen, die hingegen das Vorliegen einer Gefahr voraussetzen, sind entsprechend den Ausführungen des Bundesverfassungsgerichts verfassungskonform anzuwenden.

Im Hinblick auf die inhaltliche Weite der mit der polizeilichen Rasterfahndung verbundenen Datenerhebung und -verarbeitung und der Einbeziehung zahlreicher Personen in diese Maßnahme, ohne dass diese hierzu Anlass gegeben hätten, sind auch andere präventiv-polizeiliche Maßnahmen mit ähnlicher Eingriffstiefe und Streubreite an den vom Bundesverfassungsgericht aufgestellten Grundsätzen zu messen und auszurichten. Dies gilt z. B. für die Datenerhebungen mit besonderen Mitteln, wie die längerfristige Observation, den Einsatz technischer Mittel in einer für den Betroffenen nicht erkennbaren Weise zur Anfertigung von Bildaufnahmen oder -aufzeichnungen bzw. zum Abhören oder Aufzeichnen des nicht-öffentlich gesprochenen Wortes und den Einsatz von Vertrauenspersonen der Polizei. Diese Maßnahmen richten sich sowohl gegen den Störer als auch – unter bestimmten gesetzlich festgelegten Bedingungen – gegen Nichtstörer. Zudem können Dritte zulässigerweise von der Maßnahme betroffen werden. Auch die Kfz-Kennzeichenerfassung (vgl. 20. TB Nr. 5.1.3) hat eine große Streubreite, zumal die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Fahrzeuge mit polizeilichen Fahndungsdateien abgeglichen werden. Bei diesen Maßnahmen sollte daher die Schwelle einer hinreichend konkreten Gefahr für die bedrohten Rechtsgüter vorgesehen bzw. sollten die Regelungen entsprechend den genannten Ausführungen des Bundesverfassungsgerichts verfassungskonform angewendet werden.

Schließlich knüpft auch die polizeiliche Videoüberwachung (Nr. 4.2) in öffentlichen Räumen nicht an eine konkrete Gefahrenlage an, sondern an den Aufenthalt an bzw. in einer bestimmten Örtlichkeit. Von der Wahrnehmung der Befugnis ist jedermann betroffen, der sich im Aufnahmebereich der Geräte befindet. Die Videoüberwachung erhält Eingriffsintensität dadurch, dass Verhaltensweisen und äußeres Erscheinungsbild der erfassten Personen

polizeilich registriert werden. Auch wenn die Eingriffstiefe im Vergleich zur präventiven Rasterfahndung geringer sein dürfte, sind die hieran gestellten verfassungsgerichtlichen Anforderungen bei einem weiteren Ausbau der Videoüberwachung zu beachten bzw. würden einem flächendekkenden Einsatz von Bildaufnahme- und Bildaufzeichnungsgeräten entgegenstehen.

Kasten zu Nr. 5.2.3

Die **Rasterfahndung** ist ein automatisierter Datenabgleich anhand von bestimmten Prüfungsmerkmalen, die auf den Täter bzw. auf den potentiellen Täter vermutlich zutreffen, mit verschiedenen Datenbeständen bei nichtpolizeilichen Stellen. Ziel ist es zum einen, Personen auszuschließen, auf die die Merkmale nicht passen, bzw. die Zahl der verdächtigen Personen durch das Herausfiltern derjenigen mit tätertypischen Merkmalen zu verringern. Datenschutzrechtlich bedeutsam ist die Rasterfahndung vor allem deshalb, weil sie zunächst nicht bei einer bekannten Zielperson ansetzt, sondern ganz überwiegend Daten von Personen umfasst, für die keinerlei Verdachtsmomente vorliegen. Es handelt sich mithin um ein Mittel zur Verdachtsgewinnung, und nicht um ein klassisches Fahndungsinstrument. Selbst die Personen, die anhand der vorgegebenen Prüfmerkmale im Raster hängen bleiben, sind damit nicht im strafrechtlichen Sinne verdächtig, werden jedoch gleichwohl von den Sicherheitsbehörden sorgfältig beobachtet und sehen sich einem besonderen Rechtfertigungsdruck ausgesetzt.

### 5.2.4 Verwendung erkennungsdienstlicher Daten

Mit der Verwendung erkennungsdienstlicher Daten durch die Polizeien des Bundes und der Länder habe ich mich unter zwei Aspekten befasst: Mit der Verarbeitung erkennungsdienstlicher Unterlagen beim BKA (Nr. 5.2.4.1) und mit dem Projekt „Fast Identification“ (Nr. 5.2.4.2), bei dem getestet werden soll, ob mittels eines mobilen Identifikationssystems Personen durch die Polizei schneller vor Ort erkennungsdienstlich überprüft werden können.

Die Erfassung bestimmter persönlicher Merkmale bei Verdächtigen einer Straftat und zur Identitätsfeststellung gehört zum polizeilichen Alltag. Bei den dabei festgehaltenen Daten handelt es sich z. T. um biometrische Merkmale (insb. Gesichtsbilder, Fingerabdrücke), die digital gespeichert und zunehmend automatisiert ausgewertet werden können (vgl. Nr. 4.5). Damit erhöht sich auch die datenschutzrechtliche Relevanz erkennungsdienstlicher Daten.

#### 5.2.4.1 Verarbeitung von erkennungsdienstlichen Unterlagen der Polizeien des Bundes und der Länder beim BKA

*Das BKA muss ED-Daten löschen, wenn sie für die Zwecke der anliefernden Stelle nicht mehr erforderlich sind und auch beim BKA keine besonderen Gründe für die fortdauernde Speicherung bestehen.*

Erkennungsdienstliches Material ist Bestandteil der kriminalpolizeilichen personenbezogenen Sammlung, die das BKA gem. § 2 Abs. 4 BKA-Gesetz zur Erfüllung seiner Aufgabe als Zentralstelle der Polizeien des Bundes und der Länder führt. Diese Daten entstehen bei den polizeilichen Vollzugsbehörden durch Anlegen eines Datensatzes – der sog. E-Gruppe – und durch Erstellen eines Fingerabdruckblattes. Zu dem Datensatz wird eine Aussonderungsprüffrist vergeben. Datensatz und Fingerabdruckblatt werden dem BKA zur Speicherung bzw. Aufbewahrung übermittelt. Dieses vergibt dabei unabhängig vom Aussonderungsprüfdatum der erhebenden Stelle eine eigene Aussonderungsprüffrist, die in der Regel zehn Jahre beträgt. Das BKA begründet diese Verfahrensweise damit, dass es nach Bearbeitung des übersandten Fingerabdruckblattes den „Besitz“ an den angelieferten Daten der E-Gruppe übernehme, die anliefernde Stelle daran lediglich „Mitbesitz“ behalte. Löscht die Stelle, die ursprünglich die erkennungsdienstlichen Daten erhoben hat, den Datensatz nach Ablauf der dort vergebenen – häufig kürzeren – Aussonderungsprüffrist, führt dies nicht zu einer Löschung der entsprechenden Daten bei der Zentralstelle BKA; nach Auffassung des BKA gibt die erhebende Stelle damit lediglich ihren „Mitbesitz“ auf. Der Datensatz bleibe bis zum Eintritt der vom BKA vergebenen Aussonderungsprüffrist gespeichert. Somit kann auf diese Daten weiterhin im Rahmen des polizeilichen Informationssystems INPOL zugegriffen werden, und sie dürfen nach Maßgabe der einschlägigen Regelungen des BKA-Gesetzes an andere Stellen im In- und Ausland übermittelt werden.

In den Regelungen des BKA-Gesetzes zur Führung von INPOL gibt es keine Rechtsgrundlage für eine (Mit-)Besitztheorie und damit für die Vergabe einer eigenen Aussonderungsprüffrist durch die Zentralstelle BKA für die erkennungsdienstlichen Daten, die von den Polizeibehörden des Bundes und der Länder in eigener Zuständigkeit erhoben und dem BKA lediglich zur Speicherung in der kriminalpolizeilichen Sammlung übermittelt wurden. Die Dateien „Erkennungsdienst“ und „Automatisches Fingerabdruck-Identifizierungssystem – AFIS“ sind Bestandteil von INPOL. Für die Richtigkeit und Aktualität der hier gespeicherten Daten trägt die Behörde, die die Daten erhoben und eingegeben hat, die datenschutzrechtliche Verantwortung. Nur sie kann die betreffenden Daten verändern oder löschen. Mit einer erkennungsdienstlichen Behandlung sind polizeiliche Ermittlungen der jeweils zuständigen Polizeibehörde verbunden. Nur diese kennt Art und Ausführung der Tat sowie die Persönlichkeit des Betroffenen und kann entscheiden, ob gegen ihn künftig Strafverfahren zu führen sind und wie lange deswegen eine Speicherung seiner Daten zur Vorsorge erforderlich ist. Werden die Daten bei der verantwortlichen Stelle gelöscht, kann die betreffende erkennungsdienstliche Speicherung im polizeilichen Informationssystem INPOL nur aufrecht erhalten werden, soweit zu der betroffenen Person eigene Er-

kenntnisse des BKA oder einer anderen Landespolizei vorliegen, die eine weitere Speicherung rechtfertigen. Ansonsten ist es nicht erforderlich diese Daten bei der Zentralstelle BKA weiter vorzuhalten.

Zwar räumt das BKA ein, erkennungsdienstliche Daten nicht weiter aufbewahren zu wollen, wenn die zugrunde liegenden Erkenntnisse bei der datenerhebenden Stelle gelöscht worden sind. Die dargestellte Verfahrenspraxis gewährleistet dies jedoch nicht. Um eine rechtzeitige Löschung der Daten sicherzustellen, muss die erhebende Stelle dies bei Eintritt des dortigen Löschdatums unmittelbar veranlassen können. Sollte das BKA daran festhalten – wofür ich keine Rechtsgrundlage sehe – eine eigene Aussonderungsprüffrist zu vergeben, muss zumindest technisch sichergestellt werden, dass die betreffenden Daten dem BKA zur Aussonderungsprüfung angeboten werden, wenn der letzte „Mitbesitzer“ seinen „Mitbesitz“ daran aufgegeben hat. Dies ist nach Mitteilung des BKA derzeit nicht der Fall. Der Datensatz erscheint erst zur Aussonderungsprüfung, wenn die vom BKA vergebene Aussonderungsprüffrist eintritt.

Ein stets aktueller Bestand erkennungsdienstlicher Daten im BKA ist gerade für den zunehmenden polizeilichen Informationsaustausch mit den anderen Staaten der Europäischen Union von großer Bedeutung. So räumen sich die Unterzeichnerstaaten des „Prümer Vertrages“ (Nr. 3.2.2) einen beschränkten automatisierten Zugriff auf die jeweiligen Sammlungen erkennungsdienstlicher Daten ein. Dass auf diese Weise erkennungsdienstliche Daten, die nicht länger für die Aufgabenerfüllung der Polizeien des Bundes und der Länder erforderlich sind und damit längst hätten gelöscht werden müssen, europaweite Verbreitung finden, ist nicht hinnehmbar.

Ich bin weiterhin mit dem BKA im Gespräch, um eine datenschutzkonforme Verarbeitung erkennungsdienstlicher Daten zu erreichen.

#### 5.2.4.2 Pilotprojekt Fast Identification

*Vor Inbetriebnahme eines Systems zur schnellen automatisierten Erfassung und Auswertung von Fingerabdrücken müssen die damit verbundenen Datenschutzfragen geklärt werden.*

Das BKA hat im Frühjahr 2005 das Pilotprojekt „Fast Identification“ gestartet. Dabei handelt es sich um ein mobiles daktyloskopisches System, das es der Polizei ermöglicht, Personen schnell und überall zu identifizieren. Hierbei werden lediglich zwei Finger optoelektronisch erfasst. Sie werden dann mit einem auf dem mobilen Terminal abgespeicherten Fingerabdruck-Datenbestand oder über Funk mit dem zentralen „Automatisierten Fingerabdruck-Identifizierungs-System“ (AFIS) im BKA verglichen. Ziel ist u. a. eine signifikante Verkürzung des Verfahrens.

An dem Projekt waren neben dem BKA, der Bundespolizeidirektion und dem Bundespolizeiamt Frankfurt/Flughafen weitere Polizeibehörden aus den Ländern Bayern, Hessen, Nordrhein-Westfalen sowie Rheinland-Pfalz beteiligt. Der Einsatz der mobilen Endgeräte soll eine effektive Vorfeldkontrolle sowie das rasche Herausfiltern bekannter Gewalttäter ermöglichen. Die Fußball-WM 2006 bot dafür ein aus polizeilicher Sicht besonders geeignetes Szenario. Dabei waren Scanner über ein Netzwerk mit dem zentralen AFIS-System des BKA verbunden und machten damit eine Recherche im Gesamtdatenbestand möglich.

Mit Hilfe dieser Feldversuche wurden Informationen zur Handhabung, Zuverlässigkeit und Robustheit der Geräte, zur Stabilität und Kapazität der Netz-Verbindungen, zum Antwort-Zeit-Verhalten des lokalen und Zentralbestandes, zur Treffergenauigkeit sowie zu den im Display benötigten Angaben gesammelt. Dabei sollte unter Echteinsatz-Bedingungen getestet werden, ob sich diese für Deutschland neue Technologie bewährt.

Mein besonderer Augenmerk galt der Datenübermittlung von den mobilen Terminals zu der Datei „AFIS“ im BKA, aber auch der Sicherheit der mobilen Systeme vor Ort. Weder dürfen unberechtigte Zugriffe, noch Fehlübermittlungen erfolgen können; schließlich muss eine hohe Treffergenauigkeit sichergestellt sein.

Im Abschlussbericht vom Dezember 2006, der kurz vor Redaktionsschluss einging, hat das BKA die Ergebnisse der einzelnen Pilotprojekte ausgewertet. Danach hat sich das Projekt aus polizeilicher Sicht hervorragend bewährt. Die Technik wird als sicher, zuverlässig und störungsarm bezeichnet. Die Fehlerquote liege in einer vernachlässigbaren Größenordnung, wobei die Ursachen fast ausschließlich auf falsche Bedienung oder schlechte Qualität zurückzuführen seien. Die genutzte Technik bedeute einen spürbaren Sicherheitsgewinn für die Anwender und eine geringere Beeinträchtigung der überprüften Personen. Den Bundesländern wird die Einführung des Fast-Identification-Verfahrens empfohlen.

Leider enthält der Bericht keine Aussage zu der Frage, ob im Bereich des Bundes diese Technik künftig dauernd zum Einsatz kommen soll. Auch fehlen aussagekräftige Feststellungen zu möglichen Beeinträchtigungen von Bürgerrechten. Hierzu strebe ich mit dem BMI eine Klärung an, bevor die neue Technik in den Regelbetrieb übernommen wird. Bedeutsam erscheinen mir insbesondere die Fragen, bei welcher Gelegenheit das neue System zum Einsatz kommen soll und wie der betroffene Personenkreis abgegrenzt wird. Auf keinen Fall wäre es hinzunehmen, dass allein wegen der verbesserten technischen Abgleichsmöglichkeiten der Umfang verdachtsloser Personenkontrollen ausgeweitet würde. Außerdem ist zu gewährleisten, dass die Personalien und Fingerabdruckdaten von kontrollierten Personen im Nichttrefferfall gelöscht werden. Zudem wird wegen Fehlbedienungen während der Pilotphase eine verbesserte Systemschulung für die Anwender notwendig sein. Die Aufnahme des Wirkbetriebs mit Fast-Identification-Verfahren ist nur hinnehmbar, wenn diese Technik mindestens ebenso sicher zu handhaben ist wie das herkömmliche daktyloskopische Verfahren.

### 5.2.5 Fußball-Weltmeisterschaft 2006

*Bei den Sicherheitsmaßnahmen zur Fußball-WM 2006 standen vor allem die Verfahren zur Überprüfung der Zuverlässigkeit im Rahmen der Akkreditierung sowie zur Vergabe der Tickets im Mittelpunkt datenschutzrechtlichen Interesses. Eine Übertragung dieser Eingriffsmaßnahmen auf andere Sport- und Kulturveranstaltungen halte ich im Hinblick auf die Einmaligkeit des WM-Turniers nicht für vertretbar.*

Bei der Durchführung einer Fußball-WM denkt man sicherlich nicht vorrangig an Datenschutz. Gleichwohl hatte ich mich im Berichtszeitraum intensiv mit datenschutzrechtlichen Fragen zu beschäftigen, die sich im Zusammenhang mit Vorbereitung und Durchführung der WM 2006 in Deutschland stellten.

Dabei ging es zum einen um die Zuverlässigkeitsüberprüfung von Personen, die an der Organisation und Durchführung der WM mitwirkten. Zum anderen hatte ich mich mit dem Verfahren zur Ticketvergabe auseinanderzusetzen.

Unter Beteiligung der Polizei und des Verfassungsschutzes des Bundes und der Länder sowie des Bundesnachrichtendienstes wurden mit Einwilligung der Betroffenen insgesamt 148 351 Datensätze auf die Zuverlässigkeit der davon Betroffenen überprüft. Zu 2 055 Personen wurde eine ablehnende Empfehlung gegenüber dem OK FIFA WM 2006 ausgesprochen. Im Rahmen dieser Aktion haben sich die Datenschutzbeauftragten des Bundes und der Länder wiederholt mit den datenschutzrechtlichen Aspekten der Zuverlässigkeitsüberprüfung der bei der WM akkreditierten Personen befasst. Im Zentrum der Kritik stand dabei die Beteiligung der Verfassungsschutzbehörden. Ich verkenne nicht, dass eine herausragende Großveranstaltung, wie die Fußball-WM 2006, nicht zuletzt vor dem Hintergrund der aktuellen weltpolitischen Lage ein mögliches Handlungsfeld für terroristische und andere kriminelle Aktionen bilden kann. Soweit es jedoch um die Verhinderung von Störungen durch gewalttätige oder gewaltbereite Extremisten ging, hätte es nicht der Befassung durch die Verfassungsschutzbehörden bedurft. Wegen des ihnen gesetzlich eingeräumten Beobachtungsauftrages hätten diese die Möglichkeit bzw. die Verpflichtung gehabt, von sich aus entsprechende Erkenntnisse den Polizeibehörden zu übermitteln, die diese dann für die Überprüfung der zu akkreditierenden Personen hätten verwenden können. Ich habe zudem Zweifel, ob die Einwilligung der zu akkreditierenden Personen eine ausreichende Rechtsgrundlage für die Bearbeitung ihrer Daten durch die Verfassungsschutzbehörden gebildet hat. In den Verfassungsschutzgesetzen des Bundes und der Länder fehlt es schon an einer Aufgabenzuweisung für die Mitwirkung an Zuverlässigkeitsüberprüfungen der vorliegenden Art. Denn eine fehlende Aufgabenzuweisung kann im Sicherheitsbereich nicht durch eine Einwilligung der betroffenen Personen ersetzt werden. Gleiches gilt für die Beteiligung des Bundesnachrichtendienstes.

Die datenschutzrechtlichen Prüfungen der Zuverlässigkeitsüberprüfungen bei den verfahrensbeteiligten Behörden ergaben keinen Anlass für grundlegende Bedenken. Allerdings habe ich gegenüber dem BMI gem. § 25 BDSG beanstandet, dass Akkreditierungsdaten von Personen mit Wohnsitz im Ausland, die auf der Grundlage einer älteren Einwilligungserklärung ohne Hinweis auf die Mitwirkung des Bundesnachrichtendienstes erhoben worden waren, übermittelt wurden. Die Daten zu Personen, zu denen keine ablehnende Empfehlung abgegeben wurde, sind nach mir vorliegenden Informationen mittlerweile gelöscht.

Die Bundesregierung hat die Zuverlässigkeitsprüfungen und deren Umfang mit dem einmaligen und herausragenden Ereignis der Fußball-WM 2006 begründet. Die bayerische Landespolizei hat jedoch inzwischen anlässlich des Papstbesuches in Bayern mit Unterstützung des BKA ebenfalls eine – allerdings rein polizeiliche – Zuverlässigkeitsüberprüfung der zu akkreditierenden Personen durchgeführt. In den Datenabgleich wurden dabei dieselben polizeilichen Dateien einbezogen, wie anlässlich der Fußball-WM. Ich halte dies nicht für verhältnismäßig.

Meine Kritik an der Ticketvergabe des OK FIFA WM 2006 (vgl. 20. TB Nr. 5.3.7) wurde nicht ausgeräumt. Die Zweifel, ob die Personalisierung der Eintrittskarten im Hinblick auf die damit beabsichtigte Identifizierung gewaltbereiter Personen, die Verhinderung des Schwarzmarkthandels sowie die Trennung rivalisierender Fangruppen erforderlich waren, sind dabei eher gewachsen: Zum einen ist nach Mitteilung des BMI die Identität der Besucher mit dem auf dem Ticket dokumentierten Namen an den Eingängen der Stadien nur stichprobenartig überprüft worden. Zum anderen ist ein Teil der an WM-Sponsoren und andere nationale Fußballverbände ausgegebenen Tickets nicht personalisiert gewesen. Die generalpräventive Wirkung, die nach Auffassung des BMI aber von der Personalisierung der Tickets sowie der Ankündigung und Durchführung von Kontrollen an den Eingängen der Stadien ausgegangen sei, rechtfertigt meines Erachtens – auch vor dem Hintergrund der jüngsten Entscheidung des Bundesverfassungsgerichts zur präventiven Rasterfahndung (s. u. Nr. 5.2.3) – nicht die Erhebung personenbezogener Daten von einer Vielzahl von unverdächtigen Personen, zumal eine konkrete Gefahrenlage nicht gegeben war. Von der vom BMI empfohlenen Übertragung des Ticketvergabeverfahrens auf andere Veranstaltungen sollte daher Abstand genommen werden. Es muss weiterhin grundsätzlich möglich sein, Sport- und Kulturveranstaltungen anonym zu besuchen.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (vgl. Kasten zu Nr. 5.2.5) auf die datenschutzrechtlichen Probleme der Ticketvergabe hingewiesen.

Kasten zu Nr. 5.2.5

**Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10. und 11. März 2005 in Kiel**

**Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006**

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticket-Vergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

### 5.2.6 Forschungsprojekt Fotofahndung

*Das BKA testet im Mainzer Hauptbahnhof im Rahmen des Forschungsprojekts „Foto-Fahndung", inwieweit moderne Gesichtserkennungssysteme die Polizei bei der Suche nach bestimmten Personen unterstützen können.*

Bei diesem Projekt wurden Gesichtsbilder (biometrische Merkmale) von freiwilligen Testteilnehmern aufgenommen und zum späteren Abgleich in einer Datenbank gespeichert. Die biometrischen Systeme verglichen die Gesichter aus der Menge der vorbeigehenden Passanten mit diesen gespeicherten Bilddaten. Für die Bewertung der Messdaten wurden die Gesichtsbilder erkannter Personen fotografiert und gespeichert. Dabei ließ es sich nicht vermeiden, dass hiervon auch Personen betroffen waren, die nicht am Projekt teilnahmen, aber vom System fälschlicherweise als Treffer bezeichnet wurden. Damit die aufgenommenen Daten möglichst schnell gelöscht werden konnten, fand eine zeitnahe Auswertung der Daten statt. Die Aufnahmen und die dazugehörigen Videoaufzeichnungen wurden nach spätestens 48 Stunden gelöscht. Die Daten der freiwilligen Testteilnehmer werden spätestens nach Projektabschluss gelöscht.

Ich habe das Projekt wegen seiner datenschutzrechtlichen Bedeutung von Anfang an begleitet und datenschutzrelevante Hinweise gegeben. Dabei habe ich besonderen Wert auf eine breit angelegte Information der Öffentlichkeit gelegt. Um dem Persönlichkeitsschutz – insbesondere „unfreiwillig" aufgenommener Personen – Rechnung zu tragen, wurden die Passanten auf dem Bahnhof informiert, in welchem Bereich der Test durchgeführt wurde, damit sie dem Aufnahmebereich ausweichen konnten. So ließ sich eine Beeinträchtigung dieses Personenkreises weitgehend vermeiden. Die „freiwilligen" Testteilnehmer wurden vor Abgabe ihrer Einwilligungserklärung ausführlich informiert, wie der Test abläuft und was dabei mit ihren Daten geschieht, um einen möglichst optimalen Datenschutz sicherzustellen. Nachdem die in der Anlaufphase festgestellten Mängel bei der Information der Passanten vom BKA behoben wurden, auf die ich durch Petenten hingewiesen worden war, habe ich mich bei einem Kontrollbesuch vor Ort und bei der Datenauswertestation im BKA von der Einhaltung der datenschutzrechtlichen Vorgaben überzeugt.

Sollte sich die Fehlerrate als gering erweisen, wird der kombinierten Anwendung von Videotechnik und Biometrie eine wachsende Bedeutung zukommen. Da die Technik grundsätzlich für eine breit angelegte Überwachung geeignet ist, kommt es ganz entscheidend darauf an, wie ein eventueller späterer Echtbetrieb ausgestaltet werden wird. Die Technologie dürfte allenfalls unter den Voraussetzungen zum Einsatz kommen, unter denen auch eine Kfz-Kennzeichenerfassung (20. TB Nr. 5.1.3) zulässig ist, d.h. keinesfalls darf die Technik zur Kontrolle und Speicherung von Personen eingesetzt werden, für die die Voraussetzungen einer polizeilichen Fahndungsausschreibung nicht gegeben sind. Ferner ist auszuschließen, dass für die Identifikation eine Verknüpfung mit digitalisierten Passfotos stattfindet, die im Pass- und Personalausweisregister gespeichert werden (vgl. Nr. 4.5.3).

Die Erfahrungen aus dem Forschungsprojekt werden sicherlich in die Weiterentwicklung der biometrischen Gesichtserkennung einfließen. Bei deren Einsatz muss immer die Balance zu den Bürgerrechten gewahrt bleiben. Sie darf nicht zu einer Totalüberwachung führen. Zudem muss noch nachgewiesen werden, ob und inwieweit diese Technologie überhaupt für Fahndungsmaßnahmen geeignet ist. Ich sehe daher dem Erfahrungsbericht des BKA mit großem Interesse entgegen.

### 5.2.7 Geldwäsche

*Bei der Umsetzung der Dritten EG-Geldwäscherichtlinie müssen datenschutzrechtliche Anforderungen beachtet werden.*

Die Bekämpfung der Geldwäsche wird allgemein als ein wichtiges Instrument bei der Bekämpfung des internationalen Terrorismus und der grenzüberschreitenden organi-

sierten Kriminalität angesehen. Es liegt nahe, dass die in diesem Zusammenhang zu treffenden Maßnahmen international koordiniert werden.

Die Richtlinie 2005/60/EG des Europäischen Parlaments und des Rates zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (ABl. L 309 vom 25. November 2005, S. 15) sieht gegenüber der Richtlinie von 2001 (vgl. 19. TB Nr. 13.7) erneut eine Erweiterung der Pflichten und des Adressatenkreises vor. Sie bezieht nunmehr ausdrücklich die Bekämpfung der Finanzierung des Terrorismus als Ziel mit ein, was jedoch in Deutschland bereits mit der Novellierung des Geldwäschegesetzes vom 18. August 2002 erfolgt ist. Bei der Bekämpfung des internationalen Terrorismus und seiner Finanzströme handelt es sich um hochkomplexe Strukturen, deren Aufdeckung spezialisierten Einheiten des polizeilichen Staatsschutzes obliegt. Falschmeldungen privater Stellen könnten fatale Folgen für die Betroffenen haben. Die Anzahl der Verdachtsanzeigen mit möglicherweise terroristischem Hintergrund ist jedoch gegenüber der Gesamtzahl der Geldwäscheverdachtsanzeigen nach § 11 GwG, die sich bei etwas über 8.000 Fällen jährlich eingependelt hat, verschwindend gering (vgl. jüngste Jahresberichte der FIU Deutschland).

Während mit der Zweiten Geldwäscherichtlinie (2001) der Kreis der meldepflichtigen Stellen auf Angehörige der freien Berufe, u. a. Notare, erweitert worden ist, wenn diese sich an bestimmten Finanz- und Vermögensaktionen beteiligen, sollen nach der Dritten Geldwäscherichtlinie auch Personen darunter fallen, die mit hochwertigen Gütern handeln, sofern an sie Barzahlungen ab 15 000 Euro oder mehr geleistet werden. Der Kreis der Betroffenen, über die eine Geldwäsche-Verdachtsanzeige erstattet wird, könnte sich also nach Umsetzung der Richtlinie erheblich erweitern, mit all den negativen Folgen, die eine solche Datenübermittlung an die Strafverfolgungsbehörden für den betroffenen Bürger hat, zumal er nicht davon unterrichtet würde.

Die Richtlinie ist binnen 2 Jahren in nationales Recht umzusetzen. Ich werde darauf achten, dass bei der Umsetzung den Belangen des Datenschutzes, insbesondere im Hinblick auf die Verhältnismäßigkeit Rechnung getragen wird.

## 5.3 Bundespolizei

### 5.3.1 Neues Vorgangsbearbeitungssystem (@rtus) bei der Bundespolizei

*Das System @rtus soll der Vorgangsbearbeitung/-verwaltung sowie der Dokumentation polizeilichen Handelns dienen.*

Wegen der beim Betrieb von @rtus, des neuen Vorgangsbearbeitungssystems der Bundespolizei, anfallenden Datenmenge sind datenschutzgerechte Aspekte von besonderer Bedeutung. Ich war daher von Anfang an in die Entwicklung von @rtus eingebunden, sodass die datenschutzrechtlichen Gesichtspunkte in die polizeilichen Überlegungen eingebracht werden konnten.

Die Datei soll im Rechenzentrum der Bundespolizeidirektion betrieben werden. Dabei werden die lokalen Daten der eingebenden Stellen der Bundespolizei dort zentral gespeichert. Die Datenverantwortung verbleibt bei der eingebenden Stelle. Das System besteht aus zwei Dateien, @rtus-Zentral (Recherche) und @rtus-Bund, wobei in @rtus-Zentral deutlich weniger Daten gespeichert werden als in der anderen Datei.

Ich habe besonderen Wert auf ein ausgereiftes Berechtigungskonzept gelegt, um sicherzustellen, dass die Nutzer nur Zugriff auf diejenigen Daten erhalten, die sie für die Erfüllung ihrer jeweiligen Aufgabe kennen müssen. Hierbei ist zwischen klassischen Polizeidaten und sonstigen Polizeiverwaltungsdaten zu unterscheiden.

Ich werde weiterhin meine Überlegungen bei der Einführung von @rtus einbringen. Bei der Errichtungsanordnung bin ich nach § 36 Abs. 2 Bundespolizeigesetz grundsätzlich vorher anzuhören. Dabei werde ich ein besonderes Augenmerk auf die Lösung der bis jetzt noch offenen Fragen werfen und für eine datenschutzfreundliche Lösung eintreten. Die Einführung der Datei @rtus im Echtbetrieb ist für die 2. Jahreshälfte 2007 vorgesehen.

### 5.3.2 Datei „Gewalttäter Sport“

*Die Datei „Gewalttäter Sport“ ist eine beim BKA geführte Verbunddatei des polizeilichen Informationssystems des Bundes und der Länder, die gewalttätige Auseinandersetzungen und sonstige Straftaten im Zusammenhang mit Sportveranstaltungen verhindern soll.*

In der Datei „Gewalttäter Sport“ werden im Zusammenhang mit Sportveranstaltungen personenbezogene Daten bei bestimmten polizeilich relevanten Anlässen erfasst. Solche Anlässe können Ermittlungsverfahren sowie rechtskräftige Verurteilungen wegen der Begehung bestimmter Delikte sein. Hierzu zählen aber auch bloße Maßnahmen der Gefahrenabwehr, wie Personalienfeststellungen, Platzverweise, Ingewahrsamnahmen oder die Sicherstellung bzw. Beschlagnahme von Waffen oder anderen gefährlichen Gegenständen, sofern die Umstände der konkreten Gefahrensituation die Annahme rechtfertigen, dass der Betroffene künftig anlassbezogene Straftaten von erheblicher Bedeutung begehen wird. Die ausschreibende Behörde erhält regelmäßig eine „Treffermeldung“, wenn die in der Datei ausgeschriebene Person anlässlich einer polizeilichen Kontrolle im Inland oder an der Grenze angetroffen wird. Die in der Datei gespeicherten Daten wurden auch für die Zuverlässigkeitsüberprüfungen der zur Fußball-WM 2006 zu akkreditierenden Personen (Nr. 5.2.5) genutzt.

Seitens des Bundes speichern vor allem die Dienststellen der Bundespolizei aufgrund ihrer bahnpolizeilichen Aufgaben Daten in der Datei. Von den Ende September 2005 insgesamt gespeicherten 8705 Datensätzen entfielen auf die Bundespolizei 1190 Ausschreibungen. Hieran war das Bundespolizeiamt Köln wegen seines örtlichen Zuständigkeitsbereichs, in dem zahlreiche Vereine der 1. und 2. Fußball-Bundesliga ansässig sind, mit 435 Ausschreibungen überdurchschnittlich beteiligt. Um einen ersten

Überblick über die Datenverarbeitung durch Polizeistellen des Bundes in der Datei „Gewalttäter Sport“ zu erhalten, habe ich die Ausschreibungen des Bundespolizeiamtes Köln im November 2005 kontrolliert.

Im Rahmen dieser Kontrolle habe ich u. a. bemängelt, dass bei allen Datensätzen, unabhängig davon, ob ihnen ein strafrechtliches Ermittlungsverfahren oder eine Gefahrenabwehrmaßnahme zu Grunde lag, einheitlich eine fünfjährige Aussonderungsprüffrist vergeben wurde. Dies trägt dem Grundsatz der Verhältnismäßigkeit, wie er in § 35 Abs. 3 Satz 3 Bundespolizeigesetz zum Ausdruck kommt, nicht Rechnung; vielmehr ist bei den Aussonderungsprüffristen nach dem Zweck der Speicherung sowie Art und Schwere des Sachverhalts zu differenzieren.

Zudem habe ich empfohlen, bis zur endgültigen Festlegung der Aussonderungsprüffrist den Ausgang des staatsanwaltschaftlichen Ermittlungsverfahrens zu berücksichtigen. Kritisch habe ich bewertet, dass eine als „Gewalttäter Sport“ ausgeschriebene Person bei einer polizeilicher Kontrolle im Inland und an den Grenzen durch Dienststellen der Bundespolizei auch dann an die ausschreibende Stelle gemeldet wurde, wenn ihr Antreffen in keinem Zusammenhang mit einer Sportveranstaltung stand. So entstanden einige Treffermeldungen bei der polizeilichen Kontrolle von „Gewalttätern Sport“, die ausschließlich zu Urlaubszwecken ausreisen wollten. In einem solchen Fall wurden auch die personenbezogenen Daten der Begleitperson mitgeteilt.

Die mit der „Treffermeldung“ übermittelten Informationen über Ort und Zeit des Antreffens der Person, über Reisewege und Ziel, die Umstände des Antreffens sowie zum Teil über Begleitpersonen führen bei der ausschreibenden Behörde zu einem Kenntnisstand, der zulässigerweise nur über eine Fahndungsausschreibung zur polizeilichen Beobachtung erzielt werden kann. Die Voraussetzungen dafür waren in diesen Fällen jedoch regelmäßig nicht erfüllt. Eine Übermittlung von „Treffermeldungen“ durch die Bundespolizei an die ausschreibende Behörde halte ich nur dann für vertretbar, wenn diese unmittelbar im Zusammenhang mit Sportveranstaltungen erfolgt, z. B. wenn Informationen über die grenzpolizeiliche Kontrolle betroffener Personen bei Fußballspielen im Ausland oder über anreisende „Gewalttäter Sport“ anlässlich eines Fußballspiels im Inland mit besonderem Gefährdungspotential gemeldet werden.

Das BMI hat meine Anregungen aufgegriffen. Mit einem Rundschreiben an die Bundespolizeipräsidien weist die Bundespolizeidirektion darauf hin, dass bei einer Ersterfassung von Datensätzen in der Datei „Gewalttäter Sport“ eine höchstens zweijährige Aussonderungsprüffrist zu vergeben sei. Bei der endgültigen Festlegung der Aussonderungsprüffrist soll zudem der Ausgang des staatsanwaltschaftlichen Ermittlungsverfahrens berücksichtigt und – sofern dies nicht bekannt ist – bei den Staatsanwaltschaften nachgefragt werden. Treffermeldungen sollen künftig nicht mehr erfolgen, wenn das Antreffen der als „Gewalttäter Sport“ ausgeschriebenen Person ganz offensichtlich in keinem Zusammenhang mit einer Sportveranstaltung steht.

Ich hoffe, dass auf diese Weise eine einheitliche Verarbeitung personenbezogener Daten in der Datei „Gewalttäter Sport“ durch die Dienststellen der Bundespolizei sichergestellt wird.

## 5.4 Zollfahndung

### 5.4.1 Zollfahndungsdienstgesetz – Auswirkungen der Entscheidung des Bundesverfassungsgerichts zur präventiven Telekommunikationsüberwachung

*Das Urteil des Bundesverfassungsgerichts zum niedersächsischen SOG hat unmittelbare Auswirkung auf das Zollfahndungsdienstgesetz, in dem die präventiv-polizeiliche Telekommunikationsüberwachung durch Polizeibehörden des Bundes geregelt ist.*

Durch Urteil vom 27. Juli 2005 (1 BvR 668/04) hat das Bundesverfassungsgericht entschieden, dass die präventive Telekommunikationsüberwachung nach dem niedersächsischen Gesetz über die öffentliche Sicherheit und Ordnung (SOG) teilweise gegen Artikel 10 GG verstößt und damit verfassungswidrig ist. Wenn noch Zweifel bestanden haben sollten, ob die vom Bundesverfassungsgericht bereits in seinem Urteil vom 3. April 2004 zur akustischen Wohnraumüberwachung (1 BvR 2378/98 – s. u. Nr. 6.2; 20. TB Nr. 5.1.2) an die Durchführung heimlicher Eingriffsmethoden gestellten Anforderungen auch auf andere verdeckte Datenerhebungsbefugnisse übertragbar sind, dürften diese mit dem o. a. Urteil zur präventiven Telekommunikationsüberwachung endgültig ausgeräumt sein.

Das Gericht bekräftigt in dem jüngsten Urteil die Notwendigkeit, den Kernbereich privater Lebensgestaltung vor staatlichen Eingriffen absolut zu schützen. Es fordert den Gesetzgeber erneut auf, im Wege gesetzlicher Regelungen sicherzustellen, dass verdeckte Datenerhebungen der Sicherheitsbehörden in diesem Kernbereich unterbleiben und dass Informationen – soweit sie unerwartet im Kernbereich erhoben wurden – gelöscht und Erkenntnisse daraus nicht verwertet werden dürfen. Ausgehend von der Prämisse des Gerichts, die durch Artikel 1 Abs. 1 GG stets garantierte Unantastbarkeit der Menschenwürde erfordere auch im Schutzbereich des Artikel 10 Abs. 1 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung, muss der Kernbereichsschutz bei allen verdeckten Datenerhebungen der Sicherheitsbehörden gewährleistet sein. Einen entsprechenden Appell enthält auch die Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005 (s. Kasten zu Nr. 5.4.1).

Das Gericht hat zudem die Bedeutung des rechtstaatlichen Gebots der Normenklarheit bei der Ausgestaltung der Eingriffsbefugnisse zur Straftatenverhütung betont. Gerade bei Vorfeldermittlungen sei das Risiko einer Fehlprognose bezüglich eines möglichen strafbaren Verhaltens besonders hoch. Zudem verpflichte das Gebot des effektiven Rechtschutzes die Sicherheitsbehörden, alle

Kasten zu Nr. 5.4.1

**Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck**

**Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden**

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber auf Grund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100a und 100b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

Betroffenen über verdeckte Datenerhebungsmaßnahmen zu unterrichten.

Unter den Polizeibehörden des Bundes ist bisher allein das Zollkriminalamt zur Durchführung der präventiven Telekommunikations- und Postüberwachung befugt. Eine Neuregelung war nach der Entscheidung des Bundesverfassungsgerichts vom 3. April 2004 zur präventiven Telekommunikationsüberwachung nach dem Außenwirtschaftsgesetz (1 BvF 3/92 – vgl. 20. TB Nr. 5.4.3) erforderlich geworden. Im Hinblick auf das o. a. Urteil des Bundesverfassungsgerichts zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen SOG ist eine entsprechende Ergänzung dieser Befugnisse dringend geboten, zumal die entsprechenden Befugnisregelungen im Zollfahndungsdienstgesetz zum 30. Juli 2007 auslaufen.

Wirksame Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung sind dabei auch im Hinblick auf alle anderen heimlichen Datenerhebungsbefugnisse des Zollkriminalamtes und der Zollfahndungsämter erforderlich.

Ich werde in weiteren Gesetzgebungsverfahren darauf hinwirken, dass die verfassungs- und datenschutzrechtlichen Vorgaben gebührende Beachtung finden.

### 5.4.2 INZOLL – neu

*Mit Inkrafttreten des Zollfahndungsdienstgesetzes im August 2002 wurde die Neukonzeption des Informations- und Auskunftssystems über Straftaten und Ordnungswidrigkeiten im Zuständigkeitsbereich der Bundeszollverwaltung (INZOLL) erforderlich.*

INZOLL-neu ist eine Sammlung personenbezogener Daten im Rahmen des Zollfahndungsinformationssystems gem. §§ 3 Abs. 3, 11 bis 13 des Zollfahndungsdienstgesetzes (ZFdG). Es wird vom Zollkriminalamt in seiner Funktion als Zentralstelle für den Zollfahndungsdienst und andere Dienststellen der Zollverwaltung geführt. Der Zugriff auf die Dateien dieses Systems, die datenschutzrechtliche Verantwortung für die darin gespeicherten Daten sowie das Verfahren der Protokollierung von Zugriffen sind dabei in Anlehnung an die Regelungen nach dem BKA-Gesetz zum Informationssystem der Polizeien des Bundes und der Länder (INPOL) normiert worden. Das

Verfahren INZOLL-neu löst die bislang bestehende Sammlung personenbezogener Daten ab, die im Wesentlichen Aktennachweisfunktionen hatte. INZOLL-neu soll darüber hinaus der Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten, der Aufdeckung unbekannter Straftaten sowie der Vorsorge für künftige Strafverfahren im Zuständigkeitsbereich der Zollverwaltung sowie der Sicherstellung einer gleichmäßigen Festsetzung und Erhebung von Steuern dienen. Die datenschutzrechtlichen Anforderungen sollen u. a. durch abgestufte Zugriffsberechtigungen, durch ein differenziertes Schutzklassenkonzept zur Sicherstellung der zweckgebundenen Verarbeitung sowie durch Zugriffsprotokollierungen sichergestellt werden.

Im Rahmen des Anhörungsverfahrens gemäß § 41 ZFdG zu der Errichtungsanordnung für INZOLL-neu habe ich mich u. a. für differenzierte Speicherungsfristen für die Daten zu Beschuldigten einerseits und tatferneren Personen, wie Zeugen, Kontakt- und Begleitpersonen andererseits ausgesprochen. Zudem halte ich eine vollständige Protokollierung aller Zugriffe auf die Datei für geboten, um eine sachgerechte Datenschutzkontrolle zu gewährleisten. Das Anhörungsverfahren war bei Redaktionsschluss noch nicht abgeschlossen.

## 5.5 Verfassungsschutz

### 5.5.1 Evaluierung des Terrorismusbekämpfungsgesetzes 2002

*Der Evaluierungsbericht der Bundesregierung zum Terrorismusbekämpfungsgesetz (TBG) ist unzureichend und keine hinreichende Legitimationsgrundlage für das Terrorismusbekämpfungsergänzungsgesetz (TBEG).*

Gesetzliche Regelungen, die in Grundrechtspositionen der Bürgerinnen und Bürger eingreifen, bedürfen einer schlüssigen Begründung und müssen dem verfassungsrechtlichen Verhältnismäßigkeitsgebot entsprechen. Häufig sind aber zum Zeitpunkt der Einführung neuer Befugnisnormen die Konsequenzen dieser Regelungen nur unvollkommen prognostizierbar. Aus diesem Grund hatte der Deutsche Bundestag beschlossen, die im Rahmen des Terrorismusbekämpfungsgesetzes 2002 eingeführten neuen Befugnisse auf fünf Jahre zu befristen und rechtzeitig vor Ablauf dieser Frist einer Evaluation zu unterwerfen (vgl. 20. TB Nr. 5.5.4). Von der Evaluation wäre eigentlich zu erwarten gewesen, dass die jeweiligen Maßnahmen hinsichtlich ihrer Anwendungsbreite, ihres Erfolges und in Bezug auf ihre Eingriffsintensität in Grundrechte bewertet werden. Legt man diese Anforderungen zu Grunde, war der von der Bundesregierung im Mai 2005 vorgelegte „Bericht zu den Auswirkungen der nach Artikel 22 Abs. 2 des TBG befristeten Änderungen des Bundesverfassungsschutzgesetzes, des MAD-Gesetzes, des BND-Gesetzes, des Artikel 10-Gesetzes, des Sicherheitsüberprüfungsgesetzes und des § 7 Abs. 2 des BKA-Gesetzes“ (vgl. Drucksache des Innenausschusses des Deutschen Bundestages 15(4)218) eine Enttäuschung.

Auswertungsstichtag war der 31. Dezember 2004. Die aus der Evaluierung gewonnenen Erkenntnisse hat die Bundesregierung nach eigenen Angaben im TBEG (s. o. Nr. 5.1.2) umgesetzt (vgl. Bundestagsdrucksache 16/2921, Entwurfsbegründung, A. Allgemeiner Teil, Seite 1). Wie ich gegenüber dem Innenausschuss des Deutschen Bundestages erläutert habe (vgl. Drucksache des Innenausschusses des Deutschen Bundestages 16(4)71, Anlage 4), halte ich den Evaluierungsbericht für unzureichend. Zum einen ist der Bericht nicht das Ergebnis einer wissenschaftlich fundierten Evaluation. Die Auswirkungen der von den Sicherheitsbehörden getroffenen Eingriffsmaßnahmen auf die Grundrechte der Betroffenen werden beispielsweise nicht hinreichend untersucht und bewertet. In dem Bericht fehlen zudem wesentliche, für die Evaluation notwendige Informationen, z. B. zur Kosten-Nutzen-Relation der getroffenen Maßnahmen. Kritisch zu bewerten ist ferner die von der Bundesregierung geforderte Entfristung, d.h. die unbefristete Weitergeltung, sämtlicher durch das TBG neu geschaffener Befugnisse. Angesichts der besonderen Grundrechtsintensität der auf diese Befugnisse gestützten Maßnahmen ist eine Entfristung insbesondere in den Fällen nicht zu legitimieren, in denen die Sicherheitsbehörden von diesen Befugnissen nur geringen oder gar keinen Gebrauch gemacht haben.

Als Folge dieser Kritik hat der Gesetzgeber die Geltung der nachrichtendienstbezogenen Regelungen des TBG und des TBEG entgegen dem Petitum der Bundesregierung erneut auf fünf Jahre befristet. Zudem hat er eine Pflicht zur Evaluierung dieser Regelungen normiert und – meinem Petitum folgend – festgelegt, dass die Evaluierung auf wissenschaftlicher Grundlage unter Einbeziehung eines wissenschaftlichen Sachverständigen erfolgen muss, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist (s. o. Nr. 5.1.2).

### 5.5.2 Einsatz nachrichtendienstlicher Mittel durch den Verfassungsschutz – mobile Beobachtungstruppe

*Beim Einsatz nachrichtendienstlicher Mittel durch das Bundesamt für Verfassungsschutz (BfV) wurden anlässlich eines Beratungs- und Kontrollbesuchs datenschutzrechtliche Defizite festgestellt.*

Im Februar 2006 habe ich im BfV einen Beratungs- und Kontrollbesuch zum Einsatz nachrichtendienstlicher Mittel durchgeführt. Meine Kontrolle erstreckte sich insbesondere auf den Bereich der Observation und den damit verbundenen Einsatz technischer Mittel. Genauere Angaben hierzu sind aus Geheimschutzgründen nicht möglich.

Die Observation ist eine Methode zur heimlichen Informationsbeschaffung über Personen, Objekte und Ereignisse (vgl. § 8 Abs. 2 Satz 1 Bundesverfassungsschutzgesetz – BVerfSchG). Ausgeführt werden die Observationsmaßnahmen durch mobile Observationsteams (sog. Observationstrupps) im Auftrag der jeweiligen Fachabteilungen des BfV.

Bei der Kontrolle habe ich festgestellt, dass eine Datei ohne die gesetzlich vorgeschriebene Dateianordnung (vgl. § 14 Abs. 1 BVerfSchG) geführt worden ist. Darüber hinaus sind personenbezogene Daten in Dateien

entgegen gesetzlichen Vorgaben und der geltenden Dateianordnung gespeichert worden. Im Kontrolltermin hat das BfV die umgehende Beseitigung dieser Mängel zugesagt. Insofern habe ich von einer förmlichen Beanstandung abgesehen.

Die anlässlich der Kontrolle begonnene kritische Diskussion über Ausmaß und Intensität einzelner von mir kontrollierter Überwachungsmaßnahmen dauert an. Aus Geheimschutzgründen ist eine detailliertere Darlegung nicht möglich.

## 5.6 MAD

### 5.6.1 Ausbau der Informationsverarbeitung beim MAD

*Bei der Einführung der „elektronischen Akte" sind beim MAD Fehler aufgetreten. Ein anderes Projekt wurde wegen datenschutzrechtlicher Bedenken bislang nicht in die Praxis umgesetzt.*

Anders als bei der „elektronischen Akte" beim BfV ist das Dokumentenmanagementsystem EXA 21 des MAD so konzipiert, dass nur solche personenbezogenen Daten recherchierbar sein sollen, die der MAD nach geltendem Recht (§ 6 Abs. 1 Satz 1 MADG i. V. m. § 10 Abs. 1 BVerfSchG) speichern darf (vgl. 20. TB Nr. 5.6.3). Hierzu werden die speicherfähigen Daten von den zuständigen Bearbeitern elektronisch markiert. Das System ging im Jahre 2005 in einer Abteilung des MAD in den Wirkbetrieb.

Im Sommer 2006 erreichte mich eine Eingabe, in der ein Petent sich darüber beklagt, der MAD habe durch eine „versehentliche" Erfassung von Daten zu seiner Person sein Persönlichkeitsrecht verletzt. In seiner Stellungnahme bestätigte das BMVg, die Daten des Petenten seien tatsächlich vom MAD recherchierbar erfasst worden. Diese Erfassung sei jedoch fehlerhaft gewesen und in der Anfangsphase nach Einführung des Dokumentenmanagementsystems EXA 21 erfolgt, aber bereits im August 2005 durch eine Umstellung des Systems bereinigt worden. Die Daten des Petenten seien inzwischen vollständig gelöscht. Der MAD habe sich bei ihm entschuldigt.

Ich betrachte diesen Vorgang als eine sehr ernst zu nehmende Angelegenheit; denn gegen das Projekt EXA 21 hatte ich meine ursprünglichen Bedenken zurückgestellt, weil durch die elektronische Markierung der speicherfähigen Daten eben nur diese Daten recherchierbar sein sollten. Da der rechtswidrige Eingriff in das Persönlichkeitsrecht des Petenten inzwischen durch Löschung der Daten erledigt und der Systemfehler behoben wurde, habe ich zunächst von einer Beanstandung abgesehen. Ich werde diesen Fall jedoch zum Anlass nehmen, EXA 21 in technischer Hinsicht und im Hinblick auf die Vereinbarkeit mit dem geltenden Recht zu kontrollieren.

Im Berichtszeitraum hat der MAD mir ein weiteres IT-Projekt vorgestellt. Durch das Projekt PGS 21 sollen manuelle Arbeiten durch elektronische Datenverarbeitung weitgehend ersetzt, die Arbeitsabläufe bei den Sicherheitsüberprüfungen beim MAD optimiert und die Bearbeitungszeiten erheblich verkürzt werden. Erfreulicherweise hat mich der MAD zu einem frühen Zeitpunkt in das Vorhaben eingebunden. Dies macht es möglich, bei den weiteren Arbeiten meine datenschutzrechtlichen Vorstellungen zu berücksichtigen. Dies sind im Wesentlichen folgende:

- Das Projekt reicht weit über den Zuständigkeitsbereichs des MAD hinaus, da auch Dienststellen außerhalb des MAD-Amtes und der MAD-Stellen einbezogen werden.
- Problematisch ist die Generierung eines Datensatzes bei den Sicherheitsbevollmächtigten der Dienststellen im Hinblick auf die restriktiven Speicherbefugnisse in § 20 SÜG, z. B. durch die Einbeziehung von Familienangehörigen.
- Da mit diesem Projekt auch die Sicherheitsüberprüfungsakte beim MAD in elektronischer Form eingeführt werden soll, halte ich zuvor eine Änderung des § 20 SÜG für erforderlich.

Aufgrund der noch offenen Fragen ist dieses Vorhaben noch nicht in die Praxis umgesetzt worden. Seinen Fortgang werde ich weiter aufmerksam verfolgen.

### 5.6.2 Zusammenarbeit des MAD mit der Polizei

*Auch beim Vorgehen gegen rechtsextremistische Bestrebungen in der Bundeswehr ist die Verhältnismäßigkeit zu wahren.*

Im Frühjahr 2006 hat der MAD eine Polizeidienststelle um die Zusammenstellung von Namen bekannter militanter Personenkreise gebeten, um deren Zugehörigkeit zur Bundeswehr zu prüfen. Da die Polizei Zweifel an der Rechtmäßigkeit einer solchen Anfrage hatte, wandte es sich an den zuständigen Landesdatenschutzbeauftragten, der die Angelegenheit aus Gründen der Zuständigkeit an mich weiterleitete.

In seiner von mir erbetenen Stellungnahme rechtfertigt das BMVg die Anfrage des MAD damit, hinsichtlich eines Soldaten der Bundeswehr hätten sich Hinweise ergeben, dieser könnte in rechtsextremistische Bestrebungen verstrickt sein. Im Zuge der Ermittlungen habe der MAD bei der Polizeidienststelle um eine Zusammenstellung bekannter militanter Kreise gebeten, um die Zugehörigkeit weiterer Personen zum Geschäftsbereich des BMVg zu prüfen. Nach der Lebenserfahrung sei naheliegend, dass bei Feststellung eines anerkannten Rechtsextremisten und Bundeswehrangehörigen in einer militanten Gruppe dort weitere unerkannte Rechtsextremisten und Bundeswehrangehörige vorhanden seien.

Ich verkenne nicht, dass der MAD bei der gegebenen Sachlage und angesichts des Phänomens „Rechtsextremismus in der Bundeswehr" nach dem erhaltenen Hinweis zu weiteren Recherchen berechtigt war, halte jedoch die Bitte um Übersendung von ganzen Zusammenstellungen für unverhältnismäßig, zumal sich die Annahme, in der Gruppe könnten sich weitere Bundeswehrangehörige

befinden, nur auf bloße Vermutung oder – wie vom BMVg mitgeteilt – auf angebliche Lebenserfahrung stützte. Durch Übersendung umfangreicher Zusammenstellungen würde dem MAD unter Umständen eine Vielzahl personenbezogener Daten von Personen übermittelt, für die er keine Zuständigkeit hat. Es würde sich damit um einen Eingriff in das Persönlichkeitsrecht einer Vielzahl unbetroffener Personen handeln.

Das BMVg hat das vom MAD gewählte Verfahren verteidigt und sieht die Praxis als durch das MAD-Gesetz gedeckt an. Wegen des Eingriffs in das Persönlichkeitsrecht einer Vielzahl unbeteiligter Personen halte ich hingegen dieses Verfahren für einen Verstoß gegen den Grundsatz der Verhältnismäßigkeit (§ 4 Abs. 1 MAD-Gesetz i.V.m. § 8 Abs. 3 BVerfSchG) und habe das BMVg gebeten, diese Praxis durch eine Weisung an den MAD einzustellen.

Die Gespräche mit dem BMVg über dieses Thema werden fortgesetzt.

## 5.7 BND

### 5.7.1 Erneute Änderung des Artikel 10-Gesetzes – G 10

*Der Entwurf eines Ersten Gesetzes zur Änderung des Artikel 10-Gesetzes wurde ohne kernbereichschützende Regelungen im Parlament eingebracht.*

Über Vorüberlegungen der Bundesregierung zu einer Novellierung des Artikel 10-Gesetzes habe ich bereits berichtet (20. TB Nr. 5.7.1); diese ergaben sich im Wesentlichen aus einem Erfahrungsbericht der Bundesregierung nach zwei Jahren Anwendung des neuen G 10, vgl. Bundestagsdrucksache 15/2042. Die Erfahrungen mündeten in den Entwurf eines Ersten Gesetzes zur Änderung des Artikel 10-Gesetzes, an dessen Vorbereitung ich beteiligt war. Dabei geht es im Wesentlichen um neue Befugnisse für den BND, insbesondere

- die Datenerhebung und -verarbeitung des BND im Bereich der strategischen Telekommunikationsüberwachung,
- erstmals eine Befugnis zur Individualüberwachung von Telekommunikationsanschlüssen in bestimmten Fällen sowie
- eine klarstellende Regelung zur Übermittlung der aus der strategischen Telekommunikationsüberwachung gewonnenen Daten an ausländische öffentliche Stellen.

Die parlamentarischen Beratungen mit zusätzlichen Änderungsvorschlägen waren bei Redaktionsschluss noch nicht abgeschlossen. Gegen die vorgesehenen Detailregelungen im Gesetzentwurf bestehen keine grundlegenden datenschutzrechtlichen Bedenken; es ist jedoch zu befürchten, dass mit solchen partiellen Änderungen immer wieder neuer Änderungsbedarf hervorgerufen wird. Ärgerlich ist, dass der Entwurf entgegen meinen Mahnungen keine Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung enthält (vgl. auch Nr. 5.4.1), und zwar weder bei der Datenerhebung, noch bezüglich der Kennzeichnung der durch solche TKÜ-Maßnahmen gewonnenen Daten und schon gar nicht zur nachträglichen Unterrichtung der von solchen Überwachungsmaßnahmen betroffenen Personen. Der Entwurf trägt also ein hohes verfassungsrechtliches Risiko. Bei den weiteren Beratungen werde ich auf die Umsetzung der einschlägigen Rechtsprechung des Bundesverfassungsgerichts drängen, das mit Urteil vom 3. April 2004 zur akustischen Wohnraumüberwachung (1 BvR 2378/98) und vom 27. Juli 2005 (1 BvR 66804) zum Niedersächsischen Polizeigesetz hohe Anforderungen an den Kernbereichsschutz gestellt hat, die auch bei einer präventiven Telefonüberwachung zu beachten sind.

### 5.7.2 Beobachtung von Journalisten durch den BND

*Der BND hat über viele Jahre hinweg mit Journalisten kooperiert, einzelne unter ihnen jedoch auch observiert.*

Wie im Herbst 2005 bekannt wurde, hat der BND jahrelang im Inland Journalisten in seine Beschaffungsaktivitäten einbezogen. Anrüchig wurde die Angelegenheit jedoch erst, als öffentlich wurde, dass der BND etliche dieser Journalisten auch observiert haben soll (vgl. zur Observation durch Nachrichtendienste auch Nr. 5.5.2). Der Einsatz solcher nachrichtendienstlicher Mittel ist dem BND grundsätzlich nach § 3 BND-Gesetz gestattet, allerdings ist dabei die Verhältnismäßigkeit zu wahren. Der Dienst beruft sich beim Einsatz dieser Methoden gegenüber Journalisten auf sein Recht zur Eigensicherung (vgl. § 2 Abs. 1 Nr. 1 BND-Gesetz). Überwiegend geht es darum, sog. Nachrichtenabflüsse, also „undichte Stellen“ beim Dienst aufzudecken. Die Angelegenheit ist auch Gegenstand des Bundestagsuntersuchungsausschusses, der sich in 2006 konstituiert hat, um diverse Aktivitäten des BND aufzuklären (s. u. Nr. 5.7.4). Zudem wurden die Affären durch einen internen Bericht des BND selbst sowie einen Untersuchungsbericht eines externen Sachverständigen im Auftrag des parlamentarischen Kontrollgremiums untersucht.

Mich haben mehrere Eingaben, insbesondere von betroffenen Journalisten erreicht, in denen sie mich um die datenschutzrechtliche Kontrolle der Vorgänge baten. Diesen hatte der BND z. T. bereits in relativ ausführlicher Form Auskunft erteilt. Ich habe diese Kontrollen im Rahmen der begrenzten mir zur Verfügung stehenden personellen Ressourcen durchgeführt und datenschutzrechtlich wie folgt bewertet:

- Der erste Petent behauptete, er sei in den 1990-iger Jahren über mehrere Jahre hinweg vom BND observiert, und seine Daten seien dort gespeichert worden. Ich habe anhand des BND-internen Untersuchungsberichtes (s. o.) und weiterer Gespräche vor Ort festgestellt, dass der Petent zwar nicht Zielperson der BND-Aktivitäten war, jedoch in Kontakt mit observierten Personen stand und insofern ins Visier des BND geraten war. Die Sachlage ist dem Petenten vom BND ausführlich dargelegt worden. Eine Verletzung datenschutzrechtlicher Belange des Petenten habe ich

nicht festgestellt, obgleich vom BND noch einige personenbezogene Daten zu dem Petenten in Akten dokumentiert sind.

– Der zweite Petent war ein Journalist, der jahrelang mit dem BND zusammengearbeitet hatte. Meine schwerpunktmäßige Kontrolle erbrachte keine Erkenntnisse über datenschutzrechtliche Verstöße.

– Der dritte Petent, ebenfalls ein Journalist, hat seine Rechte, neben der Eingabe bei mir, auch vor Gericht geltend gemacht. Ihm war zuvor Auskunft durch den BND erteilt worden, allerdings beschränkt auf die Verarbeitung personenbezogener Daten in Dateien (vgl. hierzu Nr. 5.7.7). Die dateimäßige Auskunft, die der BND mir im Rahmen der datenschutzrechtlichen Kontrolle erteilt hat, war derartig lückenhaft und unsystematisch, dass ich mich zu einer Einsichtnahme in die zugrunde liegenden Aktenvorgänge veranlasst sah. Diese vertiefte Kontrolle ist noch nicht abgeschlossen. Ich werde im nächsten Bericht darauf zurückkommen.

Zusammenfassend bleibt festzuhalten, dass ich den Komplex „Observation von Journalisten durch den BND“ nur in Teilaspekten als Folge der Eingaben einzelner Betroffener untersuchen konnte. Die Petenten unterscheiden sich insofern von anderen Antragstellern, als sie zuvor in Kontakt mit dem BND gestanden hatten. Soweit sie von ihrem Recht auf Auskunft Gebrauch gemacht hatten, wurde ihnen relativ umfangreich Auskunft erteilt.

### 5.7.3 Umbau der IT-Struktur beim BND

*Beim BND stehen umfangreiche Änderungen der IT-Struktur bevor, die auf datenschutzrechtliche Bedenken stoßen.*

Der BND plant eine neue zentrale Datei, die einige bisher separat betriebene Dateien ersetzen und in einer einzigen Datenbank zusammenfassen soll. Ziel ist die Schaffung eines zentralen Datenpools.

Die Zusammenfassung verschiedener Anwendungen führt jedoch auch zur Konzentration personenbezogener Daten unterschiedlicher Kategorien in einer Datenbank. Damit entsteht eine Datei mit Mischcharakter, die neue datenschutzrechtliche Probleme aufwirft und die inhaltlich weit über den Umfang einer zentralen Hinweisdatei hinaus geht. Hiermit verbunden ist ein intensiverer Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung, da deren Daten einem größeren Anwenderkreis – losgelöst von der Notwendigkeit der Prüfung im Einzelfall – unmittelbar zugänglich gemacht werden können. Dies wirft insbesondere bei den nach dem SÜG erhobenen Daten, für die restriktivere Regelungen gelten, erhebliche Fragen auf. Es bedarf daher eines differenzierten und technisch einwandfrei funktionierenden Berechtigungskonzepts, bevor diese Datei in Wirkbetrieb gehen kann.

Nach intensiven Erörterungen hat sich der BND bereiterklärt, meine Anregungen aufzugreifen und bei der weiteren Konzeption zu berücksichtigen. Die gemäß den Anforderungen der jeweiligen Aufgabenbereiche erhobenen Daten sollen technisch separat gespeichert und nutzbar gemacht werden. Auf diese separat gespeicherten Daten sollen nur diejenigen Stellen bzw. Bediensteten zugreifen können, welche die Daten im Rahmen ihrer jeweiligen Zuständigkeit zur Aufgabenerfüllung benötigen. Die Vergabe der Zugriffsberechtigungen soll unter Wahrung der spezifischen Rechtsgrundlagen erfolgen.

Der BND hat zugesagt, mich an der weiteren Konzeption dieses Projektes zu beteiligen, dessen Umsetzung wegen seiner Komplexität sicher noch einige Zeit beanspruchen wird.

### 5.7.4 Bericht der Bundesregierung zu Auslandsaktivitäten des BND im Irak

*Der Bericht der Bundesregierung vom 25. Januar 2006 zu Vorgängen im Zusammenhang mit dem Irakkrieg und der Bekämpfung des internationalen Terrorismus war aus datenschutzrechtlicher Sicht nicht zur Veröffentlichung geeignet.*

Im Februar 2006 wurde ich von der Bundesregierung gebeten zu prüfen, ob ihr Bericht an das Parlamentarische Kontrollgremium zu Vorgängen im Zusammenhang mit dem Irakkrieg und der Bekämpfung des internationalen Terrorismus auch der Öffentlichkeit zugänglich gemacht werden dürfe. Der Bericht enthielt Informationen zum Einsatz von BND-Mitarbeitern in Bagdad, über behauptete Festnahmen und Gefangenentransporte durch ausländische Stellen außerhalb eines rechtsförmlichen Verfahrens sowie über die Befragung von Gefangenen durch Sicherheitsbehörden des Bundes im Ausland. Aus einigen der im Bericht enthaltenen Angaben konnte auf den Gesundheitszustand der Betroffenen geschlossen werden. Ein Teil der personenbezogenen Informationen stammte zudem aus Gerichts- und Ermittlungsakten von eingestellten Verfahren.

Nach Durchsicht des Berichts bin ich deshalb zu dem Ergebnis gekommen, dass die Veröffentlichung wesentlicher Teile unter datenschutzrechtlichen Gesichtspunkten nicht zulässig gewesen wäre. Zwar wurden im Bericht erwähnte Personen nur mit Namenskürzeln bezeichnet. Aus dem Kontext waren sie jedoch ohne großen Aufwand identifizierbar, so dass die Angaben gleichwohl als personenbeziehbar anzusehen waren. Die Voraussetzungen für die Veröffentlichung dieser personenbezogenen Daten gemäß § 16 BDSG waren jedoch nicht gegeben.

Gegen die Übermittlung des gesamten Berichts an die parlamentarischen Gremien des Deutschen Bundestages zur Gewährleistung der Kontrollfunktion des Parlaments bestanden hingegen keine datenschutzrechtlichen Bedenken, da insofern die Voraussetzungen für eine Übermittlung gemäß § 15 i. V. m. § 14 BDSG erfüllt waren.

Ich begrüße es, dass die Bundesregierung meinem Petitum gefolgt ist und von einer Veröffentlichung des Berichts abgesehen hat.

### 5.7.5 Altdatenbereinigungskonzept

*Das vom Bundesnachrichtendienst (BND) vorgelegte Altdatenbereinigungskonzept ist überholt. Bei einer Kontrolle (vgl. Nr. 5.7.6) wurden neue Altdatenbestände entdeckt.*

Bei früheren Kontrollen hatte ich im BND wiederholt Altdatenbestände festgestellt, die längst hätten überprüft und bereinigt werden müssen (vgl. u. a. 20. TB Nr. 5.7.3). Zur Vermeidung einer Beanstandung nach § 25 BDSG hatte ich den BND aufgefordert, ein tragfähiges abteilungsübergreifendes Konzept zur Altdatenbereinigung und zur Vermeidung zukünftiger Altdatenbestände vorzulegen (vgl. a.a.O.).

Ein solches Konzept liegt inzwischen vor. Darin hat der BND zwischen verschiedenen Arten von Altdatenbeständen differenziert, z. B. zwischen Altdaten, die durch ungeprüftes Überschreiten der fünfjährigen Wiedervorlageprüfung (§ 5 Abs. 1 des Gesetzes über den Bundesnachrichtendienst (BNDG) in Verbindung mit § 12 Abs. 3 Satz 1 Bundesverfassungsschutzgesetz (BVerfSchG)) entstanden sind, oder Datenbeständen in „alten“ Dateien, für die keine Dateianordnung gem. § 6 BNDG vorliegt. Die angebotenen Lösungsmöglichkeiten habe ich mit dem Bundeskanzleramt als zuständiger Fachaufsichtsbehörde und dem BND intensiv erörtert.

Wie ich bedauerlicherweise bei einer zwischenzeitlich durchgeführten weiteren Kontrolle einer Datei beim BND feststellen musste, sind als Folge eines schwerwiegenden Datenschutzverstoßes neue Altdatenbestände entstanden (vgl. Nr. 5.7.6), die in dem bisherigen Lösungskonzept nicht berücksichtigt waren. So sind bei vielen Datensätzen die gesetzlich vorgegebenen Prüffristen nicht nur nicht eingehalten, sondern wegen fehlender Sachkenntnis der eingesetzten Bearbeiter pauschal, d. h. ohne Einzelfallprüfung, um jeweils ein Jahr verlängert worden (vgl. a. a. O.). Aufgrund dieses von mir beanstandeten Verstoßes habe ich den BND aufgefordert, ein aktualisiertes Altdatenbereinigungskonzept vorzulegen, durch das derartige Mängel in der Zukunft ausgeschlossen werden. Dies hat der BND zugesagt; bis Redaktionsschluss lag aber noch kein neues Konzept vor.

### 5.7.6 Kontrolle einer Anti-Terrorismusdatei

*Bei der Kontrolle einer Fachdatei beim BND habe ich erneut festgestellt, dass der Dienst seiner Pflicht zur regelmäßigen Prüfung der gespeicherten Datensätze nach fünf Jahren nicht nachkommt. Diesen schwerwiegenden Verstoß habe ich nach § 25 Abs. 1 BDSG förmlich beanstandet.*

Im Berichtszeitraum habe ich eine mehrtägige Kontrolle einer der Beobachtung des internationalen Terrorismus dienenden Fachdatei beim BND durchgeführt. Bei den nach dem Zufallsprinzip überprüften Datensätzen habe ich zwar dem Grunde nach keine Mängel festgestellt; die Speicherung der personenbezogenen Daten war sowohl zur Erfüllung der Aufgaben des BND nach § 1 Abs. 2 des BND-Gesetzes als auch nach der konkreten Zweckbestimmung gemäß der Dateianordnung zulässig. Jedoch haben sich einige andere, zum Teil gravierende Fehler gezeigt:

– Wie bei früheren Kontrollen (vgl. 19. TB Nr. 19.4, 20. TB Nr. 5.7.3) musste ich erneut feststellen, dass der BND seiner Pflicht, gespeicherte Datensätze gem. § 5 Abs. 1 BND-Gesetz in Verbindung mit § 12 Abs. 3 BVerfSchG, spätestens jedoch nach fünf Jahren, im Hinblick auf eine Berichtigung oder Löschung zu prüfen, nicht mit der erforderlichen Sorgfalt nachkommt. In einer Organisationseinheit waren über einen längeren Zeitraum keine Löschungsüberprüfungen vorgenommen worden. Die Wiedervorlagefristen bei den Datensätzen, die zur Löschungsüberprüfung anstanden, waren offensichtlich wegen mangelnder Sachkenntnis in Folge eines Personalmangels in dieser Organisationseinheit jeweils pauschal um ein Jahr verlängert worden, eine Einzelprüfung hatte demnach nicht stattgefunden. Dies stellt einen schwerwiegenden Verstoß gegen § 5 Abs. 1 BND-Gesetz in Verbindung mit § 12 Abs. 3 BVerfSchG dar, den ich gem. § 25 Abs. 1 BDSG förmlich beanstandet habe, zumal eine ordentliche Datenpflege für einen Nachrichtendienst unverzichtbar ist.

  Diese Rechtsverletzung wiegt umso schwerer, als der BND erst vor Kurzem ein umfassendes Konzept zur Bereinigung solcher als auch anderer Altdaten entwickelt hat, bei dem die vorstehende Problematik aber nicht berücksichtigt wurde (vgl. Nr. 5.7.5). Zudem steht meine Feststellung in krassem Gegensatz zu den Aussagen des zuständigen Fachbereichs, die Rückstände seien abgearbeitet.

– Die Datensätze in dieser Datei enthalten in der Regel auch Volltextfelder. In zahlreichen Fällen sind hierbei Volltexte, die von einer Abteilung gespeichert wurden, auch für eine andere Abteilung im Wege eines lesenden Zugriffs nutzbar. Dies ist mit § 6 BND-Gesetz in Verbindung mit § 14 Abs. 3 BVerfSchG nicht vereinbar, wonach die Zugriffsberechtigung auf Textdateien und Dateien mit Freitextfeldern auf Personen zu beschränken ist, die unmittelbar mit Arbeiten auf dem Gebiet betraut sind, dem die Textdatei zugeordnet ist. Schon wegen der anders gearteten Aufgabenstellung dieser beiden Abteilungen sehe ich keine Notwendigkeit für einen Zugriff auf Volltexte, die von der jeweils anderen Abteilung eingestellt worden sind. Ich habe daher den BND gebeten, den Zugriff entsprechend § 14 Abs. 3 BVerfSchG zu beschränken.

– In einem Datensatz waren Lichtbilder enthalten, auf denen Kinder dargestellt waren. Nach § 4 Abs. 2 BND-Gesetz in Verbindung mit § 11 Abs. 1 BVerfSchG ist eine Speicherung von Daten oder über das Verhalten Minderjähriger vor Vollendung des 16. Lebensjahres in Dateien unzulässig. Nach einem entsprechenden Hinweis wurden diese Bilder aus der Datei gelöscht. Ich habe den BND jedoch gebeten, künftig Bildaufnahmen, bei denen eine Miterfassung von Minderjährigen unter 16 Jahren unvermeidbar ist, vor der Speicherung in Dateien so zu bearbeiten, dass die Minderjährigen nicht mehr erkennbar sind. Gleiches

gilt auch für die Aufnahme von Bildaufnahmen in Akten, sofern die Voraussetzungen des § 11 Abs. 1 BVerfSchG nicht vorliegen.

– In einigen Fällen waren die Daten der Betroffenen nicht in die Personenzentraldatei übernommen worden, obwohl für eine solche Speicherung ausreichend Daten vorhanden waren. Wegen der Bedeutung, die eine Speicherung in der Personenzentraldatei vor allem im Hinblick auf die Wahrung des Auskunftsrechts der Betroffenen hat, habe ich den BND gebeten, künftig bei allen Neuspeicherungen die Relevanz für die Personenzentraldatei sorgfältiger zu prüfen.

Eine Reaktion des Bundeskanzleramtes bzw. des BND zu meinem Kontrollbericht steht noch aus.

### 5.7.7 Auskunftspflicht des Bundesnachrichtendienstes (BND)

*Die Auskunftspflicht des BND gegenüber einem Betroffenen gilt für personenbezogene Daten nicht nur in Dateien, sondern auch in Akten.*

Nach § 7 Satz 1 des Gesetzes über den Bundesnachrichtendienst (BNDG) hat der BND einem Betroffenen auf Antrag Auskunft über die zu seiner Person nach § 4 BNDG gespeicherten Daten entsprechend § 15 des Bundesverfassungsschutzgesetzes (BVerfSchG) zu erteilen.

Ein Petent teilte mit, der BND habe ihm Auskunft zur Speicherung personenbezogener Daten lediglich in Dateien, nicht jedoch in Akten erteilt. Daraufhin habe ich die Thematik mit dem Bundeskanzleramt als der zuständigen Fachaufsichtsbehörde und mit dem BND erörtert. Beide vertreten die Auffassung, die Auskunftsverpflichtung des BND erstrecke sich lediglich auf die in Dateien gespeicherten Daten. Sie begründen dies mit dem Wortlaut des § 7 Satz 1 BNDG, wonach Auskunft nur über die nach § 4 BNDG gespeicherten Daten zu erteilen sei. § 4 Abs. 1 BNDG verweise auf die Vorschrift des § 10 BVerfSchG. Dort sei nur die Speicherung, Veränderung und Nutzung personenbezogener Daten in Dateien geregelt. Folglich bestehe für den BND im Gegensatz zum Bundesamt für Verfassungsschutz (BfV) und dem Militärischen Abschirmdienst (MAD) keine Verpflichtung zur Auskunftserteilung über in Akten gespeicherte personenbezogene Daten eines Betroffenen. Diese Privilegierung des BND entspreche im Übrigen auch dem Willen des Gesetzgebers und trage der gegenüber den anderen Nachrichtendiensten (BfV, MAD) bestehenden Sonderstellung des BND Rechnung.

Der vom BND behauptete Privilegierungswille des Gesetzgebers ist der Gesetzesbegründung nicht zu entnehmen. Der Hinweis auf den Wortlaut des § 7 Satz 1 BNDG vermag insofern nicht zu überzeugen, als die Regelungen zum Auskunftsverfahren erst in den parlamentarischen Beratungen in die Dienstegesetze eingefügt worden sind und der politische Wille in diesen Beratungen nicht auf eine Privilegierung des BND, sondern auf das zur Geheimschutzwahrung notwendige Ziel gerichtet gewesen ist, ein Akteneinsichtsrecht von Petenten zu vermeiden.

Eine mit Hinweis auf die vermeintliche Sonderstellung des BND beabsichtigte Privilegierung wäre im Übrigen wegen der zwischenzeitlichen Änderung des Aufgaben- und Befugnisrahmens des BND nicht mehr zu legitimieren. Nach der Verabschiedung des BNDG im Jahr 1990 hat sich die Aufgabenstellung dieses Dienstes, nicht zuletzt aufgrund der Terrorismusbekämpfung, wesentlich verändert. Der Tätigkeitsbereich erstreckt sich zunehmend auf die Erhebung personenbezogener Daten auch im Inland. Der BND ist nicht mehr nur strategisch aktiv, sondern mehr und mehr operativ personenbezogen im Vorfeld der Verbrechensbekämpfung. Diese Entwicklung wird sich im Zuge der von der Bundesregierung angestrebten Optimierung bzw. Neugestaltung der informationellen Zusammenarbeit der Sicherheitsbehörden des Bundes und der Länder (vgl. Nr. 5.1) weiter fortsetzen.

Die Auffassung des Bundeskanzleramtes und des BND steht auch nicht in Einklang mit der verfassungsgerichtlichen Rechtsprechung. In seinem Beschluss vom 10. Oktober 2000 zur Auskunftspflicht nach § 15 BVerfSchG hat das Bundesverfassungsgericht die elementare Bedeutung des Auskunftsanspruchs betont (vgl. 1 BvR 586/90). Mit der Ausgestaltung von Auskunftsrechten und Auskunftspflichten werde dem durch Artikel 2 Abs. 1 i. V. m. Artikel 1 Abs. 1 GG gewährleisteten Recht auf informationelle Selbstbestimmung Rechnung getragen und den Betroffenen die Möglichkeit eröffnet, gerichtlichen Rechtsschutz gegen unrechtmäßigen Umgang mit ihren Daten in Anspruch zu nehmen. Der Auskunftsanspruch ist demnach eine zentrale verfahrensrechtliche Sicherung. Die Bedeutung des Auskunftsanspruchs hat sich aufgrund der rasanten technologischen Entwicklungen und der Veränderungen der praktischen und rechtlichen Bedeutung des Datengebrauchs in der Informationsgesellschaft noch weiter gesteigert. Eine am Wortlaut orientierte Auslegung des § 7 Satz 1 BNDG ist hiermit nicht vereinbar. Im Übrigen wirkt die restriktive Auffassung des Bundeskanzleramtes und des BND eher kontraproduktiv. Denn wird die Auskunft durch den BND gemäß § 15 Abs. 4 BVerfSchG verweigert, kann sich der Betroffene zwecks Überprüfung an mich wenden, worauf der gesamte Vorgang einschließlich der personenbezogenen Daten in Akten von mir geprüft wird. Dasselbe gilt, falls ein Bürger von seinem Petitionsrecht nach § 21 Bundesdatenschutzgesetz (BDSG) Gebrauch macht.

Meinem Petitum, § 7 Satz 1 BNDG verfassungskonform dahingehend auszulegen, dass der BND – ebenso wie das BfV und der MAD – grundsätzlich auch zur Auskunftserteilung aus Akten verpflichtet ist, sind das Bundeskanzleramt und der BND bisher nicht gefolgt. Im Rahmen der vom Bundeskanzleramt für Anfang des Jahres 2007 angekündigten Beratungen zur Novellierung des BNDG werde ich darauf drängen, dass dieser datenschutzrechtliche Mangel durch eine entsprechende Klarstellung des Gesetzes schnellstmöglich behoben wird.

## 5.8 Sicherheitsüberprüfungen

### 5.8.1 Luftsicherheitsgesetz und Verordnung datenschutzrechtlich unzureichend

*Die Regelungen über die Erhebung und Verarbeitung personenbezogener Daten bei der Luftsicherheits-Zuverlässigkeitsüberprüfung sind unzureichend.*

Im 20. TB (Nr. 5.8.1) hatte ich zu dem im Januar 2005 in Kraft getretenen Luftsicherheitsgesetz kritisch angemerkt, dass die Bestimmungen über die Zuverlässigkeitsüberprüfungen auf dem Gebiet des Luftverkehrs (§ 7 des Gesetzes) datenschutzrechtlich problematisch sind, in vielen Punkten von den insoweit vergleichbaren Regelungen im Sicherheitsüberprüfungsgesetz (SÜG) abweichen und eine erheblich höhere Eingriffsintensität aufweisen. Entgegen meinen Erwartungen ist die Bundesregierung in der gem. § 17 des Gesetzes zu erlassenden Rechtsverordnung auf meine Einwände nicht eingegangen.

Der Verordnungsentwurf lässt vielmehr wesentliche Regelungen zur Verarbeitung personenbezogener Daten vermissen, die im SÜG, an das das LuftSiG inhaltlich anknüpft, vom Gesetzgeber selbst getroffen wurden. In einigen Punkten enthält der Verordnungsentwurf datenschutzrechtlich unzureichende und unverhältnismäßige Bestimmungen. Es ist nicht überzeugend, warum bei der Zuverlässigkeitsüberprüfung nach dem LuftSiG zum Teil wesentlich andere Maßstäbe angelegt werden als in § 1 Abs. 4 SÜG beim insoweit vergleichbaren vorbeugenden personellen Sabotageschutz.

Im Wesentlichen betrifft meine Kritik folgende Punkte:

- Abfrage der Wohnsitze der letzten zehn Jahre im LuftSiG statt der letzten fünf Jahre im SÜG.
- Wiederholungsüberprüfung nach jeweils fünf Jahren. Dies ist im Vergleich zum SÜG nach wie vor unbefriedigend. Während nach dem SÜG nach jeweils fünf Jahren die Sicherheitserklärung vom Betroffenen aktualisiert wird, sieht § 3 Abs. 5 des Verordnungsentwurfs eine vollständige Wiederholung der Zuverlässigkeitsüberprüfung vor. Dies ist unverhältnismäßig.
- Unklare und unzureichende Regelungen zur Speicherbefugnis und zur Löschungsverpflichtung. Die Regelungen in § 7 Abs. 7 und 9 des Gesetzes zum Speichern personenbezogener Daten sind unzureichend, da nicht klar festgelegt wird, wer welche Daten in welchem Umfang speichern darf. Die Verordnung hätte hier Klarheit schaffen können, lässt jedoch Bestimmungen zur Speicherbefugnis und zum Speicherumfang ganz vermissen.

Der Bundesrat hat der Verordnung mit einigen Maßgaben im September 2006 zugestimmt. Im Zusammenhang mit der Umsetzung dieses Beschlusses (vgl. Bundesratsdrucksache 520/06) hat die Bundesregierung eine weitere – vom Bundesrat nicht geforderte – bedenkliche Ergänzung des Verordnungsentwurfs vorgenommen. Hiernach sollen auch die für die Aufhebung der Fluglizenzen für Luftfahrer zuständigen Behörden von der Rücknahme oder dem Widerruf der Feststellung der Zuverlässigkeit unterrichtet werden. Eine solche Unterrichtung widerspricht dem Zweckbindungsgrundsatz und der Übermittlungsregelung in § 7 Abs. 7 des Gesetzes, die eine Übermittlung an die gen. Behörden nicht vorsieht. Sofern die Notwendigkeit besteht, das Ergebnis der Zuverlässigkeitsüberprüfung auch diesen Behörden mitzuteilen, müsste dies durch den Gesetzgeber selbst geregelt werden. Die von der Bundesregierung beabsichtigte Ergänzung der Verordnung übersteigt somit den Ermächtigungsrahmen des § 17 LuftSiG.

Das BMI hatte bereits im Juni 2005 angekündigt, das Gesetz in absehbarer Zeit zu novellieren, ein Gesetzentwurf liegt mir bislang aber noch nicht vor. Ich erwarte, dass die Bundesregierung mit der Novelle die datenschutzrechtlichen Mängel beseitigt, Kriterien für die Zuverlässigkeit bzw. Unzuverlässigkeit festlegt und klare Regelungen für das Auskunftsrecht der Betroffenen trifft.

### 5.8.2 Personeller Sabotageschutz – Uferlos?

*Mit den Änderungen der Sicherheitsüberprüfungsfeststellungsverordnung wird der Kreis der im Rahmen des personellen Sabotageschutzes zu überprüfenden Personen über Maß ausgeweitet.*

Bis Anfang des Jahres 2002 galt das Sicherheitsüberprüfungsgesetz (SÜG) nur für den personellen Geheimschutz, also für Personen, die Zugang zu im öffentlichen Interesse geheimhaltungsbedürftigen Informationen erhalten sollen oder sich verschaffen können (so genannte sicherheitsempfindliche Tätigkeit). Dies hat sich nach dem 11. September 2001 wesentlich geändert. Mit dem Terrorismusbekämpfungsgesetz – TBG – vom 9. Januar 2002 (vgl. 19. TB Nr. 2) wurde der so genannte vorbeugende personelle Sabotageschutz (vpS) in das SÜG eingeführt. Nach § 1 Abs. 4 SÜG übt nunmehr auch derjenige eine sicherheitsempfindliche Tätigkeit aus, der an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung beschäftigt ist. Lebenswichtig sind nach Absatz 5 der Regelung solche Einrichtungen,

- deren Beeinträchtigung auf Grund der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann

oder

- die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit und Ordnung entstehen lassen würde.

Die Betroffenen haben sich einer einfachen Sicherheitsüberprüfung (Ü1) nach § 8 SÜG zu unterziehen.

Begründet wurde diese Gesetzeserweiterung mit dem Schutz vor terroristischen Anschlägen durch so genannte Innentäter. In der nach § 34 SÜG von der Bundesregierung erlassenen „Verordnung zur Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des

Bundes und zur Feststellung der öffentlichen Stellen des Bundes und der nicht-öffentlichen Stellen mit lebens- oder verteidigungswichtigen Einrichtungen (Sicherheitsüberprüfungsfeststellungsverordnung – SÜFV)“ vom 30. Juli 2003 (BGBl. I S. 1553) wurden die lebens- oder verteidigungswichtigen Einrichtungen abschließend festgelegt.

Mit der „Ersten Verordnung zur Änderung der Sicherheitsüberprüfungsfeststellungsverordnung“ vom 17. Oktober 2005 (BGBl. I S. 2984) und der im Entwurf befindlichen Zweiten Änderungsverordnung wird der Kreis der lebenswichtigen Einrichtungen erheblich erweitert. Bereits in meiner Stellungnahme zum Evaluierungsbericht der Bundesregierung zum TBG hatte ich darauf hingewiesen, dass das Ziel des TBG und des sich darauf gründenden vpS die Bekämpfung des internationalen Terrorismus sei; so hatte ich erhebliche Zweifel geäußert, ob nach den bisher gewonnenen Erfahrungen die Festlegung der lebenswichtigen Einrichtungen – insbesondere nach deren Erweiterung auf Grund der Verordnung vom 17. Oktober 2005 und den weiter beabsichtigten Änderungen – mit der Zielrichtung des TBG im Einklang stehen, und eine Überprüfung der SÜFV angeregt. Dieser Anregung ist die Bundesregierung jedoch nicht gefolgt, sondern hat stattdessen die Bereiche der lebenswichtigen Einrichtungen stark ausgeweitet. So werden zum Beispiel die Einrichtungen in den obersten Bundesbehörden und deren Geschäftsbereichen, die den Betrieb der Informations- und Kommunikationstechnik sicherstellen und deren Ausfall die Tätigkeit der genannten Behörden unmittelbar erheblich beeinträchtigen würden, als lebenswichtige Einrichtungen festgelegt. Nach der Verordnungsbegründung hängt die Funktionsfähigkeit der genannten Bereiche entscheidend von einer uneingeschränkten Informationstechnik ab. Aus dem Merkmal „Funktionsfähigkeit“ lässt sich weder zwingend auf die in § 1 Abs. 5 SÜG geforderten Merkmale einer „ihnen anhaftenden betrieblichen Eigengefahr“ oder einer „erheblichen Unruhe in großen Teilen der Bevölkerung“ schließen noch auf eine terroristische Bedrohung oder einen terroristischen Hintergrund. Erhebliche Unruhe in weiten Teilen der Bevölkerung kann in vielen Bereichen der öffentlichen Verwaltung durch den Ausfall und/oder die Störung von Arbeitsbereichen ausgehen, ohne dass dies zwangsläufig auf einen terroristischen Hintergrund zurückzuführen ist. Gleiches gilt auch für Arbeitseinheiten der Informationsverarbeitung und der Informationstechnik im Geschäftsbereich des BMAS, die die Gewährung von unterhaltssichernden Leistungen durch die Bundesagentur für Arbeit sicherstellen. Andere Beispiele ließen sich hier anfügen. Nota bene: Nicht jeder Stromausfall ist auf einen terroristischen Hintergrund zurückzuführen.

Insgesamt gesehen wurde mit der erheblichen Ausweitung des Begriffs „lebenswichtige Einrichtung“ die zur Begründung herangezogene Zielrichtung – nämlich die Bekämpfung des internationalen Terrorismus – weit überschritten. Der Kreis der zu überprüfenden Personen wird durch die vorgenommenen und beabsichtigten Änderungen in unangemessener und unverhältnismäßiger Weise ausgedehnt. Ich werde deshalb die Anwendung der Regelungen im Hinblick auf das Verhältnismäßigkeitsprinzip sorgfältig verfolgen und erwarte von der Bundesregierung, dass sie die Bestimmungen hinsichtlich ihrer Zweckbestimmung und Angemessenheit ebenfalls einer kritischen Überprüfung unterziehen wird.

### 5.8.3 Kontrolle der Sicherheitsüberprüfungen

*Die Ergebnisse der im Berichtszeitraum durchgeführten Kontrollen zu Sicherheitsüberprüfungen im öffentlichen und im nicht-öffentlichen Bereich gaben Anlass zur grundsätzlichen Erörterung von Handlungs- und Verfahrensabläufen.*

#### 5.8.3.1 Bundespolizei

Der erste Kontrollbesuch galt einem Bundespolizeipräsidium. Dort wurden personenbezogene Daten im Rahmen des SÜG-Verfahrens auf einem nicht vernetzten Personalcomputer (PC) mittels der Datei IBVS verarbeitet. Eine stichprobenartige Kontrolle dieser Datei zeigte keine Mängel. Auf dem PC befand sich aber auch ein Ordner mit Dokumenten über durchgeführte Anhörungen. Die Speicherung von Anhörungsvermerken in diesem Ordner ist mit § 20 Abs. 1 SÜG nicht vereinbar, da der nach dieser Vorschrift nur beschränkt zulässige Umfang der automatisiert speicherfähigen personenbezogenen Daten überschritten wird. Nach entsprechendem Hinweis erfolgte die Löschung dieses Ordners.

Eine solche Verarbeitung halte ich zwar für zulässig, die elektronisch gespeicherten Unterlagen sind jedoch unmittelbar nach Abschluss des jeweiligen Vorgangs mit Aufnahme in die Sicherheitsakte auf dem PC zu löschen, um der besonderen Sensibilität dieser Daten Rechnung zu tragen.

Das System IBVS ermöglicht die Erstellung von Löschungsprotokollen unter Angabe des Namens, Vornamens, Löschungsdatums und Löschungsgrundes. Diese Protokolle können zeitlich unbeschränkt rückwirkend erstellt werden. Die Erstellung derartiger Übersichten ist mit der Regelung des § 22 Abs. 2 SÜG, wonach eine endgültige, vollständige und technisch sichere Löschung erfolgen muss, nicht zu vereinbaren. Wie mir das Bundespolizeipräsidium hierzu mitteilte, wird nunmehr nach Eingriff in das Programm das Protokoll soweit gelöscht, dass lediglich das letzte Jahr gespeichert bleibt. Da nach Aussage des Präsidiums eine andere Lösung technisch nicht möglich ist, habe ich mich mit dieser Regelung einverstanden erklärt.

Wie sich aus mehreren der überprüften Sicherheitsakten ergab, wurden Personalmitteilungen, Veränderungsanzeigen und dergleichen in Form von Sammelverfügungen durch die Personal verwaltende Stelle sowohl dem Geheimschutzbeauftragten als auch anderen Funktionsträgern (u. a. Personalrat, Gleichstellungsbeauftragte, Vertrauensperson der Schwerbehinderten) zur Kenntnis gebracht. Entsprechend dem Grundsatz, dass jede Übermittlung personenbezogener Daten unter Beachtung strikter Zweckbindung erfolgt, dürfen personenbezogene Daten in jedem Einzelfall nur der Stelle übermittelt werden,

die diese Daten zur Aufgabenerfüllung benötigt. Für die Sicherheitsüberprüfungen bedeutet dies, dass dem Geheimschutzbeauftragten nur Daten zu den von ihm betreuten sicherheitsüberprüften Mitarbeitern mitgeteilt werden dürfen. Im kontrollierten Präsidium war es jedoch gängige Praxis, Sammelverfügungen an alle Bereiche – unabhängig von deren konkreter Betroffenheit – zu übersenden. Ich habe daher das Präsidium gebeten, diese Praxis zu beenden und gemeinsam mit der Personal verwaltenden Stelle ein datenschutzgerechtes Verfahren zu entwickeln. Diese Bitte hat auch das BMI aufgegriffen und auf eine datenschutzgerechte Verfahrensweise bei allen Personalstellen im gesamten Bereich der Bundespolizei hingewirkt. Ob dies in der Praxis umgesetzt worden ist, werde ich bei nächster Gelegenheit in einem weiteren Präsidium kontrollieren.

Zwei Polizei-Bedienstete wurden von dem Geheimschutzbeauftragten vorläufig von der sicherheitsempfindlichen Tätigkeit entbunden, weil ihm von der Personalverwaltung sicherheitserhebliche Erkenntnisse mitgeteilt worden waren. Diese Maßnahme war ohne vorherige Anhörung nach § 6 Abs. 3 SÜG erfolgt. Darüber haben sich die Betroffenen in einer Eingabe bei mir beschwert. Der Geheimschutzbeauftragte hatte hierzu die Auffassung vertreten, eine Anhörung sei erst bei einer endgültigen Entscheidung nach § 14 Abs. 3 SÜG durchzuführen. Wegen der unmittelbaren und gravierenden Auswirkung, die auch eine vorläufige Ablösung aus einer sicherheitsempfindlichen Tätigkeit für den Betroffenen hat, halte ich eine Anhörung nach § 6 Abs. 3 SÜG auch in diesen Fällen für geboten. Der Geheimschutzbeauftragte revidierte nach eingehender Erörterung bei dem Kontrollbesuch seine Auffassung und wird künftig auch bei vorläufig veranlasster Ablösung aus einer sicherheitsempfindlichen Tätigkeit eine Anhörung entsprechend § 6 Abs. 3 SÜG durchführen.

#### 5.8.3.2 Nicht-öffentlicher Bereich

Bei der Prüfung von Unternehmen ist mir aufgefallen, dass in vielen Fällen Anträge an das BMWi als zuständige Stelle auf Durchführung einer Sicherheitsüberprüfung unpräzise und unzureichend begründet waren. Es fanden sich beispielsweise Begründungen wie „Mitarbeit bei VS-Projekten“, „Service in der Telekommunikation“, „Kontakte zur Bundesregierung“ oder „kann sich auf Dauer Zugang zu VS bis zur Stufe Geheim verschaffen“. Anhand solcher pauschaler Begründungen kann die zuständige Stelle der ihr obliegenden Pflicht nicht nachkommen, die Notwendigkeit einer Sicherheitsüberprüfung der beantragten Stufe zu prüfen. Diese Anträge hätten zur Ergänzung der Begründung an das Unternehmen zurückgegeben werden müssen und nicht – wie geschehen – zur Durchführung der Sicherheitsüberprüfung an die mitwirkende Behörde weitergeleitet werden dürfen. Das zuständige BMWi hat zugesagt, künftig für eindeutig und nachvollziehbar begründete Anträge zu sorgen.

In einem besonders gravierenden Fall, in dem die Notwendigkeit der Sicherheitsüberprüfung mit „Kontakten zur Bundesregierung“ begründet worden war, wurde die Ermächtigung der betroffenen Person zwischenzeitlich zurückgezogen. Die Sicherheitsüberprüfung dieser Person war von Anfang an unzulässig und die diesbezüglichen personenbezogenen Daten wurden zu Unrecht erhoben und verarbeitet. Ich habe daher die unverzügliche Löschung aller Daten und die Vernichtung der Akten bei allen beteiligten Stellen (Unternehmen, zuständige Stelle und mitwirkende Behörde) verlangt. Das BMWi ist meiner Aufforderung nachgekommen und hat die beteiligten Stellen aufgefordert, die Daten zu löschen und die Akten zu vernichten.

Bei den Kontrollen im Berichtszeitraum habe ich wiederum festgestellt, dass in zahlreichen Fällen beim Ausscheiden eines Mitarbeiters aus der sicherheitsempfindlichen Tätigkeit das Datum des Ausscheidens nicht eindeutig festgestellt wurde und in der Akte auch nicht dokumentiert war. In einigen Fällen war das Ausscheiden aus der sicherheitsempfindlichen Tätigkeit erst dadurch aufgefallen, dass die Betroffenen im Rahmen der Aktualisierung erklärten, schon seit längerer Zeit nicht mehr mit einer solchen Tätigkeit betraut gewesen zu sein. Das Ausscheiden setzt Löschungs- und Vernichtungsfristen in Gang. Aus diesem Grunde muss dieses Datum festgestellt und in der Akte festgehalten werden. In vielen Fällen wird es in Folge der verspäteten Abmeldung zu Terminüberschreitungen bei der Löschung von Daten und der Vernichtung von Akten kommen. Von besonderer Bedeutung ist in diesem Zusammenhang eine gut funktionierende Kommunikation zwischen dem Sicherheitsbevollmächtigen (Sibe) und der Personal verwaltenden Stelle. Die AVV des BMI zu § 18 Abs. 2 SÜG verpflichtet die Personalverwaltung, Informationen über persönliche, dienstliche und arbeitsrechtliche Verhältnisse dem Geheimschutzbeauftragten – bei der nicht-öffentlichen Stelle dem Sibe – mitzuteilen. Dieser Verpflichtung kommen die Personalverwaltungen nach meiner Erkenntnis aber überwiegend nicht oder nur unzureichend nach. Viele Fälle verspäteter Abmeldung ließen sich durch regelmäßige Veränderungsmitteilungen der Personalverwaltung an den Sibe vermeiden. Ich habe daher beim BMWi wiederholt angeregt, im Geheimschutzhandbuch verbindliche Handlungsanweisungen zu diesem Problem festzulegen. Das BMWi hat dies inzwischen zugesagt.

In einem anderen Unternehmen entsprach der Zugriff auf das konzerninterne Personalverwaltungssystem nicht den datenschutzrechtlichen Anforderungen. Die Zugriffsregelung erlaubte dem Sibe den Zugriff auch auf Datenfelder, die für seine Aufgabenerfüllung nicht relevant sind. Zudem hatte der Sibe Zugriff auf Daten von Mitarbeitern, die der Geheimschutzbetreuung nicht unterliegen. Deswegen sind Veränderungen der Zugriffsregelung für den Sibe unerlässlich. Hierbei sollte geprüft werden, ob das System auch dazu genutzt werden kann, die notwendige Kommunikation zwischen Sibe und Personalverwaltung – wie vorstehend beschrieben – durch einen automatisierten Abgleich zu verbessern.

Einigen kontrollierten Akten habe ich entnommen, dass dem Sibe vollständige Personalakten zur Einsichtnahme

überlassen wurden. Hierdurch erhalten der Sibe und seine Mitarbeiter auch von Inhalten Kenntnis (z. B. Leistungsbeurteilungen), die für ihre Aufgabenerfüllung nicht erforderlich sind. Nach § 13 Abs. 6 i. V. m. § 26 SÜG ist der Sibe befugt, die Personalakten – soweit dies im Einzelfall erforderlich ist – nur zum Zwecke der Prüfung der Angaben in der Sicherheitserklärung auf Vollständigkeit und Richtigkeit einzusehen. Die Einsichtnahme in die Personalakte muss sich daher auf den Abgleich der in der Sicherheitserklärung enthaltenen Angaben mit den Angaben in der Personalakte beschränken. Diese vom Gesetzgeber intendierte Beschränkung schließt eine umfassende Einsichtnahme in die vollständige Personalakte aus.

Eine Stellungnahme des BMWi hierzu lag mir bei Redaktionsschluss noch nicht vor.

### 5.8.4 Sicherheitsüberprüfung bei diplomatischen Vertretungen der USA

*Die Mitwirkung des Bundesamtes für Verfassungsschutz (BfV) an Sicherheitsüberprüfungen der Vertretungen der USA in Deutschland ist Gegenstand meiner Prüfung. Die hierfür notwendigen Informationen hat mir das Bundesministerium des Innern (BMI) bisher trotz wiederholter Aufforderung nicht im erforderlichen Umfang zur Verfügung gestellt. Damit kommt es seiner mir gegenüber bestehenden Mitwirkungspflicht nicht nach.*

Im Nachgang zu den im 20. Tätigkeitsbericht (Nr. 5.8.4) dargestellten Sicherheitsüberprüfungen durch US-amerikanische und britische Streitkräfte in der Bundesrepublik Deutschland habe ich in der Berichtsperiode aufgrund von Eingaben die Mitwirkung des BfV an Sicherheitsüberprüfungen der diplomatischen Vertretungen der USA in Deutschland überprüft.

Ebenso wie die US-Streitkräfte unterziehen auch die US-Vertretungen ihre deutschen und nicht amerikanischen Mitarbeiter sowie externe Personen, die Zugang zu den Vertretungen begehren, z. B. Mitarbeiter von Versorgungsunternehmen, einer Sicherheitsüberprüfung. An dieser Überprüfung wirkt auch das BfV gemäß § 33 des Sicherheitsüberprüfungsgesetzes (SÜG) mit. Nach Abs. 2 Satz 1 dieser Norm muss eine Mitwirkung des BfV unterbleiben, wenn überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

Um beurteilen zu können, ob die Mitwirkung des BfV an den Sicherheitsüberprüfungen der US-Vertretungen datenschutzrechtlich zulässig ist, habe ich das BMI als zuständige Fachaufsichtsbehörde um detaillierte Informationen zu Art und Umfang der vom BfV übermittelten Daten sowie zur Verwendung dieser Daten durch die US-Vertretungen gebeten. Da die Vereinigten Staaten von Amerika über ein Datenschutzniveau verfügen, das kaum den europäischen Maßstäben entspricht (vgl. 19. TB Nr. 16.1), ist insbesondere die Frage des Verbleibs der Daten und deren weitere Verwendung, z. B. durch US-Sicherheitsbehörden, zur Beurteilung der Frage von maßgeblicher Bedeutung, ob überwiegende schutzwürdige Interessen der Betroffenen einer Mitwirkung des BfV entgegenstehen.

Das BMI hat meine Prüfkompetenz im Hinblick auf die Datenverwendung durch die US-Sicherheitsbehörden verneint und eine Offenlegung der von mir insoweit erbetenen Informationen als nicht sachgerecht abgelehnt. Dies ist um so erstaunlicher, als mir vom BMI und den verantwortlichen US-Stellen im Rahmen der Prüfung der Mitwirkung des BfV an den Sicherheitsüberprüfungen der US-Streitkräfte sämtliche von mir benötigten Informationen vertrauensvoll zur Verfügung gestellt worden sind. Auf dieser Grundlage konnte unter Federführung des BMI und in enger Kooperation mit den verantwortlichen US-Stellen im Interesse der Betroffenen eine auch datenschutzrechtlich tragfähige Lösung erarbeitet und in die Praxis umgesetzt werden (vgl. 20. TB Nr. 5.8.4).

Ich habe das BMI hieran erinnert und auf seine gemäß § 24 Abs. 4 BDSG bestehende Mitwirkungspflicht hingewiesen. Zugleich habe ich deutlich gemacht, dass eine Nichterfüllung dieser Verpflichtung eine Beanstandung zur Folge haben kann.

## 6 Rechtswesen

### 6.1 Telekommunikationsüberwachung nach §§ 100a ff. StPO

*Die dringend notwendige Reform der Regelungen zur strafprozessualen Telekommunikationsüberwachung kommt endlich in Gang. Regelungsbedarf besteht außerdem im Bereich der sog. Funkzellenabfrage.*

Die Regelungen der §§ 100a ff. StPO zur Telekommunikationsüberwachung sind nach wie vor dringend reformbedürftig. Bereits in meinem 20. TB (Nr. 7.2.1) hatte ich gesetzgeberisches Handeln angemahnt, nachdem durch das Urteil des BVerfG vom 3. März 2004 zur akustischen Wohnraumüberwachung („Großer Lauschangriff“) sowie wissenschaftliche Studien erhebliche Defizite der bestehenden Vorschriften deutlich geworden waren. Inzwischen hat das BVerfG erneut eindeutige Vorgaben zum Grundrechtsschutz überwachter Personen formuliert (Urteil vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung, vgl. Nr. 5.4.1). Gleichzeitig ist die Anzahl der Telefonüberwachungen nach §§ 100a, 100b StPO weiterhin bedenklich angestiegen (29 017 Anordnungen im Jahr 2004, 35 015 im Jahr 2005, gegenüber 24 441 im Jahr 2003).

Die Datenschutzbeauftragten des Bundes und der Länder haben in einem gemeinsamen Papier die datenschutzrechtlichen Forderungen für die Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen formuliert (Kasten a zu Nr. 6.1) und diese an die Bundesministerin der Justiz herangetragen. Im November 2006 hat das BMJ endlich einen Referentenentwurf für ein Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen (sowie zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung, s. u. Nr. 10.1) vorgelegt. Der Entwurf geht grundsätzlich in die richtige Richtung, indem er die rechtsstaatlichen und grundrechtlichen

Kasten a zu Nr. 6.1

**Gemeinsames Papier der Datenschutzbeauftragten des Bundes und der Länder**

**Datenschutzrechtliche Forderungen für die Neuregelung verdeckter Ermittlungsmaßnahmen (§§ 100a ff. StPO)**

In der Koalitionsvereinbarung der Regierungsparteien vom 11. November 2005 ist festgelegt: „Wir werden die Regelungen zur Telekommunikationsüberwachung in der Strafprozessordnung im Sinne einer harmonischen Gesamtregelung der strafprozessualen heimlichen Ermittlungsmaßnahmen überarbeiten." In diesem Zusammenhang sollten insbesondere folgende datenschutzrechtliche Forderungen Beachtung finden:

1. Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100a StPO sollte im Hinblick auf Art und Schwere der Straftaten einer Überprüfung unterzogen werden. Ziel sollte dabei sein, die Telekommunikationsüberwachung auf schwere Straftaten zu begrenzen und die tatsächliche Relevanz der aufgeführten Tatbestände für die Praxis zu berücksichtigen.

   Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu gewährleisten, muss in der StPO eine Pflicht zur Erstellung aussagekräftiger Berichte geschaffen werden. Daneben muss auch die in § 110 Abs. 8 TKG geregelte statistische Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

2. Der gesetzliche Richtervorbehalt darf nicht gelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

3. Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100b StPO dahingehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnungen nach § 100a StPO einzelfallbezogen darzulegen sind.

4. Der durch die Menschenwürde garantierte Kernbereich privater Lebensgestaltung ist zu gewährleisten. Datenerhebungen in diesem Bereich sind deshalb grundsätzlich unzulässig. Werden im konkreten Fall Inhalte erfasst, die den Kernbereich der privaten Lebensgestaltung betreffen, müssen ein absolutes Beweisverwertungsverbot, ein Speicherungsverbot und ein Löschungsgebot gesetzlich normiert werden.

5. Zum Schutz von Vertrauensverhältnissen sollte eine Regelung geschaffen werden, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen, also mit Angehörigen (§ 52 StPO), Berufsgeheimnisträgern (§ 53 StPO) und Berufshelfern (§ 53a StPO), grundsätzlich nicht verwertet werden dürfen.

6. Die Verwendung der durch die Maßnahmen erlangten personenbezogenen Informationen ist einer strikten Zweckbindung, insbesondere im Hinblick auf die Einhaltung der jeweiligen Anforderungen für ihre Erhebung, zu unterwerfen. Dies bedeutet für die Verkehrsdaten, die aufgrund der Umsetzung der EG-Richtlinie zur Vorratsdatenspeicherung von den Telekommunikationsunternehmen zu Strafverfolgungszwecken bereit gehalten werden, dass sie nur zum Zwecke der Verfolgung schwerer Straftaten – insbesondere, wie in den Erwägungsgründen der Richtlinie genannt, in Fällen organisierter Kriminalität und Terrorismus – verwendet werden dürfen. § 100g StPO bedarf einer entsprechenden Überarbeitung.

7. Zur Sicherung der Zweckbindung muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

8. Der Umfang der Benachrichtigungspflichten ist im Gesetz näher zu definieren. Die Benachrichtigungsfrist und die richterliche Überprüfung ihrer Einhaltung bzw. ihres Aufschubs sollten geregelt werden.

9. Die vorstehenden Forderungen nach

   – Überprüfung der materiellen Voraussetzungen für die Maßnahme im Einzelfall,

   – strikter Zweckbindung der erhobenen Daten,

   – Kernbereichsschutz,

   – verstärktem Schutz von Vertrauensverhältnissen,

   – Regelung von Benachrichtigungspflichten und Löschungsfristen

gelten grundsätzlich für alle verdeckten Datenerhebungsmaßnahmen der Strafverfolgungsbehörden.

Sicherungen bei strafprozessualen Überwachungsmaßnahmen stärkt. Positiv bewerte ich auch das Konzept, einheitliche Regelungen für sämtliche heimliche Ermittlungsmaßnahmen zu schaffen. Ich habe das BMJ darauf aufmerksam gemacht, dass ich insbesondere in den folgenden Punkten eine Nachbesserung des Entwurfs für erforderlich halte:

- Der umfangreiche Katalog der Straftaten, zu deren Verfolgung eine Telekommunikationsüberwachung angeordnet werden darf, sollte im Hinblick auf den Schutz des Telekommunikationsgeheimnisses kritisch überprüft und reduziert werden.
- Um die Anordnungspraxis bei der Telekommunikationsüberwachung zu verbessern, sollten qualifizierte Begründungspflichten in das Gesetz aufgenommen werden. Es muss sichergestellt werden, dass der Antrag der Staatsanwaltschaft und die Anordnung durch das Gericht konkret und einzelfallbezogen begründet werden.
- Die vorgesehenen Regelungen zum Schutz des sog. Kernbereichs privater Lebensgestaltung halte ich zum Teil für zu eng. Das vorgesehene Erhebungsverbot in Fällen, in denen ausschließlich kernbereichsrelevante Inhalte zu erwarten sind, reicht nicht aus. Auf eine Telekommunikationsüberwachung sollte bereits dann verzichtet werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Maßnahme Äußerungen aus diesem privaten Bereich erfasst.
- Beim Schutz von Vertrauensverhältnissen differenziert der Entwurf zwischen Seelsorgern, Verteidigern und Abgeordneten einerseits sowie sonstigen Berufsgeheimnisträgern andererseits. Ich halte demgegenüber ein einheitliches und hohes Schutzniveau für Gespräche mit allen Arten von Berufsgeheimnisträgern für erforderlich (vgl. schon 20. TB Nr. 7.4).
- Sämtliche vorgesehene Regelungen sollten befristet und einer unabhängigen, gründlichen und wissenschaftlich unterstützten Evaluation unterzogen werden. Nur so kann gewährleistet werden, dass nicht bzw. nicht mehr erforderlich Grundrechtseingriffe ggf. reduziert bzw. wieder zurückgenommen werden.

Regelungsbedarf sehe ich darüber hinaus im Bereich der sog. Funkzellenabfrage, d. h. dem Auskunftsverlangen der Ermittlungsbehörden gegenüber Telekommunikationsdiensteanbietern im Hinblick auf Verkehrsdaten, die in einer bestimmten Funkzelle, der kleinsten geografischen Einheit im Mobilfunknetz, anfallen. Diese Ermittlungsmaßnahme zur Identifizierung eines noch unbekannten Straftäters wird gegenwärtig auf § 100h Abs. 1 Satz 2 StPO gestützt. Diese außerhalb der eigentlichen Ermächtigungsgrundlage für Verkehrsdatenabfragen (§ 100g StPO) in der bloßen Verfahrensnorm des § 100h StPO untergebrachte Regelung halte ich jedoch im Hinblick auf die Eingriffsintensität der Funkzellenabfrage, insbesondere wegen der möglichen Vielzahl betroffener unbeteiligter Personen, nicht für eine ausreichende Rechtsgrundlage. Auch hierzu haben die Datenschutzbeauftragten des Bundes und der Länder ein gemeinsames Forderungspapier verfasst (Kasten b zu Nr. 6.1), welches ich der Bundesministerin der Justiz mit der Bitte übermittelt habe, die Möglichkeit einer gesetzlichen Neuregelung zu prüfen.

Kasten b zu Nr. 6.1

**Gemeinsames Papier der Datenschutzbeauftragten des Bundes und der Länder**

**Datenschutzrechtliche Forderungen für die Durchführung von Funkzellenabfragen**

1. Für eine Funkzellenabfrage mit dem Ziel eines anschließenden automatisierten Abgleichs der übermittelten Daten fehlt es in der Strafprozessordnung an einer Rechtsgrundlage. Sie ist daher unzulässig.
2. Auch ohne das Ziel des anschließenden Abgleichs ist § 100h Abs. 1 Satz 2 StPO als Verfahrensvorschrift zu § 100g StPO keine ausreichende Rechtsgrundlage für die inzwischen als polizeiliche Standardmaßnahme zur Verdachtsschöpfung praktizierte Funkzellenabfrage. Grundrechtseingriffe sind stets auf das erforderliche Maß zu reduzieren und bedürfen einer klaren und detaillierten Regelung (vgl. auch Beschluss des 1. Senats des BVerfG vom 4. April 2006 zur Rasterfahndung, Az.: 1 BvR 518/02, Absatz-Nr. 125 ff.). Daran fehlt es hier.
3. Eine gesetzliche Regelung, die Funkzellenabfragen zulässt, müsste folgende datenschutzrechtliche Forderungen berücksichtigen:
   - Funkzellenabfragen im Sinne des § 100h Abs. 1 Satz 2 StPO dürfen nur dann durchgeführt werden, wenn eine erhebliche Straftat begangen wurde und eine hinreichend sichere Tatsachenbasis vorliegt, dass der Täter telefoniert hat.
   - Im Rahmen einer Verhältnismäßigkeitsprüfung im Einzelfall sind die Schwere der Straftat und die Anzahl der durch die Maßnahme möglicherweise betroffenen unbeteiligten Dritten gegeneinander abzuwägen.
   - Die Maßnahme ist räumlich und zeitlich auf den unbedingt notwendigen Umfang zu begrenzen.
   - Die auf der Grundlage der Funkzellenabfrage erlangten Daten dürfen nicht zur Ermittlung von Tatzeugen verwendet werden.
   - Die Verbindungsdaten der Betroffenen müssen unverzüglich gelöscht werden, sobald ihre weitere Speicherung für das Ermittlungsverfahren nicht mehr erforderlich ist.
   - Funkzellenabfragen, insbesondere die Zahl der Maßnahmen, die Zahl der Betroffenen und die Bedeutung der Maßnahmen für die Ermittlungen sollten statistisch erfasst werden, um eine datenschutzrechtliche Überprüfung und Evaluation zu ermöglichen.

Im Berichtszeitraum hatte ich außerdem die Gelegenheit, zu drei Verfassungsbeschwerden aus dem Bereich der strafprozessualen Telekommunikationsüberwachung gegenüber dem BVerfG Stellung zu nehmen.

– Eine Verfassungsbeschwerde betraf die Beschlagnahme von Verkehrsdaten, die der Beschuldigte nach Abschluss des Übertragungsvorgangs auf seinem eigenen PC oder Handy gespeichert hat. Auch wenn das BVerfG den besonderen Schutz dieser Daten nicht auf das Fernmeldegeheimnis gestützt hat, so hat es durch sein Urteil vom 2. März 2006 (Az.: 2 BvR 2099/04) doch in erfreulicher Weise seine Rechtsprechung zur Stärkung der Persönlichkeitsrechte fortgesetzt, indem es im Hinblick auf den Eingriff in das Recht auf informationelle Selbstbestimmung gefordert hat, dass bei der Prüfung der Verhältnismäßigkeit des staatlichen Zugriffs die erhöhte Schutzwürdigkeit dieser Daten besonders zu berücksichtigen ist.

– Eine andere Verfassungsbeschwerde richtete sich gegen § 100i StPO (IMSI–Catcher). Das BVerfG hat diese durch Kammerbeschluss vom 22. August 2006 (Az.: 2 BvR 1345/03) bedauerlicherweise nicht zur Entscheidung angenommen, da es – entgegen der auch von mir geäußerten Ansicht – einen Eingriff in das Fernmeldegeheimnis verneint und den Eingriff in das Recht auf informationelle Selbstbestimmung als nicht unverhältnismäßig bewertet hat. Ich begrüße allerdings, dass der Beschluss den Gesetzgeber ausdrücklich dazu aufruft, bei der Neuregelung der heimlichen Ermittlungsmaßnahmen einen effektiven Grundrechtsschutz zu gewährleisten.

– Zur Verfassungsbeschwerde gegen die Beschlagnahme von E-Mails, die nach Abschluss des Kommunikationsvorgangs auf dem Server des Serviceproviders gespeichert sind, steht die Entscheidung des BVerfG noch aus. Ich erwarte diese mit großem Interesse. In meiner Stellungnahme habe ich dargelegt, dass solche E-Mails nach meiner Auffassung bis zur Kenntnisnahme durch den Empfänger dem Schutzbereich des Fernmeldegeheimnisses unterliegen und danach durch das Recht auf informationelle Selbstbestimmung geschützt sind.

## 6.2 Akustische Wohnraumüberwachung

*Die Neuordnung der Vorschriften der StPO zum „Großen Lauschangriff", die aufgrund des Urteils des BVerfG vom 3. März 2004 erforderlich geworden war, ist in Kraft getreten.*

Über das Urteil des BVerfG zum „Großen Lauschangriff" vom 3. März 2004, mit dem ein erheblicher Teil der Vorschriften der StPO zur akustischen Wohnraumüberwachung für verfassungswidrig erklärt worden war, sowie über den Gesetzentwurf zu deren Neuregelung habe ich bereits in meinem 20. TB (Nr. 7.1.1 und Nr. 7.1.2) berichtet. Nach weiteren parlamentarischen Beratungen und Durchführung eines Vermittlungsverfahrens ist das „Gesetz zur Umsetzung des Urteils des Bundesverfassungsgerichts vom 3. März 2004 (akustische Wohnraumüberwachung)" nunmehr mit einigen Änderungen am 1. Juli 2005 in Kraft getreten (Gesetz vom 24. Juni 2005, BGBl. I S. 1841).

Die Änderungen gegenüber dem Regierungsentwurf sind aus datenschutzrechtlicher Sicht bedauerlich. So wurde der nach den Vorgaben des BVerfG im Hinblick auf die erforderliche Deliktsschwere reduzierte Katalog der Straftaten, zu deren Aufklärung eine akustische Wohnraumüberwachung angeordnet werden darf, wieder um einige Straftatbestände erweitert, z. B. die gewerbs- oder bandenmäßige Fälschung von Zahlungskarten, Schecks und Wechseln (§ 100c Abs. 2 StPO). Zudem dürfen personenbezogene Informationen, die aus einer akustischen Wohnraumüberwachung erlangt wurden, nunmehr zur Abwehr bestimmter Gefahren verwendet werden, selbst wenn sie fehlerhaft erhoben wurden und daher einem Verwertungsverbot unterliegen (§ 100d Abs. 6 Nr. 2 Satz 1 StPO). Mein Einwand, dass mit Blick auf die Rechte des Betroffenen eine solche Weiterverwendung allenfalls zur Verhinderung schwerster Straftaten, nicht aber schon zum Schutz von „bedeutenden Vermögenswerten" in Betracht kommen kann, wurde leider nicht berücksichtigt. Positiv bewerte ich jedoch, dass den insbesondere vom Bundesrat geforderten Ausweitungen dieses tief in die Privatsphäre eingreifenden Ermittlungsinstruments im Gesetzgebungsverfahren nicht entsprochen wurde. Insgesamt halte ich die Neuregelung jedoch für akzeptabel, die in weiten Teilen als Vorlage für die Überarbeitung der Vorschriften zu den sonstigen heimlichen Ermittlungsmaßnahmen (Nr. 5.4.1), insbesondere der strafprozessualen Telekommunikationsüberwachung (Nr. 6.1), dienen sollte.

Die Bundesregierung hat inzwischen einen neuen Bericht über akustische Wohnraumüberwachungen für das Jahr 2005 vorgelegt (Bundestagsdrucksache 16/3068). Dieser wurde erstmals auf der Grundlage der im Zuge der Neuregelung konkretisierten Berichtspflicht (§ 100e StPO) und des neuen Anlasstatenkatalogs erstellt. Im Jahr 2005 wurden demnach insgesamt sieben Maßnahmen der akustischen Wohnraumüberwachung angeordnet, von denen sechs durchgeführt wurden. Damit hat sich die Anzahl der akustischen Wohnraumüberwachungen gegenüber dem Jahr 2004 fast halbiert. Gegenüber 2003 beträgt der Rückgang sogar über 80 Prozent. Bei der Verteilung der Anlasstaten setzt sich der Trend fort, dass bestimmte, nach wie vor im Katalog enthaltene Delikte (wie z. B. Geld- oder Wertpapierfälschung, gewerbsmäßige Hehlerei/Bandenhehlerei, Straftaten nach dem Kriegswaffenkontrollgesetz) für die akustische Wohnraumüberwachung in der Praxis keine Rolle spielen. Bereits in meinem 19. TB (Nr. 8.4) und erst recht nach den entsprechenden Ergebnissen des Gutachtens des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung (großer Lauschangriff) nach § 100c Abs. 1 Nr. 3 StPO" (vgl. 20. TB Nr. 7.1.4) hatte ich darauf hingewiesen, dass ich die Aufnahme dieser Delikte in den Anlasstatenkatalog nicht für erforderlich halte. Ich bedauere daher, dass die Novellierung der Vorschriften zur akustischen Wohnraumüberwa-

chung trotz meines Drängens nicht dazu genutzt wurde, den Straftatenkatalog auch unter dem Aspekt des tatsächlichen Bedarfs zu überarbeiten. Eine entsprechende kritische Überprüfung werde ich auch weiterhin fordern.

### 6.3 Genomanalyse im Strafverfahren

*Das „Gesetz zur Novellierung der forensischen DNA-Analyse" vom 12. August 2005 hat die Schranken für Genomanalysen im Strafverfahren deutlich abgesenkt und eine Rechtsgrundlage für das DNA-Massenscreening geschaffen.*

Die Diskussionen um eine Ausweitung der Anwendungsmöglichkeiten der DNA-Analyse im Strafverfahren mit dem Ziel, den sog. „genetischen Fingerabdruck" in seinen Voraussetzungen mit dem herkömmlichen Fingerabdruck nach § 81b StPO gleichzusetzen (vgl. 20. TB Nr. 7.3.2), haben sich im Berichtszeitraum fortgesetzt. Anlässlich eines Gesetzesantrags mehrerer Bundesländer, der für die DNA-Analyse zur Identitätsfeststellung in künftigen Strafverfahren die Streichung des Richtervorbehalts sowie der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung und der Prognose weiterer erheblicher Straftaten vorsah (Bundesratsdrucksache 99/05), hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung vom 17. Februar 2005 die erheblichen verfassungsrechtlichen Bedenken gegen eine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck nochmals bekräftigt (s. Kasten zu Nr. 6.3).

In der Folgezeit brachten die Bundesregierung sowie die Koalitionsfraktionen der 15. Legislaturperiode ein „Gesetz zur Novellierung der forensischen DNA-Analyse" in

Kasten zu Nr. 6.3

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 17. Februar 2005 zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse**

**Keine Gleichsetzung der DNA-Analyse mit dem Fingerabdruck**

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial, z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse", weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den sog. nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungsbereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

den Deutschen Bundestag ein, das ohne Änderungen verabschiedet wurde und am 1. November 2005 in Kraft getreten ist (BGBl. I S. 2360). Die Neuregelung geht zwar nicht so weit, die DNA-Analyse mit den sonstigen erkennungsdienstlichen Maßnahmen nach § 81b StPO völlig gleichzusetzen, senkt die Schranken für DNA-Analysen in laufenden Ermittlungsverfahren (§§ 81e, 81f StPO) sowie zur Identitätsfeststellung in künftigen Strafverfahren (§ 81g StPO) aber doch deutlich ab. Im Gesetzgebungsverfahren habe ich mich sowohl gegenüber dem BMJ als auch gegenüber dem Rechtsausschuss des Deutschen Bundestages geäußert. Meinen Anregungen und Bedenken wurde jedoch nicht Rechnung getragen.

Einen wesentlichen Punkt der Neuregelung bildet die Lockerung des Richtervorbehalts. Die DNA-Analyse ist nunmehr auch auf Grundlage einer Einwilligung des Betroffenen möglich. Da Einwilligungen nur wirksam sind, wenn sie freiwillig erfolgen, habe ich erhebliche Zweifel, dass auf Einwilligungsbasis überhaupt in relevantem Umfang DNA-Analysen erfolgen können. Denn der Betroffene befindet sich im Strafverfahren regelmäßig in einer besonderen Drucksituation. Hinzu kommt bei einer Einwilligung in DNA-Analysen zur Identitätsfeststellung in künftigen Strafverfahren, dass der Betroffene sich gewissermaßen selbst die erforderliche Negativprognose im Hinblick auf die Begehung künftiger Straftaten stellen müsste, was ihm aus meiner Sicht nicht zugemutet werden kann. Eine weitere Schwächung des Richtervorbehalts liegt in der neu eingeführten Eilfallkompetenz für Staatsanwaltschaft und Polizei. Für diese Regelung sehe ich kein praktisches Bedürfnis. Es fehlt hier an rechtstatsächlichen Anhaltspunkten dafür, dass gerade durch die Notwendigkeit der Einschaltung eines Richters in Eilfällen DNA-Analysen nicht rechtzeitig durchgeführt werden können. Keine Einwände habe ich gegen die erfolgte Abschaffung des Richtervorbehalts für die molekulargenetische Untersuchung von unbekanntem Spurenmaterial. Bereits in meinem 20. TB (Nr. 7.3.2) hatte ich die richterliche Prüfung in Zweifel gezogen, wenn der Richter den Spurenleger gar nicht kennt.

Für DNA-Analysen zur Identitätsfeststellung in künftigen Strafverfahren wurden durch die Neuregelung auch die Anforderungen an die Anlasstaten und die zu prognostizierenden künftigen Straftaten des Betroffenen herabgesetzt. Für beides waren bislang Straftaten von erheblicher Bedeutung bzw. Sexualstraftaten erforderlich. Nunmehr kann jeweils auch die wiederholte Begehung nicht erheblicher Straftaten (z. B. Sachbeschädigung, Hausfriedensbruch) genügen, wenn dies im Unrechtsgehalt einer Straftat von erheblicher Bedeutung gleichsteht.

Zu begrüßen ist, dass für das DNA-Massenscreening („Massengentest“) auf freiwilliger Basis jetzt eine ausdrückliche gesetzliche Grundlage geschaffen wurde (§ 81h StPO). Dies entspricht meiner seit langem vorgebrachten Forderung nach einer klarstellenden gesetzlichen Festlegung der rechtlichen Rahmenbedingungen dieses Ermittlungsinstruments (vgl. zuletzt 20. TB Nr. 7.3.4). Leider kommt in der gesetzlichen Regelung nicht deutlich zum Ausdruck, dass der Massengentest nur als ultima ratio der strafprozessualen Ermittlungen in Betracht kommt und dass der Teilnehmerkreis, soweit er nicht klar und bestimmt ist, zunächst so klein wie möglich zu wählen und nur erforderlichenfalls in konzentrischen Kreisen zu erweitern ist.

Die Regierungsparteien haben in ihrem Koalitionsvertrag vom 11. November 2005 (S. 141) darauf hingewiesen, dass das Gesetz zur Novellierung der forensischen DNA-Analyse nach zwei Jahren zu evaluieren und im Rahmen dessen zu prüfen sei, ob die DNA-Analyse aus kriminalpolitischen Gründen ausgeweitet werden müsse. Ich werde dies kritisch verfolgen.

## 6.4 Strafbarkeitslücke bei heimlicher Ortung

*Das heimliche Ausspähen des Aufenthaltsortes einer anderen Person mit Hilfe von elektronischen Diensten sollte unter Strafe gestellt werden.*

Es ist ohne weiteres möglich, mit Mobilfunknetzen den Aufenthaltsort eines Handynutzers gegen dessen Willen auszuspionieren (vgl. 19. TB Nr. 11.10.4). Dies gilt insbesondere für die sog. Location Based Services, also jene Dienstleistungen im Mobilfunkbereich, die dem Nutzer in Abhängigkeit von seinem Standort zur Verfügung gestellt werden (z. B. Suchfunktionen für Freunde, Funktionen zum Finden eines verlegten Handys oder zur Feststellung des Standorts eines Außendienstmitarbeiters (Nr. 10.2)). Für sämtliche dieser Dienste wird mit Hilfe von Lokalisierungstechniken das Handy geortet.

Indem dem Betroffenen ein Handy mit einer solchen Funktion überlassen wird, es bei ihm (etwa im Handschuhfach des Autos) versteckt oder die Funktion unbeobachtet aktiviert wird, lässt sich der Aufenthaltsort des Betroffenen auch heimlich ermitteln. Ein solcher Missbrauch von Location Based Services ist nach gegenwärtiger Rechtslage nicht strafbar. Da er aber den persönlichen Lebens- und Geheimbereich des Opfers erheblich verletzt, sollte er nach meiner Auffassung unter Strafe gestellt werden. Vergleichbar schwere Eingriffe in die Privatsphäre stehen bereits unter Strafe, insbesondere die Verletzung der Vertraulichkeit des Wortes und heimliche Bildaufnahmen (§§ 201, 201a StGB).

Ich habe deshalb gegenüber dem BMJ angeregt, einen Tatbestand zu schaffen, der es unter Strafe stellt, wenn jemand unbefugt den Aufenthaltsort einer anderen Person ausspäht, indem er ohne Einwilligung des anderen einen standortabhängigen Mobilfunkdienst nutzt oder den anderen heimlich mit einem Ortungsgerät ausstattet. Zwar sind mir bislang erst einzelne Missbrauchsfälle bekannt geworden, wie z. B. Anbringen eines Handys mit Ortungsfunktion an der Unterseite eines Autos. Ich gehe aber davon aus, dass es in diesem Bereich eine hohe Dunkelziffer gibt. Denn Ausspionieren geschieht typischerweise heimlich und wird deshalb vom Opfer häufig gar nicht bemerkt. Ich werde daher weiterhin auf eine strafrechtliche Regelung hinwirken.

## 6.5 Verbesserung der Durchsetzung von Rechten des geistigen Eigentums – Umsetzung der IPR-Enforcement-Richtlinie

*Das geistige Eigentum soll gestärkt werden. Doch zu welchem Preis? Die vorgesehene Verpflichtung von Internetprovidern zur Auskunftserteilung über Kundendaten lässt mit Blick auf die Vorratsspeicherung von Telekommunikationsdaten nichts Gutes ahnen.*

Bereits in meinem 20. TB (Nr. 7.12.1 und 7.12.2) hatte ich über die sog. IPR-Enforcement-Richtlinie (Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums) berichtet. Artikel 8 verpflichtet die Mitgliedstaaten sicherzustellen, dass „die zuständigen Gerichte im Zusammenhang mit einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, von dem Verletzer und/oder jeder anderen Person erteilt werden ...“.

Der Referentenentwurf eines Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums sieht zur Umsetzung dieser Vorgaben in den einschlägigen Schutzgesetzen (Patentgesetz, Gebrauchsmustergesetz, Markengesetz, Halbleiterschutzgesetz, Urheberrechtsgesetz, Geschmacksmustergesetz, Sortenschutzgesetz) Auskunftsansprüche gegen Dritte vor, die selbst nicht Rechteverletzer sind. Der Rechteinhaber soll damit die Möglichkeit erhalten, den Rechteverletzer mit zivilrechtlichen Mitteln zu ermitteln, um so seine Rechte besser durchsetzen zu können.

Dies ist vor allem mit Blick auf die Auskunftsverpflichtung von Internetprovidern unter Verwendung von Verkehrsdaten im Sinne des § 3 Nr. 30 Telekommunikationsgesetz (TKG) datenschutzrechtlich bedenklich, weil damit in das Fernmeldegeheimnis eingegriffen wird. Verkehrsdaten sind alle Daten, die bei der technischen Durchführung eines Telekommunikationsdienstes anfallen. Hierzu gehören auch die IP-Adressen, die zum Surfen im Internet an die Nutzer vergeben werden. In Protokolldateien wird aufgezeichnet, wer wann welche dynamische IP-Adresse erhält. So ist es möglich, den hinter der IP-Adresse stehenden Kunden zu identifizieren.

Aus meiner Sicht ist es wegen des hiermit verbundenen massiven Eingriffs in das verfassungsrechtlich geschützte Fernmeldegeheimnis entgegen den vielfach geäußerten Wünschen der Rechteinhaber unabdingbar, für die Auskunftserteilung eine vorherige richterliche Anordnung zu verlangen. Dies sieht der Entwurf auch vor, setzt aber anders als die Richtlinie nicht voraus, dass bereits ein Gerichtsverfahren gegen den Verletzer anhängig ist. Vielmehr soll der Anspruch auch außerhalb eines anhängigen Gerichtsverfahrens in Fällen offensichtlicher Rechtsverletzung zur Ermittlung des Verletzers dienen. Hierbei hat die Bundesregierung nach der Begründung (S. 82) vor allem die Tauschbörsen im Auge, „bei denen in großem Umfang Urheberrechtsverletzungen stattfinden“.

Selbst wenn man insoweit dem Schutz des geistigen Eigentums den Vorrang einräumen wollte, kann dies nur unter engen Voraussetzungen als verhältnismäßig angesehen werden. Dies gilt zum einen für die Qualität der festgestellten Rechtsverletzung, die den Auskunftsanspruch auslöst. Dieser soll hier nur bei in gewerblichem Ausmaß vorgenommenen Rechtsverletzungen bestehen (vgl. § 101 Abs. 2 UrhG-E). Damit ist klargestellt, dass etwa bei illegalen Kopien und Verbreitungen im Internet (z. B. über Tauschbörsen) ein Umfang erreicht werden muss, der über das hinausgeht, was einer Nutzung zum privaten und sonstigen eigenen Gebrauch entsprechen würde.

Zum anderen ist für die Beurteilung der Verhältnismäßigkeit von entscheidender Bedeutung, welche Verkehrsdaten verwendet werden dürfen. Hier hatte ich mich besonders nachdrücklich dafür eingesetzt, zumindest in der Gesetzesbegründung ausdrücklich klarzustellen, dass dies ausschließlich die Daten sein können, die die Anbieter von Internet- und Telekommunikationsdiensten unter den Voraussetzungen des TKG (§§ 96 ff.) für eigene Zwecke gespeichert haben. Der Zugriff auf die gemäß der Richtlinie zur Vorratsdatenspeicherung gespeicherten Telekommunikationsdaten (s. u. Nr. 10.1) muss dagegen tabu sein und, wie von der Richtlinie vorgegeben, auf Zwecke der Verfolgung von schweren Straftaten beschränkt werden und bleiben (vgl. hierzu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Kasten zu Nr. 6.5).

Ich bedauere die Auffassung des federführenden BMJ, die „hoch brisante Frage“, ob und wie ein Zugriff auf diese Vorratsdaten erfolgen dürfe, erst bei der Umsetzung der Richtlinie zur Vorratsdatenspeicherung zu entscheiden und würde es begrüßen, wenn der Gesetzgeber bereits hier für Normenklarheit sorgen würde.

Inhalt und Umfang der Rechte und Pflichten sowohl der Rechteinhaber als auch der Provider müssen sich eindeutig aus dem Gesetz ergeben. Zudem haben sich die Rechteinhaber bereits ausdrücklich die Einbeziehung der Daten aus der Vorratsdatenspeicherung in diesen zivilrechtlichen Auskunftsanspruch gewünscht. Dies bestätigt meine Befürchtungen. Bei einer solchen Preisgabe grundrechtlich geschützter Fernmeldedaten für zivilrechtliche Zwecke nimmt eine Entwicklung ihren Anfang, an deren Ende diese Daten für kaum noch zu übersehende Zwecke zur Verfügung stünden. Dies wäre mit dem Verhältnismäßigkeitsgrundsatz nicht vereinbar. Daher bekräftige ich meine Forderung nach einer entsprechenden Klarstellung im Gesetz.

Kritisch bewerte ich auch, dass der Entwurf anders als die Richtlinie bei den übrigen Drittauskunftsansprüchen keinen Richtervorbehalt vorsieht. In den weitgehend wortgleichen Änderungen der Schutzgesetze (z. B. § 140b Abs. 2 PatG-E) heißt es, der Drittauskunftsanspruch könne bereits bei Offensichtlichkeit der Rechtsverletzung ohne vorherige richterliche Entscheidung geltend gemacht werden. Das halte ich nicht für angemessen. Damit

Kasten zu Nr. 6.5

**Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. bis 17. März 2006 in Magdeburg**

**Keine Aushöhlung des Fernmeldegeheimnisses im Urheberrecht**

Das Bundesministerium der Justiz hat den Referentenentwurf eines „Gesetzes zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums“ vorgelegt, das in Umsetzung einer europäischen Richtlinie stärkere Instrumente zum Schutz des Urheberrechts und anderer gewerblicher Schutzrechte einführen soll.

Der Gesetzentwurf gesteht den Rechteinhabenden in bestimmten Fällen Auskunftsansprüche auch gegenüber unbeteiligten Dritten zu, die selbst keine Urheberrechtsverletzungen begangen haben. So sollen etwa Internet-Provider auch über – durch das Fernmeldegeheimnis geschützte – Daten ihrer Nutzerinnen und Nutzer zur Auskunft verpflichtet werden. Damit sollen beispielsweise Anbietende und Nutzende illegal kopierter Musik- oder Videodateien oder Software leichter ermittelt werden können.

Die Datenschutzbeauftragten des Bundes und der Länder warnen vor der hiermit eingeleiteten Entwicklung. Zwar sind die vorgesehenen Eingriffe in das Fernmeldegeheimnis in dem Entwurf an formale Hürden geknüpft; insbesondere müssen Rechteinhabende eine richterliche Anordnung erwirken. Jedoch lassen die europarechtlichen Vorgaben den Mitgliedstaaten zugunsten des Datenschutzes so viel Spielraum, dass Eingriffe in das Fernmeldegeheimnis vermieden werden können. Das Bundesverfassungsgericht hat betont, dass gemeinschaftsrechtliche Spielräume zu nutzen sind.

Nachdem das grundrechtlich geschützte Fernmeldegeheimnis in den letzten Jahren immer stärker und in immer kürzeren Abständen für Zwecke der Strafverfolgung und der Geheimdienste eingeschränkt wurde, soll es nun auch erstmals zugunsten privater wirtschaftlicher Interessen nicht unerheblich weiter eingeschränkt werden. Es ist zu befürchten, dass damit ähnliche Begehrlichkeiten weiterer privater Interessengruppen geweckt werden. Dem grundrechtlich geschützten Fernmeldegeheimnis unterliegende Daten stünden am Ende der Entwicklung für kaum noch zu übersehende Zwecke zur Verfügung.

Es ist zu befürchten, dass durch die Auskunftsansprüche gegen Internet-Provider die gerade für die Verfolgung schwerer Straftaten beschlossene Verpflichtung zur Vorratsdatenspeicherung von Verkehrsdaten für die Durchsetzung privater Interessen genutzt wird. Angesichts der Tendenz, die Internet-Anbietenden in immer stärkerem Maße für die Kommunikationsinhalte ihrer Kunden verantwortlich zu machen, ist zudem zu befürchten, dass die Firmen vorsichtshalber weitere Verkehrsdaten speichern, um im Falle von Rechtsverletzungen Auskünfte erteilen zu können.

Die Datenschutzbeauftragten des Bundes und der Länder appellieren deshalb an die Bundesregierung und an den Gesetzgeber, auf eine weitere Einschränkung des Fernmeldegeheimnisses – erstmals zur Durchsetzung wirtschaftlicher Interessen – zu verzichten. Es wäre völlig unakzeptabel, wenn Daten, deren zwangsweise Speicherung mit der Abwehr terroristischer Gefahren begründet wurde, nun auf breiter Basis für die Verfolgung von Urheberrechtsverletzungen genutzt würden. Musik- und Filmindustrie müssen selbst dafür Sorge tragen, dass durch technische Maßnahmen und neue Geschäftsmodelle unrechtmäßigen Nutzungen die Grundlage entzogen wird.

würde faktisch dem Dritten die Prüfung überlassen, ob die Voraussetzungen für seine Auskunftspflicht vorliegen. Es wäre dann offenbar ausreichend, dass der Rechteinhaber schlüssig einen Sachverhalt vorträgt, der das Auskunftsbegehren rechtfertigt. Die Argumentation des BMJ, vom Richtervorbehalt sei aufgrund einer Vielzahl von zu erwartenden Auskunftsbegehren und der damit verbundenen sehr hohen Belastung der Gerichte abzusehen, vermag mich nicht zu überzeugen. Eine mögliche Belastung der Gerichte kann nicht zum Verzicht auf das nach dem Verhältnismäßigkeitsgrundsatz Gebotene führen. Zudem ist es gerade wegen der prognostizierten hohen Zahl von Auskunftsbegehren unabdingbar, diese rechtsstaatliche Hürde vorzusehen, um Missbrauch zu verhindern.

## 6.6 Digitales Rechtemanagement

*Das Digitale Rechtemanagement (DRM) darf nicht den „gläsernen Nutzer“ zur Folge haben!*

Das Urheberrecht soll das geistige Eigentum schützen, egal ob es sich dabei um Musikstücke, Filme oder auch Computerprogramme handelt. Noch vor wenigen Jahren war nicht absehbar, dass mit seiner Durchsetzung erhebliche Eingriffe in den Datenschutz verbunden sein könnten, vor allem im Hinblick auf die Registrierung des Nutzungsverhaltens. Digitalisierung bedeutet stets auch Entmaterialisierung von Information. Waren bei den traditionellen Verbreitungswegen die Daten fest an ein Trägermedium gebunden (Bücher, Zeitungen, Filme), sind digitalisierte Daten verlustfrei reproduzierbar. Die Möglichkeiten zur elektronischen Vervielfältigung haben erhebliche Auswirkungen auf den Umgang mit urheberrechtlich geschützten Werken. Mit den heutigen technischen Mitteln ist es selbst Kindern und Jugendlichen möglich, geschützte Werke zu vervielfältigen oder über das Internet zu verbreiten, Musikstücke genauso wie Computerprogramme oder ganze Filme.

Bereits im 20. TB (Nr. 7.12.2) hatte ich über den Entwurf eines Zweiten Gesetzes zur Regelung des Urheberrechts in der Informationsgesellschaft (so genannter „Zweiter Korb“) berichtet, über den der Bundestag jedoch wegen der verkürzten 15. Legislaturperiode nicht mehr entschie-

den hat. Inzwischen wird ein neuer Regierungsentwurf (Bundestagsdrucksache 16/1828 vom 15. Juni 2006) beraten, der Regelungen zum Vergütungssystem enthält. Erfreulich ist, dass grundsätzlich an dem pauschalen Vergütungssystem festgehalten werden soll, bei dem eine individuelle Registrierung der einzelnen Nutzungsvorgänge nicht erforderlich ist. Allerdings wird den Rechteinhabern die Möglichkeit eingeräumt, alternativ zur pauschalen Berechnung auch die einzelnen Nutzungsvorgänge individuell abzurechnen. Zu diesem Zweck werden Systeme des Digitalen Rechtemanagements (DRM) zugelassen.

Diese DRM-Systeme mögen zwar bei der Abrechnung für mehr Einzelfallgerechtigkeit sorgen und damit auch den Interessen der Verbraucher Rechnung tragen. Gleichwohl habe ich im Gesetzgebungsverfahren mit Nachdruck auf die hiermit verbundene Gefahr hingewiesen, dass mit Hilfe dieser Technologie umfassende Nutzerprofile erstellt werden können. Die Gesetzesbegründung enthält erfreuliche Ausführungen zum Datenschutz. Betont werden die Grundsätze der Datensparsamkeit, Datenvermeidung und des Systemdatenschutzes, wonach der Schutz der personenbezogenen Daten bereits bei der Ausgestaltung der technischen Systeme zu gewährleisten ist. Auch heißt es: „Das Datenschutzrecht wird mit Blick auf die technologische Entwicklung und die Erfahrungen der Aufsichtsbehörden laufend fortentwickelt. Es ist nicht auszuschließen, dass die Verbreitung von DRM-Systemen und die damit einhergehenden Erfahrungen zukünftig im Datenschutzrecht zu berücksichtigen sein werden."

Ich sehe darin eine Sensibilisierung für die Belange des Datenschutzes. Bei diesen guten Worten darf es aber nicht bleiben. Es ist schon jetzt zwingend geboten, die Voraussetzungen für eine Rechtstatsachenforschung zu gewährleisten, um im Interesse der Persönlichkeitsrechte der Nutzer rechtzeitig die richtigen Weichen zu stellen. Hierzu ist es notwendig, die weitere Entwicklung von DRM und den Umgang mit personenbezogenen Daten wissenschaftlich zu begleiten.

Gefragt ist aber auch die Verantwortung der Industrie und der Rechteinhaber, DRM so auszugestalten, dass die erwähnten Datenschutzgrundsätze mit Leben gefüllt werden. Auch bei einer individuellen Nutzungsabrechnung ist es durchaus möglich, auf eine personenbezogene Registrierung zu verzichten. So könnten zum Beispiel DRM-Systeme so gestaltet werden, dass keine Registrierung des Nutzungsverhaltens in externen Datenbanken erforderlich ist, etwa wenn die urheberrechtlich geschützten Werke eingebaute technische Nutzungsbeschränkungen aufweisen und nur im Rahmen der jeweiligen Nutzungsberechtigungen verwendet werden können. Ferner sollten die einzelnen Nutzungsvorgänge nicht regelhaft unter dem Namen des Nutzers registriert und abgerechnet werden. Alternativ könnten Prepaid-Modelle verwendet werden, bei denen lediglich Nutzungskennungen, nicht aber die Identität der Nutzer registriert werden. Schließlich sollten den Nutzern gegebenenfalls alternative Vertriebswege eröffnet werden, indem neben einer nutzerbezogenen Abrechnung auch ein Pauschaltarif angeboten wird.

## 6.7 Novellierung der Prozesskostenhilfe

*Der Bundesratsentwurf eines Gesetzes, mit dem Aufwendungen für Prozesskostenhilfe begrenzt werden sollen, berührt in erheblichem Maße Belange des Datenschutzes.*

Zentrales Anliegen der vom Bundesrat vorgeschlagenen Gesetzesänderungen (Bundestagsdrucksache 16/1994) ist es, die Ausgaben für die Prozesskostenhilfe zu reduzieren. Hierzu sollen u. a. die Voraussetzungen für die Bewilligung von Prozesskostenhilfe korrigiert werden, um der missbräuchlichen Inanspruchnahme entgegenzuwirken. Vorgesehen ist, in § 118 Abs. 2 Satz 3 Nr. 1 und 2 ZPO-E die Auskunftsrechte des Gerichts zu erweitern, um die Richtigkeit von Angaben des Antragstellers zu seinen persönlichen und wirtschaftlichen Verhältnissen zu überprüfen. Das Gericht soll hierfür Auskunft über das Vermögen des Antragstellers bei den Finanzämtern und über seine Kontoverbindungen im Sinne des § 24c Abs. 1 Kreditwesengesetz (KWG) nebst Name und Anschrift des Kreditinstituts bei der Bundesanstalt für Finanzdienstleistungsaufsicht (sog. Kontenabrufverfahren) einholen können. Des Weiteren soll ihm die Möglichkeit eröffnet werden, sich bei den in § 643 Abs. 2 Satz 1 Nr. 1 ZPO genannten Stellen (Arbeitgebern, Sozialleistungsträgern, sonstigen Personen oder Stellen, die Leistungen zur Versorgung im Alter und bei verminderter Erwerbsfähigkeit sowie Leistungen zur Entschädigung oder zum Nachteilsausgleich zahlen, und Versicherungsunternehmen) über die Höhe der Einkünfte Auskunft erteilen zu lassen.

Diese Möglichkeiten, bei Dritten zu ermitteln, sollen zwar ausdrücklich von der vorherigen Einwilligung des Betroffenen abhängig gemacht werden. Jedoch muss nach § 118 Abs. 2 Satz 6 ZPO-E das Gericht einen Prozesskostenhilfeantrag allein wegen der Nichterteilung dieser Einwilligung ablehnen, unabhängig davon, ob die Einholung der Auskunft im konkreten Fall tatsächlich notwendig ist. Dies ist mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar, da der Betroffene auf diese Weise ohne Rücksicht auf die Erforderlichkeit (Vorrang der Direkterhebung) faktisch zur Einwilligung genötigt wird (vgl. § 4a Abs. 1 Satz 1 BDSG). Hier muss deutlich nachgebessert werden, insbesondere muss auch die Zweckbindung dieser Datenerhebung eindeutig sein. Ich sehe die Gefahr, dass diese Daten nicht nur genutzt werden könnten, die Bedürftigkeit der Partei im Prozesskostenhilfeverfahren zu klären, sondern auch im Rahmen der Begründetheit des Klagebegehrens selbst. Hiermit würden aber die nach § 643 Abs. 2 ZPO für bestimmte, abschließend aufgezählte Unterhaltsstreitigkeiten bestehenden Auskunftspflichten auf dem Umweg über das Prozesskostenhilfeverfahren quasi flächendeckend ausgedehnt.

Gänzlich abzulehnen ist mit Blick auf die bevorstehende Entscheidung des BVerfG über die Verfassungsmäßigkeit des Kontenabrufs durch die Finanz-, Sozialbehörden und Gerichte (s. u. Nr. 8.2) die vorgeschlagene Teilnahme der Zivilgerichte an diesem Verfahren.

Im Gesetzentwurf ist ferner vorgesehen, dem Gegner ausdrücklich auch Gelegenheit zur Äußerung zu den wirtschaftlichen und persönlichen Verhältnissen des Antragstellers einzuräumen (§ 118 Abs. 1 Satz 1 ZPO-E). Hier bedarf es der Klarstellung, dass etwaige vom Gericht eingeholte Auskünfte ebenso wenig dem Gegner ohne Einwilligung des Antragstellers zugänglich gemacht werden dürfen wie dessen eigene Erklärung zu seinen persönlichen und wirtschaftlichen Verhältnissen (§ 117 Abs. 2 Satz 2 ZPO). Es wäre datenschutzrechtlich nicht vertretbar, die bei Dritten erhobenen Daten in weitergehendem Umfang an den Gegner zu übermitteln als dies bei den direkt erhobenen Daten zulässig ist.

### 6.8 Das Betreuungsbehördengesetz soll ergänzt werden

*Die Länder wollen aus Gründen der Verfahrensvereinfachung die Befugnisse der Betreuungsbehörden im Rahmen ihrer Sachverhaltsermittlungstätigkeit für die Vormundschaftsgerichte erweitern.*

Betreuungsbehörden unterstützen nach § 8 des Betreuungsbehördengesetzes (BtBG) das Vormundschaftsgericht (§§ 1896 ff. BGB). Dies gilt vor allem für die Feststellung von Sachverhalten, die das Gericht für aufklärungsbedürftig hält, insbesondere, ob für einen Betroffenen ein Betreuer zu bestellen ist.

Mit dem Entwurf des Bundesrates vom 26. April 2006 (Bundestagsdrucksache 16/1339) sollen die Befugnisse der Betreuungsbehörde erweitert werden, indem ihr im Rahmen des vom Vormundschaftsgericht erteilten Auftrags erlaubt wird, die für die Feststellung des Sachverhalts und für den Vorschlag eines Betreuers erforderlichen Daten zu erheben. Die Daten sollen vorrangig beim Betroffen erhoben werden. Jedoch soll die Erhebung von Daten bei Dritten dann zulässig sein, wenn der Betroffene einwilligt oder krankheits- oder behinderungsbedingt seine Einwilligung nicht erteilen kann und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Letztere Voraussetzung wird insbesondere damit begründet, dass die Klärung des Sachverhalts nur beim Betroffenen häufig nicht ausreiche, um entsprechend der Intentionen des Betreuungsrechts familiäre und andere soziale Zusammenhänge bei der Entscheidung über die Notwendigkeit einer Betreuerbestellung einzubeziehen. Die Betreuungsbehörde benötige nach der geltenden Rechtslage das ausdrückliche schriftliche Einverständnis des Betroffenen, wenn sie zur Aufklärung des Sachverhalts auch bei anderen Stellen oder Personen ermitteln müsse. Viele der Betroffenen seien zur Erteilung eines Einverständnisses aber krankheits- oder behinderungsbedingt nicht in der Lage. Das Gericht müsse dann eigenen weiteren Aufwand zur Klärung des Sachverhalts betreiben oder die Betreuungsbehörde erneut mit dezidierten Fragestellungen beauftragen. Dies bedeute unnötige Verfahrensverzögerungen zum Nachteil des Betroffenen und zusätzlichen Verwaltungsaufwand (Bundestagsdrucksache, a. a. O., S. 6). Hier soll die vorgeschlagene Gesetzesänderung Abhilfe schaffen.

Die Initiative des Bundesrates ist in ihrer Zielrichtung, nämlich für die Datenerhebung durch die Betreuungsbehörde eine normenklare, bereichsspezifische gesetzliche Regelung zu schaffen, zu begrüßen. Einige wichtige Aspekte wie Ersterhebungsgrundsatz, Einwilligung und Abwägung mit den schutzwürdigen Interessen des Betroffenen sind schon einbezogen. Allerdings teile ich die Auffassung der Bundesregierung (Bundestagsdrucksache, a. a. O., S. 7), dass die vorgesehenen Regelungen noch verbesserungsbedürftig sind. Insbesondere bedarf es im Hinblick auf die konkreten Einzelheiten und Umstände der Datenerhebung und -verarbeitung noch verfahrenssichernder Maßnahmen. Die vorgesehene eigene Ermittlungstätigkeit der Betreuungsbehörden bei Dritten stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Gerade hilfebedürftige Kranke haben ein Recht darauf, dass mit ihren Gesundheitsdaten sensibel umgegangen wird.

Ich werde im weiteren Gesetzgebungsverfahren darauf hinwirken, dass diesen Anforderungen Rechnung getragen wird.

## 7 Innere Verwaltung

### 7.1 Ausländerrecht

#### 7.1.1 Entwurf eines Gesetzes zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union

*Der Gesetzentwurf dient vor allem der Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union und sieht daneben weitere Änderungen im Ausländer- und Asylrecht vor. Einige Bestimmungen begegnen erheblichen datenschutzrechtlichen Bedenken.*

Positiv zu bewerten ist, dass endlich meiner seit dem 16. Tätigkeitsbericht (vgl. dort Nr. 5.7, zuletzt 20. TB Nr. 6.8) erhobenen Forderung nachgekommen wird, eine Rechtsgrundlage für die beim Bundesverwaltungsamt bereits seit 1982 geführte Staatsangehörigkeitsdatei (STADA) zu schaffen. Der Gesetzentwurf enthält jedoch auch erhebliche datenschutzrechtliche Verschlechterungen.

Kritisch bewerte ich insbesondere, dass in Zukunft Lichtbilder aller Ausländer (auch der Unionsbürger) im allgemeinen Datenbestand des Ausländerzentralregisters (AZR) gespeichert werden sollen (§ 3 Nr. 5a AZRG-E). Die von mir vorgeschlagene Begrenzung auf bestimmte Speicheranlässe, insbesondere auf Personen, gegen deren Einreise Bedenken bestehen, hat das BMI nicht übernommen. Auch wenn die Zuspeicherung erst ab Inkrafttreten des Gesetzes und nicht rückwirkend erfolgen soll, ist davon auszugehen, dass in relativer kurzer Zeit ein sehr großer Bestand an Lichtbildern im AZR gespeichert sein wird. Das Argument, die Lichtbilder seien für die Feststellung der Identität der Betroffenen erforderlich, überzeugt nicht. Zum einen wird dabei außer Acht gelassen, dass Identitätsfeststellungen auch mit weniger einschneidenden Maßnahmen als mit einer Speicherung sämtlicher Lichtbilder in einer online abrufbaren Zentraldatei mög-

lich sind, etwa durch Vergleich mit Identitätspapieren und ggf. mit Lichtbildern, die sich in Ausländerakten befinden.

Ferner ist nicht nachvollziehbar, warum nicht zwischen Drittstaatsangehörigen und Staatsangehörigen der EU unterschieden wird. Ich unterstreiche erneut (vgl. 20. TB Nr. 6.1.3), dass die generelle Speicherung der Daten von Unionsbürgern im AZR gegen europäisches Gemeinschaftsrecht verstößt. Unionsbürger benötigen nach § 2 Abs. 4 Freizügigkeitsgesetz/EU für die Einreise weder ein Visum noch einen Aufenthaltstitel. Sie erhalten von der Ausländerbehörde lediglich eine Bescheinigung über ihr Aufenthaltsrecht (§ 5 Abs. 1 Freizügigkeitsgesetz/EU). Im Hinblick auf das zur Zeit in dieser Sache anhängige Verwaltungsstreitverfahren und im Hinblick auf das von der Europäischen Kommission gegen die Bundesrepublik Deutschland eingeleitete Vertragsverletzungsverfahren (vgl. 20. TB Nr. 6.1.4) sollten zumindest weitere Zuspeicherungen für Staatsangehörige von EU-Mitgliedstaaten vermieden und Unionsbürger von der beabsichtigten Regelung in § 3 Nr. 5a AZRG-E ausgenommen werden.

Im Zusammenhang mit den gescheiterten Kofferbombenattentaten im Juli 2006 hat das BMI den Gesetzentwurf ergänzt. Über die Notwendigkeit der Änderungen „aus Gründen der Inneren Sicherheit“ habe ich verschiedene Gespräche mit dem BMI geführt. In zwei Punkten blieben meine Zweifel bestehen:

Ich erkenne nicht die Erforderlichkeit der in § 73 Abs. 3 AufenthG-E vorgesehenen Regelung, dass auch sämtliche von den Sicherheitsbehörden an die am Überprüfungsverfahren beteiligten Stellen übermittelten Daten, bei denen keine Gründe für Sicherheitsbedenken festgestellt wurden (Nichttrefferfälle), dort für den gesamten Gültigkeitszeitraum des Aufenthaltstitels gespeichert sein müssen. Die Speicherung personenbezogener Daten auf Vorrat zu Personen, bei denen solche Erkenntnisse fehlen, halte ich – wie bei Dateien der Polizeien und der Nachrichtendienste des Bundes und der Länder – auch hier nicht für erforderlich. Ich bin deshalb der Ansicht, dass die übermittelten Daten nach der Überprüfung gelöscht werden müssen.

Weiter sehe ich es kritisch, dass der Gesetzentwurf die bisherige abgestufte Regelung bei der Abfrage des AZR nicht beibehält. Schon die angestrebte unbegrenzte Zugriffsmöglichkeit für alle in § 15 AZRG-E genannten Behörden stellt eine bedeutsame datenschutzrechtliche Verschlechterung dar. Bisher ist für sonstige Polizeivollzugsbehörden, Staatsanwaltschaften und Gerichte für die Abfrage des AZR in § 16 AZRG ein gestuftes Verfahren vorgesehen. Abfragen dürfen danach in drei Stufen erfolgen. In jeder ist die Erforderlichkeit für die Aufgabenerfüllung neu zu prüfen; wird diese bejaht, erhalten die Stellen weitergehende Informationen. In der dritten und weitestgehenden Stufe ist ein automatisierter Abruf nach § 22 Abs. 1 AZRG ausgeschlossen.

Bei dem beabsichtigten unbeschränkten und stufenlosen Online-Zugriff auf das AZR wird – anders als bisher – der Grundsatz der Verhältnismäßigkeit nicht ausreichend beachtet. Für den beabsichtigten Wegfall der datenschutzrechtlich bedeutsamen Sicherungen des Datenabrufs liefert die Gesetzesbegründung keine überzeugenden Argumente. Der angeführte schnelle Zugriff reicht jedenfalls nicht aus; einen solchen haben die Stellen bei entsprechendem Bedarf bereits jetzt.

Ich hoffe, dass das BMI die von mir vorgebrachten Argumente im weiteren Verfahren berücksichtigt. Ergebnisse lagen bei Redaktionsschluss noch nicht vor.

### 7.1.2 Die Integrationsgeschäftsdatei beim Bundesamt für Migration und Flüchtlinge

*Das Bundesamt für Migration und Flüchtlinge hat ein IT-unterstütztes System zur Koordinierung, Steuerung und Abrechnung von Integrationskursen entwickelt.*

In §§ 43, 44, 44a AufenthG, § 9 Abs. 1 Bundesvertriebenengesetz sowie § 11 Abs. 1 Freizügigkeitsgesetz/EU werden erstmals Integrationskurse für alle Zuwanderer (Ausländer, Spätaussiedler und Staatsangehörige eines EU-Mitgliedstaates) einheitlich gesetzlich geregelt (vgl. 20. TB Nr. 6.1.2 und 6.1.2.2). Dem Bundesamt für Migration und Flüchtlinge wurde durch das Zuwanderungsgesetz (§ 75 Nr. 2 Aufenthaltsgesetz – AufenthG) die Aufgabe übertragen, die Durchführung von Integrationskursen zu koordinieren und zu steuern. Dabei ergeben sich Schnittstellen zu den beteiligten Ausländerbehörden (ABH), dem Bundesverwaltungsamt (BVA) und zu Kursträgern, die im Auftrag des Bundesamtes die Integrationskurse durchführen. Daher hat das Bundesamt zur Erledigung seiner Aufgaben eine IT-unterstützte „Integrationsgeschäftsdatei (InGe)“ entwickelt. Bei dieser Datei, seit 1. Januar 2005 im Echtbetrieb, handelt es sich um ein Datenverwaltungs- und Informationssystem zur Erfassung, Speicherung, Verarbeitung, Pflege und Anzeige von Daten über die Teilnehmer von Integrationskursen.

Zur Konzeption des Systems und dessen Weiterentwicklung habe ich mehrere Informations- und Beratungsbesuche durchgeführt. Zunächst wurde InGe als interne Datenbank für die zuständigen Mitarbeiter des Bundesamtes konzipiert. Die nunmehr beabsichtigte Online-Anbindung der Kursträger bildet vorerst den Endpunkt bei der Fortentwicklung der Datenbank (Kursträger Online). Die flächendeckende Umstellung ist bis zum Herbst 2007 vorgesehen.

Gegen die vorliegenden Planungen und insbesondere die beabsichtigten Maßnahmen im Bereich der Daten- und Anwendungssicherheit bestehen keine datenschutzrechtlichen Bedenken, zumal wegen der Anbindung der Kursträger über das Internet der Datenschutz mittels zusätzlicher Sicherheitskomponenten gewährleistet werden soll. Ich habe dem Bundesamt angeboten, auch die weiteren Realisierungsschritte beratend zu begleiten.

### 7.1.3 AZR: Datenerhebung zu Forschungszwecken ohne Rechtsgrundlage

*Eine problematische Auswertung des Ausländerzentralregisters (AZR) für eine repräsentative Studie soll nachträglich durch eine Forschungsklausel im AZR-Gesetz auf eine rechtliche Grundlage gestellt werden.*

Im Juni 2006 informierte mich das Bundesministerium des Innern über eine groß angelegte Studie des Bundesamtes für Migration und Flüchtlinge (BAMF) zur Situation ausländischer Arbeitnehmer und ihrer Familienangehörigen in Deutschland. Darin sollen repräsentativ 4 500 ausländische Mitbürger der fünf bevölkerungsstärksten Migrantengruppen durch ein privates Forschungsinstitut zu Hause besucht und zu Deutschkenntnissen, Bildung und Berufsausbildung sowie zu ihrer beruflichen, sozialen und familiären Situation befragt werden. Um an die hierfür erforderlichen Daten zu kommen, wurde eine namentliche Auswertung des AZR vorgenommen.

Nach dem AZR-Gesetz ist eine solche Auswertung ohne vollständige Personalien (Gruppenauskunft) jedoch nur in bestimmten, gesetzlich genau geregelten Fällen zulässig, z. B. zur Terrorismusbekämpfung oder Verfolgung von Bandenverbrechen. Eine Datenerhebung zu Forschungszwecken, wie sie in einer Reihe anderer Gesetze (z. B. § 75 des SGB X) geregelt ist, sieht das AZR-Gesetz nicht vor. Die vorgenommene Auswertung des AZR hatte daher nach meiner Auffassung keine rechtliche Grundlage. Auf meinen entsprechenden Hinweis hat mir das BMI zugesichert, die erforderliche Rechtsgrundlage bei der nächsten Gelegenheit in das AZR-Gesetz einzubringen. Aufgrund dieser Zusicherung habe ich von einer Beanstandung abgesehen und zugestimmt, dass die bereits erhobenen Daten im Rahmen des Forschungsprojektes vom BAMF weiter verwendet werden dürfen.

### 7.1.4 Das Visa-Informationssystem

*Mittlerweile hat die Europäische Kommission ein ganzes Bündel von Rechtsvorschriften zur Neuregelung des Visum-Verfahrens auf den Weg gebracht, die zum Teil datenschutzrechtlichen Bedenken begegnen.*

In meinem 20. TB (Nr. 6.2.3) habe ich über das Bestreben der EU berichtet, biometrische Merkmale auch in die Verfahren für Visa- und Aufenthaltserlaubnisse einzuführen. Bereits im Jahr 2003 hatte die Kommission einen Verordnungsvorschlag vorgelegt, der eine zentrale Datenbank über Anträge auf Erteilung eines Visums zur Einreise in einen sog. Schengen-Staat vorsah. Mit der Entscheidung 2004/512/EG vom 8. Juni 2004 wurden die finanziellen Weichen für die Errichtung des Visa-Informationssystem (VIS) gestellt und am 28. Dezember 2004 ein „Vorschlag für eine Verordnung des EP und des Rates betreffend das Visa-Informationssystem (VIS) und den Austausch von Daten zwischen den Mitgliedstaaten über Kurzzeitvisa“ vorgelegt. In diesem Vorschlag hat die Kommission die von der Artikel 29-Gruppe mit ihrer Stellungnahme 7/2004 vom 11. August 2004 (WP 96) gemachten Forderungen teilweise berücksichtigt. Dies hat die Artikel 29-Gruppe in ihrer Stellungnahme vom 23. Juni 2005 (WP 110) gewürdigt, dabei ein weiteres Mal auf die potenziellen Risiken eines solchen Vorhabens hingewiesen und die Beachtung der Grundsätze des Datenschutzes gefordert.

Das VIS soll aus einer zentralen Datei und nationalen Schnittstellen bestehen, ergänzt durch die Einrichtung entsprechender Systeme einschließlich fester Verbindungen zu Konsulaten und Grenzkontrollpunkten auf nationaler Ebene. Der Verordnungsvorschlag sieht vor, in das VIS alphanumerische und biometrische Daten (digitalisiertes Lichtbild, Fingerabdrücke) der Visum-Antragsteller zu speichern. Auch Verknüpfungen zu anderen Anträgen sollen gespeichert werden. Für die Daten ist entsprechend meiner Forderung eine Löschungsfrist von fünf Jahren vorgesehen. Genutzt werden soll das VIS nicht nur bei Visaverfahren, sondern auch im Asylverfahren und zur Identifizierung und Rückführung illegaler Einwanderer.

Zusätzlich hatte Deutschland gefordert, das VIS durch weitere Angaben über die Einlader mit der Funktion als Einlader- und Warndatei zu nutzen. Diese Forderung wird jedoch von anderen Mitgliedstaaten nicht befürwortet. Umstritten ist zudem der Kreis der Visumbehörden, die Zugriff auf das VIS erhalten sollen. Im Hinblick auf die Zweckbestimmung von VIS als Hilfsmittel zur Unterstützung des Verfahrens der Visavergabe und zur Vermeidung des Visamissbrauchs habe auch ich eine derartige Anreicherung des Speicherungsumfangs und die Ausweitung des Kreises der zugriffsberechtigten Stellen abgelehnt.

Um diesen Verordnungsvorschlag herum sind im Berichtszeitraum eine Reihe von weiteren Vorschlägen der Kommission für rechtliche Regelungen entstanden, die das Visa-Verfahren in der EU einheitlich gestalten sollen. So sollen mit der „Verordnung zur Änderung der Verordnung (EG) Nr. 1030/2002 des Rates vom 13. Juni 2002 zur einheitlichen Gestaltung des Aufenthaltstitels für Drittstaatsangehörige“ die europarechtlichen Vorgaben für das sog. Touristenvisa auch auf den Personenkreis angewandt werden, der aus visumpflichtigen Staaten kommend dauerhaft in einem Mitgliedstaat der EU lebt. Hinzu kommt die Änderung des sog. Visakodexes über die Erteilung von Schengenvisa sowie der „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Gemeinsamen Konsularischen Instruktion an die diplomatischen Missionen und die konsularischen Vertretungen, die von Berufskonsularbeamten geleitet werden, zur Aufnahme biometrischer Identifikatoren einschließlich Bestimmungen über die Organisation der Entgegennahme und Bearbeitung von Visumanträgen“ vom 31. Mai 2006.

Zudem sollen den für die innere Sicherheit zuständigen Behörden der Mitgliedstaaten und Europol der Zugang zum Visa-Informationssystem (VIS) für Datenabfragen „zum Zwecke der Prävention, Aufdeckung und Untersuchung terroristischer und sonstiger schwerwiegender Straftaten“ eingeräumt werden (vgl. Nr. 3.2.7).

Im Rahmen dieses komplexen Regelwerks ist insbesondere die Einführung weiterer biometrischer Merkmale in

die bisherigen und neu entstehenden Datenbanken über das Visa-Verfahren sowohl im nationalen wie auch im europäischen Bereich von datenschutzrechtlicher Relevanz.

### 7.1.5 „Scheinvaterschaften“ sollen angefochten werden können

*Die Überprüfung von Vaterschaftsanerkennungen muss auf solche Fälle beschränkt bleiben, in denen konkrete Verdachtsmomente vorliegen, dass sie dem alleinigen Zwecke der Erlangung eines Aufenthaltstitels bzw. der deutschen Staatsangehörigkeit dient.*

Die Bundesregierung hat am 29. August 2006 einen Gesetzentwurf verabschiedet, der die Anfechtung von missbräuchlichen Vaterschaftsanerkennungen durch staatliche Behörden erlaubt. Auslöser dieses Gesetzesvorhabens waren Fälle, in denen der Anerkennung weder eine leibliche Vaterschaft noch eine – ebenfalls verfassungsrechtlich schützenswerte – sozial-familiäre Beziehung zugrunde lag. Aufgrund des deutschen Staatsangehörigkeits- und Ausländerrechts kann zum Beispiel ein deutscher Staatsangehöriger durch die Anerkennung seiner Vaterschaft dem Kind einer ausreisepflichtigen Ausländerin zur deutschen Staatsangehörigkeit und der Mutter zu einem Bleiberecht verhelfen. Damit die zuständigen anfechtungsberechtigten Landesbehörden von derartigen Sachverhalten Kenntnis erlangen und ihr neues Anfechtungsrecht ausüben können, sieht der Gesetzesentwurf Mitteilungspflichten öffentlicher Stellen vor. Ausländerbehörden und Auslandsvertretungen sind künftig verpflichtet, bei Kenntnis von konkreten, die Annahme einer missbräuchlichen Vaterschaftsanerkennung nahe legenden Tatsachen diese der anfechtungsberechtigten Behörde mitzuteilen (§ 90 Abs. 4 AufenthG-E). Zudem sollen andere öffentliche Stellen unverzüglich die zuständige Ausländerbehörde unterrichten, wenn sie Kenntnis von derartigen Tatsachen erhalten; handelt es sich allerdings um das Jugendamt, so besteht die Mitteilungspflicht nur, soweit dadurch die Erfüllung der eigenen Aufgaben nicht gefährdet wird (vgl. § 87 Abs. 2 AufenthG-E).

Die Ausarbeitung des Gesetzentwurfs habe ich begleitet. Ich konnte erreichen, dass die genannten Mitteilungspflichten nur bei Vorliegen von *konkreten* verdachtsbegründenden Tatsachen bestehen. Wie die Gesetzesbegründung nunmehr ausdrücklich klarstellt, reichen bloße Vermutungen und Hypothesen nicht aus. Meiner aus Gründen des Sozialdatenschutzes geäußerten Anregung, das Jugendamt aus dem Kreise der mitteilungspflichtigen öffentlichen Stellen heraus zu nehmen, wurde zwar nicht entsprochen. Insoweit gelang es allerdings, die Mitteilungspflicht des Jugendamtes einzuschränken. So ist das Jugendamt dann nicht zur Mitteilung verpflichtet, wenn dies mit seinem Auftrag in Konflikt geriete, Eltern in Angelegenheiten ihrer Kinder Hilfe und Unterstützung anzubieten.

### 7.1.6 Vereinsrecht

*Im Rahmen des Kampfes gegen Extremismus und Terrorismus soll auch das öffentliche Vereinsrecht neu geregelt werden.*

Im BMI bestehen seit einigen Jahren Bestrebungen das öffentliche Vereinsrecht mit dem Ziel neu zu regeln, Extremismus und Terrorismus auch durch das Vereinsrecht den Boden zu entziehen. Dies soll – wenn Zweck oder Tätigkeit des Vereins der verfassungsmäßigen Ordnung zuwiderlaufen – durch eine praxisgerechtere Ausgestaltung der Verbotsvorschriften sowie durch Verbesserung der Befugnisse der Verbotsbehörden, insbesondere zur Ermittlung und ggf. Sicherstellung des Vereinsvermögens, erreicht werden. Zusätzlich sollen die behördlichen Erkenntnismöglichkeiten u. a. durch Einrichtung eines bundesweiten elektronischen Registers über sog. Drittstaatsausländer-Vereine optimiert und der Vollzug von Vereinsverboten flexibilisiert und kostengünstiger gestaltet werden. Für zu weit gehend halte ich vor allem die geplanten Regelungen zur Einrichtung eines allgemeinen bundesweiten elektronischen Registers über Vereine von Ausländern aus Drittstaaten.

## 7.2 Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und das Stasi-Unterlagen-Gesetz (StUG)

*Neben dem Umgang mit Stasiunterlagen beherrschte die Neuregelung des StUG die Diskussion während der Berichtsperiode.*

Das Stasi-Unterlagen-Gesetz vom 20. Dezember 1991 enthielt Fristen, nach deren Ablauf die Unterlagen nicht mehr zur Überprüfung einer Tätigkeit für den Staatssicherheitsdienst verwendet und die Tätigkeit für die Stasi dem Mitarbeiter im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden sollten. Die bisweilen emotionsgeladen geführte Diskussion zwischen den Positionen einer Resozialisierung auch in diesem Bereich und dem Vorwurf einer Schlussstrich-Mentalität führte letztlich zu einem mit großer Mehrheit gefundenen Kompromiss (Nr. 7.2.1), in dem auch ich eine akzeptable Lösung sehe.

Im Berichtszeitraum habe ich zwei Außenstellen der BStU kontrolliert und die Arbeit der Behörde durch mehrere Beratungen auf Arbeits- und Leitungsebene begleitet. Ich kann dabei ein weiteres Mal eine konstruktive Zusammenarbeit und einen sorgfältigen Umgang mit den sensiblen Unterlagen bescheinigen.

### 7.2.1 7. Änderung des Stasi-Unterlagen-Gesetzes

*Fristen für Überprüfung von Personen mit Stasi-Vergangenheit verlängert.*

Mit dem Ablauf von im Stasi-Unterlagen-Gesetz (StUG) vorgesehenen Fristen zum 29. Dezember 2006 wäre die Verwendung von Stasiunterlagen zur Überprüfung von Personen nach den einschlägigen beamtenrechtlichen und sonstigen Vorschriften generell unzulässig geworden. Die mit der Novelle vom 21. Dezember 2006 beschlossenen neuen Regelungen ermöglichen nun weiterhin Überprüfungen für einen eingeschränkten Personenkreis. Personen, die sich in gesellschaftlich oder politisch herausge-

hobenen Positionen befinden, z. B. Mitglieder der Bundes- oder einer Landesregierung, Abgeordnete, hohe Beamten oder Soldaten sowie Richter, können weiter bis zum 31. Dezember 2011 überprüft werden. Unbefristet können im Interesse der Glaubwürdigkeit Personen auf eine Stasi-Tätigkeit überprüft werden, die von Amts wegen die Tätigkeit des Staatssicherheitsdienstes aufarbeiten. Dies gilt insbesondere für die BStU und die jeweiligen Landesbeauftragten für die Stasi-Unterlagen sowie deren Beschäftigte.

Durch eine Änderung darf die BStU auch weiter Identifizierungsdaten (u. a. Personenkennzeichen) des Zentralen Einwohnerregisters der DDR nutzen, weil häufig nur auf diese Weise die Identität inoffizieller Mitarbeiter der Stasi ermittelt werden kann; eine solche Regelung war der BStU bereits früher eingeräumt worden, aber am 31. Dezember 2005 ausgelaufen. Auch die Nutzung elektronischer Informations- und Kommunikationssysteme wurde neu geregelt. Dadurch wird es der BStU ermöglicht, insbesondere auch das Internet für Veröffentlichungen zu nutzen, wobei sie in diesen Fällen besonders sorgfältig prüfen muss, ob hierdurch eventuell Persönlichkeitsrechte verletzt werden könnten. Weitere Änderungen betreffen den Aktenzugang für Forschung und Medien und das Einsichtsrecht naher Angehöriger von Vermissten und Verstorbenen. Außerdem wurde ein Wissenschaftliches Beratungsgremium für die BStU eingerichtet. Gegen die Änderungen habe ich keine Bedenken erhoben.

## 7.3 Bundesmeldegesetz

*Durch die Föderalismusreform ist die bisherige Rahmengesetzgebung des Bundes für das Meldewesen in eine ausschließliche Gesetzgebungskompetenz überführt worden.*

Das Gesetz zur Änderung des Grundgesetzes (Föderalismusreform), das am 1. September 2006 in Kraft getreten ist, hat auch Auswirkungen auf das Meldewesen. Auch wenn die Gesetzgebungskompetenz durch die Föderalismusreform auf den Bund übergegangen ist, bedeutet das keineswegs, dass es in Zukunft nur noch ein riesiges Bundesmelderegister mit allen möglichen Daten geben kann. In der Vergangenheit wurden etliche Daten in die Melderegister aufgenommen, die dort eigentlich nichts zu suchen haben, etwa zu Waffenscheinen und die Steueridentifikationsnummer. Wenn jetzt über eine Neuordnung nachgedacht wird, muss auch der Datenumfang einer kritischen Überprüfung unterzogen werden. Ansonsten wäre zu befürchten, dass die Einführung eines Bundesmelderegisters gegenüber den bisherigen, voneinander abgeschotteten Registern zu neuen Zugriffswünschen von weiteren Stellen führen und damit den Datenschutz verschlechtern würde. Grundsätzlich muss gelten: Jede Behörde darf nur die Daten erhalten, die sie für ihre Aufgaben benötigt. Sofern für bestimmte kommunale Aufgaben zusätzliche Daten benötigt werden, gehören diese nicht in ein Bundesregister, sondern sie müssen auch weiterhin in der Verantwortung der Gemeinden geführt werden und der Zugriff muss sich auf kommunale Stellen beschränken.

Ich trete dafür ein, die Neukonzeption des Meldewesens dazu zu nutzen, den Datenschutz für die Bürgerinnen und Bürger zu verbessern. Generell sollte überlegt werden, die bestehenden Widerspruchsregelungen durch Einwilligungslösungen abzulösen. So hielte ich es für denkbar, Melderegisterauskünfte nur noch mit Einwilligung der Betroffenen zu erteilen. Auch Gruppenauskünfte an Parteien zur Wahlwerbung, z. B. über Erstwähler, sollten deutlich eingeschränkt werden. Zumindest sollte aber, wie vom Bundesverwaltungsgericht gefordert, den Betroffenen die Möglichkeit eingeräumt werden, der Weitergabe von Meldedaten für Marketingzwecke generell ohne Angabe von Gründen zu widersprechen. Manche Landesmelderegister enthalten in diesen Fragen bereits jetzt bessere Datenschutzbestimmungen als das Melderechtsrahmengesetz. Im Sinne von „best practices“ sollten alle Bundesbürger von diesen Errungenschaften profitieren. Eine Nivellierung auf dem jeweils niedrigsten Datenschutzniveau würde ich hingegen ablehnen.

Der Bundesinnenminister hat angekündigt, unverzüglich den Entwurf eines Bundesmeldegesetzes erarbeiten zu lassen. Mit der Problematik hatte sich zwischenzeitlich unter Federführung des BMI eine Bund-Länder-Arbeitsgruppe befasst und einen „Bericht der AG zur Fortentwicklung des Meldewesens“ vorgelegt. Darin wird für die Organisation des künftigen Meldewesens die Schaffung eines sog. „Mischmodells“ vorgeschlagen, wonach die lokalen Melderegister erhalten bleiben, jedoch um ein zentrales Bundesmelderegister ergänzt werden sollen.

Ich habe zugesagt, die Erarbeitung des Entwurfs eines Bundesmeldegesetzes konstruktiv zu begleiten. Eine der Hauptschwierigkeiten sehe ich bei einer so großen und umfassenden Datei in der organisatorischen und technischen Ausgestaltung des „Identitätsmanagements“, zumal die Verwendung eines Personenkennzeichens nach dem sog. „Volkszählungsurteil“ des Bundesverfassungsgerichts von 1983 verfassungswidrig wäre.

## 7.4 Reform des Personenstandsrechts – Erleichterung der Ahnenforschung

*Bei der Reform des Personenstandsrechts wird auch die Ahnenforschung erleichtert.*

Die seit langem geplante Reform des Personenstandsrechts (vgl. 20. TB Nr. 6.7) hat nun doch noch Gestalt angenommen. Nachdem eine erste Vorlage aus dem Jahre 2005 aufgrund der vorgezogenen Bundestagswahl der Diskontinuität anheim fiel, hat die Bundesregierung im Juni 2006 den Entwurf eines Gesetzes zur Reform des Personenstandsrechts (Personenstandsrechtsreformgesetz – PStRG) eingebracht. Der Bundesrat hat dem Gesetz am 15. Dezember 2006 zugestimmt. Durch das Gesetz werden insbesondere die elektronischen Möglichkeiten zur Registerführung und zur Kommunikation mit dem Bürger sowie mit Behörden und anderen Stellen eröffnet. Ferner wird auch der Zugang vor allem zu den älteren Personenstandseintragungen erleichtert. Nach Ablauf der Fristen für die Führung der Personenstandsregister ist nunmehr eine Nutzung nach den allgemeinen archivrechtlichen Regeln vorgesehen. Eine weitere Erleich-

terung bei der Nutzung der Register ist für Geschwister der beurkundeten Person vorgesehen.

Gegen die Änderungen bestanden keine datenschutzrechtlichen Bedenken.

## 7.5 Volkszählung 2011 – Der Countdown hat begonnen

*1983 sorgte die geplante Volkszählung für große Aufregung und führte zu breiten Protesten in der Bevölkerung. Für die angesetzte neue Zählung erwarte ich keine vergleichbaren Diskussionen.*

Jetzt steht fest: Deutschland wird sich an der 2010/2011 anstehenden EU-weiten Volkszählungsrunde mit einem registergestützten Verfahren beteiligen. Auf Grund der Ergebnisse des Zensustestlaufs in den Jahren 2001 bis 2003 (vgl. 20. TB Nr. 6.12) hat das Bundeskabinett am 29. August 2006 einen entsprechenden Beschluss gefasst. Das BMI hat inzwischen einen Referenten-„Entwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011“ vorgelegt. Im Wesentlichen wird darin der Inhalt und Aufbau eines umfassenden Adress- und Gebäuderegisters geregelt, das alle in Deutschland vorhandenen Gebäude, Wohnungen und Anschriften der Gebäudeeigentümer oder -verwalter für die vorgesehene postalische Gebäude- und Wohnungszählung enthalten soll. Diese Datei soll zudem das zentrale Instrument für die Erhebungsorganisation und -unterstützung beim registergestützten Zensus sein, auf das alle Verfahren, für die ein Adress- und Gebäudebezug besteht, zurückgreifen sollen. Das Register wird gespeist aus Daten der Vermessungsbehörden, der Meldebehörden und der Bundesagentur für Arbeit. Die Aufbauarbeit soll bis zum 31. Dezember 2010 abgeschlossen sein. Spätestens 6 Jahre nach dem Zensusstichtag soll das Register gelöscht werden.

Gegen die Grundkonzeption der Volkszählung habe ich keine datenschutzrechtlichen Bedenken.

Datenschutzrechtlich kritisch sehe ich hingegen die geplante Einführung eines Systems der Georeferenzierung unterhalb der Gemeinde- oder Stadtteilebene durch die erstmalige Erhebung von geografischen Gebäudekoordinaten für jedes einzelne Gebäude. Diese sollen von den Landesvermessungsbehörden an das StBA für eine kleinräumige Darstellung der Zensusergebnisse übermittelt werden. Nach der Entwurfsbegründung bestehe der Vorteil dieser Georeferenzierung in der Möglichkeit, Daten nach Bedarf kleinräumig zusammen zu fassen, ohne an vorgegebene Verwaltungsgrenzen gebunden zu sein. Im Entwurf wird ausgeführt, dass eine verlässliche Methode der Anonymisierung derartiger georeferenzierter Ergebnisse erst noch entwickelt werden muss. Gedacht ist dabei an eine Art räumlicher „Gitterzelle“ anstelle der adressscharfen Koordinaten.

Ich hatte bereits bei einer ersten Präsentation derartiger Vorstellungen durch das StBA auf die mit dieser Methode verbundenen Gefahren für die informationelle Selbstbestimmung hingewiesen. Durch die vielfältige Nutzung von statistischen Ergebnissen ergeben sich vielfältige Möglichkeiten, verschiedene Ergebnisse und Analysen für einen geographischen Bezugspunkt zu kombinieren, sie quasi wie Folien übereinander zu legen, und hierdurch für ganz bestimmte geographische Raumeinheiten sehr aussagekräftige und umfassende Informationen zu erhalten. Die so erreichte Informationsdichte für kleine Raumeinheiten birgt ein hohes Reidentifizierungsrisiko. Dieses Risiko wird dadurch verstärkt, dass künftig andere Statistiken georeferenziert werden sollen. Damit wird es zukünftig möglich sein, statistische Ergebnisse aus verschiedenen Bereichen in zahllosen Varianten kleinräumig zu kombinieren. Die für die Datenerhebung im Statistikbereich typische Verwendbarkeit der Erhebungsdaten für die unterschiedlichsten Zwecke würde hierdurch drastisch erweitert. Es liegt zudem auf der Hand, dass die kleinräumige Darstellung statistischer Ergebnisse auch die Risiken der individuellen Profilbildung (s. u. Nr. 9.1) deutlich erhöhen wird.

Die mit der Georeferenzierung verbundenen Gefahren werden in der Begründung des Gesetzentwurfs zwar durchaus gesehen. Insoweit ist von noch zu entwickelnden Anonymisierungsmethoden die Rede, die den Belangen des Datenschutzes Rechnung tragen sollen. Leider ist dem Entwurf über die Absicht hinaus nichts Konkretes zu entnehmen.

## 7.6 Datenschutzgerechter Zugang von Wissenschaftlern zu statistischen Einzelangaben

*Angesichts der steigenden Nachfrage nach individuell für bestimmte Forschungsvorhaben erstellten Einzeldatenbeständen prüft das StBA zur Zeit die Einrichtung eines Wissenschaftsservers für wissenschaftliche Analysen.*

Die von den Forschungsdatenzentren des StBA und der Statistischen Landesämter (StLÄ) eröffneten Möglichkeiten des Zugangs zu statistischen Einzeldaten haben sich bewährt und werden intensiv genutzt (vgl. auch 20. TB, Nr. 24.3). Inzwischen hat auch das gemeinsame FDZ der StLÄ seine Arbeit aufgenommen und bietet dezentral an den Standorten der Landesämter Zugangsmöglichkeiten zu Einzeldaten für die wissenschaftliche Forschung. Beide FDZ eröffnen an allen Standorten Zugang zu demselben Einzeldatenbestand und einheitliche Zugangsmöglichkeiten, nämlich on-site den Gastwissenschaftlerarbeitsplatz und off-site die für eine Vielzahl von Forschungsinteressen aus verschiedenen Disziplinen erstellten so genannten Scientific Use Files und das kontrollierte Datenfernrechnen. Von diesen Zugangsmöglichkeiten bieten nur der Gastwissenschaftlerarbeitsplatz im FDZ und das kontrollierte Fernrechnen das volle Analysepotential von Einzeldaten, wobei die erstgenannte Zugangsmöglichkeit für die Wissenschaftler, die zweite für die Statistischen Ämter sehr aufwändig ist. Angesichts der steigenden Nachfrage der Wissenschaft nach dem vollen Datenmaterial bei knapper werdenden finanziellen und personellen Ressourcen bei den FDZ des Bundes und der Länder wurde vom StBA, in Anlehnung an in anderen EU-Staaten praktizierte Verfahren, das Modell des Wis-

senschaftsservers entwickelt, durch das der Gastwissenschaftlerarbeitsplatz quasi an den normalen Arbeitsplatz des Forschers exportiert werden soll.

Auch bei diesem Verfahren muss das Statistikgeheimnis insbesondere beim Export der Einzeldaten gewährleistet werden. Das StBA beabsichtigt, das Konzept in einer internen Machbarkeitsstudie zusammen mit den StLÄ zu testen. Ein Schwerpunkt des Tests wird die Entwicklung von Vorkehrungen zum Schutz der statistischen Geheimhaltung sein. Ich werde die Ergebnisse des Tests sorgfältig prüfen. Der Export des Gastwissenschaftlerarbeitsplatzes muss aus datenschutzrechtlicher Sicht dieselbe Sicherheit bieten wie der Arbeitsplatz in den Forschungsdatenzentren.

## 8 Finanzwesen

### 8.1 Identifikationsnummer für steuerliche Zwecke (Steuer-ID) wird eingeführt

*Die Steuer-ID kommt. Wenn auch einige datenschutzrechtliche Forderungen berücksichtigt sind, bleiben grundlegende Zweifel an dem Vorhaben bestehen.*

Die Einführung der Steuer-ID und damit die Einrichtung eines zentralen Registers aller in Deutschland steuerpflichtigen Personen wurde mit dem Steueränderungsgesetz 2003 beschlossen (§§ 139a ff. Abgabenordnung – AO). Mit der vorgesehenen Datenbank wird erstmals ein zentrales Register der gesamten Bevölkerung geschaffen, in dem neben den Personalien auch die jeweils aktuellen Anschriften erfasst sind. Diese Daten müssen von den kommunalen Melderegistern übermittelt werden.

Zwar konnte ich im Gesetzgebungsverfahren eine Reduzierung des Datenkatalogs der künftigen Datei beim Bundeszentralamt für Steuern (BZSt) und eine strikte Zweckbegrenzung auf steuerliche Zwecke erreichen, die Einführung der Steuer-ID jedoch nicht verhindern (vgl. 20. TB Nr. 8.2). Nach dieser grundsätzlichen Entscheidung konnte ich nur noch den Erlass der erforderlichen Rechtsverordnung nach § 139d AO und damit die datenschutzgemäße Einführung der Steuer-ID begleiten.

Trotz mehrfacher Sachstandsanfragen meinerseits legte das Bundesministerium der Finanzen (BMF) zunächst keinen Entwurf dieser Rechtsverordnung vor, sondern bereitete Tests und einen Probebetrieb vor und forderte von den Einwohnermeldeämtern ausgewählter Länder die Übermittlung von Daten aus ihren Melderegistern, weil es der Auffassung war, für einen Probebetrieb sei eine Rechtsverordnung noch nicht erforderlich. Ich wies das BMF darauf hin, dass eine derartige Datenübermittlung ohne Rechtsverordnung auch für Testzwecke unzulässig ist. Nachdem die Landesbeauftragten für den Datenschutz auch die Kommunen über meine Rechtsauffassung informiert hatten, sahen diese von Datenübermittlungen ab, und das BMF brachte schließlich einen ersten Entwurf einer Rechtsverordnung zur Einführung der Steuer-ID ein.

An den Beratungen dieses Verordnungsentwurfs habe ich mich intensiv beteiligt. Dabei konnte ich erreichen, dass

- die Speicherung des für die Vergabe der Steuer-ID erforderlichen „vorläufigen Bearbeitungsmerkmals – VBM“ gesetzlich geregelt wird, was eine Änderung der Bundesmeldedatenübermittlungsverordnung und des Melderechtsrahmengesetzes erforderte,
- Löschungsregelungen, insbesondere für die Daten des Probebetriebs und das VBM aufgenommen wurden,
- eine unverzügliche Information der Steuerpflichtigen über die Vergabe der Steuer-ID und alle beim BZSt gespeicherten Daten erfolgt,
- detaillierte Regelungen zur sicheren Datenübermittlung getroffen wurden und
- auch für den Test bzw. Probebetrieb genaue Regelungen, insbesondere im Hinblick auf die zu übermittelnden Speichersachverhalte, Löschfristen und Sicherheitsanforderungen bei der Datenübermittlung in der Verordnung festgelegt wurden.

Nicht durchsetzen konnte ich mich mit der Forderung, die Steuer-ID nicht schon bei der Geburt, sondern erst bei einer tatsächlichen persönlichen Steuerpflicht zu vergeben. Diese Forderung war auch im parlamentarischen Bereich bei den Beratungen zum Steueränderungsgesetz 2003 erhoben worden (vgl. 20. TB Nr. 8.2).

Hinsichtlich der nunmehr erlassenen Rechtsverordnung bleiben meine grundlegenden Zweifel an dem Gesamtvorhaben bestehen. Es ist nicht zu erkennen, dass effektive Besteuerungsverfahren und Bekämpfung der Steuerhinterziehung zukünftig nur möglich sein sollen, wenn alle Bürgerinnen und Bürger von Geburt an lückenlos registriert und mit einer lebenslangen Identifikationsnummer versehen werden. Auch sehe ich weiterhin die Gefahr, dass die von mir erreichte Zweckbindung schon bald durch entsprechende Gesetzesänderungen aufgeweicht und die jetzt beim Bundeszentralamt für Steuern entstehende Datenbank für eine Vielzahl anderer Zwecke genutzt werden wird. Das Kontenabrufverfahren (s. u. Nr. 8.2) und die LKW-Maut (s. u. Nr. 12.1) sind dafür anschauliche Beispiele.

Ich werde das weitere Verfahren zur Vergabe der Steuer-ID, insbesondere den Testbetrieb und den Aufbau sowie die Nutzung der Datenbank beim BZSt, aufmerksam begleiten.

### 8.2 Kontenabruf durch die Finanzämter und andere Behörden

*Obwohl eine Entscheidung des Bundesverfassungsgerichts zur Rechtmäßigkeit des Kontenabrufverfahrens noch aussteht, will die Finanzverwaltung das Volumen in 2007 weiter auf bis zu 5 000 Abfragen pro Tag steigern.*

Immer wieder musste ich mich im Berichtszeitraum mit dem Verfahren zum automatisierten Abruf von Kontostammdaten beschäftigen, das durch das Gesetz zur Förderung der Steuerehrlichkeit Ende 2003 eingeführt worden war (vgl. 20. TB Nr. 8.3).

Dadurch wurde den Finanz- und anderen Behörden und auch Gerichten der Zugriff auf Kontenstammdaten (u. a. Name, Geburtsdatum, Anzahl und Nummern der Konten, nicht jedoch Kontostand oder -bewegungen) der Bürger ermöglicht (§ 93 Abs. 7 und 8 der Abgabenordnung – AO). Die Abfrage erfolgt über das Bundeszentralamt für Steuern (BZSt).

Die Banken müssen die Kontostammdaten seit dem 1. April 2003 in besonderen Dateien bereitstellen. Die Abfragen durften ursprünglich gemäß § 24c Kreditwesengesetz (KWG) nur zur Bekämpfung illegaler Finanztransaktionen im Bereich des Terrorismus und der organisierten Kriminalität erfolgen. Das o. g. Gesetz hat die Zwecke des Kontenabrufs auf die „Festsetzung und Erhebung" von Steuern erweitert. Dies wurde damit begründet, dass die Finanzverwaltung die Möglichkeit haben müsse, nicht deklarierte Kapitalerträge aufzuspüren.

Schon im Gesetzgebungsverfahren hatte ich auf datenschutzrechtliche Mängel des Gesetzes hingewiesen (s. Kasten zu Nr. 8.2). Gegen die Regelungen wurden Ende 2004 Verfassungsbeschwerden eingereicht, über die das Bundesverfassungsgericht (BVerfG) noch nicht ent-

Kasten zu Nr. 8.2

**Datenschutzrechtliche Kritik**

Datenschutzrechtlichen Nachbesserungsbedarf an den Vorschriften zum Kontenabruf nach § 93 AO sehe ich in folgenden Punkten.

**Normenklarheit**

Die Regelungen in § 93 Abs. 8 Abgabenordnung (AO) entsprechen nicht dem Gebot der Normenklarheit. Es wird nicht geregelt, welche Behörden zu welchem Zweck eine Abfrage durchführen dürfen. Auch die Zulässigkeit der Anfragen ist nicht gesetzlich geregelt. Das Gesetz räumt anderen Behörden dann eine Abfragebefugnis ein, wenn die gesetzlichen Vorschriften, die sie ausführen, an Begriffe des Einkommenssteuerrechts anknüpfen, ohne dass diese konkret benannt werden. Zwar sind in einem vom Bundesfinanzministerium (BMF) herausgegebenen Anwendungserlass zur AO (AEAO – vgl. Nr. 8.2) sieben Gesetze aufgeführt, die nach Ansicht des BMF zur Abfrage berechtigen. Damit wird aber nicht abschließend und für den Betroffenen nachvollziehbar geregelt, welche Stellen für welche Zwecke Kontenabrufe veranlassen können. Damit bleibt der Anwendungsrahmen dieser Vorschriften gesetzlich zu unbestimmt.

**Verhältnismäßigkeit**

Eine Einschränkung des Grundrechts auf informationelle Selbstbestimmung ist nur zulässig, soweit diese zur Erreichung des jeweiligen Zwecks geeignet, erforderlich und angemessen, also verhältnismäßig ist. Zur Wahrung des Verhältnismäßigkeitsprinzips muss der Gesetzgeber zwischen dem Allgemeininteresse (gleichmäßige Besteuerung) und den Individualinteressen der Betroffenen einen angemessenen Ausgleich herbeiführen (BVerfGE 100, 313, (376)). Dies wurde im Gesetz nicht angemessen berücksichtigt.

Zwar sollen nach dem AEAO die Kontenabfragen anlassbezogen und zielgerichtet im Einzelfall durchgeführt werden. Dabei ist die Erforderlichkeit eines Kontenabrufs von der zuständigen Finanzbehörde nach pflichtgemäßem Ermessen anhand einer Prognoseentscheidung zu beurteilen. Dies schließt jedoch nicht eine umfassende Kontenabfrage als „Routine" bei der Bearbeitung einer Steuererklärung aus. Um „Routineabfragen" auf dem datenschutzrechtlich sensiblen Gebiet der Steuerdaten und des Bankgeheimnisses nach § 30a AO entgegen zu wirken, hätte im Gesetz geregelt werden müssen, wer in den entsprechenden Behörden und Gerichten eine Kontenabfrage anordnen bzw. darum ersuchen darf.

**Transparenz**

Datenschutzrechtlich problematisch bleibt, dass der betroffene Steuerzahler – jedenfalls zunächst – nichts von dem Kontenabruf erfährt. Zwar sieht der AEAO vor, dass der Betroffene nachträglich, z.B. mit dem nächsten Steuerbescheid, über den Kontenabruf zu informieren ist. Auch wenn damit die Transparenz für Abrufe nach § 93 Abs. 7 AO in gewissem Umfang gegeben ist, halte ich eine gesetzliche Regelung für erforderlich, nach der ein Betroffener grundsätzlich zu unterrichten ist, wenn ohne sein Wissen seine personenbezogenen Daten erhoben, verarbeitet oder genutzt werden. Eine solche Regelung ist insbesondere deshalb unverzichtbar, weil der AEAO für Fälle nach § 93 Abs. 8 AO keine Wirkung entfalten kann, da er Behörden außerhalb der Finanzverwaltung nicht bindet.

Neben einer nachträglichen Benachrichtigung halte ich es für notwendig, dass die Betroffenen vor einer Kontenabfrage über deren Möglichkeit und Voraussetzungen informiert werden. Weiter müssten die Informationen auch eine Aussage über die verantwortliche Stelle sowie über die Zweckbestimmung, Verarbeitung oder Nutzung – wie in § 19a BDSG – enthalten, um dem substanziellen Anspruch der Betroffenen auf eine tatsächlich wirksame gerichtliche Kontrolle zu entsprechen.

**Verfahrenssicherung**

Das Gesetz enthält keine Dokumentationspflichten. Ohne entsprechende Dokumentation ist es für den Betroffenen und die Gerichte schwierig, die tatsächlichen Abläufe nachzuvollziehen. Zu dokumentieren wäre z. B., wer aus welchen Gründen eine Kontenabfrage angeordnet hat und warum diese erforderlich war.

schieden hat. Im Rahmen einer Folgenabwägung hat es mit Beschluss vom 22. März 2005 jedoch darauf verzichtet, das Gesetz mit einer einstweiligen Anordnung auszusetzen, so dass die Vorschriften am 1. April 2005 in Kraft getreten sind. Ausschlaggebend war, dass das Bundesministerium der Finanzen (BMF) kurz zuvor einen Anwendungserlass zur Abgabenordnung (AEAO) herausgegeben hatte, der einen Missbrauch des Verfahrens ausschließen und eine unberechtigte Datenabfrage verhindern sollte.

Wie die Möglichkeit der Kontenabfragen in der Praxis genutzt wird, haben meine Länderkollegen bei den antragstellenden Behörden und ich beim BZSt mehrfach kontrolliert. Dabei wurden eine Reihe von Mängeln festgestellt. So wurden Kontenabrufe von unbefugten Personen angeordnet, Vordrucke falsch oder unvollständig ausgefüllt und die Kontenabrufe falsch begründet, Ermessenserwägungen nicht durchgeführt bzw. nicht dokumentiert, Betroffene nicht über den Kontenabruf informiert oder ihnen keine Gelegenheit gegeben, selbst die erforderlichen Auskünfte zu erteilen. Außerdem wurden Kontenabrufe entgegen den gesetzlichen Bestimmungen protokolliert und es wurden häufig mehr Daten zur Verfügung gestellt, als von den antragstellenden Behörden benötigt wurden. Die Landesbeauftragten für den Datenschutz (LfD) und ich haben hier auf Abhilfe gedrungen. Auch wenn noch nicht alle Mängel behoben sind, arbeite ich gemeinsam mit allen beteiligten Stellen an entsprechenden Lösungen. So wurde ein Vordruck entwickelt, mit dem sich systematisch die Voraussetzungen für eine solche Maßnahme prüfen und dokumentieren lassen. Der Vordruck wurde inzwischen vom BMF mit den Landesfinanzministerien erörtert und überwiegend von den Ländern übernommen.

Ein weiteres Problem sehe ich darin, dass vom BZSt Betroffenen bisher keine Auskunft darüber erteilt wird, ob ein sie betreffender Kontenabruf durchgeführt wurde. Das BMF vertritt die Auffassung, eine Auskunftserteilung sei nicht erforderlich, da die Betroffenen regelmäßig von den Abrufbehörden informiert würden. Zudem bestünde die Gefahr, dass eine Auskunftserteilung den Ermittlungszweck gefährden könnte, was jedoch nur von der Abrufbehörde beurteilt werden könne. Diese Auffassung vermag nicht zu überzeugen, zumal die datenschutzrechtlichen Kontrollen ergeben haben, dass die Betroffenen regelmäßig nicht über den erfolgten Kontenabruf informiert werden (s. o.). Auch ist nicht ersichtlich, wie der Ermittlungszweck gefährdet werden könnte, wenn der Kontenabruf bereits erfolgt ist. Das BZSt muss dem Betroffenen daher die begehrte Auskunft erteilen.

Das Beispiel zeigt einmal mehr, dass die Auskunftsansprüche der Betroffenen dringend in der AO geregelt werden müssen. Diese Forderung wird von den Datenschutzbeauftragten seit Jahren erhoben (vgl. 20. TB Nr. 8.1). Das BMF hat zwar hierzu kürzlich erneut seine Bereitschaft signalisiert; ein Entwurf liegt mir aber noch nicht vor.

Darüber hinaus habe ich festgestellt, dass Kontenabrufe derzeit in den weitaus meisten Fällen nicht, wie in der Gesetzesbegründung ausgeführt, zur Entdeckung hinterzogener Kapitalerträge, sondern im Rahmen von Zwangsvollstreckungen erfolgen. Das BMF sieht die Vollstreckung als Teil des Erhebungsverfahrens und hält daher Kontenabrufe auch in diesem Bereich für zulässig. Ob diese Rechtsauffassung vom Bundesverfassungsgericht geteilt wird, bleibt abzuwarten.

Unterdessen hat die Finanzverwaltung die Zahl der Kontenabrufe ständig gesteigert. Während anfangs 60 Abfragen pro Tag möglich waren, sind es heute schon über 100. Im Jahr 2007 soll die Abfragemöglichkeit auf täglich 5 000 Abfragen erhöht werden. Ich halte dies angesichts der anhängigen Verfahren vor dem BVerfG für problematisch. Schließlich gibt es im BMF Überlegungen, doch noch die von mir im Gesetzgebungsverfahren als Alternative zum Kontenabrufverfahren angeregte Abgeltungssteuer einzuführen, was zwangsläufig Auswirkungen auf das Verfahren hätte.

## 8.3 Schwarzarbeitsbekämpfungsgesetz – Erfahrungen in der Praxis

*Fast 7 000 Zollbedienstete bekämpfen bundesweit die Schwarzarbeit. Bei den Ermittlungen vor Ort bleiben Datenschutzvorschriften jedoch oftmals unbeachtet.*

Am 1. August 2004 trat das Gesetz zur Bekämpfung der Schwarzarbeit und illegalen Beschäftigung (SchwarzArbG) als Teil eines Artikelgesetzes in Kraft, mit dem die Verfolgungszuständigkeit für diese Delikte auf Bundesebene bei der Zollverwaltung gebündelt wurde. Aus Beschäftigten der Bereiche Zoll, Arbeitsverwaltung, Post, Telekom und Bahn entstand bei den Hauptzollämtern die Finanzkontrolle Schwarzarbeit (FKS) mit derzeit etwa 7 000 Bediensteten an 113 Standorten.

Nachdem ich bereits das Gesetzgebungsverfahren intensiv begleitet hatte (vgl. 20. TB Nr. 8.4), habe ich die Auswirkungen und die datenschutzgerechte Anwendung der Vorschriften in der Praxis geprüft. Dabei hat mich besonders interessiert, aus welchen Anlässen Ermittlungen aufgenommen bzw. Kontrollen durchgeführt werden und welche Kriterien Art und Umfang der Ermittlungen bestimmen.

Die Kontrollen erfolgen entweder aufgrund von Hinweisen oder verdachtsunabhängig, wobei derzeit noch die verdachtslosen Ermittlungen überwiegen. Schwerpunkte liegen bei Baustellen und Gastronomiebetrieben, weil hier nach Angaben der FKS oftmals Leistungsmissbrauch beim Arbeitslosengeld I und II und Verstöße gegen das Ausländerrecht auftreten. Im Prüfungsfall werde möglichst die gesamte Baustelle oder Gastwirtschaft umfassend kontrolliert (jeder Angetroffene; zum Ablauf vgl. Kasten zu Nr. 8.3).

Zahlreiche Beschwerden zeigen, dass gerade bei den Befragungen durch die FKS Datenschutzvorschriften bisweilen unbeachtet blieben. Beispielsweise wurden Mitarbeiter in Restaurants und auf Messen während des normalen Betriebs und vor unbeteiligten Gästen bzw. Kunden befragt und dabei umfangreiche persönliche Daten (Name, Geburtsdatum, Gehalt) erhoben. Ich habe daher für diese Befragungen klare Dienstanweisungen und entsprechende Schulungen der Mitarbeiter gefordert, was das BMF auch zugesagt hat.

Bei Aktenprüfungen habe ich in Ermittlungsakten umfangreiche Daten gefunden, die für den Ermittlungszweck nicht benötigt wurden, wie z. B. Lebensläufe, ärztliche Bescheinigungen und sämtliche Angaben zum Leistungsbezug durch die Bundesagentur für Arbeit (BA). Nach meiner Auffassung sind auch bei diesen Ermittlungen Datenerhebungen nur insoweit zulässig, als sie für den jeweiligen Ermittlungszweck erforderlich sind. Insbesondere habe ich darauf hingewiesen, dass die FKS keinen umfassenden Zugriff auf die Leistungsdatenbank der BA benötigt.

Weitere Eingaben erreichten mich zu einer besonderen Form der „Öffentlichkeitsarbeit". Einige FKS-Standorte hatten auf ihre Briefe als Absender neben der neutralen Bezeichnung „Hauptzollamt" deutlich „Finanzkontrolle Schwarzarbeit" angegeben. Damit verstießen sie neben datenschutzrechtlichen Vorschriften auch gegen einen ausdrücklichen Erlass des BMF, das aufgrund meiner Intervention die FKS-Standorte wiederholt auf die eindeutige Gesetz- und Weisungslage hingewiesen hat.

Keine datenschutzrechtlichen Mängel wurden bei der Prüfung von zwei von der FKS genutzten und nunmehr bundesweit zur Verfügung stehenden IT-Verfahren festgestellt. Hier konnte ich mich davon überzeugen, dass den Benutzern nur die jeweils zulässigen Daten zur Verfügung stehen.

Auch in Zukunft werde ich die Arbeit der FKS aufmerksam begleiten. Das gilt besonders für die weiteren geplanten und in der Entwicklung befindlichen IT-Verfahren und die Durchführung der Mitarbeiterschulungen.

Kasten zu Nr. 8.3

**Was und wie prüft die Finanzkontrolle Schwarzarbeit**

Kontrollen erfolgen entweder gezielt aufgrund von Hinweisen oder verdachtsunabhängig. Es wird kontrolliert, ob

- Sozialleistungen zu Unrecht bezogen werden,
- bei ausländischen Arbeitnehmern die erforderlichen Arbeitsgenehmigungen vorliegen,
- ausländische Arbeitnehmer nicht zu ungünstigeren Arbeitsbedingungen als vergleichbare deutsche Arbeitnehmer beschäftigt werden,
- Arbeitgeber ihren Meldepflichten nachkommen und
- die Arbeitsbedingungen nach dem Arbeitnehmer-Entsendegesetz eingehalten werden.

Angetroffene Personen werden befragt, deren Auskünfte erfasst und überprüft. Nicht benötigte Daten werden vernichtet, sobald feststeht, dass kein Verfahren einzuleiten ist. In diesem Falle werden die Daten auch nicht erfasst. Sowohl Arbeitgeber als auch Arbeitnehmer sind gesetzlich verpflichtet, bei den Prüfungen mitzuwirken. Sie müssen die erforderlichen Auskünfte erteilen, Unterlagen vorlegen und das Betreten der Grundstücke und der Geschäftsräume des Arbeitgebers dulden. Bei Privaträumen ist hierzu jedoch ein gerichtlicher Durchsuchungsbefehl erforderlich. Die Prüfungen erfassen immer auch vergangene Zeiträume.

## 8.4 ELSTER-Portal und StDÜV

*Mit der Änderung der Steuerdatenübermittlungsverordnung können für die Finanzverwaltung „andere sichere Verfahren" als die qualifizierte elektronische Signatur zugelassen und damit u. a. Steuererklärungen im ELSTER-Verfahren auch ohne Unterschrift abgegeben werden. Dabei ist die nötige Datensicherheit noch nicht gewährleistet.*

Mit der Steuerdatenübermittlungsverordnung (StDÜV) des Bundesministeriums der Finanzen (BMF) wird für die Finanzverwaltung grundsätzlich die elektronische Übermittlung der im Besteuerungsverfahren erforderlichen Daten zugelassen. Gleichzeitig wird festgelegt, welche Sicherheitsanforderungen dabei erfüllt werden müssen. Rechtsgrundlage für die Verordnung ist § 87a Abs. 6 der Abgabenordnung (AO). Während bisher eine rechtsverbindliche Datenübermittlung in der Regel nur mit einer qualifizierten elektronischen Signatur zulässig war, sah diese Vorschrift bis zum 31. Dezember 2005 hiervon Ausnahmen vor. Ab dem 1. Januar 2006 hätte eine Datenübermittlung deshalb nur noch unter Verwendung der qualifizierten elektronischen Signatur erfolgen dürfen. Wegen ihrer immer noch geringen Verbreitung will das BMF jedoch auch künftig darauf verzichten, soweit ein anderes sicheres Verfahren eingesetzt wird, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt. Dabei ist an ein Authentisierungsverfahren gedacht, wie es beispielsweise beim ELSTER-Verfahren (elektronische Steuererklärung) schon eingesetzt wird. Hier kann anstelle der qualifizierten elektronischen Signatur zur Authentifizierung auch ein Softwarezertifikat benutzt werden, das auf der Festplatte oder einem Speicherstick gespeichert werden kann.

Bei der hierzu erforderlichen Änderung des § 87a Abs. 6 AO wollte das BMF für „andere sichere Verfahren" eine rechtliche Gleichstellung mit der qualifizierten elektronischen Signatur erreichen. Obwohl diese Verfahren nicht die gleiche Sicherheit aufweisen, sollte der Steuerpflichtige rechtlich wie bei Verwendung der qualifizierten elektronischen Signatur behandelt werden. Hätte danach jemand falsche Dokumente unter Nutzung der Authentifizierung des Steuerpflichtigen eingereicht, hätte dieser im Zweifel beweisen müssen, dass sie nicht von ihm stammen (Beweislastumkehr). Diesen Nachweis hätte er regelmäßig nicht führen können.

Ich habe mich daher an den Finanzausschuss des Deutschen Bundestages gewandt und konnte erreichen, dass auf diese Beweislastumkehr bei der Neufassung des § 87a Abs. 6 AO (BGBl. I S. 2878) verzichtet wurde. Außerdem wurde die Zulassung „anderer sicherer Verfahren" bis zum 31. Dezember 2011 befristet und eine Evaluierung vorgeschrieben. Im Hinblick auf diese Änderungen habe ich meine weiteren Bedenken gegen die Zulassung anderer sicherer Verfahren neben der qualifizierten elektronischen Signatur zurückgestellt.

Dieser Erfolg wurde jedoch teilweise dadurch zunichte gemacht, dass der Bundesrat zwischenzeitlich die StDÜV in einer Version gebilligt hat, in der meine gegenüber dem

BMF geäußerten Bedenken und eine entsprechende Entschließung der Datenschutzbeauftragten des Bundes und der Länder (vgl. Anlage 14) nicht berücksichtigt wurden.

Auch ein Schreiben des Vorsitzenden der Datenschutzkonferenz des Bundes und der Länder vom 5. Dezember 2006, das nochmals die datenschutzrechtlichen Probleme aufzeigte, hat den Bundesrat nicht davon abgehalten, der StDÜV ohne datenschutzrechtliche Nachbesserungen am 15. Dezember 2006 zuzustimmen.

Die von mir kritisierten Punkte könnten deshalb erst wieder bei einer Novellierung der StDÜV berücksichtigt werden.

## 9 Wirtschaft

### 9.1 Profilbildung verhindern

*Die Bildung von Persönlichkeits-, Nutzungs- und Kundenprofilen ist weiter dramatisch fortgeschritten, vor allem aufgrund neuerer Technologien und der Nutzung der neuen technischen Möglichkeiten, insbesondere durch die Auskunfteien.*

Auf das Problem der fortschreitenden Profilbildung habe ich bereits in meinem letzten Tätigkeitsbericht (vgl. 20. TB Nr. 11.7) hingewiesen. Der Deutsche Bundestag hatte die Bundesregierung mit Entschließung vom 17. Februar 2005 (Bundestagsdrucksache 15/4597) aufgefordert, zu prüfen, ob und wie der besorgniserregenden Entwicklung der Profilbildung entgegengewirkt werden könne. Leider sind bisher noch keine Maßnahmen in dieser Richtung ergriffen worden. Neben den steigenden Datenmengen und der ohnehin vielfältigen Verknüpfungsmöglichkeiten, hat sich eine neue Dimension der Nutzung der gesammelten Informationen herausgebildet: die Verknüpfung der Daten mit digitalen Stadtplänen und Landkarten, das sog. Geomarketing. Marktforscher verknüpfen Kaufverhalten, Krankheitsrisiken und Zahlungsmoral mit digitalen Landkarten. So werden anhand der Adressen individuelle Profile erstellt, unabhängig davon, ob die darin gespeicherten Angaben bezogen auf den Betroffenen zutreffen. Die Verantwortlichen sprechen davon, dass sie nur statistische Wahrscheinlichkeiten beschreiben würden, nicht jedoch Menschen. Doch genau hier liegt das Datenschutzproblem: Wer am „falschen“ Ort wohnt, wird pauschal negativ beurteilt und muss ggf. mit negativen Konsequenzen rechnen.

Das geltende Recht trägt diesen problematischen Entwicklungen nur unzureichend Rechnung. Es ist höchste Zeit für gesetzgeberisches Handeln.

**Gesetzliche Regelung von Scoreverfahren:**

Mittels Scoreverfahren werden Kunden anhand verschiedenster Kriterien nach ihrer wirtschaftlichen Leistungsfähigkeit benotet. Solche Verfahren spielen mittlerweile in fast allen Bereichen des Wirtschaftslebens eine Rolle und können für die Verbraucher immense Konsequenzen haben: Kunden mit schlechtem Score bekommen ungünstige Konditionen; sie zahlen höhere Zinsen für Kredite, können Waren nur per Vorkasse bestellen, müssen bei Anrufen in Call-Centern länger in der Warteschleife bleiben und werden oftmals als Vertragspartner gar nicht erst akzeptiert. Bei immer mehr wirtschaftlichen Entscheidungen sind Scorewerte von entscheidender Bedeutung. Die Prognose über das künftige Kauf- und Zahlungsverhalten von Personen wird maßgeblich durch Daten gewonnen, die keinen direkten Bonitätsbezug haben.

Für den Scorewert werden neben Angaben über das tatsächliche Verhalten des Betroffenen die unterschiedlichsten Daten gescort, wie z. B.:

- Soziodemographische Daten (z. B. Wohngegend mit überdurchschnittlich vielen Sozialhilfeempfängern; Straße, in der überwiegend Wirtschaftsmagazine abonniert werden);
- Wohnumfeldanalysen;
- repräsentative Beobachtungen (z. B. reale oder elektronische Straßenbegehungen);
- angekaufte Daten aus den verschiedensten Bereichen (z. B. Kfz–Daten vom Kraftfahrtbundesamt);
- sonstige Erfahrungswerte (z. B. Staatsangehörigkeit, Geschlecht).

Das hat zur Folge, dass die Bonität des Einzelnen auch ohne relevante individuelle Informationen, z. B. Zahlungsverhalten, Einkommens- und Vermögensverhältnisse, bewertet wird. Dem Betroffenen wird damit weitgehend die Möglichkeit genommen, durch eigenes rechtstreues Verhalten sein Erscheinungsbild in der Öffentlichkeit zu beeinflussen. Hinzu kommt, dass der Betroffene mangels Transparenz des Verfahrens ein „falsches Bild“ nicht berichtigen kann.

Dieser kritischen Entwicklung muss durch gesetzliche Regelungen entgegengewirkt werden.

Dabei sollte klargestellt werden, dass nur bonitätsrelevante Merkmale für die Berechnung des Scorewertes genutzt werden dürfen. Allein eine statistische Korrelation ist für die Einstellung in das Scoreverfahren keine hinreichende Bedingung (vgl. Nr. 9.2, die Ausführungen zu einer gleichgelagerten Regelung für Rating-Verfahren bei Banken im Rahmen von Basel II).

Für die Betroffenen (wie auch für die Aufsichtsbehörden) muss nachvollziehbar sein,

- welche Faktoren mit welcher Gewichtung in die Berechnung des Scorewertes einfließen,
- welche konkreten personenbezogenen Merkmale genutzt wurden,
- welche Merkmale den konkreten Scorewert der betroffenen Person negativ beeinflusst haben. Die maßgeblichen Merkmale sollten nach ihrer Bedeutung bzw. dem Grad ihres Einflusses auf den konkreten Scorewert mitgeteilt werden,
- jeder Betroffene sollte zudem die Möglichkeit erhalten, den Scorewert zu erfahren, der an einen bestimmten Vertragspartner übermittelt worden ist. Da im Regelfall der Scorewert bei jeder Abfrage neu generiert

wird, kann es nicht ausreichen, den gerade aktuellen Wert zum Zeitpunkt der Auskunftserteilung an den Betroffenen zu erfahren.

Nur unter diesen Voraussetzungen erhält der Betroffene die Möglichkeit, die Merkmale zu überprüfen und ggf. richtig zu stellen und bestimmte negativ gewichtete Faktoren gegenüber dem Vertragspartner zu erläutern.

**Gesetzliche Regelung für die Erhebung anonymisierter und georeferenzierter Daten**

Gerade in jüngster Zeit ist insbesondere durch den Fortschritt bei der Verknüpfung personenbezogener Daten mit geographischen Angaben (sog. Georeferenzierung) das Problem entstanden, dass mittels einer Anschrift das für diesen geographischen Punkt verfügbare Wissen (z. B. regionale Kreditausfallwahrscheinlichkeiten, kartierte Daten über Gesundheitsrisiken oder Lebenserwartung) einer dort wohnenden Person zugeordnet werden kann. Ebenso werden zunächst anonymisierte Daten durch die Verbindung mit einer bestimmten Adresse den dort wohnenden Personen zugerechnet.

So liefert das Kraftfahrtbundesamt (KBA) auf vertraglicher Basis Adressverlagen gegen Entgelt Daten über den Bestand von Pkw und Krafträdern in mikrogeographischer Gliederung. Der Adressverlag als Auftraggeber liefert eine flächendeckende Gebäudedatei inklusive Mikrozellen (durchschnittlich 20 Haushalte) an das KBA. Das KBA verknüpft diese Datei mit seinen eigenen Daten, indem Angaben über Pkw und Krafträder in die jeweiligen Gebäude eingezählt und auf die Gebäude bezogenen Mikrozellen verdichtet werden. Diese Datei liefert das KBA dann an den Auftraggeber.

Diese so aufbereiteten und ergänzten Daten werden von den Adressverlagen an Wirtschaftsunternehmen verkauft, die sie für Werbung, Markt– und Meinungsforschung auswerten und für Kundenprofile verwenden. In diese Scoreverfahren gehen auch die vom KBA übermittelten Daten ein. Selbst ursprünglich statistische Angaben, wie z. B. Bewohner eines bestimmten Hauses oder einer bestimmten Adresse seien zu 30 Prozent Eigentümer eines bestimmten Fahrzeugtyps, sind nur solange nicht personenbezogen, wie damit lediglich der Bezug zu mehreren Bewohnern bzw. Haushalten hergestellt wird. Werden diese Daten jedoch mit der Information verbunden, dass eine bestimmte Person an einer Adresse wohnt, so werden mit der individuellen Zuordnung der Wahrscheinlichkeiten die Daten personenbezogen. Spätestens jetzt finden die Vorschriften des BDSG Anwendung. Ein Auskunftsersuchen des Betroffenen vor diesem Zeitpunkt geht allerdings bislang ins Leere, da es insoweit an dem Personenbezug mangelt. Welche Informationen in den Scorewert eingeflossen sind, wie diese bewertet und an Dritte weitergegeben wurden, bleibt deshalb dem Betroffenen verborgen.

Die Verknüpfung von ursprünglich anonymisierten Informationen mit Identifikationsdaten oder mit georeferenzierten Daten bedarf dringend einer Regelung. Ich halte es für erforderlich, auch die Verwendung georeferenzierter Daten dem Anwendungsbereich des BDSG zu unterwerfen und angemessen zu schützen.

**Keine Auskunft ohne das Vorliegen eines kreditorischen Risikos**

Während sich bisher der Kreis der Geschäftspartner der klassischen Auskunfteien auf die kreditgebende Wirtschaft (Bankenbereich, Telekommunikationsunternehmen, Versandhandel) beschränkt hat, öffnen sich die Auskunfteien verstärkt auch anderen Sparten, die ebenfalls an der Bonität ihrer Kunden interessiert sind, obwohl sie kein kreditorisches Risiko eingehen. So hat z. B. die SCHUFA sowohl die Wohnungswirtschaft als auch die Versicherungswirtschaft, entgegen dem Votum der Datenschutzaufsichtsbehörden, an ihr Auskunftssystem angeschlossen.

Ganz überwiegend tragen Versicherungen kein über das allgemeine wirtschaftliche Risiko (in Form von Bearbeitungsgebühren oder Ertragserwartungen) hinausgehendes kreditorisches Risiko. Zahlt der Versicherte seine Versicherungsprämie nicht, erlischt der Versicherungsschutz. Der Versicherer wird von seiner Leistungspflicht befreit, er muss grundsätzlich nicht in Vorleistung treten. Die Wohnungswirtschaft sichert sich gegen Mietausfälle mittels Mietvorauszahlungen ab.

Die immer weitere Ausdehnung der Vertragspartner der Auskunfteien bedeutet eine noch breitere Streuung personenbezogener Daten praktisch aller Bürgerinnen und Bürger. Die Betroffenen werden in zunehmendem Maße und ohne ihr Wissen und Wollen in ihrem Verhalten abgebildet. Da Daten aus immer mehr Bereichen in den Datenbestand der Auskunfteien eingehen und auch abgerufen werden können, verschärft sich das Problem der Profilbildung. Ein negativer Eintrag in die Auskunfteisysteme, ob berechtigt oder unberechtigt, kann etwa dazu führen, dass der Betroffene keine Wohnung findet oder er keine Versicherungspolice bekommt.

Das Vorliegen eines kreditorischen Risikos sollte als Zulässigkeitsvoraussetzung für die Datenübermittlung von Auskunfteien an Dritte in das BDSG explizit aufgenommen werden, damit nicht jegliche Branchen bis hin zu potentiellen Arbeitgebern diverse Informationen bei Dritten über das Gegenüber einholen können, die für andere Zwecke erhoben wurden.

**Branchenspezifische Auskunftssysteme**

Nach geltendem Recht dürfen Daten, die eine Auskunftei in ihrem System gespeichert hat, an einen Dritten übermittelt werden, wenn dieser ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft machen kann und der Betroffene kein schutzwürdiges Interesse an der Nichtübermittlung hat. Diese generelle Regelung hat dazu geführt, dass Auskunfteien Zentraldateien mit umfassenden Informationen aufgebaut haben, auf die alle Partner der Auskunfteien ungefiltert Zugriff nehmen können.

Vermieter wenden sich z. B. vermehrt an Auskunfteien, um ein allgemeines und umfassendes Bonitätsprofil über einen Mietinteressenten zu erhalten.

Auch können sich Versicherungen, Ärzte etc. zunächst über die „weiße Weste“ ihrer Kunden oder Patienten informieren, bevor sie mit den Betroffenen Vertragsverhältnisse eingehen.

Durch gesetzliche Klarstellung sollte dafür gesorgt werden, dass umfassende Zentraldateien durch branchenspezifische Auskunftssysteme abgelöst werden. Um auch dem Schutzbedürfnis einzelner Wirtschaftssparten angemessen Rechnung zu tragen, sollte ihnen die Möglichkeit, sich über das Vorverhalten des potentiellen Vertragspartners zu informieren, nicht gänzlich verwehrt werden. Derartige Systeme sollten branchenspezifisch beschränkt werden. Das bedeutet, dass z. B. ein Vermieter Auskünfte darüber erhalten darf, ob der potentielle Mieter in früheren Mietverhältnissen negativ aufgefallen ist; nicht aber, ob dieser eine Versandhausrechnung nicht bezahlt hat.

Derartige branchenspezifische Ansätze haben sich im Ausland bewährt, etwa in Frankreich, das ein derart umfangreiches Auskunftssystem, wie es sich in Deutschland etabliert hat, nicht kennt.

**Folgenbeseitigungsanspruch**

Bislang steht der Betroffene elektronischen Warnsystemen weitgehend schutzlos gegenüber. Eingaben belegen, dass viele Bürger ohne eigenes Fehlverhalten in elektronische Warnsysteme geraten, sei es aufgrund einer Verwechslung oder durch nachlässiges oder nicht vertragskonformes Meldeverhalten von Teilnehmern solcher Systeme und/oder mangelnder Prüfung der Korrektheit der eingemeldeten Daten durch die Systembetreiber. Selbst wenn ein Datum als fehlerhaft erkannt und dies berichtigt wird, weiß der Betroffene nicht, an wen das Datum bereits übermittelt wurde und welcher Schaden dadurch bereits entstanden ist.

Dem könnte durch Einführung eines gesetzlichen Folgenbeseitigungsanspruchs in das BDSG entgegengewirkt werden. Dieser müsste bei Weitergabe unrichtiger Informationen oder bei rechtswidrigen Übermittlungen (z. B. bestrittener Forderungen) der verantwortlichen Stelle aufgeben, daraus resultierende Folgen für den Betroffenen zu beseitigen und zwar nicht nur im eigenen System, sondern auch überall dort, wo sich durch Fortpflanzung des Fehlers für den Betroffenen nachteilige Auswirkungen ergeben haben können. Konkret bedeutet dies, dass die Auskunfteien alle Stellen, an die sie das unrichtige Datum übermittelt haben, von der Unrichtigkeit verständigen müssen. Wenn das unrichtige Datum in einen Scorewert eingeflossen ist, so müsste dieser in berichtigter Form erneut an den Empfänger übermittelt werden. Dieser hätte dann dafür zu sorgen, dass negative Folgen, die sich aus dem falschen Scorewert für den Betroffenen ergeben haben, ebenfalls beseitigt würden.

## 9.2 Umsetzung von Basel II schafft eine gesetzliche Grundlage zum Ratingverfahren der Kreditinstitute

*Die Umsetzung der Eigenkapitalvereinbarung Basel II führt erstmals zu einer gesetzlichen Regelung des Ratingverfahrens. Wird sie auch Einfluss auf eine gesetzliche Regelung zum Scoreverfahren haben?*

Mit dem Gesetz zur Umsetzung der neugefassten Bankenrichtlinie und der Kapitaladäquanzrichtlinie (BGBl. I S. 2606) vom 17. November 2006 wurden inzwischen die Vorgaben von Basel II (vgl. 20. TB Nr. 11.5.3) in deutsches Recht umgesetzt. Dabei geht es nicht um die Bewertung der individuellen Kreditwürdigkeit eines Kunden im Rahmen konkreter Kreditentscheidungen. Vielmehr liegt der Schwerpunkt der neuen Vorschriften in der Ermittlung der Angemessenheit der Eigenmittelausstattung der Kreditinstitute und den hierfür künftig zur Verfügung stehenden Verfahren. Der Gesetzgeber gibt den Instituten dabei Vorgaben für die Nutzung unterschiedlicher Risikomessverfahren und für die Heranziehung sowohl externer Ratings als auch interner Schätzungen. Insbesondere die internen Schätzverfahren basieren auf der Erhebung und Verwendung personenbezogener Daten durch die Institute. Aus diesem Grund ist in § 10 Abs. 1 Sätze 3 bis 8 Kreditwesengesetz (KWG) erstmals eine bereichsspezifische Regelung für den Umgang mit personenbezogenen Daten im Zusammenhang mit den Risikomessverfahren geschaffen worden, an deren Entstehung ich maßgeblich mitgewirkt habe (vgl. Kasten zu Nr. 9.2).

Diese Regelung trägt einerseits dem Interesse der Institute und der Bankaufsicht am Aufbau und Betrieb solcher Systeme Rechnung, berücksichtigt andererseits aber auch die schutzwürdigen Interessen der Kunden. So werden Datenerhebung und Datenverwendung grundsätzlich nur in dem Umfang zugelassen, in dem diese Daten für den Aufbau und Betrieb des internen Ratingsystems erforderlich sind (Satz 3 Nr. 2). Darüber hinaus müssen diese Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar bonitätsrelevant sein (Satz 1 Nr. 1). Die in Frage kommenden bonitätsrelevanten Daten wie Einkommens-, Vermögens- und Beschäftigungsverhältnisse sind in einer Aufzählung von Kategorien enthalten (Satz 6); bedauerlicherweise ist diese Aufzählung nicht abschließend geregelt. Die Verwendung besonders sensibler Daten im Sinne von § 3 Abs. 9 BDSG wird jedoch ausgeschlossen. Die Daten sind nach Satz 7 zunächst beim Betroffenen zu erheben, allerdings ist auch der Zugang zu anderen Datenquellen wie z. B. Auskunfteien zulässig. Letzteres sehe ich sehr kritisch, weil die Gefahr besteht, über diese Quellen Daten in das Ratingsystem einzuführen, die den strengen Maßstäben der Bonitätsrelevanz nicht genügen.

Eine wichtige Frage blieb offen. Die neue Vorschrift des § 10 Abs. 1 KWG dient zwar allein der Implementierung eines bankaufsichtsrechtlich notwendigen Ratingsystems, regelt aber gleichzeitig den Umgang mit genau den perso-

nenbezogenen Daten, die eigentlich nur im konkreten Verhältnis „Institut/Kunde“ eine Rolle spielen, nämlich bei der Frage, ob und mit welchen Konditionen ein konkreter Kreditvertrag abgeschlossen werden kann. Diese Frage ist Gegenstand des Scoreverfahrens. Da sowohl beim Rating- als auch beim Scoreverfahren dieselben personenbezogenen Daten verwendet werden, ist davon auszugehen, dass das Ratingverfahren zumindest eine mittelbare Auswirkung auf das Scoreverfahren haben wird.

Aus diesem Grund habe ich dem Finanzausschuss des Deutschen Bundestages empfohlen, an den Regelungen in § 10 Abs. 1 KWG festzuhalten, im Gesetz aber klarzustellen, dass es sich um zwei verschiedene Verfahren handelt. Für das Scoreverfahren gelten die Regelungen des Bundesdatenschutzgesetzes, die durch die Vorschrift des § 10 Abs. 1 KWG nicht tangiert werden. Der Finanzausschuss hat mein Anliegen unterstützt, ist aber zu dem Ergebnis gelangt, dass das KWG nicht die geeignete Norm

Kasten zu Nr. 9.2

**§ 10 Abs. 1 Sätze 3 bis 8 Kreditwesengesetz**

Institute dürfen personenbezogene Daten ihrer Kunden, von Personen, mit denen sie Vertragsverhandlungen über Adressenausfallrisiken begründende Geschäfte aufnehmen, sowie von Personen, die für die Erfüllung eines Adressenausfallrisikos einstehen sollen, erheben und verwenden, soweit diese Daten

1. unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Bestimmung und Berücksichtigung von Adressenausfallrisiken erheblich und
2. zum Aufbau und Betrieb einschließlich der Entwicklung und Weiterentwicklung von internen Ratingsystemen für die Schätzung von Risikoparametern des Adressenausfallrisikos des Instituts erforderlich sind und es sich nicht um Angaben zur Staatsangehörigkeit oder Daten nach § 3 Abs. 9 des Bundesdatenschutzgesetzes handelt. Betriebs- und Geschäftsgeheimnisse stehen personenbezogenen Daten gleich. Zur Entwicklung und Weiterentwicklung der Ratingsysteme dürfen abweichend von Satz 3 Nr. 1 auch Daten erhoben und verwendet werden, die bei nachvollziehbarer wirtschaftlicher Betrachtungsweise für die Bestimmung und Berücksichtigung von Adressenausfallrisiken erheblich sein können. Für die Bestimmung und Berücksichtigung von Adressenausfallrisiken können insbesondere Daten erheblich sein, die den folgenden Kategorien angehören oder aus Daten der folgenden Kategorien gewonnen worden sind:
   1. Einkommens-, Vermögens- und Beschäftigungsverhältnisse sowie die sonstigen wirtschaftlichen Verhältnisse, insbesondere Art, Umfang und Wirtschaftlichkeit der Geschäftstätigkeit des Betroffenen,
   2. Zahlungsverhalten und Vertragstreue des Betroffenen,
   3. vollstreckbare Forderungen sowie Zwangsvollstreckungsverfahren und -maßnahmen gegen den Betroffenen,
   4. Insolvenzverfahren über das Vermögen des Betroffenen, sofern diese eröffnet worden sind oder die Eröffnung beantragt worden ist.

Diese Daten dürfen erhoben werden

1. beim Betroffenen,
2. bei Instituten, die derselben Institutsgruppe angehören,
3. bei Ratingagenturen und Auskunfteien und
4. aus allgemein zugänglichen Quellen.

Die Institute dürfen anderen Instituten derselben Institutsgruppe und in pseudonymisierter Form auch von ihnen mit dem Aufbau und Betrieb einschließlich der Entwicklung und Weiterentwicklung von Ratingsystemen beauftragten Dienstleistern nach Satz 3 erhobene personenbezogene Daten übermitteln, soweit dies zum Aufbau und Betrieb einschließlich der Entwicklung und Weiterentwicklung von internen Ratingsystemen für die Schätzung von Risikoparametern des Adressenausfallrisikos erforderlich ist. Das Bundesministerium der Finanzen wird ermächtigt, durch Rechtsverordnung im Benehmen mit der Deutschen Bundesbank nähere Bestimmungen über die angemessene Eigenmittelausstattung (Solvabilität) der Institute sowie der Institutsgruppen und Finanzholding-Gruppen zu erlassen, insbesondere über

...

4. die näheren Einzelheiten der Erhebung und Verwendung personenbezogener Daten zur Bestimmung und Berücksichtigung von Adressenausfallrisiken; in der Rechtsverordnung sind Höchstfristen für die Löschung oder Anonymisierung der Daten zu bestimmen.

sei, den erforderlichen Datenschutz beim Scoreverfahren zu regeln. Das BMI hat zugesagt, zu prüfen, ob es einer Klarstellung im Bundesdatenschutzgesetz bedarf. Die Vorschrift des § 10 KWG könnte eine präjudizierende Wirkung für Regelungen zum Scoreverfahren haben.

## 9.3 Research-Systeme der Banken zur Aufdeckung von Geldwäsche

*Zur Prävention vor Geldwäsche, Betrug und Terrorismusfinanzierung müssen die Kreditinstitute nach § 25a Kreditwesengesetz angemessene Sicherungssysteme einrichten. Diese müssen neben einer wirkungsvollen Prävention auch einen angemessenen Datenschutz gewährleisten.*

In der Vergangenheit hatten die für die Banken zuständigen Datenschutzaufsichtsbehörden der Länder und ich wiederholt Hinweise von Kreditinstituten erhalten, nach denen die BaFin ihnen bei Prüfungen vor Ort bankenaufsichtsrechtliche Vorgaben für die Einrichtung von Research-Systemen zur Aufdeckung von Geldwäsche gemacht hat, die nicht datenschutzgerecht waren. So erwartete die BaFin von den Banken u. a. eine Beobachtung aller Transaktionen auf Geldwäscheverdachtsfälle, was einer unzulässigen Rasterfahndung (vgl. Nr. 5.2.3) gleich gekommen wäre. Darüber hinaus sollten Transaktionen über einen möglichst langen Zeitraum ausgewertet werden, d.h. aktuelle Zahlungsvorgänge sollten mit Zahlungsvorgängen aus dem letzten Jahr verglichen werden, um Besonderheiten im Zahlungsverkehr erkennen zu können. Die Kreditinstitute hatten zu Recht die Befürchtung, dass die Datenschutzaufsichtsbehörden die Umsetzung dieser Vorgaben beanstanden würden.

Dieses offensichtliche Spannungsverhältnis zwischen bankenaufsichtsrechtlichen und datenschutzrechtlichen Anforderungen galt es aufzulösen, um den Kreditinstituten durch verlässliche Vorgaben wieder Planungs- und Handlungsmöglichkeiten zu geben.

Die gesetzlichen Vorgaben aus dem Bereich der Bankenaufsicht sind nicht separat, sondern auch im Lichte datenschutzrechtlicher Anforderungen zu sehen. Nicht alles, was seitens der Bankenaufsicht wünschenswert wäre, ist datenschutzrechtlich zulässig. Nach zahlreichen Gesprächen zwischen den obersten Datenschutzaufsichtsbehörden der Länder, der Kreditwirtschaft, der BaFin und mir haben die Datenschutzaufsichtsbehörden ein Papier erarbeitet, das die datenschutzrechtlichen Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche aufzeigt (s. auch Kasten zu Nr. 9.3).

Die BaFin hat versichert, den Forderungskatalog beachten zu wollen.

Ich bin zuversichtlich, hiermit eine Basis für eine gute Zusammenarbeit der Beteiligten geschaffen zu haben. Ich werde die Entwicklung weiter beobachten.

Kasten zu Nr. 9.3

**Auszüge aus dem Arbeitspapier der obersten Datenschutzaufsichtsbehörden der Länder und des Bundes:**

**Datenschutzrechtliche Anforderungen für Research-Systeme zur Aufdeckung von Geldwäsche**

- Geldwäsche-Research-Systeme der Banken sollen sich grundsätzlich auf anlassbezogene Rasterungen beschränken. Eine flächendeckende Rasterung aller für eine Verdachtsakquirierung relevanten Kontobewegungen ist nur in eng begrenzten Ausnahmefällen möglich.
- Der Einsatz der Research-Systeme für andere Zwecke als dem der Bekämpfung der Geldwäsche, Terrorismusfinanzierung und Betrug ist unzulässig.
- Die datenschutzrechtlichen Grundsätze der Datenvermeidung, Datensparsamkeit und der frühestmöglichen Löschung sind einzuhalten.
- Der Grundsatz der Zweckbindung der Speicherung und unterschiedliche gesetzliche Anforderungen bei den einzelnen Verdachtsfällen (Geldwäsche, Terrorismusfinanzierung, Betrug) erfordern eine Kennzeichnung bzw. Separierung der Datensätze, soweit möglich.
- Die Bankkunden sind von der Bank über eine flächendeckende Rasterung aller Kontobewegungen zu informieren.
- Der Datenbestand in den Systemen darf nicht älter sein, als dies nach den wissenschaftlich statistischen Erkenntnissen und den Erfahrungen der Bankpraktiker zur Optimierung der Ergebnisse erforderlich ist. Eine Speicherlänge von drei Monaten gibt insoweit einen ersten Anhaltspunkt.
- Die Verwendung bestimmter Parameter muss sachlich nachvollziehbar sein.
- Für besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG gilt ein Verbot der Rasterung.
- Die Rechtmäßigkeit eines Research-Systems orientiert sich auch an seinem Erfolg.

## 9.4 SWIFT – Unzulässige Datenlieferung an US-Behörden

*Die Datenübermittlung im Rahmen der Durchführung von internationalen Zahlungsanweisungen in die USA verstößt gegen europäisches Datenschutzrecht.*

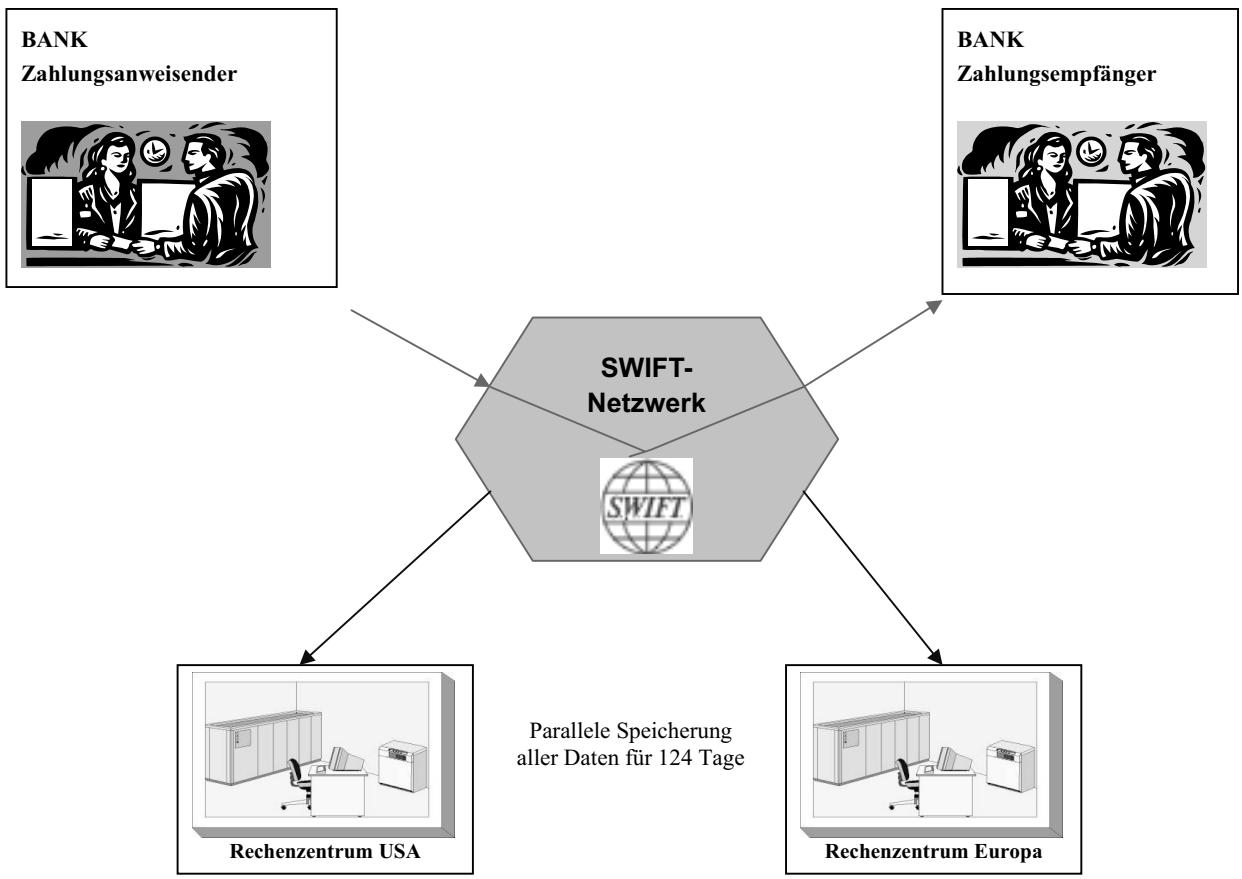
Durch Veröffentlichungen in Medien wurde Ende Juni 2006 bekannt, dass US-Behörden seit 2001 Zugang zu den Zahlungsverkehrsdaten von SWIFT (Society for Worldwide Interbank Financial Telecommunication) erhielten, um sie im Rahmen der Bekämpfung des Terrorismus auszuwerten. SWIFT ist eine 1973 von der internationalen Kreditwirtschaft gegründete Genossenschaft

belgischen Rechts. Die Zahlungsanweisungen, die durch den SWIFTNet FIN Service transportiert werden, enthalten personenbezogene Daten wie z. B. den Namen des Absenders und des Empfängers. SWIFT speichert alle Überweisungsdaten für 124 Tage in zwei Rechenzentren, von denen sich eines in Europa, das andere in den USA befindet. Amerikanische Behörden haben auf Grundlage behördlicher Beschlagnahmeanordnungen mehrfach Transaktionsdaten von SWIFT durchgesetzt, wobei der technische und rechtliche Anknüpfungspunkt für diese Anordnungen ausschließlich das in den USA befindliche SWIFT-Rechenzentrum war. SWIFT und die US-Behörden haben 2003 eine Vereinbarung geschlossen, in der das Verfahren der Datenübermittlung festgelegt wurde. SWIFT hat daraufhin Daten herausgegeben, ohne dass es zu einer richterlichen Überprüfung gekommen ist. Die SWIFT-Nutzer wurden generell nicht über die Tatsache, den Umfang und den Zweck der Übermittlung informiert.

Der Düsseldorfer Kreis der deutschen Datenschutzaufsichtsbehörden und die Artikel 29-Gruppe der Datenschutzbehörden der EU-Mitgliedstaaten haben festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US-Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist. Insbesondere verfügten die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA seien sowohl SWIFT als auch die Banken, die sich der Dienstleistungen von SWIFT bedienten. Die Banken wurden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden könne oder aber zumindest die übermittelten Datensätze hinreichend gesichert würden, damit der bislang mögliche Zugriff der amerikanischen Behörden künftig ausgeschlossen sei. Unabhängig davon müssten die Banken ihre Kunden unverzüglich darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zah-

Abbildung 8 zu 9.4

**So funktioniert SWIFT**



lungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT-Rechenzentrum übermittelt würden.

Die jetzige Situation bedarf auch einer Klärung der Aufsichtsstrukturen bei SWIFT, die gegenwärtig den Zentralbanken obliegt. Dazu gehört insbesondere, dass die Umsetzung von datenschutzrechtlichen Regelungen unter diese Aufsichtspflicht fällt, unbeschadet der Befugnisse der nationalen Datenschutzaufsichtsbehörden. Auch ist sicherzustellen, dass die zuständigen Behörden bei Bedarf vorschriftsmäßig und rechtzeitig unterrichtet werden. Alle Finanzinstitute in der EU, einschließlich der Zentralbanken, die die Dienstleistungen des SWIFTNet FIN Dienstes nutzen, haben gemäß Artikel 10 und 11 der Richtlinie 95/46/EG sicherzustellen, dass sie ihre Kunden angemessen über deren Datenverarbeitung und ihre diesbezüglichen Rechte unterrichten. In diesem Rahmen müssen die Kunden auch darüber informiert werden, dass die US-Behörden Zugriff auf ihre Daten nehmen können. Die Datenschutzaufsichtsbehörden werden diese Informationspflicht für alle Finanzinstitute europaweit durchsetzen. Darüber hinaus sollten die Finanzinstitute und Zentralbanken technische Alternativen zu den derzeitigen Verfahren entwickeln, um einen mit den Grundsätzen der Richtlinie im Einklang stehenden Zahlungstransfer zu gewährleisten (vgl. Beschluss des Düsseldorfer Kreises vom 9. November 2006, Anlage 16 sowie Stellungnahme Nr. 128 der Artikel 29-Gruppe vom 22. November 2006, Anlage 9).

## 9.5 Warn- und Hinweissystem der Versicherungswirtschaft – Uniwagnis

*Warn- und Hinweissysteme müssen datenschutzgerecht ausgestaltet sein. Das System Uniwagnis der Versicherungswirtschaft erfüllt diese Voraussetzungen nicht.*

Bei der Prüfung eines Versicherungsantrages oder im Schadensfall kann es zur Risikobeurteilung, zur weiteren Sachverhaltsaufklärung oder zur Verhinderung von Versicherungsmissbrauch notwendig sein, bei anderen Versicherungen Auskünfte einzuholen oder Daten an andere Versicherer weiter zu geben. Die Versicherungswirtschaft hat aus diesem Grund für die verschiedenen Versicherungssparten ein Warn- und Hinweissystem (Uniwagnis) entwickelt, mit dem Informationen über Versicherungsnehmer ausgetauscht werden können. Hierzu wird im Versicherungsantrag eine Einwilligungserklärung des Versicherungsnehmers eingeholt. Das Warn- und Hinweissystem wird vom Gesamtverband der Versicherungswirtschaft (GDV) im Auftrag der angeschlossenen Versicherungsunternehmen betrieben (vgl. Kasten zu Nr. 9.5).

Die Datenschutzaufsichtsbehörden hatten Uniwagnis und die bei Vertragsabschluss verwendete allgemeine Einwilligungserklärung beim Start des Systems im Jahr 1996 zunächst als datenschutzrechtlich unbedenklich eingestuft. Inzwischen muss jedoch davon ausgegangen werden, dass die bisherige Einwilligungsklausel nicht mehr der geltenden Rechtslage entspricht, weil seit der BDSG-Novellierung im Jahr 2001 eine hinreichend bestimmte Erklärung notwendig ist, die die Wirksamkeitsvoraussetzungen des § 4a Abs. 1 und 3 BDSG erfüllt. Aus der Klausel ist nicht erkennbar, welchen Umfang und welche Auswirkungen die Einmeldung und Weitergabe von personenbezogenen Daten im Rahmen des Warn- und Hinweissystems hat und zu welchem Zeitpunkt aufgrund welcher Kriterien eine Einmeldung erfolgt. Auch eine bessere Information über die Zweckbestimmung des Systems ist dringend geboten. Insoweit sei auch an dieser Stelle auf die Entscheidung des BVerfG vom 23. Oktober 2006 (s. u. Nr. 9.6) hingewiesen.

Ungeachtet der Frage der Wirksamkeit der Einwilligung bestehen bei den Datenschutzaufsichtbehörden grundsätzliche datenschutzrechtliche Bedenken in Bezug auf Uniwagnis. Diese beziehen sich u. a. auf die mangelnde Transparenz und Kontrollierbarkeit des Datenaustausches zwischen den beteiligten Versicherungen im Trefferfall. So ist nicht festgelegt, wie das berechtigte Interesse an einer Auskunft geprüft sowie der Informationsaustausch zwischen den beteiligten Versicherungsunternehmen im Trefferfall protokolliert bzw. dokumentiert wird. Die als relevant angesehenen Daten werden zwar in den Sachakten festgehalten, jedoch existieren keine einheitlichen Vorgaben. Der GDV hat angekündigt, Abhilfe durch die Erstellung eines so genannten Compliance-Leitfadens zu schaffen.

Problematisch ist aus Datenschutzsicht vor allem die Weitergabe der codierten Daten an sämtliche Versicherungsunternehmen, weil es sich dabei um eine Weitergabe personenbeziehbarer Daten auf Vorrat handelt. Weitere Problemfelder sind die von der Versicherungswirtschaft festgelegten Einmeldekriterien und die fehlende Möglichkeit für die Betroffenen, ihren Anspruch auf Löschung oder Berichtigung geltend zu machen, weil sie über die Einmeldungen nicht benachrichtigt werden. Ferner die Einmeldung Dritter (z. B. Unfallgeschädigte, Zeugen, Sachverständige) in das System ohne deren Benachrichtigung. Dies ist als besonders kritisch anzusehen, weil diese Dritten keine Einwilligung in die Übermittlung ihrer personenbezogenen Daten in das System Uniwagnis abgegeben haben und die Übermittlung nicht auf §§ 28, 29 BDSG gestützt werden kann, weil eine Beeinträchtigung schutzwürdiger Belange der Betroffenen anzunehmen ist, wenn ihre Daten ohne vorherige Information eingemeldet werden.

Über die rechtliche Bewertung von Uniwagnis bestehen zwischen der Versicherungswirtschaft und den Datenschutzaufsichtbehörden unterschiedliche Auffassungen. Daher hat der Düsseldorfer Kreis der Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich mit dem GDV eine umfassende Bestandsaufnahme über die Datenverarbeitung bei Uniwagnis in Angriff genommen, um eine breite Grundlage für die weitere rechtliche Bewertung im Rahmen der Aufsichtstätigkeit der Datenschutzkontrollbehörden zu schaffen. Bei Redaktionsschluss lag noch kein Ergebnis vor.

Ich werde mich weiterhin dafür einsetzen, das Hinweis- und Warnsystem datenschutzgerecht zu gestalten.

Kasten zu Nr. 9.5

**So funktioniert Uniwagnis:**

Einmeldungen in das Warn- und Hinweissystem erfolgen im Schadens- bzw. Leistungsfall durch die einzelnen Versicherungsunternehmen nach festgelegten Einmeldekriterien. Diese Kriterien sind weitestgehend nicht öffentlich, um zu verhindern, dass sich Versicherungsnehmer hierauf in betrügerischer Absicht einstellen können. Der Gesamtverband der Versicherungswirtschaft (GDV) erfasst und verschlüsselt – getrennt nach den einzelnen Versicherungssparten – die ihm von den Versicherungsunternehmen gemeldeten Daten des Versicherungsnehmers mittels eines phonetischen Strukturcode-Verfahrens unter Einsatz der Software UNIWAGNIS I. Dabei werden phonetisch ähnlich klingende Laute in die gleiche numerische Reihenfolge verwandelt. Der Code besteht aus mehreren Ziffern, von denen fünf für den Nachnamen, zwei für die Postleitzahl, sechs für das Geburtsdatum und eine für das Geschlecht vorgesehen sind. Das Verschlüsselungsverfahren kann dazu führen, dass die Datensätze verschiedener Personen den gleichen Code zugewiesen bekommen. Einzelne personenbezogene Daten können aus dem Datenbestand nicht ohne weiteres herausgelesen werden.

Die codierten Daten werden vom GDV mittels Datenträger mindestens einmal im Monat an die angeschlossenen Versicherungsunternehmen übermittelt. Diesen dient die Software UNIWAGNIS II, welche die Suchdaten ebenfalls in einen Strukturcode umwandelt, zum Suchen und Lesen im Datenbestand. Im Schadensfall oder beim Vorliegen eines Antrags auf Abschluss eines Versicherungsvertrages gibt das Versicherungsunternehmen die Identifizierungsdaten des Versicherungsnehmers oder Antragstellers zum Abgleich in das System ein. Im Trefferfall erfährt das abfragende Unternehmen den Namen des einmeldenden Unternehmens und kann Kontakt mit diesem aufnehmen, um abzuklären, ob hinter der Identität der phonetischen Strukturcodes auch eine Personenidentität steckt und der Datensatz zu dem Anfrageanlass passt. Dies ist erforderlich, weil mehreren Personen der gleiche Code zugewiesen sein kann. Die Kontaktaufnahme erfolgt in der Regel telefonisch.

## 9.6 Bundesverfassungsgericht stoppt formularmäßige Einwilligungserklärungen von Versicherungen

*Das Bundesverfassungsgericht hat festgestellt, dass formularmäßige allgemeine Einwilligungserklärungen in Versicherungsverträgen das Interesse des Betroffenen an einem wirksamen informationellen Selbstschutz unangemessen beeinträchtigen.*

Seit langem (vgl. 20. TB Nr. 17.1.9) bemängele ich die von den Versicherungsunternehmen seit mehr als 15 Jahren verwendete und überholte allgemeine Mustererklärung, wonach sich Versicherte bei Vertragsabschluss damit einverstanden erklären müssen, dass in der Zukunft zu jeder Zeit sensible Gesundheitsdaten, die der ärztlichen Schweigepflicht unterliegen, abgefragt werden dürfen. Solche unbefristeten und unkonkreten „Freibriefe“ entsprechen nicht den Voraussetzungen einer informierten Einwilligung nach dem Bundesdatenschutzgesetz. Die Versicherungen müssen deshalb in jedem Einzelfall eine gesonderte ärztliche Schweigepflichtentbindungserklärung einholen. Nur so hat der Versicherte den Überblick, welche seiner Gesundheitsdaten und zu welcher Zeit weitergegeben werden. Die Bemühungen der Datenschutzaufsichtsbehörden, sich mit dem Gesamtverband der Deutschen Versicherungswirtschaft auf eine neue, den gesetzlichen Anforderungen entsprechende Einwilligungsklausel zu verständigen, blieben leider erfolglos. Der fortbestehende Dissens hat derzeit zur Folge, dass die Ärzte bei einer auf einer pauschalen Schweigepflichtentbindungserklärung gestützten Übermittlung von Patientendaten an Versicherungen das Risiko eingehen, ihre ärztliche Schweigepflicht nach § 203 StGB zu verletzen. Aus diesem Grund ist in den Entwurf eines Gesetzes zur Reform des Versicherungsvertragsrechts (§ 213 VVG-E – Bundestagsdrucksache 16/3945) auf meine Anregung hin eine Regelung für die Erhebung von Gesundheitsdaten durch die privaten Krankenversicherungen aufgenommen worden.

Das Bundesverfassungsgericht (BVerfG) hat in seinem Beschluss vom 23. Oktober 2006 (1 BvR 2027/02) die Verletzung des Rechts auf informationelle Selbstbestimmung durch eine allgemeine Schweigepflichtentbindungserklärung in Versicherungsverträgen gerügt. In der Entscheidung wird festgestellt, dass eine formularmäßige und zum Teil sehr allgemein umschriebene Erklärung das Interesse des Betroffenen an einem wirksamen informationellen Selbstschutz erheblich beeinträchtige. Weil wegen der weiten Fassung der Erklärung nicht absehbar sei, welche Auskünfte von wem eingeholt werden können, werde dem Betroffenen die Möglichkeit genommen, die Wahrung seiner Geheimhaltungsinteressen selbst zu kontrollieren. Das Gericht hat ferner auf eine staatliche Verantwortung hingewiesen, mit Blick auf das allgemeine Persönlichkeitsrecht die rechtlichen Voraussetzungen für einen wirkungsvollen informationellen Selbstschutz zu gewährleisten und bereitzustellen.

Die vom BVerfG aufgestellten Grundsätze gelten aber nicht nur für die Schweigepflichtentbindungserklärung, sondern müssen bei allen bei Vertragsabschluss abzugebenden Einwilligungserklärungen in die Erhebung, Verarbeitung und Nutzung personenbezogener Daten berücksichtigt werden. Ich hoffe, dass die Versicherungswirtschaft die Entscheidung des Bundesverfassungsgerichts nun endlich zum Anlass nimmt, auch die seit 1994 verwendete und überholte allgemeine Einwilligungsklausel in Versicherungsverträgen – wie von den Datenschutzaufsichtsbehörden mehrfach gefordert – den gesetzlichen Anforderungen anzupassen. Die alte Klausel entspricht nicht der Vorschrift des § 4a BDSG, wonach die Einwilligung auf der freien Entscheidung des Versicherungsnehmers beruhen muss. Sie lässt zudem nicht hinreichend genug erkennen, was mit der Erhebung, Verarbeitung und Nutzung seiner Daten bezweckt wird und welche Konse-

quenzen sich daraus ergeben können. Die Verwendung einer einheitlichen Klausel mit einem dazugehörigen einheitlichen Merkblatt für verschiedene Vertragstypen ist nicht datenschutzgerecht. Das Merkblatt enthält Informationen zu allen in Frage kommenden Datenverarbeitungsmöglichkeiten, obwohl nur ein Teil dieser Informationen für den einzelnen Vertrag relevant ist. Der Betroffene wird dadurch nicht deutlich genug über den Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten für das Vertragsverhältnis unterrichtet.

Ungeachtet der Notwendigkeit, die Einwilligungsklausel zu ändern, halte ich es nach der ausdrücklichen Aufforderung des BVerfG an die staatlichen Stellen für wünschenswert, die rechtlichen Grundlagen für einen informationellen Selbstschutz zu schaffen und für eine sich streng am Erforderlich- und Verhältnismäßigkeitsgrundsatz orientierende und Transparenz bewirkende Rechtsgrundlage zu sorgen. Da sich hierzu das Gesetz zur Reform des Versicherungsvertragsrechts (s. o.) anbietet, habe ich die Vorsitzenden des Innen- und Rechtsausschusses des Deutschen Bundestages gebeten, diese Erwägungen bei den anstehenden Beratungen über den Gesetzentwurf zu berücksichtigen.

Die Entscheidung hat auch Konsequenzen für andere Branchen, in denen personenbezogene Daten auf Basis von Einwilligungserklärungen erhoben und verarbeitet werden. Einwilligungen sind nur dann wirksam, wenn die Betroffenen ihre Reichweite überblicken und konkret entscheiden können, wem welche Daten für welche Zwecke zur Verfügung stehen sollen. Ob formularmäßige Erklärungen diesen Voraussetzungen entsprechen, muss jeweils sorgfältig geprüft werden.

### 9.7 Datenschutz bei Rechtsanwälten

*Auch Rechtsanwälte unterliegen wie andere nicht-öffentliche Stellen den Regeln des Bundesdatenschutzgesetzes.*

Die Rechtsanwaltskammern in Deutschland haben, zuletzt in einem Beschluss der Hauptversammlung der Bundesrechtsanwaltskammer (BRAK), ihre gemeinsame Auffassung deutlich gemacht, dass das BDSG hinsichtlich mandatsbezogener Daten auf Rechtsanwaltskanzleien nicht anwendbar sei. Dies habe zur Folge, dass

- sich die Verarbeitung mandatsbezogener Daten durch Rechtsanwälte nicht an den Vorschriften des BDSG messen lassen müsse,
- Rechtsanwälte wegen des Mandatsgeheimnisses weder verpflichtet noch berechtigt seien, einer Aufsichtsbehörde für den Datenschutz Antwort auf deren Fragen zu erteilen; die Datenschutzaufsicht bei Rechtsanwälten vielmehr von den Rechtsanwaltskammern wahrgenommen würde.

Diese Auffassung wird von mir nicht geteilt. Die Vorschriften des BDSG treten nur insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. In der Bundesrechtsanwaltsordnung (BRAO) finden sich aber nur punktuelle Regelungen zum Datenschutz (z. B. §§ 43a Abs. 2, 50 BRAO). Daher bleibt es im übrigen bei der Anwendung des BDSG. Entgegen der Ansicht der BRAK steht dem nicht etwa das Mandatsgeheimnis entgegen. Die durch das Mittelstandsentlastungsgesetz vorgenommenen Änderungen des BDSG für Berufsgeheimnisträger (vgl. § 4f Abs. 2 Satz 3 BDSG) zeigen vielmehr, dass der Gesetzgeber voraussetzt, dass das BDSG für Berufsgeheimnisträger gilt. So erkennen auch die Steuerberater und Wirtschaftsprüfer, Ärzte etc. – gleichfalls Berufsgeheimnisträger – die Anwendbarkeit des BDSG an.

Aufgrund der von der BRAK verbreiteten Rechtsmeinung, der sich die Kammermitglieder anschließen müssen, wenn sie nicht Gefahr laufen wollen, wegen Verletzung des Mandatsgeheimnisses berufrechtlich belangt zu werden, ist es in der Praxis bereits zu ernsthaften Schwierigkeiten bei der Datenschutzkontrolle von Anwaltskanzleien gekommen. So verweigert z. B. eine große Rechtsanwaltskanzlei, die Beitreibungen für die Deutsche Telekom durchführt und in dieser Funktion wie jedes andere Inkassounternehmen agiert, der zuständigen Datenschutzaufsichtsbehörde die Datenschutzkontrolle unter Bezugnahme auf den o. g. Beschluss der BRAK. Dies ist kein Einzelfall. Immer wieder beschweren sich Dritte oder auch Mandanten von Rechtsanwälten bei den Datenschutzaufsichtsbehörden über fehlerhafte Datenverarbeitungen in Kanzleien. Deshalb muss es möglich sein, die Datenverarbeitung bei den Rechtsanwälten zu überprüfen und sie im Bedarfsfall zu rechtmäßigem Handeln anzuhalten. Den Beschwerdeführern wird durch die derzeitige Verweigerung der Rechtsanwälte ihr Recht, sich an die zuständige Datenschutzaufsichtsbehörde wenden zu können mit der Folge, dass diese den Vorgang prüft und bewertet, genommen. Rechtsanwaltskammern können die Aufsichtsbehörden als Datenschutzkontrollstellen nicht ersetzen, da sie nur die allgemeine Berufsaufsicht ausüben. Sie unterliegen der Staatsaufsicht der Justizverwaltungen und handeln nicht in völliger Unabhängigkeit, wie es die Europäische Datenschutzrichtlinie 95/46/EG für die Datenschutzkontrollstellen verlangt.

Ich habe mich in dieser Angelegenheit bereits an das Bundesjustizministerium gewandt, damit eine Klärung der Rechtslage herbeigeführt wird.

## 10 Telekommunikations- und Teledienste

### 10.1 Brüsseler Sündenfall – Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten

*Im Mai 2006 trat die Richtlinie zur Vorratsdatenspeicherung in Kraft. Sie muss bis zum 15. September 2007 umgesetzt werden.*

Nach dem „bisher schnellsten Gesetzgebungsverfahren in der EU-Geschichte“ – so der EP-Abgeordnete und Berichterstatter des federführenden Ausschusses für bürgerliche Freiheiten, Justiz und Inneres, Alexander Alvaro – trat im Mai 2006 die europäische Richtlinie zur Einführung einer europaweiten Vorratsspeicherung von Telekommunikationsdaten in Kraft. Sie verpflichtet die Anbieter von Telekommunikations- und Internetdiensten,

umfangreiche Telefon- und Internetdaten auf Vorrat für die Strafverfolgungsbehörden zu speichern, ohne dass ein konkreter Verdacht oder Hinweise auf eine bevorstehende Gefahr vorliegen müssen. Umzusetzen in nationales Recht ist die Richtlinie bis zum 15. September 2007; für den Bereich des Internet-Zugangs, E-Mail- und VoIP-Dienste gilt eine verlängerte Frist bis zum 15. März 2009.

Mit der Vorratsdatenspeicherung ist ein erheblicher Eingriff in die Privatsphäre und die Vertraulichkeit der Kommunikation unverdächtiger Bürgerinnen und Bürger verbunden. Hiervon sind besonders sensible Informationen betroffen, die dem Fernmeldegeheimnis unterliegen. Deshalb hat es auch im Laufe des Verfahrens grundsätzliche Bedenken und Kritik von Datenschützern, Bürgerrechtlern, aber auch Telekommunikationsdiensteanbietern u. a. gegeben.

Aus Sicht des Datenschutzes lassen sich die wichtigsten Forderungen wie folgt zusammenfassen:

- Der Speicherungszeitraum muss sich an der derzeit geltenden Höchstfrist für Abrechnungszwecke orientieren, d.h. nach deutschem Recht 6 Monate (§ 97 Abs. 3 Satz 3 TKG). Diese Frist von 6 Monaten sieht die Richtlinie als Mindestspeicherfrist vor. Nach der Richtlinie können die EU-Mitgliedstaaten im nationalen Recht eine Vorratsdatenspeicherung für maximal 2 Jahre vorsehen.
- Der Zweck der Vorratsdatenspeicherung zur Bekämpfung des Terrorismus und schwerer Kriminalität muss klar definiert und – wie von der Richtlinie vorgegeben – auf diese Bereiche begrenzt werden.
- Die gespeicherten Daten dürfen nur den staatlichen Strafverfolgungsbehörden zur Verfügung gestellt werden. Private Dritte, aber auch andere staatliche Stellen, dürfen keinen Zugang zu den Daten haben.
- Die von der Speicherungspflicht betroffenen Datenarten müssen festgelegt und eng begrenzt werden.
- Grundsätzlich sollte in jedem Einzelfall ein Richter über die Herausgabe der Daten entscheiden.
- Die Daten dürfen weder von den Telekommunikations- bzw. den Internetdiensteanbietern noch von anderen Stellen für weitere, etwa wirtschaftliche Zwecke genutzt werden.
- Die Entstehung von Datenpools, die auch für andere als die genannten Zwecke dienen könnten, ist zu vermeiden. Die auf Vorrat gespeicherten Daten sollten daher in separaten Systemen verarbeitet werden. Dabei müssen technische und organisatorische Maßnahmen vorgesehen werden, die die Datensicherheit gewährleisten.
- Die Möglichkeit zur anonymen E-Mail-Kommunikation ist auch weiterhin zu gewährleisten. Eine Vorratsdatenspeicherung von Namen, Anschrift und Geburtsdatum des Nutzers sowie seiner E-Mail-Adresse muss deshalb unterbleiben.

Zur Zeit wird auf Antrag Irlands und der Slowakei vom Europäischen Gerichtshof überprüft, ob mit der gewählten Rechtsgrundlage die Vorratsdatenspeicherung überhaupt eingeführt werden kann. Sollte der EuGH analog zur Frage der Rechtsgrundlage bei der Übermittlung von Flugpassagierdaten an die USA entscheiden, d. h. die Richtlinie „kassieren“, so wird möglicherweise wieder – trotz Scheiterns mangels Einstimmigkeit beim ersten Versuch im Jahre 2004 – der „alte“ Weg eingeschlagen und versucht werden, die europaweite Vorratsdatenspeicherung über einen Rahmenbeschluss durchzusetzen.

Die Bundesrepublik hat die Richtlinie umzusetzen, solange der EuGH die Europarechtswidrigkeit nicht feststellt. Daher hat das BMJ im November 2006 einen Entwurf für ein „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmethoden sowie zur Umsetzung der Richtlinie 2006/24/EG“ vorgelegt (s. dazu auch Nr. 6.1). Mit diesem Artikelgesetzes soll auch die Vorratsdatenspeicherung im Telekommunikationsgesetz vorgeschrieben werden. Leider blieb meine Forderung bisher unberücksichtigt, die Provider zu verpflichten, die für Strafverfolgungszwecke bevorrateten Daten getrennt von denen zu speichern, die für die eigenen Geschäftszwecke, d.h. für die Erbringung und Abrechnung der Dienstleistung benötigt werden. Ebenfalls ist eine Beschränkung der Verwendungszwecke auf die Verfolgung von Terrorismus und schweren Straftaten nicht vorgesehen. Im Gegenteil: Die sehr vage Formulierung „mittels Telekommunikation begangene Straftaten“ geht weit darüber hinaus und wird auch durch eine ergänzende Abwägungsklausel nicht hinreichend kompensiert. Hinsichtlich der Speicherungsfrist wurde das von der Richtlinie vorgegebene Minimum von 6 Monaten übernommen.

Die weitere Entwicklung bleibt abzuwarten. Das Bundesverfassungsgericht wird sich voraussichtlich in wenigen Monaten mit der Frage der Vereinbarkeit der Vorratsdatenspeicherung mit dem Grundgesetz zu beschäftigen haben, da Bürgerrechtsorganisationen Verfassungsbeschwerden angekündigt haben.

## 10.2 Neue Geschäftsmodelle durch Location Based Services

*Handyortungsdienste können darüber informieren, wo sich die Freunde oder die Service-Techniker eines Betriebs aufhalten – oder aber der mutmaßlich untreue Ehemann.*

Wer ein Handy in der Tasche hat, dessen Aufenthalt kann zumindest ungefähr ermittelt werden. Dies ergibt sich aus der Funktionsweise moderner Mobilfunknetze, die sich aus einer Vielzahl von Funkzellen zusammensetzen. Der Durchmesser der Funkzellen liegt zwischen 200 Metern und 50 Kilometern. Damit ein mobiles Gerät erreichbar ist, muss dem Netz bekannt sein, in welcher Funkzelle es sich gerade befindet. Deshalb senden eingeschaltete Mobilteile laufend „Aktivmeldungen“. Aufgrund der Aktivmeldungen („location update“) wird der Standort des jeweiligen Teilnehmers ermittelt und an zentraler Stelle im Netz gespeichert. Sofern eine Verbindung zu Stande

kommt, werden die Standortdaten (insbesondere zur Ermittlung der Telefongebühren) in einem Verkehrsdatensatz gespeichert. Bei der Vorratsdatenspeicherung (s. o. Nr. 10.1) ist auch diese Ortungsinformation zu speichern.

Neue Mobilfunktechniken gestatten eine noch wesentlich genauere Ermittlung des Standortes. Dies wird zum einen ermöglicht, wenn die herkömmlichen Mobilfunknetze um besondere Lokalisierungsmodule erweitert werden. Dabei erfolgt eine Peilung anhand der Auswertung der Signallaufzeiten durch mindestens drei Basisstationen. Diese Standortdaten können an zentraler Stelle durch den Netzbetreiber oder in dem mobilen Gerät gespeichert werden. Zum anderen bedienen sich Lokalisierungsdienste zunehmend der Satellitenortung, die eine metergenaue Standortbestimmung ermöglicht, soweit die Geräte mit einem entsprechenden Modul ausgestattet sind.

Bislang wird für die Satellitenortung das GPS (Global Positioning System) eingesetzt, das eine satellitengestützten Positionsbestimmung an einem beliebigen Ort der Erde ermöglicht. GPS besteht aus etwa 30 Satelliten, die die Erde umkreisen. Mit einem entsprechenden Empfangsgerät werden die dem Standort am nächsten befindlichen Satelliten angepeilt. Auf der Grundlage der Signallaufzeiten wird der Standort berechnet. Derzeit hat der Aufbau eines von der EG geförderten eigenen Satellitenortungssystems namens GALILEO begonnen, das 2010 seinen Betrieb aufnehmen soll und eine gegenüber GPS noch päzisisere Lokalisierung erlauben wird. GPS ist ein passives System, das selbst keine aktive Ortung durch Dritte ermöglicht. Die Positionsdaten werden jeweils zunächst nur von dem abfragenden Empfangsgerät ermittelt und können nur durch dieses – etwa mittels Mobilfunk – an andere Systeme übertragen werden.

Zukünftig werden viele neue Mobiltelefone mit Satellitenortungsmodulen ausgestattet sein. Dies wird auch damit begründet, dass nur so der Standort hilfloser Personen mit Genauigkeit ermittelt werden kann, die einen Notruf auslösen, aber selbst nicht in der Lage sind, ihren genauen Aufenthaltsort mitzuteilen.

Unternehmen bedienen sich dieser Eigenschaft der Mobilfunknetze und bieten standortbasierte Dienste („local based services“, LBS) an.

LBS können für verschiedene Zwecke sinnvoll sein. Zum Einen gibt es die Möglichkeit, per Handy lokale Informationen zu erhalten, etwa die regionale Wettervorhersage oder die Restaurants in der Umgebung. Zum Anderen kann der Aufenthaltsort eines Handys oder einer Person bestimmt werden und etwa auf einer Karte in einem Webbrowser dargestellt werden. Unter der Voraussetzung, dass der Datenschutz beachtet wird, kann dies etwa in Speditionen oder im Service-Bereich ein sinnvoller Einsatz sein.

Diese Ortungsdienste sind datenschutzrechtlich zulässig, soweit der Nutzer eingewilligt und ggf. Mitbenutzer informiert hat. Dies ist in § 98 TKG geregelt. Bei Diensten für Endkunden erfolgt die Einwilligung meist per SMS. Hierbei ist jedoch nicht sichergestellt, dass die Einwilligung wirklich durch den Nutzer erfolgt. Gerade im privaten Umfeld besteht die Möglichkeit, dass die SMS zur Einwilligung von einem Dritten, etwa vom eifersüchtigen Partner, versandt wird, der anschließend den Aufenthaltsort per Internet abfragt.

Im professionellen Umfeld, etwa bei Logistikunternehmen, müssen Einwilligungen sorgfältig geprüft werden. Bei Angeboten für Privatkunden halte ich den Versand von SMS an geortete Handys für ein geeignetes Mittel, einen Missbrauch zeitnah zu erkennen. Dabei kann es auch ausreichend sein, bei häufiger Nutzung nur zufallsgesteuert Informations-SMS zu versenden. Es sollte aber sicher gestellt werden, dass die Neugier eines Lebenspartners oder Kollegen zeitnah erkannt und Missbrauch unverzüglich gestoppt wird. Über diese Forderungen habe ich Mobilfunkanbieter und einige Betreiber von Plattformen informiert.

Solche Schutzmassnahmen sind auch vor dem Hintergrund wichtig, dass das Nachspionieren derzeit keine strafrechtlichen Konsequenzen hat (s. o. Nr. 6.4).

Viele LBS, unabhängig davon, ob die Ortung durch das Mobilfunknetz oder Satelliten erfolgt, haben den aus Datenschutzsicht negativen Nebeneffekt, dass mit ihrer Hilfe Bewegungsprofile erstellt werden können. Die Geo-Daten der Aufenthaltsorte können mit sonstigen personenbezogenen Daten zu sehr aussagekräftigen Profilen über die Nutzer zusammengeführt werden. Schließlich könnten Dritte diese Informationen zur heimlichen Überwachung verwenden. Bereits heute werden entsprechende Geräte verkauft, die von Eltern, die den Aufenthaltsort ihrer Kinder wissen wollen, von eifersüchtigen Ehepartnern und von Privatdetektiven verwendet werden. Auch bei Systemen, die in umfassende Dienste eingebunden sind, etwa zur Ortung gestohlener Fahrzeuge, zur Mauterhebung (s. u. Nr. 12.1) oder zum Flottenmanagement, können die Informationen zur Erzeugung von Bewegungsbildern genutzt werden.

Eine ganz andere Anwendung dient der Lebensrettung. Eine Stiftung, die sich für Verbesserungen bei der Unfallrettung einsetzt, bietet einen Ortungsdienst für Rettungsleitstellen an. Hier wird die gleiche Technik eingesetzt, die auch bei den oben erwähnten kommerziellen Ortungsdiensten verwendet wird. Über einen Internetzugang – natürlich mit Authentifizierung des Mitarbeiters – können bei den Rettungsleitstellen Ortungen veranlasst werden. Eine solche Ortung, bei der die Ortungsinformation bei einem Anruf zur Rettungsleitstelle durch den Netzbetreiber direkt mitgeliefert wird, ist bereits in § 108 TKG vorgesehen; bis zur praktischen Umsetzung dürfte jedoch noch einige Zeit vergehen. Insofern halte ich das von der Stiftung vorgesehene Verfahren für einen Übergangszeitraum für angemessen. Es sind jedoch – insbesondere aus Sicht der Rettungsleitstellen – noch nicht alle rechtlichen Fragen abschließend geklärt.

Weitere Informationen zu Location Bases Services enthalten mein 19. TB (Nr. 11.6, 11.10.4) und 20. TB (Nr. 13.2.2).

Kasten zu Nr. 10.2

**Werde ich geortet?**

Die Möglichkeiten unterscheiden sich bei den Netzbetreibern. Bei einem Netzbetreiber ist eine Sperre für alle Ortungsdienste möglich. Bei einem anderen kann die Freischaltung für einen Dienst per SMS abgefragt und ggf. widerrufen werden. Hier sollte man sich an den Service seines Netzbetreibers wenden.

### 10.3 Anzeige der Kundennummer im Call-Center trotz Rufnummernunterdrückung

*Service-Rufnummern können dank des sog. Intelligenten Netzes einigen Komfort bieten. Manches, was technisch machbar ist, verstößt jedoch gegen den Datenschutz.*

Bei einem Versandhaus ist der persönliche Kundenservice sehr wichtig. Einige Kunden waren aber verwundert, dass Sie am Telefon bereits persönlich begrüßt wurden, ohne ihren Namen genannt oder die Rufnummer übertragen zu haben. Es stellte sich heraus, dass ein großer Telekommunikationsanbieter einen besonderen Dienst für Servicerufnummern anbietet. Dabei wird zwar nicht generell die Rufnummernunterdrückung aufgehoben, allerdings kann zu den, dem Versandhaus bekannten Rufnummern, eine Kundennummer übertragen werden. Eine Liste mit Rufnummern und dazugehörenden Kundennummern wird dabei dem Telekommunikationsanbieter vom Versandhaus zur Verfügung gestellt. Die Rufnummer wird in den Bestellformularen der Versandhäuser vom Kunden abgefragt.

Der Telekommunikationsanbieter hatte zwar in seinen AGB verlangt, dass bei Rufnummernunterdrückung durch den Kunden dessen Einwilligung erforderlich wäre; die Versandhäuser haben sich daran allerdings nicht gehalten. Zusammen mit der Bundesnetzagentur und dem TK-Anbieter habe ich die rechtliche Situation diskutiert. Da die Aufhebung bzw. Umgehung der Rufnummernunterdrückung beim TK-Anbieter erfolgt, muss eine Einwilligung des Kunden gegenüber diesem abgegeben werden. Es ist allerdings auch möglich, dass die Einwilligung des Kunden vom Versandhaus abgefragt wird und dieses mit der Aufnahme des Kunden in die entsprechende Liste dokumentiert wird. Der TK-Anbieter steht dabei allerdings weiter in der Pflicht, die korrekte Einholung der Einwilligungen zu überprüfen. Dies stellte sich zunächst als problematisch heraus.

Es dauerte einige Monate, bis der TK-Anbieter nachvollziehbar darlegte, dass die Einwilligungen korrekt eingeholt werden und nur die Kunden, die eingewilligt haben, in die Liste übernommen werden. Dennoch ist eine datenschutzgerechte Ausgestaltung unverzichtbar, da ansonsten das im Telekommunikationsgesetz festgelegte Recht der Kunden umgangen wird. Ich werde den Bereich der Servicerufnummern weiter beobachten und eingreifen, falls Rechtsverstöße festgestellt werden.

### 10.4 Übersendung des Einzelverbindungsnachweises per E-Mail

*Der Einzelverbindungsnachweis enthält sensible Daten, die dem Fernmeldegeheimnis unterliegen und muss von den TK-Anbietern entsprechend behandelt werden.*

Um bei hohem Preisdruck anfallende Kosten zu reduzieren, gehen viele Telekommunikationsanbieter dazu über, Telefonrechnungen, auf Wunsch des Kunden auch mit Einzelverbindungsnachweis (EVN), elektronisch zu versenden. Bei einigen Tarifen wird der Versand per Brief gar nicht oder nur gegen Aufpreis zur Verfügung gestellt. Durch die zunehmende Verbreitung des Internet ist dies für viele Kunden kein Problem. Bereits in meinem 18. TB (Nr. 10.12) habe ich ein Verfahren eines großen TK-Anbieters vorgestellt, bei dem die Rechnung, ggf. mit EVN, über ein Internetportal eingesehen werden kann. Dieses Verfahren hinterließ einen positiven Eindruck. Später wurde dieses Angebot um den Versand der Rechnung mit EVN per E-Mail erweitert, allerdings ohne Verschlüsselung. Die Sicherheit von unverschlüsselten E-Mails vor unberechtigter Kenntnisnahme ist allenfalls mit der einer Postkarte vergleichbar. Jede Person, die Zugriff auf die E-Mail erhält, kann deren Inhalt lesen, sofern die Daten unverschlüsselt übertragen werden. Bei E-Mail-Adressen in Firmen besteht etwa die Gefahr, dass bei Urlaub oder Erkrankung eines Mitarbeiters dessen Vertreter Zugriff auf das E-Mail-Postfach seines Kollegen nehmen kann. Der E-Mail-Abruf mittels Laptop an einem öffentlichen WLAN-Zugang kann als Einladung für Dritte zum Mitlesen missverstanden werden. Bei regulären Internetzugängen ist zu beachten, dass die Daten über mehrere Rechner geleitet werden, die sich auch im Ausland befinden können. Vor dem Hintergrund dieser Gefahren verlangt § 109 Abs. 1 Telekommunikationsgesetz ausreichende technische Vorkehrungen und sonstige Maßnahmen zum Schutz des Fernmeldegeheimnisses und der personenbezogenen Daten. Ein ausreichendes Schutzniveau kann etwa dadurch erreicht werden, dass der Einzelverbindungsnachweis den Kunden verschlüsselt und als Anhang einer E-Mail zugesandt wird. Möglich und ausreichend ist es auch, dass nur die Rechnung per E-Mail versendet wird und der Einzelverbindungsnachweis in einem gesicherten Internet-Portal des Telekommunikationsunternehmens von den Kunden eingesehen werden kann.

Eine Wahlmöglichkeit zwischen „offener“ und verschlüsselter Übermittlung des EVN halte ich für problematisch, da nicht nur der Kunde selbst, sondern auch Mitbenutzer des Anschlusses – etwa Familienmitglieder – betroffen sind und im EVN ihr Kommunikationsprofil erkennbar werden kann. Ebenso ist auch der Schutz der Gesprächspartner zu berücksichtigen, was mit Blick auf besonders sensible Verbindungsdaten, z. B. von Strafverteidigern oder Fachärzten, besonders deutlich wird. Aus diesen Gründen habe ich darauf bestanden, dass alle Kunden den EVN verschlüsselt erhalten.

Als die Umstellung schließlich auf verschlüsseltem EVN erfolgte, konnten die Kunden in ihrer Rechnungs-E-Mail lesen: „Aufgrund der Vorgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit senden

wir Ihnen Ihre EVÜ – sofern beauftragt – ab sofort immer verschlüsselt per E-Mail zu.“ Hierauf reagierten einige Kunden mit Unverständnis. Andere Kunden fragten mich nach dem Sinn dieser Vorgabe, da das Passwort doch im Klartext in der E-Mail enthalten wäre. Eine genauere Betrachtung zeigte, dass bei einem bestimmten Kundenkreis die für die Verschlüsselung verwendete Kennung die Kundennummer war.

Ich habe hier weitere Nachbesserungen verlangt und werde mich für ein insgesamt sicheres und anwenderfreundliches Verfahren einsetzen.

## 10.5 EVNde gut, alles gut

*Das Telekommunikationsgesetz sieht bisher einen Einzelverbindungsnachweis bei Flatrate-Tarifen nicht vor. Das soll sich zukünftig ändern.*

Neue Geschäftsmodelle sollen oft den Wünschen der Kunden entsprechen. Dass sie aber nicht immer auch den gesetzlichen Regelungen genügen, kann aufgrund der schnell fortschreitenden technischen Entwicklung nicht wirklich überraschen. Im Falle der Einzelverbindungsnachweise (EVN) bei der Abrechnung von Telefongesprächen ist es gelungen, beides zukünftig wieder in Einklang zu bringen. Dabei war es mir besonders wichtig, dass die Kunden selbst darüber entscheiden können, in welchem Umfang die sie betreffenden Daten in einen EVN eingehen. Es entspricht dem Recht auf informationelle Selbstbestimmung, dass auch bei Flatrates die einzelnen Nutzungsvorgänge dokumentiert werden, soweit die Betroffenen dies wünschen.

Das geltende Telekommunikationsgesetz sieht vor, dass die Verkehrsdaten von entgeltpflichtigen Verbindungen in einem EVN aufgeführt werden dürfen, damit der Kunde die Abrechnung seiner Telefongespräche kontrollieren kann, und dass der Kunde den EVN ausdrücklich verlangen muss. Nach diesem Wortlaut – eigentlich folgerichtig – haben viele Kunden bei ihrem Provider auch einen EVN beantragt, wenn sie eine sog. Flatrate vereinbart hatten. Bei diesem Tarif werden die Gebühren nicht pro Gespräch berechnet, sondern pauschal durch einen festen Betrag bezahlt. Leider sah der EVN nicht wie erwartet aus. Er enthielt nämlich nur die Verkehrsdaten von – trotz Flatrate – kostenpflichtigen Verbindungen, z. B. zu Auskunfts- und Servicenummern oder ins Ausland, nicht aber die Daten für die Gespräche, deren Kosten mit der Flatrate abgegolten waren. Was die Kunden nicht bedacht hatten: Die Inanspruchnahme einer Flatrate ist zwar insgesamt entgeltpflichtig, die einzelnen Verbindungen sind aber nicht entgeltrelevant, so dass ein detaillierter Nachweis der geführten Gespräche zur Überprüfung der Rechnung nicht erforderlich und damit von der geltenden gesetzlichen Regelung nicht abgedeckt ist.

Da es aber aus Sicht der Kunden gute Gründe gibt, die Dauer einzelner oder aller Gespräche zu kennen oder einfach zu wissen, dass überhaupt ein Gespräch stattgefunden hat, habe ich gemeinsam mit den Providern und der Bundesnetzagentur nach möglichen Lösungen gesucht. Letztendlich hat sich als die beste Lösung erwiesen, die gesetzliche Regelung im Zuge der TKG-Änderung den Kundenwünschen anzupassen. Angesichts der überzeugenden Argumente der Telefon-Kunden und der „Macht des Faktischen“ – einige Provider waren der rechtlichen Entwicklung schon voraus – hat das zuständige BMWi in das Gesetzgebungsverfahren noch einen Änderungsvorschlag eingebracht, der dann auch akzeptiert wurde. Somit können die Kunden – sobald die Änderungen in Kraft getreten sind – auch bei einer Flatrate die Verkehrsdaten ihrer einzelnen Gespräche überprüfen, für die Steuererklärung verwenden oder einem Tarif-Wechsel zugrunde legen.

## 10.6 Datenschutz beim Abschluss von Telekommunikationsverträgen

### Datenschutzgerechte Gestaltung von Auftragsformularen im Internet

Bei vielen Mobilfunkanbietern können die Kunden die gewünschte Dienstleistung nur über eine vorgegebene Bestellmaske auf der Internetseite der Anbieter bestellen. Petenten haben mich darauf aufmerksam gemacht, dass die Anmeldemasken einiger Anbieter für die Beantragung eines Mobilfunkvertrages oder einer Prepaid-Karte die Annahme einer so genannten Datenschutzerklärung durch das Setzen eines „Häkchens“ vorsehen. Unterblieb das Setzen dieses „Häkchens“, wurde die elektronische Anmeldung nicht fortgesetzt, sondern abgebrochen. In der Datenschutzerklärung war unter anderem angeführt, dass die Vertragsdaten der Kunden für Kundenberatung, Werbezwecke und Marktforschung verwendet werden dürften. Der Kunde könnte seine Zustimmung zu dieser erweiterten Verwendung seiner Daten nachträglich widerrufen.

Diese Vorgehensweise war nicht mit den Bestimmungen des § 95 Abs. 2 Satz 1 des Telekommunikationsgesetzes (TKG) vereinbar. Danach muss ein Kunde in die entsprechende Verwendung seiner Vertragsdaten einwilligen. Ihm muss bereits im Rahmen der Vertragsanbahnung die Wahlmöglichkeit gegeben sein, die Verwendung seiner Vertragsdaten für Kundenberatung, Werbe- und Marktforschungszwecke zu akzeptieren oder abzulehnen. Lehnt der Kunde die Verwendung seiner Vertragsdaten für diese Zwecke ab, darf dies kein Ausschlusskriterium für das Zustandekommen des Mobilfunkvertrages sein.

Ich habe die betreffenden Mobilfunkanbieter aufgefordert, ihre elektronischen Anmeldemasken auf den Internetseiten unter Beachtung der gesetzlichen Vorgaben des TKG zu ändern. In allen mir bekannten Fällen sind die Mobilfunkanbieter meinem Verlangen gefolgt.

### Nutzung von Bestandsdaten zu Werbezwecken

Für viele Bürgerinnen und Bürger ist die Vielzahl der Werbeaktionen ein wachsendes Ärgernis, gerade bei telefonischer Werbung. Dazu gehört, dass inzwischen Telekommunikationsdiensteanbieter oder von ihnen beauftragte Call-Center nicht nur Werbung für eigene Angebote machen, sondern auch für Produkte von anderen Firmen (z. T. als Partnerunternehmen bezeichnet). Solche Aktionen werden in der Branche „Far-Selling“ genannt.

Im Telekommunikationssektor ist unstrittig, dass Werbeaktionen nur mit dem ausdrücklichen Einverständnis der betroffenen Kunden durchgeführt werden dürfen. Da § 95 Abs. 2 Satz 1 TKG unter der Voraussetzung der Einwilligung ausschließlich eine Werbung für eigene Angebote der Telekommunikationsdiensteanbieter regelt, kann diese Bestimmung hierfür nicht herangezogen werden. Ein Rückgriff auf die Regelung in § 28 Abs. 4 BDSG ist nicht zulässig. Danach können personenbezogene Daten bereits dann für Werbezwecke verwendet werden, wenn der Betroffene dem nicht widersprochen hat (opt-out). Da aber die bereichsspezifische Sonderregelung des § 95 Abs. 2 Satz 1 TKG bereits für die Verwendung der Bestandsdaten für eigene Werbezwecke des Providers die ausdrückliche Einwilligung („opt-in“) voraussetzt, muss dies – erst recht – gelten, wenn Produkte und Dienstleistungen anderer Unternehmen beworben werden sollen. Die Nutzung von Bestandsdaten ist im Rahmen einer Far-Selling-Aktion also nur zulässig, wenn der Kunde zuvor seine Einwilligung hierzu ausdrücklich erklärt hat („opt-in“).

Zu beachten ist auch, dass nach § 95 Abs. 5 TKG die Erbringung von Telekommunikationsdiensten nicht von einer Einwilligung in eine Verwendung der Daten für andere Zwecke abhängig gemacht werden darf.

Ferner ist zu beachten, dass neben der Einwilligungserklärung nach § 95 Abs. 2 TKG eine zweite eigenständige Klausel aufzunehmen ist, die ausschließlich die für „Partnerunternehmen“ vorgesehenen Werbeaktionen zum Gegenstand hat. Zudem setzt eine wirksame Einwilligung voraus, dass sie besonders hervorgehoben ist (z. B. Fettdruck, Großschrift oder Umrahmung). Ziel muss es sein, die Aufmerksamkeit auf die Einwilligung zu lenken, damit der Kunde eine eigenständige Entscheidung treffen kann. Keinesfalls darf eine solche Klausel im „Kleingedruckten versteckt“ werden.

Wegen der grundsätzlichen Bedeutung dieser Problematik habe ich meine Auffassung mit der Bundesnetzagentur abgestimmt.

**Mangelhafter Datenschutz wegen fehlender Auftragsbestätigung im T-Punkt**

Ein Telekomkunde, der zwecks Beratung über einen Produktwechsel eine Vertriebsstelle (T-Punkt) der Deutschen Telekom AG (DTAG) aufgesucht hatte, beschwerte sich darüber, dass er sich anschließend mit Namen, Anschrift und Beruf in einem gedruckten oder elektronischen öffentlichen Kundenverzeichnis fand, obwohl er dies nicht beantragt hatte. Meine Prüfung hat ergeben, dass die vom Kunden monierte Praxis der Telekom gegen datenschutzrechtliche Vorschriften verstieß. Erst nach Korrektur des Datensatzes hat die Telekom gewährleistet, dass dem Wunsch des Petenten auf Nichtveröffentlichung der Anschrift in Telefonverzeichnissen künftig, das heißt bei deren Neuauflagen, wieder entsprochen wird. Gleiches gilt auch für die Veröffentlichung von Daten auf Telefon-CDs.

Da fehlerhafte Einträge in öffentlichen Kundenverzeichnissen im Zusammenhang mit Änderungen im Vertragsverhältnis häufiger aufgetreten sind, habe ich bei mehreren T-Punkt-Filialen Beratungs- und Kontrollbesuche durchgeführt. Im Vordergrund stand dabei die Vorgehensweise bzw. die Verfahrensanweisungen bei der Erfassung von neuen Anträgen, bei Vertragsänderungen und bei Änderungen der Einträge im T-Punkt. Dabei stellte sich heraus, dass es den Mitarbeitern nicht möglich bzw. nicht gestattet ist, dem Kunden direkt vor Ort eine vollständige Information über das bestellte Produkt auszuhändigen. Dies betrifft auch den Eintrag in öffentliche Verzeichnisse. Erst nach einigen Tagen erhält der Kunde eine schriftliche Bestätigung über die Art seines Telefonbucheintrags. Bei einem Missverständnis können die Daten zu diesem Zeitpunkt bereits in der Telefonauskunft bzw. im Internet verfügbar und in ungünstigen Fällen auch im Telefonbuch abgedruckt sein.

Wenn dem Kunden auf Wunsch ein Ausdruck über die beauftragten Daten direkt vor Ort ausgehändigt würde, hätte dieser die Möglichkeit einer sofortigen Korrektur. Auch im Hinblick auf die Vermeidung von Beratungsfehlern kann ein Ausdruck hilfreich sein, etwa wenn ein entsprechender Hinweis auf die Widerspruchsmöglichkeit bei der Inverssuche gegeben werden muss. Ich habe die DTAG daher aufgefordert, zeitnah die Möglichkeit einer sofortigen Aushändigung der vollständigen Auftragsbestätigung im T-Punkt zu schaffen. Dies ist nicht allein aus Datenschutzgründen erforderlich, sondern würde auch die Kundenfreundlichkeit der Produkte und Dienstleistungen in den T-Punkt-Filialen steigern und effektiveres Arbeiten ermöglichen. Das Unternehmen hat zugesagt, meine Forderung kurzfristig umzusetzen.

**Datenschutzrechtliche Probleme bei der Verarbeitung von „alten“ Vertragsdaten**

Die Liberalisierung des Telekommunikationsmarktes hat zu einem scharfen Wettbewerb um Marktanteile und Kunden geführt. Dabei geht es neben der Gewinnung neuer Kunden zunehmend auch um Strategien, den eigenen Kundenstamm zu halten. Die TK-Unternehmen und -Diensteanbieter nutzen ihre Kundendaten – Name, Anschrift und weitere Informationen – für vielfältige Formen der Werbung und der Kundenberatung.

Immer wieder erreichen mich daher Fragen von Kunden, welche Daten das TK-Unternehmen für welche Zwecke nutzen darf. Bis zur Novellierung des TKG im Jahr 2004 durften TK-Unternehmen und -Diensteanbieter nach § 89 Abs. 7 TKG a.F. die Bestandsdaten ihrer Kunden für Zwecke der Werbung, Kundenberatung oder auch Marktforschung nutzen, soweit der Kunde seine Einwilligung erteilt hatte (Opt-in-Prinzip). Seit das novellierte TKG am 26. Juni 2004 in Kraft getreten ist, enthält § 95 Abs. 2 TKG eine wesentliche Neuregelung. Während z. B. für das Telefonmarketing und die Faxwerbung weiterhin das Opt-in-Prinzip gilt, wird dieser Grundsatz in § 95 Abs. 2 Satz 2 TKG eingeschränkt. Dort wird z. B. die Nutzung der Postadresse für die Übersendung von Textmitteilungen gestattet, wenn der Teilnehmer der Ver-

wendung nicht widersprochen hat (Opt-out-Prinzip). Diese Vorschrift bezieht sich allerdings nur auf die Nutzung für eigene Zwecke, also z. B. Werbung für das eigene Unternehmen, wie etwa die Unterbreitung eines Angebots über eine günstigere Tarifierung. Für eine weitergehende Nutzung von Kundendaten, wie z. B. ihre Übermittlung an andere Unternehmen (z. B. im Rahmen des Adressenhandels), ist nach wie vor eine gesonderte Einwilligung des Kunden erforderlich (§ 95 Abs. 1 Satz 3 TKG).

Aufgrund einer Eingabe wurde ich darauf aufmerksam, dass ein TK-Unternehmen die geschilderte Gesetzesänderung zum Anlass nahm, „Alt"-Kunden ohne deren Einwilligung zu bewerben. Dieses Unternehmen verkannte offensichtlich, dass die Regelungen in § 95 Abs. 2 TKG nur für Verträge angewendet werden können, die nach Inkrafttreten des neuen TKG abgeschlossen wurden. Ich habe diesen Vorfall zum Anlass genommen, alle TK-Unternehmen und -Diensteanbieter nochmals auf die Rechtslage und die diesbezüglichen Kundenrechte hinzuweisen. Wegen der grundsätzlichen Bedeutung des Falles habe ich auch die Bundesnetzagentur informiert.

## 10.7 Neue Vertriebswege und Datenschutz

*Ein deutsches Mobilfunkunternehmen ließ seine Kunden von Mitarbeitern eines beauftragten Call-Centers anrufen. Diese Anrufe und deren Folgen waren für viele Bürger Anlass, sich an mich zu wenden.*

Die Kunden des Mobilfunkunternehmens wurden in der Vorweihnachtszeit des Jahres 2005 von Mitarbeitern eines beauftragten Call-Centers angerufen und gefragt, ob die Kundenadresse beim Vertragsunternehmen noch richtig registriert sei. Die Anrufer lasen die Adresse vor, ließen sich die Angaben bestätigen und bedankten sich für die Unterstützung. Die Kunden bekamen anschließend ein Schreiben des Mobilfunkunternehmens, in dem man sich noch einmal für das freundliche Telefonat bedankte. Weiter hieß es in dem Schreiben: „Gerne informieren die Unternehmen unserer Gruppe Sie künftig über aktuelle Produkte und Dienstleistungen über den von Ihnen gewünschten Kontaktkanal. Wie mit Ihnen telefonisch besprochen, dürfen wir die Vertragsdaten innerhalb unserer Gruppe zur Kundenberatung, Werbung und Marktforschung nutzen". Es folgte der Wortlaut der Datenschutzerklärung und der Verweis auf das Merkblatt „Hinweise zum Datenschutz", das auch die Möglichkeit eines Widerrufs der Einwilligung aufzeigte.

Empört wandten sich viele der betroffenen Kunden des Mobilfunkunternehmens an mich und trugen vor, dass eine Einwilligung zur Verwendung der Vertragsdaten für Kundenberatung, Werbung und Marktforschung niemals Gegenstand der besagten Telefonate gewesen sei. Einige schrieben mir sogar, dass sie das Schreiben des Mobilfunkanbieters erhalten hätten, ohne dass zuvor mit ihnen telefoniert worden wäre.

Bei meiner Sachverhaltsaufklärung stellte sich heraus, dass das Mobilfunkunternehmen ein nicht firmengebundenes Call-Center beauftragt hatte, die Einwilligungen der Kunden telefonisch einzuholen und im Falle der Zustimmung des Kunden die Bestätigung der Angaben per Brief anzukündigen. Dabei hatten die Mitarbeiter des Call-Centers offensichtlich „unsauber" gearbeitet und wohl auch von Fall zu Fall mit Blick auf die zu erwartenden Provisionszahlungen bewusst den wahren Grund ihres Anrufs verschwiegen.

Das Mobilfunkunternehmen reagierte nach dieser Sachverhaltsaufklärung sofort. Die Eintragungen der betroffenen Kunden, die sich an mich gewandt hatten, wurden entsprechend geändert bzw. rückgängig gemacht. Das Mobilfunkunternehmen kündigte an, bis auf Weiteres auf die telefonische Einholung von Einwilligungen der Kunden zu verzichten.

In einem speziell zu diesem Themenkomplex anberaumten Beratungsgespräch mit dem Mobilfunkunternehmen habe ich eine Einhaltung der datenschutzrechtlichen Vorgaben beim Umgang mit den Daten der Kunden angemahnt und dabei insbesondere auf die Beachtung der besonderen Sorgfaltspflichten bei künftigen Marketing- und Telefonaktionen hingewiesen.

## 10.8 Veröffentlichungen im Internet

### 10.8.1 Internetdatenbanken – Pranger oder Wissensdatenbank?

*Zunehmend werden Informationen oder Bewertungen von Personen, Unternehmen oder Sachverhalten in Datenbanken gesammelt und im Internet veröffentlicht. Ob es sich dabei um eine berechtigte Informationsweitergabe oder aber um einen mittelalterlichen Pranger in modernem Gewand handelt, ist im Einzelfall zu prüfen.*

Immer mehr Datenbanken mit „angeblich" unzuverlässigen Schuldnern, Mietern oder Handwerkern werden in das weltweite Web gestellt. Interessengruppen veröffentlichen Informationen über Unternehmen, um auf Defizite in der Wirtschaft hinzuweisen. Auf der Website „MeinProf.de" können Studenten Dozenten bewerten. Auf der Internetseite von Fußballverbänden sind die ungekürzten Urteile des Sportgerichts abrufbar. Darüber hinaus werden Spielersperren bzw. andere Strafen für Spieler durch die Rechtsorgane der Fußballverbände veröffentlicht.

Eine einheitliche rechtliche Würdigung von Datenbanken im Internet ist nicht möglich. In manchen Fällen – wie z. B. bei der Veröffentlichung von Spielersperren – müssen die Vereinsmitglieder bei Eintritt in den Verein eine entsprechende Einwilligungserklärung abgeben. In anderen Fällen sind die zusammengetragenen Fakten, die erst in ihrer Komplexität Bewertungen schaffen, öffentlich zugänglich, wie z. B. bei einem Unternehmen, das anhand von ebay-Profilen Bewertungen über ebay-Mitglieder aufbereitet und neu generiert, die bei ebay selbst in dieser Form nicht abrufbar sind. Bei manchen Bewertungsdatenbanken stellt sich zudem die Abgrenzungsfrage personenbezogener Daten von Meinungsäußerungen.

Nicht immer hängt die Frage der Zulässigkeit von Internetdatenbanken von datenschutzrechtlichen Gesichtspunkten ab. Handelt es sich nicht um personenbezogene Daten natürlicher Personen, richtet sich die Zulässigkeit

nach zivilrechtlichen oder auch strafrechtlichen Regelungen. So kann der Inhalt der Veröffentlichung möglicherweise einen Straftatbestand der Beleidigung, üblen Nachrede oder Verleumdung erfüllen oder gegen das Urheberrecht verstoßen.

Soweit das Datenschutzrecht einschlägig ist, wird in die Beurteilung der Zulässigkeit der einzelnen Datenbank eine Interessenabwägung einfließen müssen. In vielen Fällen besteht ein unbestreitbares Informationsinteresse an der Veröffentlichung. Es müssen aber auch hier die Interessen der Betroffenen berücksichtigt werden. So kann es z. B. für einen „angeblichen" Schuldner gute Gründe geben, die Forderung nicht zu begleichen, wenn er sie nicht anerkennt. Zu berücksichtigen ist in jedem Einzelfall auch die Besonderheit von Veröffentlichungen im Internet. Allen Internetdatenbanken ist gemeinsam, dass die Informationen an eine weltweite, unbestimmte und grundsätzlich unbegrenzte Öffentlichkeit gelangen. Die Nutzbarkeit der Daten wird durch eine Vielzahl von Suchdiensten erleichtert, die nicht allein das Auffinden der Information ermöglichen, sondern auch die Informationsverknüpfung unter Einbeziehung anderer im Netz verfügbarer Inhalte. Darüber hinaus ist davon auszugehen, dass die Informationen im Internet für einen langen oder gar unbegrenzten Zeitraum bereitgehalten werden.

Datenbanken müssen auch im Internet bestimmten Regeln unterliegen. Betreiber dürfen durch die Veröffentlichung negativer Informationen Menschen nicht schutzlos einem weltweiten Publikum preisgeben. Ich werde daher die Entwicklung weiter beobachten und daraufhin prüfen, ob die bestehenden Sanktionsmöglichkeiten ausreichend sind.

### 10.8.2 Insolvenzbekanntmachungen in Zukunft nur noch elektronisch

*Der Trend zum endgültigen Abschied von Printveröffentlichungen bei amtlichen Bekanntmachungen setzt sich fort. Damit darf jedoch das technisch machbare Schutzkonzept nicht aufgegeben werden.*

Wie das zum 1. Januar 2007 in Kraft getretene Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) setzt auch das Insolvenzrecht zukünftig auf elektronische Bekanntmachungen. Der Entwurf eines Gesetzes zur Vereinfachung des Insolvenzverfahrens (Bundesratsdrucksache 549/06) sieht eine völlige Abkehr von den Printveröffentlichungen und als Regelfall nur noch die bislang fakultativ mögliche (§ 9 Abs. 1 Satz l Insolvenzordnung (InsO)) elektronische Bekanntmachung im Internet vor. Sämtliche Insolvenzbekanntmachungen sollen auf einer bundeseinheitlichen Internetplattform dokumentiert werden und auf diese Weise die Senkung der Bekanntmachungskosten bewirken und die Recherchemöglichkeiten verbessern.

Auf der anderen Seite aber berührt dieser „Medienwechsel" die Persönlichkeitsrechte der betroffenen Insolvenzschuldner in einer anderen Qualität, da die Daten nun weltweit von jedermann abgerufen werden können. Zudem besteht die Gefahr, dass die Daten auch dann noch im Internet gefunden werden können, wenn sie von der eingebenden Stelle längst gelöscht wurden, da Originalseiten auf anderen Internet-Servern gespiegelt werden. Die Gewährleistung des erforderlichen Datenschutzniveaus ist daher von entscheidender Bedeutung. Bisher maßgeblich sind die nach den Vorgaben des § 9 Abs. 2 Satz 3 InsO vom Bundesministerium der Justiz in der Rechtsverordnung vom 12. Februar 2002 (BGBl. I S. 677) – unter meiner Beteiligung – getroffenen Regelungen. Diese enthalten insbesondere Löschungsfristen sowie Vorschriften, die sicherstellen, dass die Veröffentlichungen unversehrt, vollständig und aktuell bleiben, jederzeit ihrem Ursprung nach zugeordnet und nach dem Stand der Technik durch Dritte nicht kopiert werden können.

Auf Betreiben des Bundesrates ist nun bereits mit Wirkung zum 1. Januar 2007 die bisher in § 9 Abs. 2 Satz 3 Nr. 3 InsO enthaltene Kopierschutzregelung entfallen (Artikel 12 Abs. 2 EHUG), weil sie nach dem gegenwärtigen Stand der Technik weitgehend leer laufe.

Ich halte dies vor dem Hintergrund der Umstellung ausschließlich auf den elektronischen Betrieb nicht für das richtige Signal. Der Gesetzgeber ist vielmehr in der Pflicht, im Interesse der Persönlichkeitsrechte der Betroffenen ausdrücklich klarzustellen, dass die Verbreitung der Insolvenzdaten durch Dritte im Internet – insbesondere nach Löschung der Veröffentlichung aus dem amtlichen Informationssystem – verboten ist. Auch wenn ein hundertprozentiger Kopierschutz technisch tatsächlich nicht möglich ist, so wird mit dem Festhalten an dieser Forderung jedenfalls das technisch machbare Schutzniveau vorgeschrieben. Dies kann nicht ersatzlos entfallen. Zumindest muss über technische und rechtliche Alternativen nachgedacht werden, wie zukünftig wirkungsvoll verhindert werden kann, dass amtlich bekannt gemachte personenbezogene Daten missbräuchlich genutzt werden. Hierbei handelt es sich angesichts des allgemeinen Trends zur Internetveröffentlichung nicht um ein speziell insolvenzrechtliches, sondern um ein grundsätzliches datenschutzrechtliches Problem. Im Hinblick auf technische Möglichkeiten zum Schutz von Internetveröffentlichungen hilft u. U. ein Blick auf Verfahren, durch die kommerzielle Urheberrechte geschützt werden sollen (vgl. Nr. 6.6). Ein möglicher rechtlicher Ansatzpunkt ist die Bewehrung durch eine Straf- bzw. Bußgeldvorschrift. Hierüber diskutiere ich bereits mit meinen Länderkolleginnen und -kollegen. Darüber hinaus sind die bestehenden zivilrechtlichen Unterlassungs- und Schadensersatzansprüche auf ihre Effizienz und möglichen Nachbesserungsbedarf hin zu überprüfen. Den hierfür federführenden Ressorts biete ich meine Unterstützung an.

## 10.9 Das Telemediengesetz – was lange währt, ...?

*Das Telemediengesetz befindet sich zur Zeit in der parlamentarischen Beratung und soll voraussichtlich im Frühjahr 2007 in Kraft treten.*

Seit Juni 2006 liegt der Entwurf des Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz (ElGVG) vor. Hinter der sperrigen Bezeichnung verbirgt sich im wesentlichen das Telemediengesetz, mit dem die Regelungen im Bereich der Tele- und der Mediendienste vereinheitlicht werden (vgl. 20. TB Nr. 13.7). Die Datenschutzvorschriften, die bislang noch im Teledienstedatenschutzgesetz (TDDSG) bzw. im Mediendienstestaatsvertrag (MDStV) der Länder festgelegt sind, wurden integriert. Wie vorgesehen, hat es dabei im Wesentlichen keine materiell-rechtlichen Änderungen gegeben. Ich begrüße, dass endlich eine Rechtsunsicherheit beseitigt wird: In der Begründung zum Gesetzesentwurf wird klargestellt, dass für Internet-Zugangsprovider, Anbieter von Internet-Telefonie und E-Mail-Diensten ausschließlich das Telekommunikationsdatenschutzrecht gilt. Damit wird auch die bisweilen strittig diskutierte Frage meiner Zuständigkeit für diese Bereiche eindeutig beantwortet.

Allerdings soll die bereits bestehende Befugnis der Diensteanbieter ausgeweitet werden, Daten ihrer Kunden für Strafverfolgungszwecke an die zuständigen Stellen herauszugeben. Zukünftig dürfen auch Anfragen der Verfassungschutzbehörden und Nachrichtendienste zu deren Aufgabenerfüllung beantwortet werden. Im Vorgriff auf die Umsetzung der IP-Enforcement-Richtlinie (vgl. Nr. 6.5) wird die Herausgabebefugnis ebenfalls zur Durchsetzung der Rechte am geistigen Eigentum erteilt. Diese Aufweichung der Zweckbindung halte ich für sehr bedenklich, da zu befürchten ist, dass dies nur der Anfang einer Entwicklung ist, die immer mehr Begehrlichkeiten weckt und die Daten der Nutzer für immer weitere Dritte verfügbar macht.

Zum Schutz der Empfänger elektronischer Werbung wurden im Sinne einer größeren Transparenz Regelungen aufgenommen, die das Verschleiern oder Verheimlichen des Absenders und des kommerziellen Charakters einer Werbe-E-Mail verbieten und ein Zuwiderhandeln mit einem Bußgeld belegen. Die tägliche Spam-Flut wird dadurch wohl kaum gemindert, befinden sich doch die meisten und „dreistesten Spammer“ außerhalb des Geltungsbereichs deutscher Gesetze und außer Reichweite der zuständigen Behörden (vgl. 20. TB Nr. 13.8). Die vormals „Anti-Spam-Gesetz“ genannten Regelungen stellen sich nun – realistischer – als Vorschriften für Firmen dar, die ganz legal elektronische Werbung versenden wollen.

Zu meinem Bedauern wurden Selbstregulierungsmodelle, wie z. B. Auditierungsverfahren oder Gütesiegel, in den Gesetzentwurf nicht aufgenommen. Nach wie vor halte ich angesichts der immer größer und damit unübersichtlicher werdenden Angebote im Internet solche Modelle, die neben den staatlichen Datenschutzaufsichtsstrukturen bestehen könnten, für nutzbringend: Sie erleichtern dem Nutzer die Auswahl der Angebote, stärken die Eigenverantwortung der Wirtschaft, stellen die Qualität der Angebote hinsichtlich der gesetzlichen Anforderungen und der notwendigen Transparenz sicher und verbessern letztendlich auch den Datenschutz.

## 10.10 Suchmaschinen: Wohl und Wehe einer hilfreichen Erfindung

*Will man den Datenschutz bei Suchmaschinen verbessern, hilft nur eine weltweite Aktion.*

Ohne Suchmaschinen würde sich wohl kaum einer im Internet zurechtfinden. Soviel zu der positiven Seite. Die Kehrseite der Medaille: Die Inanspruchnahme führt zu erheblichen Gefährdungen der Privatsphäre der Nutzer, da die Anbieter von Suchmaschinen die Möglichkeit haben, Interessensprofile aufzuzeichnen. Wenn sie dann mit den Daten z. B. aus Anmeldeformularen zusammengeführt werden, ist eine Personalisierung der Profile ein Leichtes. Und bei Forenbeiträgen, die unter einer persönlichen E-Mail-Adresse eingestellt werden, ist die Zusammenführung gar nicht mehr erforderlich.

In der letzten Zeit haben sich viele Nutzer von Suchmaschinen bei mir beschwert und gebeten, Abhilfe zu schaffen. Bei deutschen Suchmaschinenbetreibern ist das einfach, aber sobald es um im Ausland ansässige Anbieter geht, wird es ungleich schwerer. Daher kann nur eine weltweite konzertierte Aktion so viel Druck auf die Suchmaschinenanbieter ausüben, dass ein nachhaltiger Erfolg gewährleistet ist.

Die 28. Internationale Konferenz der Datenschutzbeauftragten fordert in einer Entschließung (vgl. Anlage 7) die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern (s. Kasten zu Nr. 10.10).

## 10.11 Sechstes und siebtes Symposium in Bonn

*Beide Symposien wurden erneut mit großem Interesse aufgenommen.*

Mit jeweils rund 100 Teilnehmern wurde das sechste Symposium „Datenschutz in der Telekommunikation und bei Telediensten“ am 22. November 2005 und das siebte Symposium „Datenschutz bei der Telekommunikation und im Internet“ am 14. November 2006 durchgeführt. Es hat sich inzwischen als Wissensforum für die Teilnehmer aus Wirtschaft und Datenschutzbehörden etabliert.

Anlässlich des sechsten Symposiums habe ich u. a. die Weiterentwicklung des traditionellen Fernmeldegeheimnisses zu einem allgemeinen Mediennutzungsgeheimnis gefordert. Denn das Fernmeldegeheimnis hat angesichts der Digitalisierung und der Vernetzung immer weiterer Lebensbereiche heute größere Bedeutung denn je und ist Gradmesser unserer freiheitlich-demokratischen Gesellschaft. Eine Informations- und Wissensgesellschaft kann sich nur demokratisch ausbilden, wenn gerade auch die

digitale Kommunikation frei von Überwachung durch Dritte ist, egal ob es sich dabei um staatliche Stellen oder um Unternehmen handelt.

Das siebte Symposium gab einen weit gefächerten Überblick über die Novellierung des Telekommunikationsgesetzes, über neue Entwicklungen des Datenschutzrechts im Bereich des Internets, zur Neuordnung der verdeckten Ermittlungsmaßnahmen im Strafrecht und zur Umsetzung der Europäischen Richtlinie zur Einführung einer Vorratsdatenspeicherung von Telefon- und Internetdaten (s. o. Nr. 10.1).

Ich habe anlässlich des siebten Symposiums darauf hingewiesen, dass effektive Strafverfolgung einerseits und Grundrechtswahrung andererseits sorgsam austariert werden müssen, der Kernbereich privater Lebensgestaltung zu respektieren ist und die grundrechtsschützenden Verfahrenssicherungen gestärkt werden müssen. Die Telekommunikationsüberwachung stellt einen tiefen Eingriff in das Fernmeldegeheimnis dar und muss deshalb „ultima ratio“ bleiben.

Kasten zu Nr. 10.10

- Anbieter von Suchmaschinen sollten ihre Nutzer in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.
- Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollen Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und Weise anbieten. Insbesondere sollen sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden kann, oder über die Nutzer von Suchmaschinen selbst, aufzeichnen. Nach dem Ende eines Suchvorgangs sollen keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, die für die Erbringung eines Dienstes notwendig sind, speichern zu lassen (z.B. zur Nutzung für spätere Suchvorgänge).
- In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.

## 11 Postunternehmen

### 11.1 Datenschutz bei der Deutschen Post AG

Die Deutsche Post AG zählt nach wie vor zu den größten Postdienstleistern auf dem deutschen Markt. Täglich befördert und verteilt sie 70 Millionen Sendungen innerhalb Deutschlands, aber auch vom und in das Ausland.

Doch der Bürger zieht um, fährt in Urlaub oder ist zum Zeitpunkt der Zustellung auf der Arbeit. Wird auch unter diesen Umständen Datenschutz gewährleistet?

**Die Ablagestellen der Deutschen Post AG**

*In verschiedenen Städten wurden Postsendungen in unverschlossenen Behältnissen oder in unsicheren Ablagestellen deponiert. Dieser Mangel wurde nach einer Beanstandung behoben.*

Seit 20 Jahren gibt es für Briefzusteller Postablagekästen bzw. Postablagestellen. Hier werden Sendungen der Deutschen Post AG abgelegt, die die Zustellkraft im Laufe des Zustellgangs aufnimmt. Neben den Postablagekästen, die nur mit Genehmigung der betroffenen Kommunalverwaltung im öffentlichen Verkehrsraum aufgestellt werden dürfen, werden Ladenlokale oder Räumlichkeiten bei Privatpersonen als Postablagestellen genutzt.

Eine Postablagestelle soll für den allgemeinen Publikumsverkehr uneinsehbar sowie vor dem Zugriff Dritter und vor Witterungseinflüssen geschützt sein. In der Vergangenheit wurden jedoch mit den Betroffenen nur mündliche Vereinbarungen hierüber getroffen. Postablagestellen und -kästen werden teils durch eigenes Personal der Deutschen Post AG, teils durch Auftragnehmer von Transportleistungen beliefert. Alle Auftragnehmer von Transportleistungen sind vertraglich auf die Einhaltung des Post-, Daten- und Betriebsgeheimnisses verpflichtet.

In der Vergangenheit, zuletzt zu Beginn des Jahres 2006, wurden wiederholt Kisten oder Beutel unverschlossen oder in unsicheren Ablagestellen gelagert, die für Dritte zugänglich waren. Dritte konnten dadurch Kenntnis vom Inhalt der Postsendungen, zumindest aber von den näheren Umständen des Postverkehrs (Empfänger, Absender) bekommen.

Somit lag ein Verstoß gegen die Verpflichtung zur Wahrung des Postgeheimnisses vor.

Da man hier nicht von nur vereinzelten Vorfällen oder unerheblichen Mängeln sprechen konnte, habe ich diesen Verstoß als schwerwiegend bewertet und eine Beanstandung gemäß § 25 BDSG ausgesprochen.

Die Deutsche Post AG hat daraufhin bundesweit Maßnahmen zur Beseitigung der Mängel eingeleitet. Neben einer ausreichenden Ausstattung der Zustellstützpunkte mit geeigneten Behältnissen und Verschlussmaterial wurden die Zustellkräfte und Fahrer über den korrekten Umgang mit dem Postablagegut belehrt. Darüber hinaus wurden vereinzelt problematische Ablagestellen aufgegeben. Im Herbst 2006 wurden die Maßnahmen nach Angaben der Deutschen Post AG erfolgreich beendet.

Auf meine Anregung schließt die Deutsche Post AG nunmehr Verträge mit Postablagestellengebern ausschließlich schriftlich; bereits bestehende Verträge werden nachträglich schriftlich fixiert. Dies unterstreicht die Verpflich-

tung zur Wahrung des Postgeheimnisses und trägt damit der Einhaltung des Datenschutzes Rechnung.

Insgesamt bewerte ich die getroffenen Maßnahmen als geeignet, um die Wahrung des Postgeheimnisses sicherzustellen. Ich erkenne an, dass die Deutsche Post AG unmittelbar nach den Vorfällen erste Maßnahmen zur Beseitigung der Mängel eingeleitet hat.

Darüber hinaus begrüße ich die Bereitschaft der Deutschen Post AG, ihr Qualitätsmanagement durch intensivere Kontrollen der Zustellpraxis zu verbessern. Diesen Prozess werde ich durch Besichtigungen von Zustellstützpunkten und Ablagestellen weiter begleiten.

**Kontrolle des Nachsendeauftragszentrums München**

*Die Deutsche Post AG verarbeitet jährlich Daten aus 3,5 Millionen Nachsendeaufträgen.*

Die Deutsche Post AG bietet im Falle eines Umzugs oder einer Abwesenheit vom Wohnort die Zustellung an eine neue oder vorübergehend andere Anschrift an. Damit die Nachsendung funktioniert, hat die Deutsche Post AG 1996 ein IT-gestütztes Nachsendeauftragszentrum (INA) eingerichtet, in dem sämtliche für diese Dienstleistung erforderliche Daten verarbeitet werden. Inzwischen wurde der Aufgabenbereich auf die Lagerung und Rücksendung von nicht zustellbaren Postsendungen ausgedehnt. Weitere Zentren für Nachsendung und Lagerung (ZNL) – so inzwischen die offizielle Bezeichnung – wurden in Magdeburg, Köln und Bremen eingerichtet.

Im vergangenen Jahr habe ich mich von dem korrekten Umgang des Nachsendezentrums der Deutschen Post AG mit den ihm anvertrauten Daten überzeugt. Jährlich werden ca. 3,5 Millionen Nachsende- bzw. Lagerungsaufträge erteilt, 20 v. H. davon über das Internet. Bei Beantragung einer Nachsendung oder Lagerung in einer Postfiliale werden Name und Vorname sowie entgeltrelevante Daten erhoben. Die weiteren Daten des vollständig ausgefüllten und unterschriebenen Nachsendeantrags werden im ZNL München mittels Videocodierung automatisch erfasst. Enthält ein Antrag Angaben, die nicht automatisch gelesen werden können oder die fehlerhaft sind, wird er an einem Bildschirmplatz unter Zuhilfenahme allgemein zugänglicher Datenquellen überprüft und korrigiert. Somit ist trotz der weit reichenden Automatisierung im Nachsendeverfahren menschliches Eingreifen weiterhin erforderlich. Einen unsachgemäßen Umgang mit den Daten aus den Nachsendeanträgen oder die Nutzung unzulässiger Datenquellen konnte ich nicht feststellen.

In mehreren Eingaben haben Petenten angeregt, bei Erteilung eines Nachsendeauftrags die Vorlage des Ausweises vorzuschreiben. Diese Anregung unterstütze ich nicht, weil das Verfahren durch ein Bestätigungsschreiben der Deutschen Post AG an die alte Anschrift des Antragsstellers abgesichert ist. Ich halte dies für ausreichend, um Missbrauchsfälle weitgehend auszuschließen.

**Empfängerdateien bei der Deutschen Post AG – Was weiß Ihr Zusteller wirklich?**

*Welche Daten sind für die tägliche Zustellung notwendig? Welche Daten darf die Deutsche Post AG speichern?*

Auch die tägliche Zustellung an die übliche Hausanschrift kann zuweilen problematisch sein. Im Berichtszeitraum habe ich mich beim Besuch eines Briefzentrums sowie verschiedener Zustellstützpunkte der Deutschen Post AG über die Arbeitsabläufe und über die dabei verwendeten Daten informiert. Die Deutsche Post AG hat durch eine hochgradige Technisierung der Bearbeitungsabläufe und durch die Konzentration der Bearbeitungsstellen die Briefbeförderung und Einhaltung der Zustellzeiten optimiert. Ferner wird durch die Technisierung menschliches Fehlverhalten reduziert. Darüber hinaus führt die Deutsche Post AG in ihren Zustellbezirken sog. „Mieterbücher“, um Zustellfehler zu vermeiden. Aus datenschutzrechtlicher Sicht sind diese Mieterbücher, in denen Empfänger und Zustellbesonderheiten vermerkt sind, sehr problematisch. Nach der Postdienste-Datenschutzverordnung (PDSV), die den Schutz personenbezogener Daten von Absendern und Empfängern regelt (s. Kasten zu Nr. 11.1), dürfen Empfängerdaten ohne Einwilligung des Betroffenen grundsätzlich nicht gespeichert werden. Eine Ausnahme liegt jedoch vor, wenn Daten über Zustellbesonderheiten zum Zweck der ordnungsgemäßen Zustellung im Einzelfall erhoben werden (§ 7 Abs. 4 PDSV). Hingegen reicht es nicht aus, wenn diese Datei nur zur Erleichterung innerbetrieblicher Abläufe genutzt wird. Die Regelungen der PDSV sollen in erster Linie die Interessen der Kunden und der Empfänger von Postsendungen schützen; eine Auslegung im Sinne der Interessen der Postdienstleister erfolgt nur nachrangig. Insofern dürfen Mieterbücher nicht generell in allen Zustellbezirken geführt werden. Die Zustellkräfte der Deutschen Post AG nutzen die Informationen über die Empfänger als Hilfe für die Sortierung der zuzustellenden Sendungen. Dies erscheint in Zustellbezirken mit unübersichtlichen Briefkastenanlagen, häufig wechselnden Empfängern oder ausländischen Nachnamen nicht nur sinnvoll, sondern auch notwendig. Hierin sehe ich die Anforderung des § 7 Abs. 4 PDSV für eine ordnungsgemäße Zustellung als erfüllt an. Da die Postdienste-Datenschutzverordnung keine flächendeckende Erfassung der Empfängerdaten erlaubt, habe ich die Deutsche Post AG aufgefordert, ihre Mieterbücher zu prüfen und an die gesetzlichen Voraussetzungen anzupassen. Durch laufende Kontrollen werde ich die Einhaltung dieser Vorschrift weiterhin überwachen.

**Ausweispflicht bei der Abholung nachweispflichtiger Sendungen**

*Warum werden die Daten aus dem Personalausweis erfasst, wenn eine nachweispflichtige Sendung abgeholt wird?*

Immer wieder erreichen mich Eingaben, in denen die Speicherung der Daten aus Personalausweis oder Reisepass bei Abholung einer nachweispflichtigen Sendung

beklagt wird. Bereits in meinem 19. Tätigkeitsbericht habe ich die Rechtmäßigkeit dieses Verfahren anhand der Paketabholung erläutert (Nr. 12.3). Dennoch stellt man mir nach wie vor die Frage, wieso es der Deutschen Post AG nicht genügt, wenn ein Ausweis zur Feststellung der Identität vorgezeigt wird. Bei nachweispflichtigen Sendungen verpflichtet sich der Postdienstleister zur Zustellung an die richtige Empfangsperson. Doch nicht immer kennt der Postdienstleister den Empfänger einer Sendung – ob bei Auslieferung an der Haustür oder bei Aushändigung in einer Filiale. Insofern dient die Vorlage des Ausweises zur Feststellung der Identität. Darüber hinaus erfasst der Dienstleister Ausweisart, Ausweisnummer, Ausstellungsdatum und ausstellende Behörde, um gegenüber dem Absender belegen zu können, dass er die Identität geprüft hat und somit seinen Pflichten aus dem Beförderungsvertrag nachgekommen ist. Dies ist nicht nur der Deutschen Post AG vorbehalten; die dem Verfahren zugrunde liegende Vorschrift der Postdienst-Datenschutzverordnung richtet sich an alle Postdienstleister. Die wiederholten Eingaben zu diesem Thema führe ich auf zwei Umstände zurück: Zum einen hat die Beförderung nachweispflichtiger Sendungen in den vergangenen Jahren – nicht zuletzt durch einen gestiegenen Handel via Internet – zugenommen. Andererseits werden die Bürger immer kritischer, wenn es um die Erfassung ihrer Daten geht; im Grunde eine erfreuliche Entwicklung.

**Mobile Infopoints der Deutschen Post AG – Wenn die Werbung das Handy anruft ...**

*Bereits im Jahr 2005 hat die Deutsche Post AG probeweise mobile Werbetrailer eingesetzt, die die Werbung direkt aufs Handy bringen.*

Alles wird mobiler – auch die Werbung. So bekommt man heutzutage Reklame direkt auf sein Mobiltelefon, wenn man über eine aktive Infrarot- oder Bluetooth-Schnittstelle verfügt. Erstmals wurde diese Technik im Jahr 2004 auf Messen eingesetzt. Auch die Deutsche Post AG setzt auf die mobile Werbung: Auf Mobile-Point-Stellen werden der Öffentlichkeit eigene Produktinformationen oder die Angebote von Kooperationspartnern präsentiert. Hierbei werden verschiedene Daten generiert. Zum einen werden Mobilfunknummer, Mobiltelefontyp sowie Standort, Datum und Uhrzeit über die aktive Schnittstelle erfasst. Zum anderen löst die Antwort des Handynutzers die Erhebung von Name und Vorname, der postalischen sowie der E-Mail-Adresse und anderen – je nach Produkt unterschiedlichen – Daten aus.

Aus datenschutzrechtlicher Sicht ist die Vorgehensweise akzeptabel, sofern der Nutzer aktiv in die Datenerhebung einwilligt. Ferner dürfen die Daten nur für die eine angebotene Aktion (z. B. Teilnahme am Gewinnspiel, Herunterladen eines Klingeltons etc.) verwendet werden. Sollen die Daten für weitere Werbemaßnahmen genutzt werden, muss der Betroffene auch hierin aktiv einwilligen.

Kasten zu Nr. 11.1

**Auszug aus der Postdienste-Datenschutzverordnung; Zustellbesonderheiten**

§ 3 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Diensteanbieter dürfen im Zusammenhang mit der Erbringung von Postdiensten personenbezogene Daten der am Postverkehr Beteiligten erheben, verarbeiten und nutzen, soweit diese Verordnung es erlaubt oder der Beteiligte eine Einwilligung erteilt hat, die den Vorschriften des Bundesdatenschutzgesetzes und dieser Verordnung entspricht. Der Beteiligte kann die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Satz 1 gilt auch für Postsendungen, die in den Betriebsablauf eines Diensteanbieters gelangt sind, jedoch nicht zur Beförderung durch ihn bestimmt waren.

§ 7 Adressdaten

(4) Diensteanbieter dürfen im Einzelfall zur Gewährleistung einer ordnungsgemäßen Zustellung von Postsendungen personenbezogene Daten über besondere bei der Zustellung an einen Adressaten zu beachtende Umstände erheben, verarbeiten und nutzen. Die Übermittlung dieser Daten an Dritte bedarf der Einwilligung des Beteiligten; zur Einwilligung sind ihm die zur Übermittlung vorgesehenen Daten mitzuteilen. Satz 2 gilt nicht, soweit die Übermittlung der Daten an den Absender für den Nachweis erforderlich ist, dass die förmliche Zustellung von Schriftstücken nach den Vorschriften der Prozessordnungen und der Gesetze, die die Verwaltungszustellung regeln, erfolgt ist.

Zustellbesonderheiten:

Eine Zustellbesonderheit liegt dann vor, wenn die Umstände deutlich vom Standard abweichen: 9 Briefkästen in einer Briefkastenanlage zählen nicht dazu, eine Briefkastenanlage mit 120 Briefkästen sehr wohl. Ferner fallen Umstände darunter, die das Auffinden des Briefkastens erschweren, z. B. Vorrichtung hinter dem Haus, die eine Gefahr bei der Zuführung zum Briefkasten darstellen (bissiger Hund) sowie örtliche und zeitliche Besonderheiten, z. B. Abgabe beim Kiosk auf der anderen Straßenseite; Zustellung nur nach 16.00 Uhr.

### 11.2 UPS – Verbindliche Vertragsregeln für alle Töchter in Europa (Europäisches Addendum)

*UPS (United Parcel Service) beabsichtigt, den weltweiten Datenverkehr zwischen den Konzernunternehmen auf eine einheitliche rechtliche Grundlage zu stellen, die den datenschutzrechtlichen Anforderungen in Deutschland und in der Europäischen Union genügt.*

Im Sommer 2003 habe ich UPS eine Genehmigung zur Übermittlung der in Deutschland erhobenen Daten in die USA nach § 4c Abs. 2 BDSG erteilt (vgl. 20. TB Nr. 14.1.2). Nunmehr soll der weltweite konzerninterne Datenverkehr auf eine einheitlich rechtliche Grundlage gestellt werden. Dazu hat UPS zunächst allgemein verbindliche Regelungen (Global Data Transfer Agreement) für den Datenverkehr der Unternehmen untereinander geschaffen. Darüber hinaus möchte UPS die Übermittlung von Daten aus der EU in Drittstaaten in einem speziellen EU-Addendum (*Nachtrag, Ergänzung*) zum Global Data Transfer Agreement regeln, um den besonderen Anforderungen des europäischen Datenschutzrechtes zu genügen. So weist das Addendum ein höheres Datenschutzniveau gegenüber dem Global Data Transfer Agreement auf: Werden Datenschutzrechte verletzt, können betroffene Personen – auch aus Drittstaaten – in jedem EU-Mitgliedsstaat ihr Recht gegenüber UPS geltend machen. Als Vorsitzender der Artikel 29-Gruppe werde ich das Vorhaben von UPS auf europäischer Ebene koordinieren, um eine einheitliche Genehmigungspraxis für alle Mitgliedstaaten sicherzustellen (vgl. Nr. 3.3.6).

## 12 Verkehr

*Der Einsatz elektronischer Systeme im Straßenverkehr darf nicht zum gläsernen Autofahrer führen.*

Wir leben in einer mobilen Gesellschaft. Auf unseren Straßen fahren mehr als 54 Millionen zugelassene Kraftfahrzeuge, darunter 45 Millionen Personenkraftwagen und 2,5 Millionen Lastkraftwagen. Dazu kommen viele Millionen ausländische Fahrzeuge. Die meisten Fahrzeuge werden täglich oder beinahe täglich genutzt: Für den Weg zur Arbeit, zum Kindergarten, zum Arzt oder um Güter zu transportieren. Dabei werden jedes Jahr Milliarden Kilometer zurückgelegt.

Auf der anderen Seite haben sich die technischen Möglichkeiten zur Ortung von Fahrzeugen und zur Registrierung und Auswertung der von ihnen zurückgelegten Wege in den letzten Jahren stark verbessert: Navigationssysteme erleichtern es, schneller zum Ziel zu gelangen. In manchen Fahrzeugen sind Ortungseinrichtungen angebracht, um sie im Falle eines Diebstahls aufspüren zu können. Auch beim Flottenmanagement kommen in zunehmendem Umfang Ortungssysteme zum Einsatz. Eine Vielzahl elektronischer „Helferlein“ sind mittlerweile in fast jedem neuen Kraftfahrzeug serienmäßig eingebaut, um dem Fahrer oder der Fahrerin zur Seite zu stehen und Fahrfehler automatisch zu korrigieren. Damit sie dies leisten können, müssen sie laufend bestimmte Fahrtparameter auswerten: Geschwindigkeit, Bremsfunktion, Kurvenverhalten, Verbrauchswerte. Der Bordcomputer zeigt an, wenn eine Fehlfunktion vorliegt und wann das Fahrzeug wieder gewartet werden muss. Durch Verbindung verschiedener Technologien, Satellitenortung (GPS oder bald noch genauer: Galileo), Sensorik und Funk- bzw. Mobiltelefontechnik (GPS, UMTS) wird eine Vielzahl neuer Dienste möglich, an die noch vor wenigen Jahren nicht zu denken war. Zu diesen neuen Anwendungen gehört auch das Anfang 2005 in Betrieb gegangene Autobahnmaut–System für schwere LKW.

Wo viel Licht ist, da ist bekanntlich auch viel Schatten. Dieses Sprichwort gilt auch für die Verkehrstelematik. Die neuen Techniken haben das Potenzial, die Verkehrsteilnehmer lückenlos zu überwachen, zu registrieren und die dabei gewonnenen Daten mit umfangreichen anderen Datensammlungen, etwa mit Verbindungsdaten der Telekommunikation, staatlichen Datenbanken oder auch Kundenprofilen abzugleichen. Im Folgenden sollen verschiedene Anwendungsbereiche näher beleuchtet werden: Von der LKW–Autobahnmaut bis zu Systemen, die die Verkehrssicherheit erhöhen sollen (Unfalldatenschreiber und eCall).

### 12.1 LKW-Maut

Seit Anfang 2005 erhebt Toll Collect GmbH im Auftrag des Bundesamtes für Güterverkehr (BAG) auf Grund des Autobahnmautgesetzes (ABMG) für schwere LKW über 12 t Gesamtgewicht Maut. Beim Betrieb fallen zwei Arten von Bewegungsdaten an: Fahrtbezogene Daten (§ 4 Abs. 2 ABMG), z. B. Strecke, Ort und Zeit, und kontrollbezogene Daten (§ 7 Abs. 2 ABMG), z. B. Bild des Fahrzeugs, Name der Person. Die Mautdaten dürfen ausschließlich für die Zwecke des ABMG verarbeitet und genutzt werden. Dadurch sind alle fahrtbezogenen Daten, die im Rahmen des Mautsystems erhoben werden, dem Zugriff der Ermittlungsbehörden entzogen.

Der Umfang der bei der Autobahnmaut erhobenen Daten und ihre Verwendung müssen auch bei der immer wieder aufflammenden Diskussion über die Ausweitung der Mautpflicht auf andere Fahrzeuge beachtet werden. Ich hielte es für keineswegs akzeptabel, das jetzige, auf schwere LKW beschränkte Verfahren, bei dem eine Vielzahl von Daten über jeden zurückgelegten Kilometer erfasst werden, unverändert auf PKW zu übertragen. Vielmehr muss frühzeitig über Alternativen nachgedacht werden, bei denen es nicht zu einer fahrzeugbezogenen Vollüberwachung kommt.

#### Dürfen Mautdaten zur Verbrechensbekämpfung genutzt werden?

*Die Bundesregierung strebt eine Lockerung der Zweckbindungsregelung im ABMG an.*

Bereits lange vor Einführung der LKW-Maut wurde darüber diskutiert, ob derartige Systeme den Datenschutz beeinträchtigen könnten. Im Mittelpunkt der Diskussion stand dabei die Frage, wie sich das Mautsystem datenschutzfreundlich ausgestalten lässt. So heißt es in einer

Entschließung in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9. März 1995:

„Mit der Einführung derartiger Verkehrstelematiksysteme besteht die Gefahr, dass personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Exakte Bewegungsprofile können dadurch erstellt werden. Damit wären technische Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil das Grundrecht auf freie Entfaltung der Persönlichkeit auch das Recht umfasst, sich möglichst frei und unbeobachtet zu bewegen. Vor diesem Hintergrund ist es besonders wichtig, elektronische Mautsysteme datenschutzgerecht auszugestalten. Bei den anstehenden Entscheidungen sind andere Verfahren wie z. B. die Vignette einzubeziehen."

Bekanntlich hat sich der Gesetzgeber bei der Einführung der Autobahnmaut für schwere LKW gleichwohl für ein System entschieden, bei dem in großem Umfang individualisierte Daten sowohl beim Betreiber des Mautsystems als auch beim Bundesamt für Güterverkehr anfallen (s. Kasten zu Nr. 12.1). Um den mit der Datenspeicherung verbundenen Risiken für den Datenschutz Rechnung zu tragen, wurde zugleich eine strikte Zweckbindung dieser Daten in §§ 2 Abs. 2 und 7 Abs. 2 ABMG verankert. Nachdem das Amtsgericht Gummersbach (Az.: 10a GS 239/03) gleichwohl die Verwendung von Mautdaten für Zwecke der Strafverfolgung zugelassen hatte, wurde diese Zweckbindungsregelung durch eine gesetzliche Klarstellung vom 2. Dezember 2004 noch verstärkt (vgl. 20. TB Nr. 22.1.2).

Damit waren die Diskussionen über die Verwendung der Mautdaten allerdings noch lange nicht beendet. Nach verschiedenen Kapitalverbrechen, in die schwere Lastwagen beziehungsweise ihre Fahrer verwickelt waren, wurde im parlamentarischen Bereich die Frage aufgeworfen, inwieweit die im Gesetz verankerte strikte Zweckbindungsregelung wirklich angemessen sei. In der anschließenden Debatte habe ich darauf aufmerksam gemacht, dass zahlreiche Beispiele belegen, dass die Lockerung einer Zweckbindung zu letztlich sehr weitgehenden Verwendungsmöglichkeiten geführt hat. Gleichwohl habe ich die politischen Forderungen nicht schlichtweg abgelehnt, sondern eine sorgfältige Verhältnismäßigkeitsprüfung angemahnt. Dabei geht es mir zunächst um die Frage, ob die Mautdaten überhaupt für Strafverfolgungszwecke geeignet sind. Falls der Nachweis hierfür geführt werden kann, hielte ich nur eine Verwendung für bestimmte sehr schwere Delikte, etwa Kapitalverbrechen, für vertretbar. Zudem wäre sicherzustellen, dass entsprechende Zugriffe nur nach einer richterlichen Anordnung erfolgen. Dabei müsste zudem gewährleistet sein, dass nur Daten verwendet werden, die in einem engen zeitlichen und örtlichen Zusammenhang mit der Straftat stehen, und nicht – wie bei einer Rasterfahndung – viele Unverdächtige einbezogen werden. Es darf nicht zu einer Erweiterung des bisher erhobenen Datenumfangs oder zu einer Verlängerung der Speicherdauer kommen. Wenn der Mautbetreiber Daten, die er selbst nicht benötigt, für eventuelle spätere Nachfragen der Ermittlungsbehörden vorhalten müsste, wäre das – entgegen den Vorgaben unserer Verfassung – eine unzulässige Vorratsspeicherung.

Ein erster Referentenentwurf des BMI sieht vor, die Verarbeitung und Nutzung der Mautdaten auch zur Verfolgung von „Straftaten von erheblicher Bedeutung" oder zur „Gefahrenabwehr" zuzulassen. Dies geht mir zu weit. Ich werde darauf hinwirken, eine Lösung zu finden, bei der das Gebot der Verhältnismäßigkeit gewahrt wird.

**Überprüfung des Löschkonzeptes bei Toll Collect**

*Das Löschkonzept von Toll Collect hat bei einer Kontrolle die datenschutzrechtlichen Anforderungen erfüllt.*

Ungefähr ein Jahr nach dem Start der Autobahnmaut, habe ich das Datenschutzmanagement bei Toll Collect geprüft. Nach dem ABMG hat Toll Collect die gespeicherten fahrtbezogenen Daten unverzüglich zu löschen, wenn ein Mauterstattungsverlangen nicht fristgerecht gestellt worden ist. Toll Collect führt im Rahmen des von ihr entwickelten Löschkonzeptes interne Audits durch, um die datenschutzgerechte Funktionsweise zu kontrollieren. Am Beispiel des Überwachungssystems (ÜWS), das zur Überwachung der eigenen Systeme sowie zur langfristigen Erkennung potentiellen Missbrauchs von Mautpflichtigen dient, hat mir Toll Collect die Durchführung eines solchen Audits demonstriert. Damit sollte nachgewiesen werden, dass die sich aus dem Systemlöschkonzept ergebenden Lösch- bzw. Anonymisierungsregeln greifen. Zu meiner Zufriedenheit konnte ich feststellen, dass die Löschgebote gemäß § 9 ABMG korrekt umgesetzt werden.

**Der Umgang mit den Mautdaten beim BAG auf dem Prüfstand**

*Die datenschutzrechtliche Aufsichtspflicht über Toll Collect war ein Thema eines Kontrollbesuches beim BAG.*

Bei einem neuerlichen Kontrollbesuch standen die Frage, wie das BAG seiner datenschutzrechtlichen Aufsichtspflicht gegenüber Toll Collect nachkommt, sowie der Umgang mit personenbezogenen Daten im Mittelpunkt. Nach § 7 ABMG obliegt dem BAG die Kontrolle über die Durchführung des Mautverfahrens. Hierzu liefert das interne ÜWS von Toll Collect täglich Daten an verschiedene Datenbanken des BAG. Zum einen dienen diese Daten dazu, den Betreibervertrag sowie den Datenschutz selbst bei Toll Collect zu überwachen, zum anderen verwertet das BAG diese Daten, um seinen Aufgaben aus dem ABMG gerecht zu werden. Zudem obliegt es dem BAG, für die Einhaltung der Löschfristen nach dem ABMG zu sorgen. Eine abschließende Überprüfung des Löschkonzepts war zum Zeitpunkt meines Besuches nicht möglich, da für den überwiegenden Teil der Daten der Fristablauf noch nicht eingetreten war. Soweit Daten bereits zu löschen waren, habe ich mich von der ordnungsgemäßen Durchführung überzeugt.

Bei der Besichtigung des Rechenzentrums habe ich festgestellt, dass das BAG Sicherungskopien seiner Datenbestände zieht, die derzeit unbefristet aufbewahrt werden. Aus datenschutzrechtlicher Sicht ist dies bedenklich, da diese Sicherungskopien Daten enthalten, die nach Vorgaben des ABMG bereits zu löschen gewesen wären. Das BAG hat zugesagt, ein entsprechendes Löschkonzept zu erarbeiten.

Kasten zu Nr. 12.1

Daten, die bei der LKW-Maut erhoben und gespeichert werden:

- die Höhe der entrichteten Maut,
- die Strecke, für die die Maut entrichtet wurde,
- Ort und Zeit der Mautentrichtung,
- bei Entrichtung der Maut vor der Benutzung mautpflichtiger Bundesautobahnen der für die Durchführung der Fahrt zulässige Zeitraum sowie die Belegnummer,
- Kennzeichen des Fahrzeugs oder der Fahrzeugkombination,
- für die Mauthöhe maßgebliche Merkmale des Fahrzeugs oder der Fahrzeugkombination.

**Einsatz von Videoüberwachung zur Überprüfung des Betreibervertrages**

*Die Videoüberwachung ist datenschutzrechtlich nicht zu beanstanden, da keine personenbezogene Daten erhoben werden.*

Das BAG kontrolliert, ob die im Betreibervertrag vereinbarten Leistungen von Toll Collect erbracht werden (vgl. 20. TB Nr. 22.1.4). Hierzu bedient es sich u. a. einer Videoüberwachung an den Kontrollbrücken, um deren ordnungsgemäße Funktion zu überprüfen. Das BAG setzt Videokameras ein, die den laufenden Verkehr, also mautpflichtige und nicht mautpflichtige Fahrzeuge, in einer Fahrtrichtung für ca. vier Stunden aufzeichnen. Die gewonnenen Daten werden später mit den Daten von Toll Collect abgeglichen. Gegen die Aufzeichnung der nicht mautpflichtigen Fahrzeuge hatte ich zunächst datenschutzrechtliche Bedenken, denn eine Aufzeichnung von PKW ist nach dem ABMG nicht zulässig. Deshalb hatte ich angeregt, die Videokamera dergestalt zu verwenden, dass Kfz-Kennzeichen nicht erkannt werden können, so dass keine personenbezogene Datenerhebung vorliegt. Gleichzeitig hatte ich dem BAG im Interesse höchstmöglicher Transparenz die Veröffentlichung der Tatsache und des Zwecks der Prüfung in seinem Internetportal empfohlen.

Die Videoüberwachung des BAG an den Kontrollbrücken habe ich nunmehr vor Ort überprüft und festgestellt, dass meine Anregungen umgesetzt worden sind. Auch bei der anschließenden Auswertung der Messungen beim BAG, bei der die Videoaufzeichnungen des fließenden Verkehrs den jeweiligen Bildern der Übersichtskamera an der Mautbrücke gegenübergestellt werden, werden die datenschutzrechtlichen Vorgaben eingehalten.

## 12.2 eCall

*Die EU-Kommission strebt im Rahmen ihrer im Frühjahr 2002 zusammen mit der Industrie gestarteten so genannten „eSafety-Initiative" zur Verbesserung der Verkehrssicherheit in Europa den standardmäßigen Einbau von automatischen Notrufgeräten (In-Vehicle eCall) in neue Kraftfahrzeuge an.*

Die Einführung des In-Vehicle eCall (eCall) hat bei den Bemühungen der EU-Kommission um eine nachhaltige Verbesserung der Verkehrssicherheit in Europa hohe Priorität. Nach den Vorstellungen der Kommission sollen ab September 2010 alle Neufahrzeuge standardmäßig mit einem Gerät versehen werden, durch das bei einem Unfall ein Notruf an die europaweit einheitliche Notrufnummer 112 ausgelöst wird. Damit sollen alle für eine schnelle Hilfe notwendigen Daten, insbesondere der Fahrzeugstandort und der Unfallzeitpunkt, an die nächstgelegene Notrufstelle mitgeteilt werden (s. auch Kasten zu Nr. 12.2 sowie Abbildung 9.). Hiervon verspricht man sich eine deutliche Verkürzung der Zeit zwischen Unfallereignis und dem Eintreffen von professionellen Helfern am Unfallort, womit wesentlich mehr Menschenleben als bisher gerettet werden könnten. Einzelheiten, wie die Art der Aktivierung des eCall, die Möglichkeit einer Deaktivierung durch den Fahrzeugführer und der Inhalt des zu übermittelnden Mindestdatensatzes, müssen noch näher festgelegt werden.

Aus datenschutzrechtlicher Sicht stellt sich zunächst die Frage, ob eine Einbaupflicht überhaupt einen Sinn macht. Wer sich überwiegend in städtischer Umgebung oder auf stärker frequentierten Straßen bewegt, dürfte kaum je in eine Situation kommen, in der er ein solches System benötigt. Und in abgelegenen Gebieten, im sog. „Funkloch", nützt das eCall-System ebenso wenig wie das Handy. Wenn ein System, mit dem personenbezogene Daten erhoben werden, nicht erforderlich ist, dann stellt sich automatisch auch die Frage der Notwendigkeit entsprechender Verpflichtungen. Ich trete hier nachdrücklich für eine freiwillige Lösung ein. Ferner sollten entsprechende Systeme so gestaltet werden, dass die Fahrer weitgehend die Kontrolle über die zu ihrem Schutz installierten Systeme behalten. Dies bedeutet insbesondere, dass der Fahrer bzw. die Fahrerin das Gerät selbst aktivieren bzw. abschalten kann.

Umgekehrt will ich aber die Betroffenen auch nicht gegen ihren Willen mit datenschutzrechtlichen Vorgaben konfrontieren. Wer ein derartiges Gerät in sein Auto einbauen will, sollte dies ruhig tun. Er oder sie sollte dann allerdings darauf achten, dass die entstehenden Daten geschützt bleiben. Hier sehe ich gleichermaßen auch eine Bringschuld der Hersteller und der Anbieter entsprechender Dienste. Ferner muss die Zweckbindung des Notrufsystems sichergestellt sein, d. h. das jeweilige Modul darf

bis zum Zeitpunkt des Unfalls weder senden noch empfangsbereit sein und nicht im Mobilfunknetz eingebucht sein. Andernfalls wäre die Ortung durch Dritte – auch ohne Einwilligung des Betroffenen – möglich, und es könnten etwa zu Überwachungs- oder Werbezwecken Bewegungsprofile erstellt werden. Weitere Anwendungen des Moduls sollten nur mit Einwilligung der Betroffenen bzw. durch ihre bewusste Handlung (etwa Nutzung des Moduls als eingebautes Mobilfunkgerät) statthaft sein; eine einmal geleistete Einwilligung muss aber auch jederzeit widerrufen werden können.

Das Thema „eCall“ hat auch die so genannte Artikel 29-Gruppe der europäischen Datenschutzbeauftragten beschäftigt, die hierzu ein Positionspapier beschlossen hat (s. o. Nr. 3.3.). Gemeinsam mit den europäischen Datenschutzbeauftragten werde ich die weitere Entwicklung des eCall-Systems beobachten und auf die Berücksichtigung der datenschutzrechtlichen Belange hinwirken.

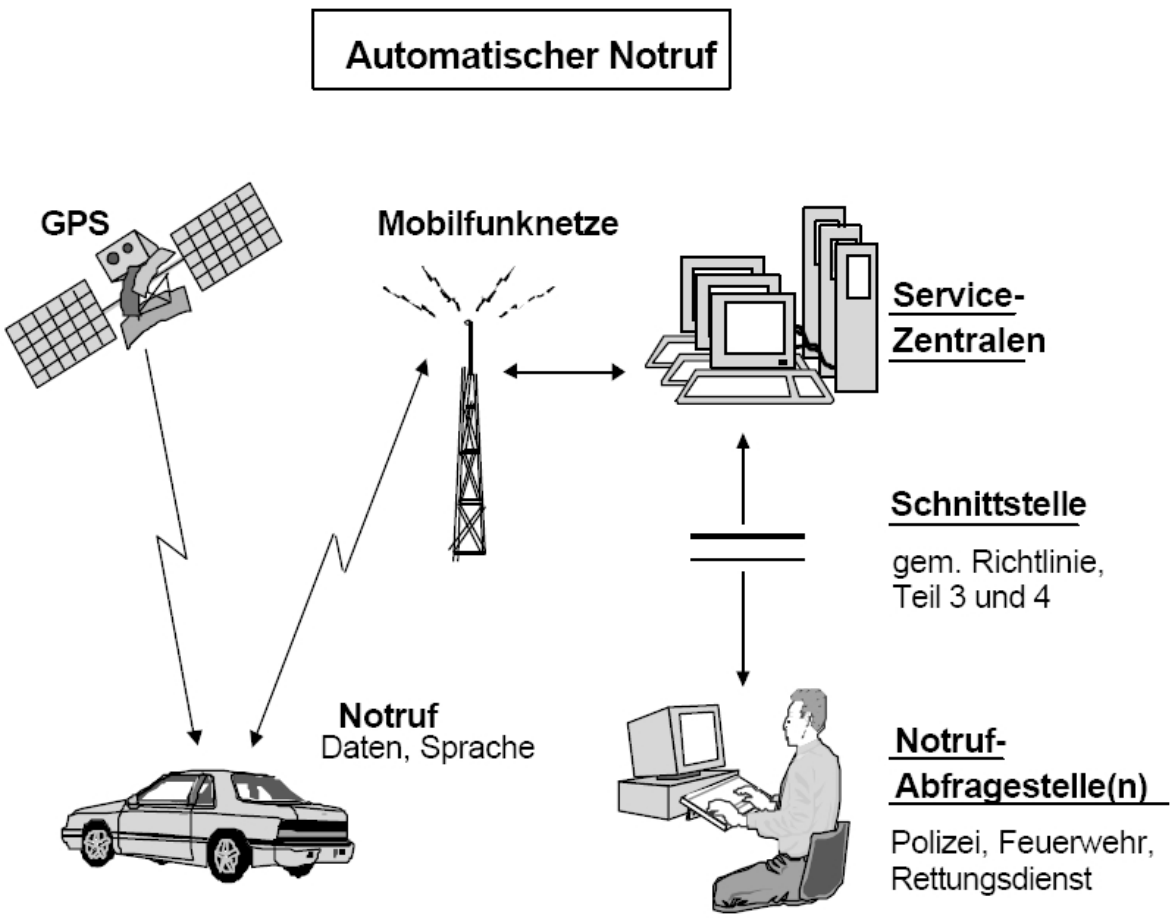
Kasten zu Nr. 12.2

**Wie soll eCall funktionieren?**

Der bordeigene eCall-Notruf wird entweder manuell von den Fahrzeuginsassen oder nach einem schweren Unfall automatisch durch Aktivierung bestimmter Sensoren im Fahrzeug ausgelöst. Das bordeigene eCall-Gerät setzt nach seiner Auslösung einen Notruf mit direkter Sprach- und Datenverbindung zum nächstgelegenen Notdienst ab - in der Regel zur nächstgelegenen "112"-Notrufzentrale. Über die Sprachverbindung können die Fahrzeuginsassen mit einem geschulten eCall-Mitarbeiter sprechen. Gleichzeitig werden bestimmte Mindestdaten an den eCall-Mitarbeiter, der den Anruf entgegennimmt, übermittelt.

Zu den Mindestdaten gehören Informationen über den Unfall wie Zeitpunkt, genauer Standort, Fahrzeugkennung und eCall-Status (zumindest die Angabe, ob der Notruf manuell oder automatisch ausgelöst wurde) sowie Angaben über einen möglichen Diensteanbieter.

Abbildung 9 zu Nr. 12.2



### 12.3 Event Data Recorder – Der im Auto eingebaute „Große Bruder“?

*Die rasant fortschreitende technologische Entwicklung bietet vielfältige Möglichkeiten, individuelle Fahrtdaten eines Kraftfahrzeugs durch eingebaute Geräte aufzuzeichnen und zu speichern.*

Im Rahmen der erwähnten EU-Initiative zur Verbesserung der Sicherheit im Straßenverkehr (s. o. Nr. 12.2) wird auch die Nutzung von in die Fahrzeuge eingebauten Fahrtdatenaufzeichnungsgeräten erwogen und in einem von der Kommission geförderten, breit angelegten Forschungsprojekt untersucht. Dabei geht es der Kommission vor allem um den Einsatz von Unfalldatenschreibern. Dies sind Geräte, die fahrtbezogene Daten, wie Zeit, Längs- und Querbeschleunigung, Geschwindigkeit etc. aufnehmen, aber nur für den Zeitraum von ca. 30 Sekunden vor und 15 Sekunden nach dem Unfall speichern. In wissenschaftlichen Studien hat sich gezeigt, dass das Fahrerbewusstsein durch die Existenz eines die Fahrt begleitenden Geräts im Sinne einer vorsichtigeren Fahrweise beeinflusst wird, wobei sich allerdings der Effekt mit der Zeit abschwächt. Außerdem führt die Datenaufzeichnung beim Unfallgeschehen zu einer wesentlichen Verbesserung der Unfallrekonstruktion, weshalb sich auch der 44. Deutsche Verkehrsgerichtstag Anfang 2006 für den standardmäßigen Einbau von Unfalldatenschreibern ausgesprochen hat.

Darüber hinaus entwickelt die Industrie auf Satellitentechnik gestützte Geräte, die Informationen über die einzelne Fahrt und die genaue Fahrtstrecke aufzeichnen und zusätzlich eine automatisierte Kommunikation zwischen den Fahrzeugen und anderen Stellen ermöglichen. Durch derartige, der im Autobahnmautverfahren eingesetzten „On-Board-Unit“ vergleichbare Geräte können ganz individuelle Fahr- und Nutzungsprofile erstellt werden.

Diesen immer breiteren Einsatz von Fahrtdatenaufzeichnungsgeräten beobachte ich mit Sorge, da er zusammen mit der sonstigen technischen Überwachung des Straßenverkehrs deutlich in Richtung des „gläsernen Autofahrers“ führen kann. Deshalb darf es eine Verpflichtung zum Einbau und zur Nutzung dieser Geräte allenfalls in engen Grenzen geben. Ich könnte mir dies beim Unfalldatenschreiber vorstellen, dessen Aufzeichnungen auf das Unfallgeschehen beschränkt sind. Der Einbau solcher Geräte sollte grundsätzlich auf freiwilliger Basis erfolgen. Lediglich bei Lkw und Bussen halte ich einen verpflichtenden Einbau von Unfalldatenschreibern für angemessen.

Bei der technischen Ausgestaltung derartiger Fahrtdatenaufzeichnungssysteme ist aus datenschutzrechtlicher Sicht darauf zu achten, dass von vorneherein keine oder nur möglichst wenige Daten in personenbezogener Form erhoben werden und dass eine zentrale Speicherung vermieden wird. Erfahrungsgemäß wecken zentrale Datenbanken stets die Begehrlichkeit, die einmal erfassten Daten auch für andere Zwecke zu verwenden.

### 12.4 Pay as You Drive – Know where You Go

*In Fahrtdatenaufzeichnungsgeräten sehen Kraftfahrzeugversicherer eine Möglichkeit zum Angebot „maßgeschneiderter“ Versicherungstarife.*

Von Versicherungsgesellschaften wird der Einsatz von Fahrtdatenaufzeichnungsgeräten getestet, um einen ganz auf die individuelle Fahrzeugnutzung und das damit verbundene Versicherungsrisiko abgestellten Tarif anzubieten, sog. „Pay-as-you-Drive“-Tarife. Durch das ins Fahrzeug eingebaute Gerät sollen dann vor allem die Tageszeit und die gefahrene Strecke festgehalten werden. Es ist auch daran gedacht, bestimmte Fahrergruppen, wie zum Beispiel die besonders unfallgefährdeten jungen (18- bis 24-jährigen) Autofahrer anzusprechen und vor Verkehrsverstößen zu bewahren, etwa durch vom Gerät ausgelöste Warnhinweise bei Geschwindigkeitsübertretungen und Berücksichtigung derartiger Verkehrsverstöße in der Prämiengestaltung.

Aus datenschutzrechtlicher Sicht muss gewährleistet sein, dass der Abschluss derartiger Versicherungsverträge auf freiwilliger Basis erfolgt. Die Versicherungsgesellschaften dürfen durch die Tarifgestaltung auch keinen unverhältnismäßigen ökonomischen Zwang ausüben.

### 12.5 Online-Anbindung der örtlichen Fahrerlaubnisbehörden an das Zentrale Fahrerlaubnisregister des Kraftfahrt-Bundesamtes (KBA)

*Nach Wegfall der örtlichen Fahrerlaubnisregister zum 1. Januar 2007 können die Fahrerlaubnisbehörden ihre Datensätze in das Zentrale Fahrerlaubnisregister (ZFER) einstellen.*

Bereits in meinem 20. TB (Nr. 22.3) hatte ich über den Datentransfer zwischen den örtlichen Fahrerlaubnisbehörden und dem KBA in Form einer Ende-zu-Ende-Verschlüsselung berichtet. Infolge der Neuorganisation ihrer IT–Strukturen äußerten einige Kommunen den Wunsch, den Datentransfer zum KBA über ihre Netze abzuwickeln, so dass eine durch das KBA garantierte Ende-zu-Ende-Verschlüsselung bis zum Arbeitsplatz des Bearbeiters nicht mehr möglich wäre. Ich hatte die Auffassung vertreten, dass die Anbindung der Fahrerlaubnisbehörden an das KBA auch durch Einrichtung einer „Kopfstelle“, die die Daten aus den kommunalen Netzen übernimmt und sie in geeigneter Form in das Netz des KBA überleitet, datenschutzgerecht realisiert werden könne. Das KBA als für die Datenspeicherung verantwortliche Stelle kann die Kriterien für die Anschlussbedingungen an sein Netz und bezüglich der Datensicherheit festlegen. Diesen Weg hat das KBA gewählt und einen Anforderungskatalog zur Datensicherheit erstellt, der mit den Ländern und Kommunen abgestimmt wurde.

Ungeachtet der technischen Anbindung war zu klären, wer für die Authentizität und Integrität der im ZFER gespeicherten Datensätze verantwortlich ist. Das Straßenverkehrsgesetz und die Fahrerlaubnisverordnung beziehen sich nur auf Online-Datenübermittlungen aus dem ZFER (Abrufe) an die zuständigen Stellen. Regelungen

zur Online-Datenübermittlung und -änderung der örtlichen Fahrerlaubnisbehörden an das ZFER sowie Regelungen über die Verantwortlichkeit fehlen, obwohl ab 2007 keine örtlichen Fahrerlaubnisregister mehr geführt werden und zukünftig alle Fahrerlaubnisdaten ausschließlich im ZFER zu speichern sind. Die örtlichen Fahrerlaubnisbehörden haben dann nicht nur lesenden Zugriff auf die Datensätze des Registers, sondern können sie auch verändern. Das ZFER ist somit – ähnlich dem polizeilichen Informationssystem INPOL – als eine Verbunddatei anzusehen, so dass die Fahrerlaubnisbehörden die Authentizität und Integrität ihrer Datensätze sicherstellen müssen. Ich halte deshalb eine klarstellende gesetzliche Regelung für erforderlich.

### 12.6 Übermittlung von medizinischen Untersuchungsbefunden an das Luftfahrt-Bundesamt (LBA)

*Durch eine Änderung des Luftverkehrsgesetzes (LuftVG) ist die Speicherung medizinischer Einzelbefunde im Rahmen der flugmedizinischen Untersuchung von Luftfahrern in der vom LBA geführten Zentralen Luftfahrerdatei entfallen.*

In der Vergangenheit haben flugmedizinische Sachverständige im Zuge der flugmedizinischen Untersuchung von Luftfahrern dem LBA auf Anweisung medizinische Befunde übermittelt, sofern sie für Auflagen (z. B. Brille) oder Verkürzungen der Fluglizenz benötigt wurden. Diese Daten wurden in der Luftfahrerdatei des LBA gespeichert. Flugmedizinische Sachverständige haben in zahlreichen Eingaben datenschutzrechtliche Bedenken gegen diese Speicherung erhoben. Bei einer Kontrolle des Verfahrens beim LBA habe ich festgestellt, dass der Fachbereich „Flugmedizin“ des LBA medizinische Untersuchungsergebnisse in der Luftfahrerdatei gespeichert hatte, die größtenteils über das erforderliche Maß hinausgingen. Daraufhin habe ich gefordert, dass die flugmedizinischen Sachverständigen im Rahmen medizinischer Untersuchungen die Entscheidung über die Erteilung der Fluglizenzen alleine treffen und dem LBA nur noch reine Verwaltungsaufgaben sowie die Bestellung und die Beaufsichtigung der Fliegerärzte übertragen werden.

Durch die Änderung des § 65 Abs. 3 Nr. 4 b LuftVG vom 24. Mai 2006 wurde meinen Anregungen Rechnung getragen. Künftig dürfen nur noch anonymisierte medizinische Befunde an die Luftfahrtbehörden übermittelt werden, damit sie die Arbeit der flugmedizinischen Sachverständigen beaufsichtigen können. Auf die Speicherung der Einzelbefunde in der Luftfahrerdatei wurde verzichtet.

## 13 Gesundheit und Soziales

*Im Sozialleistungsbereich hat es immer wieder Vorstöße gegeben, zentrale Datenabgleichsverfahren zu installieren, um Missbrauchsfälle aufzudecken. Ohne Anhaltspunkte für Missbrauchsfälle in nennenswertem Umfang sollte auf die Einführung derartiger weitgreifender Kontrollinstrumente verzichtet werden. Eine allgemeine Befugnis zum Abgleich von Sozialdaten wäre auch verfassungsrechtlich bedenklich.*

Im Entwurf eines Gesetzes zur Entlastung der Kommunen im sozialen Bereich (KEG) (Bundestagsdrucksache 15/4532 vom 15. Dezember 2004) war in Artikel 4 u. a. vorgesehen, zur Bekämpfung von Sozialleistungsmissbrauch im SGB X eine generelle Regelung zu schaffen, indem § 67a Abs. 1 SGB X um den Satz ergänzt werden sollte: „Die Erhebung von Daten zur Missbrauchskontrolle setzt einen Anfangsverdacht nicht voraus.“ Da dieses Gesetzgebungsvorhaben aufgrund des vorzeitigen Endes der Legislaturperiode nicht abgeschlossen werden konnte, griff der Bundesrat in seiner Entschließung vom 10. Februar 2006 (Bundesratsdrucksache 892/05) das Thema erneut auf.

Gegen die vom Bundesrat angestrebten Regelungen hatte ich erhebliche datenschutzrechtliche Bedenken. Pauschale und undifferenzierte Datenübermittlungen ohne tatsächliche Anhaltspunkte für das Vorliegen von Missbrauchsfällen in relevanter Größenordnung hielte ich für unverhältnismäßig. Die Möglichkeit zur Durchführung anlassunabhängiger Kontrollen im gesamten Sozialleistungsbereich wäre zudem eine Abkehr von dem im Sozialdatenschutz bisher geltenden Grundsatz der Erforderlichkeit der Datenerhebung im Einzelfall, denn die angestrebte Regelung sollte für alle bedürftigkeitsabhängigen Sozialleistungen gelten, die an Einkommen und Vermögen der Antragsteller anknüpfen. Irgendeine Differenzierung war danach nicht vorgesehen. Ich begrüße es, dass sich die Bundesregierung in ihrer Stellungnahme auch unter Berücksichtigung meiner erheblichen datenschutzrechtlichen Bedenken zu der Forderung des Bundesrats kritisch geäußert hat, insbesondere im Hinblick auf die Notwendigkeit und Verhältnismäßigkeit einer derart weiten Regelung.

Ich werde mich weiterhin entsprechend der gemeinsamen Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 20. Oktober 1997 (17. TB, Anlage 12 zu Nr. 19.8) dafür einsetzen, dass auch bei der Aufdeckung und Bekämpfung von Sozialleistungsbetrug die verfassungsrechtlichen und datenschutzrechtlichen Grundsätze gewahrt bleiben.

### 13.1 Gesetzliche Krankenversicherung

#### 13.1.1 Gesundheitsreform 2006/2007

*Die im Rahmen der Gesundheitsreform 2006/2007 vorgesehene Neuordnung des Vergütungssystems berührt den Datenschutz. Durch datenschutzfreundliche Technologien sollte die Verarbeitung medizinischer Daten begrenzt werden.*

Eines der vorrangigen Ziele der Gesundheitsreform durch das Gesetz zur Stärkung der Wirtschaftlichkeit (GKV-WSG) ist die Einführung eines neuen Vergütungssystems in der ambulanten Krankenversorgung. Durch die Abkehr von dem geltenden Punktewertesystem, bei dem der Arzt erst am Ende eines Abrechnungszeitraumes weiß, wie viel er verdient hat, soll nunmehr für jede ärztliche Leistung ein fester Betrag gezahlt werden. In dem

neuen Vergütungssystem wird die Morbiditätsstruktur der Versicherten der einzelnen Krankenkassen für die Höhe des von den Krankenkassen an die Kassenärztliche Vereinigung zu zahlenden Honorarvolumens von zentraler Bedeutung sein. Die vorgesehene Ermittlung des für die Vergütung ausschlaggebenden Behandlungsbedarfs sowie die Nachverfolgung von Veränderungen der Erkrankungen macht eine Änderung der Regelungen zur Datenverarbeitung erforderlich.

Bereits nach geltendem Recht verfügen die einzelnen Krankenkassen über alle erforderlichen Daten, die sie zur Vereinbarung und Durchführung von Vergütungsverträgen erheben, speichern, verarbeiten und nutzen dürfen (§ 284 Abs. 1 Satz 1 Nr. 12 und Abs. 3 SGB V). Der für die Krankenkasse verhandlungsführende und vertragschließende Krankenkassenverband verfügt aber nicht über diese Daten und den Kassenärztlichen Vereinigungen steht nur ein Teil dieser Daten zur Verfügung. Aus diesem Grunde enthält § 85a Abs. 6 des Gesetzesentwurfes ergänzende Regelungen zur Übermittlung der erforderlichen Sozialdaten von Krankenkassen an die Vertragspartner. Dem Krankenkassenverband wird auch die Befugnis zur Verarbeitung versichertenbezogener Daten gegeben, für die Kassenärztlichen Vereinigungen erfolgt eine entsprechende Ergänzung.

Schon im Zusammenhang mit dem Gesetz zur Modernisierung der Krankenversicherung (GKV-Modernisierungsgesetz, vgl. 20. TB Nr. 17.1.1) hatte ich gemeinsam mit allen Landesdatenschutzbeauftragten gefordert, Pseudonymisierungsverfahren bei der versichertenbezogenen Erhebung von Behandlungs- und Abrechungsdaten einzuführen. Zu meinem Bedauern ist auch im neuen Gesetzesentwurf der Einsatz datenschutzfreundlicher Technologien, beispielsweise durch Pseudonymisierungsverfahren, nicht vorgesehen. Vor dem Hintergrund der geplanten Einrichtung weiterer großer Datenbestände halte ich die Entwicklung pseudonymisierter Verfahren für geboten.

Ich werde mich weiterhin für eine solche datenschutzfreundliche Lösung einsetzen.

### 13.1.2 Risikostruktur-Ausgleichsverordnung

*Mit der Weiterentwicklung des Risikostrukturausgleichs soll die Morbidität aller Versicherten unmittelbar berücksichtigt werden. Aus diesem Grunde sollen zur Feststellung des Morbiditätsrisikos der Versicherten u. a. Daten über Diagnosen, Indikationen und medizinische Leistungen erhoben werden.*

Mit der Einführung des Risikostrukturausgleichs zum 1. Januar 1994 wurde der Ausgabenstandard der gesetzlichen Krankenkassen je nach Alter, Geschlecht, Berufs- und Erwerbsfähigkeitsstatus und die Anzahl der beitragsfrei mitversicherten Familienangehörigen festgelegt. In dem Ausgleichsverfahren wurden auch besonders intensive Behandlungen chronisch erkrankter Menschen berücksichtigt. Aufgrund der ermittelten Werte sollte innerhalb der gesetzlichen Krankenkassen ein finanzieller Ausgleich durchgeführt werden, um zu verhindern, dass Kassen mit einem überproportionalen Anteil einkommensschwacher, älterer, kinderreicher oder chronisch erkrankter Versicherte benachteiligt würden (s. 19. TB Nr. 24.1.2 und 20. TB Nr. 17.1.4).

Mit dem vom BMG vorgelegten Entwurf der „14. Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung“ soll der Risikostrukturausgleich zielgenauer ausgestaltet werden. Kernstück ist die Festlegung der zusätzlichen Daten, die neben den bisher schon berücksichtigten Merkmalen Alter und Geschlecht und Bezug einer Erwerbsminderungsrente das Morbiditätsrisiko der Versicherten unmittelbar kennzeichnen. Abweichend von den bisherigen Disease-Management-Programmen werden die Versicherten nicht mehr in gesonderten Versichertengruppen erfasst. Nunmehr soll die Morbidität gemäß der Regelung des § 268 Abs. 1 Satz 1 Nr. 1 SGB V auf der Grundlage von Diagnosen, Diagnosegruppen, Indikationen, Indikationsgruppen, medizinischen Leistungen oder Kombinationen dieser Merkmale unmittelbar berücksichtigt werden. Mit dem beabsichtigten Einstieg in die direkte Morbiditätsorientierung wäre die Erfassung in gesonderten Versichertengruppen im Rahmen der Disease-Management-Programme nicht mehr erforderlich.

Da die direkte Morbiditätsorientierung von der gesetzlichen Regelung des § 268 Abs. 1 Satz 1 Nr. 1 SGB V auf der Grundlage von Diagnosen und Arzneimittelwirkstoffen vorgesehen ist, habe ich meine datenschutzrechtlichen Bedenken gegen die beabsichtigten umfangreichen Datenerhebungen einschließlich der Möglichkeit, die erhobenen Daten miteinander zu verknüpfen, zurückgestellt. Im Rahmen meiner Mitarbeit an der 14. Verordnung zur Änderung der Risikostruktur-Ausgleichsverordnung habe ich aber darauf gedrungen, dass die vorgesehenen Regelungen zur Datenerhebung so klar wie möglich gefasst werden. Ein weiteres datenschutzrechtliches Anliegen war die strikte Zweckbindung der erhobenen Daten ausschließlich für die Zwecke der Weiterentwicklung des Risikostrukturausgleichs sowie klare Löschungsregelungen.

Im Hinblick auf die durch die Neuregelung des Risikostrukturausgleichs erheblich ausgeweitete Verarbeitung und Nutzung sensibler medizinischer Daten erwarte ich, dass das neue Verfahren hinsichtlich seiner Wirkung und Angemessenheit evaluiert wird, sobald entsprechende Erfahrungen vorliegen.

### 13.1.3 Datenerhebung ohne gesetzliche Grundlage? – „Selbstauskunftsbögen“ der Krankenkassen

*Die Krankenkassen dürfen personenbezogene Daten nur im Rahmen ihrer gesetzlichen Befugnisse erheben. Darüber hinaus erbetene Selbstauskünfte der Versicherten und darauf basierende Erhebungen bei Ärzten unter Rückgriff auf entsprechende Schweigepflichtentbindungserklärungen sind datenschutzrechtlich äußerst bedenklich.*

Mit der Erhebung medizinischer Daten durch gesetzliche Krankenkassen habe ich mich in der Vergangenheit häufig beschäftigen müssen (vgl. 18. TB Nrn. 21.3; 19. TB Nrn. 24.1.4, 24.2.2; 20. TB Nrn. 17.1.5, 17.1.6, 17.2.1).

Immer wieder ging und geht es dabei um die Frage der Zulässigkeit der Erhebung medizinischer Daten durch die Krankenkassen außerhalb der Zuständigkeit des Medizinischen Dienstes der Krankenkassen (MDK). Meine Haltung zu dieser Rechtsfrage ist nach wie vor eindeutig: Die Krankenkassen haben in den in § 275 genannten Fällen (z. B. Arbeitsunfähigkeit, Leistungen zur medizinischen Rehabilitation) den MDK mit einer Begutachtung bzw. Prüfung zu beauftragen. Eine darüber hinaus gehende pauschale Datenerhebung durch die Kassen selbst sieht das SGB V nicht vor. Nur der MDK darf, nachdem er von den Krankenkassen mit einer Begutachtung bzw. Prüfung beauftragt wurde, weitergehende Daten erheben oder speichern, sofern dies im konkreten Einzelfall erforderlich ist (§ 276 Abs. 2 Satz 1, 1. Halbsatz SGB V). Ergänzend verweise ich auf meine Ausführungen in den oben zitierten Textstellen der letzten drei Tätigkeitsberichte zum Thema „Krankenhausentlassungsberichte“, denen auch die Bundesregierung zugestimmt hat (vgl. Kasten a zu Nr. 13.1.3).

Kasten a zu Nr. 13.1.3

**Auszug**

**Stellungnahme der Bundesregierung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes – Bundestagsdrucksache 15/5252 –**

Zu Nr. 17.1.5 – Krankenhausentlassungsberichte

Der BfD kritisiert, dass weiterhin Krankenkassen Krankenhausentlassungsberichte und andere ärztliche Unterlagen bei den Leistungserbringern anfordern.

Die Bundesregierung vertritt hierzu die Auffassung, dass diese ärztlichen Daten nur im Rahmen der Aufgaben der Medizinischen Dienste der Krankenversicherung ohne Kenntnisnahme der Krankenkassen verarbeitet werden dürfen. Den Ausführungen des BfD wird insofern zugestimmt.

Der Gesetzgeber hat mit der Einräumung dieser eigenständigen Datenerhebungskompetenz des MDK entschieden, dass die Krankenkassen diese Informationen gerade nicht erhalten sollen. Die Kassen dürfen lediglich um die Übermittlung der Behandlungsdaten unmittelbar an den MDK ersuchen. Dies verdeutlicht auch die Regelung des § 277 Abs. 1 Satz 1 SGB V, wonach der MDK der jeweiligen Krankenkasse nur das Ergebnis der Begutachtung mitteilen darf, nicht aber die Informationen, aufgrund derer der MDK zu seiner Bewertung gekommen ist. Dementsprechend kritisch beobachte ich Bestrebungen von Kassen, beispielsweise über vorformulierte Auskunftsbögen und allgemeine Schweigepflichtentbindungserklärungen selbst an Informationen zum Gesundheitszustand ihrer Versicherten bis hin zu konkreten Behandlungsunterlagen zu gelangen, die nach dem Willen des Gesetzgebers allein der Einsichtnahme und Begutachtung durch den MDK vorbehalten sind.

Da lediglich der MDK nach § 276 Abs. 2 Satz 1 SGB V zur Erhebung und Speicherung der zur Begutachtung erforderlichen Sozialdaten befugt ist, halte ich folglich die weit verbreitete Praxis der Krankenkassen, bei den Versicherten über sog. „Selbstauskunftsbögen“ (Fragebögen/Auskunftsersuchen) ergänzende Angaben über ihren Gesundheitszustand und ihre Befindlichkeiten zu erfragen, in der mir bekannt gewordenen Form für unzulässig. Insbesondere zur Feststellung der Arbeitsunfähigkeit, zur Prüfung der Voraussetzungen bei Mutter-Kind-Kuren oder anderen Leistungen der medizinischen Vorsorge- und Rehabilitationsmaßnamen werden teilweise sehr sensible personenbezogene Daten erhoben und die Versicherten darüber hinaus sehr weit gehend zu ihrem persönlichen Lebensumfeld befragt (siehe die Beispiele in Kasten b zu Nr. 13.1.3).

Kasten b zu Nr. 13.1.3

**Beispiele aus mir vorliegenden „Selbstauskunftsbögen“**

**Konnten Sie in den letzten 12 Monaten eine oder mehrere der folgenden Beratungsangebote in Anspruch nehmen:**

- Familien-/Ehe-/Erziehungsberatung
- Suchtberatung
- Schuldnerberatung
- Selbsthilfegruppen

**Belasten Sie eine oder mehrere der folgenden Umstände:**

- Ehe- oder Partnerschaftskonflikte
- Arbeitslosigkeit
- beengte Wohnverhältnisse
- finanzielle Sorgen

**Zur Selbsteinschätzung:**

- Welche beruflichen Belastungen bestehen?
- Welche Konflikte im privaten oder familiären Umfeld belasten Sie?
- Halten Sie eine Wiedereingliederung am derzeitigen Arbeitsplatz für möglich?
- Wurde von Ihnen/Ihrem Arzt bereits erwogen, einen Psychotherapeuten hinzuzuziehen?

Die Fragen zur Selbsteinschätzung sind mit Freitextfeldern versehen, die Versicherte mit „nein“ oder „... ja und zwar ...“ beantworten sollen.

Ob die auf diese Weise gewonnenen Erkenntnisse überhaupt erforderlich und vor allem geeignet sind, eine konkrete Leistungsentscheidung der Kasse zu stützen, muss schon deshalb bezweifelt werden, weil die Angaben lediglich auf pauschalen Fragestellungen in standardisier-

ten Erhebungsbögen beruhen und – soweit Selbsteinschätzungen der Betroffenen angesprochen werden – in der Regel Mutmaßungen wiedergeben, die selbst für eine Begutachtung durch den MDK kaum verwertbar sein dürften. Hier ist im Übrigen zu berücksichtigen, dass leistungserheblich nur Tatsachen sein können, mithin keine Meinungen oder bloße Werturteile.

Soweit Krankenkassen in diesem Zusammenhang und gestützt auf eine entsprechende Einwilligungserklärung des Versicherten selbst Krankenhäuser und andere Einrichtungen für medizinische Vorsorge- und Rehabilitationsmaßnahmen auffordern, ärztliche Behandlungsunterlagen wie Entlassungsberichte, Arztbriefe, Befundberichte, ärztliche Gutachten oder Röntgenaufnahmen an diese zu übermitteln, sehe ich dazu keine Ermächtigungsgrundlage. In § 301 Abs. 1 SGB V ist spezialgesetzlich und abschließend festgelegt, welche Daten zu welchem Zweck im Fall einer Krankenhausbehandlung der jeweiligen Krankenkasse zur Verfügung zu stellen sind. Dazu gehören jedoch nicht die aufgeführten Behandlungsdokumente (siehe dazu auch meine Ausführungen im 19. TB Nr. 24.1.4 unter Hinweis auf das Urteil des Bundessozialgerichts vom 23. Juli 2002 sowie im 18. TB Nr. 21.3).

Erhebliche Zweifel habe ich schließlich an der Wirksamkeit der mit den Erhebungsbögen regelmäßig gleichzeitig erbetenen Einwilligung der Versicherten in die Übermittlung ihrer Gesundheitsdaten unmittelbar an die Krankenkasse. Abgesehen davon, dass schon mit dieser Vorgehensweise eine Missachtung des in §§ 275 ff. SGB V dokumentierten Willens des Gesetzgebers, ausschließlich den MDK zur Prüfung medizinischer Sachverhalte zu berechtigen, zum Ausdruck kommt, genügen die mir bekannt gewordenen formularmäßigen Erklärungen nicht den notwendigen Anforderungen an die Bestimmtheit und Eindeutigkeit einer solchen Entbindung von der ärztlichen Schweigepflicht. Das Bundesverfassungsgericht hat in einer jüngst veröffentlichten Entscheidung (Beschluss vom 23. Oktober 2006 – 1 BvR 2027/02) klar gestellt, dass auch bei einer Schweigepflichtentbindung das Interesse des Betroffenen an einem wirkungsvollen informationellen Selbstschutz gewahrt bleiben muss und dies die Möglichkeit beinhaltet, die Wahrung seiner Geheimhaltungsinteressen selbst zu kontrollieren. Dazu muss der Erklärende absehen können, welche konkreten Auskünfte von wem und zu welchem Zweck über ihn eingeholt werden. Diese Voraussetzungen sehe ich bei den hier verwendeten, formularmäßigen und sehr weit gefassten Schweigepflichtentbindungserklärungen durchweg nicht gegeben.

Ich habe diese Thematik mit dem Bundesministerium für Gesundheit, dem Bundesversicherungsamt (BVA) als zuständige Fachaufsichtsbehörde und dem Verband der Angestellten-Krankenkassen (VdAK) in einer gemeinsamen Besprechung intensiv erörtert. Meine rechtliche Bewertung wird durch das Bundesministerium für Gesundheit und das BVA uneingeschränkt geteilt. Auch der Deutsche Bundestag hat im Rahmen der parlamentarischen Beratung des Berichts der Spitzenverbände der Krankenkassen zu den Erfahrungen mit den durch das Elfte SGB-V-Änderungsgesetz bewirkten Rechtsänderungen im Zusammenhang mit der Bewilligung von Mutter-Kind-Kuren meine Haltung ausdrücklich bestätigt.

### 13.1.4 Qualitätssicherung – Richtlinie Dialyse/ Allgemeine Anforderungen an eine einrichtungsübergreifende Qualitätssicherung

*Im Rahmen der Gesundheitsreform wird eine datenschutzkonforme gesetzliche Regelung für die seit Jahren diskutierte Zulässigkeit einer Qualitätssicherung in der Dialyse geschaffen.*

In den letzten Jahren war von Fachleuten immer wieder eine Qualitätssicherung in der Nierenersatztherapie – insbesondere in der Dialyse – gefordert worden. Die regelmäßige Beobachtung möglichst aller Behandlungen über die gesamte Behandlungsdauer der Patienten wird für unverzichtbar gehalten. Aus diesem Grunde sollten Informationen aller Behandlungszentren in Deutschland über die Behandlung von chronisch niereninsuffizienten Patienten zusammengetragen werden. Da keine gesetzliche Regelung hinsichtlich der Qualitätssicherung bestand, konnten die Daten nur aufgrund der Einwilligung der Patienten weitergegeben bzw. ausgewertet werden.

Für eine flächendeckende Datenerhebung war jedoch eine gesetzliche Regelung erforderlich. Gemeinsam mit den Datenschutzbeauftragten der Länder hatte ich einen Kriterienkatalog für die Anforderungen an eine klarstellende gesetzliche Regelung einer einrichtungsübergreifenden Qualitätssicherung im Bereich des SGB V aufgestellt:

- Durchführung von einrichtungsübergreifenden Maßnahmen der Qualitätssicherung nur mittels pseudonymisierter Patientendaten/Versichertendaten und nur durch ein Prüfungsgremium, das mit neutralen, objektiven und der wissenschaftlichen Unabhängigkeit verpflichteten Personen besetzt ist;
- Ausschluss der Re-Identifizierung von Patienten/Versicherten;
- Verwendung eines sicheren Pseudonymisierungsverfahrens;
- Pseudonymisierung durch eine von den Krankenkassen und Kassenärztlichen Vereinigungen rechtlich unabhängige Vertrauensstelle, die räumlich, organisatorisch und personell abgeschottet ist;
- Beschlagnahmeschutz der Daten bei der Vertrauensstelle;
- keine Zusammenführung unterschiedlicher Qualitätssicherungsverfahren;
- gesetzliche Klarstellung, welche Stelle für die einrichtungsübergreifende Qualitätssicherung zuständig ist;
- Normierung einer Übermittlungsverpflichtung der Leistungserbringer;
- Normierung einer Informationsverpflichtung gegenüber den Patienten/Versicherten zu Beginn der Behandlung.

Ich begrüße sehr, dass der Gesetzgeber mit der Regelung des § 137a SGB V diesen Anforderungen weitgehend Rechnung getragen hat. Damit wird die Qualitätssicherung auf eine datenschutzrechtlich einwandfreie Grundlage gestellt.

### 13.1.5 Kostendämpfungsmaßnahmen bei Heil- und Hilfsmitteln – um jeden Preis?

*Die gesetzlichen Krankenkassen dürfen Daten ihrer Versicherten nur ohne Personenbezug an Hersteller übermitteln.*

Mehrere Petenten haben mich auf die von gesetzlichen Krankenkassen praktizierte Weitergabe von Sozialdaten inklusive Diagnosedaten an Hersteller von Heil- und Hilfsmitteln oder auch an so genannte private „Hilfsmittelberater“ aufmerksam gemacht. Die Anfragen betreffen folgende Fallkonstellationen:

- Sozialdaten von Versicherten werden an Hersteller von Rollstühlen zur Erstellung von Kostenvoranschlägen weitergeleitet.
- Bei der Versorgung mit Hilfsmitteln werden so genannte „Hilfsmittelberater“ beauftragt, ein technisches Gutachten zu erstellen. Die entsprechenden Sozialdaten einschließlich Diagnosedaten werden dem „Hilfsmittelberater“ von der Krankenkasse zur Verfügung gestellt. Musterverträge mit Hilfsmittelberatern liegen mir vor.
- Gesetzliche Krankenkassen fordern von Herstellern orthopädischer Produkte Bildmaterial der Patienten, um den Einsatz von nicht konfektionierten Sonderanfertigungen (wie z. B. Brustprothesen) besser beurteilen zu können.
- Bei der Versorgung mit Hilfsmitteln wird von einer Krankenkasse im Zusammenhang mit einem entsprechenden Antrag ein Vergleichsangebot bei anderen Herstellern eingeholt. Dabei werden die Sozialdaten des Versicherten einschließlich der Diagnosedaten übermittelt.

Die Krankenkassen begründen diese Übermittlung überwiegend mit dem allgemeinen Wirtschaftlichkeitsgebot (§ 12 SGB V). Diese Vorschrift gibt den Krankenkassen vor, dass Leistungen ausreichend, zweckmäßig und wirtschaftlich sein müssen (§ 12 Abs. 1 Satz 1 SGB V). Demgegenüber habe ich erhebliche Zweifel, ob eine Übermittlung von derart sensiblen Sozialdaten auf diese allgemeinen Grundsätze gestützt werden kann.

Vertragliche Kontakte zu Leistungserbringern sind in § 127 SGB V geregelt. Nach § 127 Abs. 2 SGB V können die Kassen zwar Verträge mit einzelnen Leistungserbringern schließen, in diesen Fällen ist allerdings lediglich eine allgemeine Information der Versicherten und der Leistungserbringer vorgesehen (§ 127 Abs. 2 Satz 3, 2. Hs. und Abs. 3 SGB V). Eine Befugnis zur Übermittlung von Sozialdaten an Hersteller von Heil- und Hilfsmitteln sehe ich in § 127 SGB V ebenfalls nicht.

Auch für die Weitergabe von Sozialdaten an externe „Hilfsmittelberater“ zur Begutachtung der Versicherten vermag ich eine gesetzliche Grundlage für deren Tätigwerden nicht zu erkennen. Die abgeschlossenen Verträge können eine gesetzliche Grundlage nicht ersetzen. § 275 SGB V gibt den Krankenkassen u. a. vor, wenn es bei der Erbringung von Leistungen, insbesondere zur Prüfung der Voraussetzungen sowie Art und Umfang der Leistung erforderlich ist, eine gutachterliche Stellungnahme des Medizinischen Dienstes der Krankenversicherung (MDK) einzuholen (§ 275 Abs. 1 Nr. 1 SGB V).

Vor diesem Hintergrund gibt es keinen Raum für die Begutachtung von Versicherten durch externe „Hilfsmittelberater“ im Auftrag einer gesetzlichen Krankenkasse. Mit dem Abschluss von Verträgen zwischen Krankenkasse und „Hilfsmittelberatern“ im Einzelfall wird meines Erachtens der gesetzliche Auftrag des MDK vielmehr umgangen.

Eine Lösungsmöglichkeit könnte darin bestehen, dass Versicherte, insbesondere bei aufwendigen, nicht konfektionierten Hilfsmitteln gebeten werden, der Kasse sowohl ein Angebot des Hilfsmittelherstellers ihrer Wahl, als auch (alternativ) ein Angebot des von der Kasse vorgeschlagenen Herstellers mit dem Leistungsantrag vorzulegen. Die Kasse könnte dann eine Kostenzusage auf der Grundlage des wirtschaftlichsten Angebotes abgeben. Auch bestehen keine Bedenken, wenn die Kasse auf Wunsch des Versicherten tätig wird. Entsprechende interne Vorgaben sind von einer Krankenkasse bereits umgesetzt. Diese Praxis belegt, dass das Wirtschaftlichkeitsgebot bei der Versorgung von Versicherten mit Heil- und Hilfsmitteln umgesetzt werden kann, ohne deren Sozialdaten weiterzugeben.

Die dargestellten Fallkonstellationen sowie meine datenschutzrechtliche Bewertung habe ich mit dem BMG erörtert und im Gesetzgebungsverfahren zur Gesundheitsreform vorgetragen. Im Gesetzentwurf der Bundesregierung (Wettbewerbsstärkungsgesetz – GKV-WSG) ist daher vorgesehen, dass von Krankenkassen bei anderen Leistungserbringern in pseudonymisierter Form Preisangebote eingeholt werden können. Ich erwarte, dass im Zusammenhang mit der Gesundheitsreform eine datenschutzgerechte gesetzliche Klarstellung erfolgt.

### 13.1.6 „Freier Eintritt“ bei Vorlage der Krankenversichertenkarte

*Eine andere als die gesetzlich vorgegebene Nutzung der Krankenversichertenkarte ist mit dem Datenschutz nicht vereinbar.*

Gleich in mehreren Eingaben bin ich im Jahr 2005 darauf hingewiesen worden, dass einzelne Krankenkassen im Rahmen von Mitgliederbindungs- oder -werbungsaktionen (Bonusprogramme) mit der Inanspruchnahme vergünstigter Leistungen kommerzieller Geschäftspartner lediglich gegen Vorlage des Krankenversichertenausweises geworben haben. Versicherte konnten so Preisnachlässe auf bestimmte Fitness-Artikel, einen vergünstigten oder gar kostenlosen Eintritt zu einem Fußballspiel oder in ei-

nen Wildpark und sogar stundenweise Kinderbetreuung zwecks Entlastung der Eltern während ihrer Weihnachtseinkäufe in Anspruch nehmen.

Die Versichertenkarte wurde hier allein dazu genutzt, die Berechtigung zur Inanspruchnahme vergünstigter Leistungen privater Vertragspartner der Krankenkasse nachzuweisen, was eindeutig nicht dem durch § 291 Absatz 1 Satz 3 SGB V abschließend vorgezeichneten Rahmen für den Einsatz dieser Karte entspricht, nämlich die Inanspruchnahme vertragsärztlicher Leistungen und die Abrechnung mit den Leistungserbringern. Schon der klare Wortlaut dieser Vorschrift, vor allem aber die ohne großen technischen Aufwand realisierbare Möglichkeit, die auf der Karte jetzt schon hinterlegten Daten auszulesen, und die damit verbundene Gefahr eines Missbrauchs dieser Informationen, lassen eine erweiterte Interpretation des Anwendungsbereichs der Versichertenkarte nicht zu.

Da die betroffenen Krankenkassen alle dem Bundesverband der Betriebskrankenkassen angehören, habe ich auch diesem meine Rechtsauffassung mitgeteilt und darum gebeten, seine Mitglieder in geeigneter Weise zu informieren. Der Bundesverband hat dieser Bitte mit einem entsprechenden Rundschreiben an seine Mitglieder im Oktober 2005 entsprochen.

### 13.1.7 „Barmer Hausarzt- und Hausapotheken – Modell“

*Bei dem von der Barmer Ersatzkasse initiierten „Hausarzt- und Hausapotheken – Modell“ waren datenschutzrechtliche Nachbesserungen erforderlich.*

Während des Berichtszeitraumes habe ich mich mit den datenschutzrechtlichen Fragen im Zusammenhang mit einem Vertragsmodell zwischen der Barmer Ersatzkasse, der Hausärztlichen Vertragsgemeinschaft e. G. (HÄVG) und der Marketinggesellschaft Deutscher Apotheker mbH (MGDA) befasst. Gegenstand dieses sog. „Barmer Hausarzt- und Hausapotheken-Vertrages“ ist ein durch eine enge Zusammenarbeit zwischen Hausarzt und einer vom Patienten gewählten Apotheke geprägtes Versorgungsangebot der Krankenkasse mit der Zielsetzung einer optimierten medizinischen Behandlung, einer Erhöhung der Arzneimittelsicherheit und einer finanziellen Entlastung zugunsten der freiwillig an diesem Modell teilnehmenden Versicherten.

Bereits kurz nach Inkrafttreten dieses Vertrages haben mir zahlreiche Bürgerinnen und Bürger ihre Besorgnis und Unsicherheit über die Wahrung datenschutzrechtlicher Belange bei Teilnahme an dieser Art der Versorgung zum Ausdruck gebracht. Die Befürchtungen, die auch von Hausärzten und Apothekern geteilt wurden, konzentrierten sich vor allem auf eine nur unzureichende Transparenz der Datenerhebungen und -verarbeitung, insbesondere im Hinblick auf die Information der Betroffenen. Der teilnahmewillige Versicherte konnte nicht im notwendigen Umfang nachvollziehen, welche Informationen über ihn von wem und zu welchen Zwecken erhoben und in welchen Fällen an wen weitergegeben wurden. Ebenso unklar blieb für ihn die Frage, ob und gegebenenfalls welche Auswirkungen eine Teilnahme oder Nichtteilnahme auf das bestehende Versicherungsverhältnis haben würde.

Die Bedenken habe ich mit den Verantwortlichen der Krankenkasse erörtert. Ungeachtet der rechtlichen Einordnung dieses Versorgungsmodells – die Krankenkasse selbst spricht von einer „additiven“ integrierten Versorgung mit einer „Lotsenfunktion des Hausarztes“ in Abgrenzung zu einer „substituierenden“ integrierten Versorgungsform, wie sie in § 140a SGB V als Alternative zur Regelversorgung zugelassen ist – waren neben einigen Passagen des Vertrages selbst insbesondere die zur Teilnahmeerklärung dienenden Vordrucke und Erläuterungen änderungs- und ergänzungsbedürftig. Meine Hinweise und Formulierungsvorschläge zur Sicherstellung einer datenschutzgerechten Aufklärung der teilnehmenden Versicherten über die Rechtsgrundlagen, die Beteiligten und alle die Erhebung und Verarbeitung ihrer personenbezogenen Daten betreffenden Verfahrensabläufe innerhalb der integrierten Versorgung nach diesem Modell sind von der Krankenkasse aufgegriffen worden und zwischenzeitlich in eine überarbeitete „Erklärung zur Teilnahme an der Integrierten Versorgung durch Hausärzte und Hausapotheken“, ebenso in die „Einwilligungserklärung zu datenschutzrechtlichen Bestimmungen“ und das „Merkblatt zur datenschutzrechtlichen Einwilligung“ eingeflossen. Ich bin zuversichtlich, dass mit diesen Verbesserungen das nötige Vertrauen der Beteiligten in ein transparentes und die Selbstbestimmung über die eigenen personenbezogenen Daten wahrendes Verfahren in der Verantwortung der betreffenden Krankenkasse (wieder) hergestellt werden kann.

### 13.1.8 Häusliche Krankenpflege – Was will eine gesetzliche Krankenkasse mit den medizinischen Daten ihrer Versicherten?

*Der Umfang der Erhebung von medizinischen Daten durch Krankenkassen ist im Gesetz abschließend geregelt. Die Erhebung weiterer Daten auf Basis von Einwilligungserklärungen verstößt gegen diese gesetzlichen Begrenzungen.*

Die City BKK verwendet ein „Merkblatt zur Datenweitergabeerklärung“ sowie eine „Einwilligungserklärung zur Datenerhebung und Datenweitergabe“ mit denen sich Versicherte bei der Gewährung von Leistungen der häuslichen Krankenpflege – HKP – (§ 37 SGB V) mit der Weitergabe ihrer Daten, wie z. B. Medikamentenplänen, Wundprotokollen etc. einverstanden erklären. In dem Merkblatt zur Datenweitergabeerklärung informiert die City BKK ihre Versicherten auch darüber, dass sie für eine „bedarfsgerechte Versorgung“ u. a. Daten aus Pflege-/Behandlungsdokumentationen erhebt und speichert.

Mit der Datenerhebung aus Pflege- oder Behandlungsdokumentationen durch Kranken-/Pflegekassen habe ich mich in der Vergangenheit ausführlich beschäftigt (vgl. 19. TB Nr. 24.2.2, 20. TB Nr. 17.2.1 und 17.1.6). Meine Rechtsauffassung wird von der Bundesregierung ausdrücklich geteilt (s. Kasten zu Nr. 13.1.8).

Kasten zu Nr. 13.1.8

**Auszug**

**Stellungnahme der Bundesregierung zum 20. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes – Bundestagsdrucksache 15/5252 –**

Zu Nr. 17.1.6 – Verarbeitung medizinischer Daten bei der häuslichen Krankenpflege durch die Kassen

Der BfD stellt fest, dass Krankenkassen für die Prüfung der Leistungsvoraussetzungen von häuslicher Krankenpflege Gesundheitsdaten erheben, die unter die ärztliche Schweigepflicht fallen, weil ihnen entsprechende Aufträge an den Medizinischen Dienst der Krankenkasse offenbar zu aufwändig sind.

Für den Bereich der häuslichen Krankenpflege vertritt die Bundesregierung die Auffassung, dass eine Übermittlung von Pflegedokumentationen an die Krankenkassen durch die Regelung des § 302 SGB V nicht gestattet ist. In diesem Zusammenhang ist eine Übermittlung der Pflegedokumentationsdaten durch die Leistungserbringer nach § 276 Abs. 2 Satz 1 SGB V nur unmittelbar an den Medizinischen Dienst zulässig, sofern dieser von den Krankenkassen nach § 275 Abs. 1 bis 3 SGB V zu einer gutachterlichen Stellungnahme veranlasst wurde und die Datenübermittlung erforderlich ist.

Ich habe die City BKK mehrfach auf die Rechtslage sowohl im Zusammenhang mit der Einsichtnahme in Pflegedokumentationen und Krankenhausentlassungsberichte als auch bei der Forderung von Schweigepflichtentbindungserklärungen hingewiesen. Sie hält jedoch weiterhin an der Erhebung von medizinischen Daten auf der Grundlage von Schweigepflichtentbindungserklärungen ihrer Versicherten fest.

Die Datenerhebungsbefugnis für die Zwecke der gesetzlichen Krankenversicherung ist in § 284 SGB V bereichsspezifisch abschließend geregelt. Das gleiche gilt für die Übermittlungsbefugnisse der Leistungserbringer, wie zum Beispiel Krankenhäuser (§ 301 SGB V) und Ärzte (§ 295 SGB V). Dieser Vorrang abschließender spezialgesetzlicher Regelungen kann weder durch allgemeine gesetzliche Regelungen, wie etwa im SGB I oder SGB X (vgl. Nr. 13.1.3), noch durch Vereinbarungen, wie etwa Einwilligungs- oder Schweigepflichtentbindungserklärungen der Versicherten umgangen werden. Das Einholen einer Einwilligung der Versicherten in die Übermittlung von Gesundheitsdaten unmittelbar an die Kranken-/Pflegekasse stellt eine unzulässige Umgehung dieser gesetzlichen Restriktion und eine Missachtung des in den §§ 275 ff. SGB V dokumentierten Willens des Gesetzgebers, wonach ausschließlich der Medizinische Dienst der Krankenkassen zur Prüfung medizinischer Sachverhalte berechtigt ist, dar.

Die fortlaufende rechtswidrige Erhebung von Sozial- und Gesundheitsdaten der Versicherten durch die City BKK habe ich gem. § 25 Abs. 1 BDSG beanstandet. In ihrer Antwort stellt das Justiziariat der Krankenkasse erneut die in den genannten Tätigkeitsberichten dargelegte Auffassung in Frage. Eine Stellungnahmen durch den Vorstand (§ 25 Abs. 3 BDSG) steht noch aus.

### 13.1.9 Öffentliche Ausschreibungen für Sozialleistungen

*Öffentliche Ausschreibungen für Sozialleistungen sind so zu gestalten, dass kein Rückschluss auf betroffene Personen möglich ist.*

Auf einer über das Internet für jeden Interessierten zugänglichen Ausschreibungsplattform für Patientenfahrten hatte eine große bundesunmittelbare Krankenkasse Daten aus dem persönlichen Umfeld ihrer Versicherten veröffentlicht, um auf diese Weise das preisgünstigste Fuhrunternehmen für ärztlich verordnete Transporte dieser Versicherten zu ermitteln. Die zur Angebotsabgabe dienende Leistungsbeschreibung der einzelnen Fahrten enthielt dabei nicht nur den Ortsnamen mit Postleitzahl und die Bezeichnung der Straßen als Abfahrts- und Zielorte, sondern regelmäßig auch den Zeitraum der durchzuführenden Fahrten mit taggenauer Angabe der ersten Fahrt und teilweise auch der Wochentage aller weiteren Fahrten sowie der voraussichtlichen Wartezeit zwischen Hin- und Rückfahrt. Ein Freitextfeld „Sonstige Angaben zu den Fahrten“ offenbarte darüber hinaus vereinzelt Hinweise auf das Gebrechen des zu transportierenden Patienten, seinen derzeitigen Aufenthaltsort oder sogar die Angabe der vollständigen Adresse oder des Nachnamens des Versicherten.

Ich habe die Krankenkasse darauf hingewiesen, dass diese detaillierten Angaben aufgrund ihrer öffentlichen Zugänglichkeit in Einzelfällen – z. B. in kleineren Ortschaften oder bei überschaubaren Straßenzügen – auch noch zu anderen Zwecken als zur Abgabe eines Angebotes missbraucht werden könnten und um eine unverzügliche Änderung des Ausschreibungsverfahrens gebeten. Der Kreis der Nutzungsberechtigten dieser Internetseite ist von vornherein einzuschränken, z. B. auf registrierte Fuhrunternehmen, und die Leistungsbeschreibung der zur Ausschreibung gelangenden Patientenfahrten so weit zu begrenzen, wie es zur Abgabe eines vergleichbaren Angebotes unbedingt notwendig ist. Die Möglichkeit eines Personenbezuges muss auf jeden Fall ausgeschlossen sein.

Die Krankenkasse hat das Verfahren zwischenzeitlich überarbeitet und dabei meine Änderungsvorschläge im Wesentlichen übernommen.

## 13.2 Gendiagnostikgesetz dringend erforderlich

*Das Gendiagnostikgesetz lässt noch auf sich warten, obwohl der Umgang mit Gentests immer größere Bedeutung gewinnt.*

Die Entschlüsselung des menschlichen Genoms führt zu immer neuen medizinischen Erkenntnissen mit weit reichenden Folgen für unser tägliches Leben. Genanalysen erlauben heutzutage bereits lange vor dem tatsächlichen

Ausbruch einer Krankheit Vorhersagen über deren Eintrittswahrscheinlichkeit, selbst wenn dem Betroffenen seine Anfälligkeit für diese Krankheit nicht bekannt ist. Auch lassen Genanalysen Rückschlüsse auf die medizinische Konstellation von Blutsverwandten zu, ohne dass diese an dem Verfahren beteiligt sind. Die vorhandenen rechtlichen Rahmenbedingungen werden der Sensibilität und Komplexität dieser Materie nicht mehr gerecht. Obwohl der Deutsche Bundestag die Verabschiedung eines Gendiagnostikgesetzes angemahnt hat (Bundestagsdrucksache 15/4597), vgl. auch 20. TB Nr. 2.6, liegt noch nicht einmal ein Referentenentwurf vor.

Einen wichtigen Beitrag zur Problematik hat im August 2005 der Nationale Ethikrat durch die Veröffentlichung seiner Stellungnahme „Prädiktive Gesundheitsinformationen bei Einstellungsuntersuchungen“ geleistet. Die darin enthaltene Empfehlung für einen restriktiven Umgang mit Gentests verdeutlicht, dass der Umgang mit Gentests einer klaren normativen Grundlage bedarf. Im Vordergrund muss dabei die Stärkung des Selbstbestimmungsrechts des Betroffenen stehen. Genetische Untersuchungen sollen grundsätzlich nur durchgeführt werden, wenn die betroffene Person nach umfassender Aufklärung über Zweck und mögliche Konsequenzen in eine solche Untersuchung eingewilligt hat. Zur informationellen Selbstbestimmung gehört auch die Gewährleistung des Rechts auf Nichtwissen. Heimliche Gentests müssen ebenso verhindert werden wie die missbräuchliche Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis. Ich befürworte ein grundsätzliches Verbot, Gentests als Voraussetzung für Einstellungen oder den Abschluss von Versicherungsverträgen zu fordern. Zuwiderhandlungen gegen grundlegende Vorschriften der Regelung, insbesondere bei heimlichen Gentests ohne Einwilligung der betroffenen Person, müssen entsprechend der Schwere des Verstoßes durch Straf- oder Bußgeldbestimmungen sanktioniert werden.

Ich halte die Schaffung eines Gendiagnostikgesetzes für eines der dringendsten datenschutzrechtlichen Vorhaben und hoffe, dass es in dieser Legislaturperiode endlich beschlossen wird.

## 13.3 Unfallversicherung

### 13.3.1 Gutachterregelung

*Mit einer Ausnahme weisen alle Berufsgenossenschaften die Versicherten auf das eigene Gutachtervorschlagsrecht hin. Insgesamt ist dieses in einer Selbstverpflichtung durchgeführte Verfahren der Berufsgenossenschaft als positiv zu bewerten.*

**Gutachtervorschlagsrecht/Erfahrungen mit der „Selbstverpflichtung“**

Alle Berufsgenossenschaften erkennen im Wege der „Selbstverpflichtung“ das Recht der Versicherten an, selbst einen Gutachter vorschlagen zu können (vgl. 20. TB Nr. 19.1.1). Die Unfallversicherungsträger verwenden nunmehr Vordrucke, in denen die Versicherten auf dieses Recht hingewiesen werden. Dies haben meine Stichprobenkontrollen bestätigt. Nur die Berufsgenossenschaft Druck und Papierverarbeitung hält einen Hinweis auf das Gutachtervorschlagsrecht in den Vordrucken für nicht angebracht, da dieses Recht gesetzlich nicht normiert sei. Ich bedaure diese Praxis der Berufsgenossenschaft, weil deren Versicherte so von ihrem Recht nichts erfahren, das die übrigen Berufsgenossenschaften anerkennen. Vor dem Hintergrund, dass auch gerichtliche Entscheidungen ein Gutachtervorschlagsrecht der Versicherten mangels expliziter gesetzlicher Erwähnung nicht sehen, habe ich davon abgesehen, die Verfahrensweise der Berufsgenossenschaft zu beanstanden.

In der Praxis üben die Versicherten ihr Gutachtervorschlagsrecht überwiegend nicht aus. Hatten die Versicherten selbst einen Gutachter vorgeschlagen, war dieser nur in Einzelfällen von den Berufsgenossenschaften mit einer zu pauschalen Begründung abgelehnt worden. Insoweit habe ich stets darauf hingewiesen, dass die Berufsgenossenschaften die Ablehnung eines vorgeschlagenen Gutachters gegenüber dem Versicherten in dem konkreten Einzelfall nachvollziehbar zu begründen haben.

Insgesamt sind die Ergebnisse aufgrund der von den Berufsgenossenschaften getroffenen Selbstverpflichtung jedoch als positiv zu bewerten, und ich bin zuversichtlich, dass die positiven Erfahrungen, die auch die Berufsgenossenschaften mit dem eigenen Gutachtervorschlagsrecht der Versicherten gemacht haben, zu einer großzügigen Gewährung dieses Rechts führen werden.

**Beratender Arzt**

Obwohl sich die gemeinsam vom Hauptverband der gewerblichen Berufsgenossenschaften, dem BVA und mir entwickelten Kriterien zur Abgrenzung zwischen der Tätigkeit eines beratenden Arztes und eines Gutachters in der Praxis der Berufsgenossenschaften bewährt haben (vgl. 20. TB Nr. 19.1), ist die Anwendbarkeit der Gutachterregelung bei der Einschaltung eines beratenden Arztes in dem Verfahren wieder in die Diskussion geraten. Das Landessozialgericht Nordrhein-Westfalen hat – unter Rückgriff auf die vor Einführung des § 200 Abs. 2 SGB VII übliche Rechtsprechung – den beratenden Arzt als Teil der Verwaltungsbehörde bewertet und damit eine Übermittlung von Gesundheitsdaten der Versicherten an einen Dritten abgelehnt. Aus diesem Grund würde die Gutachterregelung keine Anwendung finden, wenn ein beratender Arzt ein Gutachten erstattet. In einer Vielzahl von Einzelfällen haben sich die Berufsgenossenschaften auf diese Rechtsprechung berufen, wenn ein Verstoß gegen § 200 Abs. 2 SGB VII festgestellt worden war.

Nach dem Wortlaut des § 200 Abs. 2 SGB VII sind den Versicherten die genannten Rechte „vor Erteilung eines Gutachtenauftrages“ zu gewähren. Damit knüpft die Regelung erkennbar an ein inhaltliches Gutachten an, unabhängig davon, ob es ein beratender Arzt oder ein externer Gutachter erstattet. Auch die Absicht des Gesetzgebers, die Mitwirkungsrechte der Versicherten zu stärken und die Verfahrenstransparenz zu erhöhen, ist nur dann zu erreichen, wenn sich die Gutachterregelung auch auf die Gutachten eines beratenden Arztes erstreckt.

Auf meine Intervention hin hat die überwiegende Mehrzahl der Berufsgenossenschaften ihre Zustimmung zu den Kriterien erteilt und zugesagt, auch künftig einen beratenden Arzt lediglich mit einer Stellungnahme zu beauftragen und vor der Erteilung eines Gutachtenauftrages den Versicherten die in § 200 Abs. 2 SGB VII genannten Rechte zu gewähren. Dies begrüße ich.

Angesichts der noch unklaren Rechtslage erhoffe ich mir eine Klärung der offenen Rechtsfragen durch das Bundessozialgericht.

### 13.3.2 Rechtsfolgen bei Missachtung der Gutachterregelung

*Als Folge der Missachtung des § 200 Abs. 2 SGB VII bei der Einholung eines Gutachtens ist das Gutachten gem. § 84 Abs. 2 Satz 1 SGB X zu löschen.*

Im Berichtszeitraum hat sich eine Vielzahl von Berufsgenossenschaften auf zwei Urteile von Landessozialgerichten berufen, die die Regelung des § 200 Abs. 2 SGB VII als reine Verfahrensvorschrift und einen Verstoß gegen diese Regelung als unbeachtlich bewertet haben. Die rechtliche Bewertung in den Urteilen erfolgt wiederum unter Berufung auf die Literatur, die sich auf die bloße Behauptung, der Verstoß gegen § 200 Abs. 2 SGB VII sei unbeachtlich, beschränkt. Eine Auseinandersetzung mit der systematischen Einordnung der Gutachterregelung des § 200 Abs. 2 SGB VII unter Berücksichtigung des vom Gesetzgeber beabsichtigten Schutzzwecks der Vorschrift führt jedoch zu einer anderen Beurteilung. Mit der in der Begründung festgehaltenen gesetzgeberischen Intention, mehr Verfahrenstransparenz zu schaffen und die Mitwirkungsrechte der Versicherten zu stärken, geht die Regelung weit über eine reine Verfahrensregelung hinaus. Die Einschränkung der Übermittlungsbefugnis hat vor diesem Hintergrund materiell-rechtlichen Charakter. Dafür sprechen auch die Entstehungsgeschichte der Vorschrift, die im Wesentlichen auf die parlamentarischen Beratungen unter meiner Einbeziehung zurückzuführen ist, sowie die Einordnung der Vorschrift im Gesetz unter dem Begriff „Datenschutz".

Selbst wenn man die Gutachterregelung als Verfahrensregelung sehen will, ist die Meinung, dass ein Verstoß unbeachtlich ist, nicht überzeugend:

- Das Auswahlrecht des Versicherten nach § 200 Abs. 2 SGB VII geht in seiner rechtlichen Gewichtung über die in § 41 SGB X genannten Verfahrens- und Formfehler hinaus, da dem Betroffenen ein eigener Entscheidungsspielraum eingeräumt wird.
- Es liegt keine „gebundene" Entscheidung im Sinne des § 42 Satz 1 SGB X vor, da bei der Auswahl eines anderen Gutachters auch eine andere Entscheidung in der Sache denkbar ist. Bei einem Gutachten handelt es sich um eine persönliche Einschätzung eines Sachverständigen, deren Ergebnis nicht von vornherein feststeht und nicht berechenbar ist.
- Die in § 42 Satz 2 SGB X genannte Anhörung ist wegen der hohen Bedeutung mit dem Auswahlrecht der Gutachterregelung vergleichbar, da beide Rechte des Versicherten auf einem Grundrecht oder einem diesem gleichgestellten Recht beruhen (Grundsatz des rechtlichen Gehörs, Artikel 108 GG; Recht auf informationelle Selbstbestimmung). Dabei ist zu berücksichtigen, dass das Auswahlrecht des § 200 Abs. 2 SGB VII noch stärker ausgeprägt ist als das Recht auf Anhörung; denn während eine Berufsgenossenschaft ihre Entscheidung ungeachtet des Ergebnisses einer Anhörung treffen kann, ist sie an die Auswahl, die ein Versicherter unter mehreren vorgeschlagenen Gutachtern trifft, gebunden.

Unter Berücksichtigung dieser rechtlichen Aspekte kann ein Verstoß gegen die Gutachterregelung des § 200 Abs. 2 SGB VII nicht als unbeachtlich bewertet werden, mit der Folge, dass das Gutachten gem. § 84 Abs. 2 Satz 1 SGB X zu löschen ist. In allen mir im Berichtszeitraum bekannt gewordenen Fällen der Nichtbeachtung der Gutachterregelung habe ich jedoch im Hinblick auf die von den Berufsgenossenschaften zitierten Urteile des Landessozialgerichts Nordrhein-Westfalen und des Landessozialgerichts Baden-Württemberg von einer Beanstandung abgesehen.

### 13.3.3 Anforderung von Krankenhausentlassungsberichten durch Unfallversicherungsträger

*Die Anforderung von Entlassungs- und Operationsberichten durch Unfallversicherungsträger sollte ausdrücklich gesetzlich geklärt werden.*

Im Berichtszeitraum hatte ich mich mehrfach mit der Frage zu befassen, ob Unfallversicherungsträger befugt sind, zur Überprüfung ihrer Leistungsverpflichtung Krankenhausentlassungsberichte und Operationsberichte anzufordern. Bei derartigen Anfragen sehen sich die Krankenhäuser immer wieder in dem Zwiespalt, dass sie als Vorbedingung zur Begleichung der jeweiligen Rechnung die angeforderten Entlassungsberichte und Operationsberichte übersenden müssen und damit in Gefahr geraten, sich einer Verletzung der Schweigepflicht schuldig zu machen, da die Berichte medizinische Daten enthalten, die dem Arztgeheimnis unterliegen.

Vor dem Hintergrund der Erläuterungen des Ministeriums für Arbeit und Sozialordnung halte ich jedoch die Anforderung von Krankenhausentlassungsberichten und Operationsberichten auf der Grundlage des § 199 Abs. 1 Satz 1 und Satz 2 Nr. 2 i.V.m. Abs. 2 Satz 2 SGB VII für vertretbar. Das Ministerium hatte die Aufgabenbeschreibung für die Unfallversicherungsträger in § 199 Abs. 1 SGB VII dahingehend erläutert, dass die Befugnis zur Datenerhebung und Datenspeicherung zur „Erbringung der Leistungen" auch die Abrechnung der Leistungen beinhalte. Das Ministerium hält eine besondere Nennung der Abrechnungsdaten im datenschutzrechtlichen Aufgabenkatalog der Unfallversicherung nicht für erforderlich, da das SGB VII – abweichend von der Systematik in den Regelungen für die gesetzliche Krankenversicherung nach SGB V – keine abschließende Aufzählung der datenschutzrechtlichen Befugnisse kennt.

Aus Gründen der Normenklarheit und aus Gründen der Rechtssicherheit habe ich mich jedoch gegenüber dem Ministerium für eine gesetzliche Klarstellung im SGB VII eingesetzt.

### 13.3.4 Prüfdatei bei fehlerhafter Abrechnung

*Unfallversicherungsträger dürfen Ärztedaten nur speichern, soweit dies für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.*

Im Berichtszeitraum hat eine Berufsgenossenschaft eine sog. „Rechnungsprüfungsdatei“ eingerichtet, in die Namen und Rechnungsdaten der Ärzte aufgenommen werden, die nach Auffassung der Berufsgenossenschaft unrichtig abgerechnet haben. Sobald eine von einem Arzt eingereichte Rechnung um insgesamt 50 Euro nach unten korrigiert wird, speichert die Berufsgenossenschaft die persönlichen Daten des Arztes und erfasst dessen künftige Abrechnungen – bis zu einer Löschung – ebenfalls in der Datei.

Die Berufsgenossenschaft hält aufgrund ihrer Verpflichtung nach § 69 Abs. 2 SGB IV, bei der Ausführung der ihr obliegenden Aufgaben wirtschaftlich und sparsam zu handeln, die Datei für zulässig. Sie soll der Berufsgenossenschaft ermöglichen, darauf hinzuwirken, dass Ärzte und andere medizinische Leistungserbringer ihr Honorar im Einklang mit den gesetzlichen sowie vertraglichen Pflichten abrechnen. Der Arzt soll über die Tatsache der Aufnahme seiner Daten sowie über die gespeicherten Daten informiert und damit zu einer intensiveren Prüfung seiner Rechnungen angehalten werden. Nach Auffassung der Berufsgenossenschaft ist das Verfahren geeignet, zur Erfüllung des Gebots der Wirtschaftlichkeit und Sparsamkeit beizutragen, weil damit die Anzahl unrichtiger Abrechnungen mit möglichst geringem Aufwand reduziert werde. Der Begriff der Erforderlichkeit sei mit dem Begriff der Eignung gleichzusetzen, da die Berufsgenossenschaft hinsichtlich des Wirtschaftlichkeitsgebots ein Beurteilungsspielraum zustehe.

Diese Argumentation vermag nicht zu überzeugen. Es ist bereits zweifelhaft, ob die „Rechnungsprüfungsdatei“ überhaupt geeignet ist, einer Berufsgenossenschaft eine wirtschaftlichere Abrechnungsprüfung zu erleichtern, denn es ist nicht ersichtlich, ob und ggf. in welchem Umfang Einsparungen zu erwarten sind, wenn eingereichte Rechnungen bestimmter Ärzte einer besonderen Prüfung unterzogen werden. Nach der Argumentation der Berufsgenossenschaft ist dies auch nicht der unmittelbare Zweck der „Rechnungsprüfungsdatei“. Ein wirtschaftlicher Vorteil soll vielmehr erst mittelbar dadurch erreicht werden, dass die Leistungserbringer zur sorgfältigen Prüfung ihrer Rechnungen angehalten würden. Steht jedoch ein rein erzieherisches Ziel im Vordergrund, nicht aber unmittelbare Einsparungen, ist zweifelhaft, ob die Datei dem gesetzlichen Gebot der Wirtschaftlichkeit und Sparsamkeit überhaupt dient. Entscheidend ist jedoch, dass die „Rechnungsprüfungsdatei“ nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit entspricht. Dabei ist zu berücksichtigen, dass den in die Datei aufgenommenen Ärzten in den wenigsten Fällen Sorgfaltspflichtverletzungen in Bezug auf ihre Abrechnungen vorzuwerfen bzw. nachzuweisen sind. Die Vielzahl von Meinungsverschiedenheiten und Rechtsstreitigkeiten über die Art und Weise bzw. die Höhe von Abrechnungen deutet vielmehr darauf hin, dass von den Unfallversicherungsträgern als unrichtig empfundene Abrechnungen nicht überwiegend auf ein fehlerhaftes oder gar betrügerisches Abrechnungsverhalten von Ärzten oder Krankenhäusern zurückzuführen sind.

Von der Führung einer derartigen Prüfdatei sollte daher Abstand genommen werden. In die noch laufende Diskussion mit der Berufsgenossenschaft ist auch das Bundesversicherungsamt eingeschaltet worden.

## 13.4 Rentenversicherung

### 13.4.1 Beratung der Deutschen Rentenversicherung Bund

*Die datenschutzrechtliche Beratung der Deutschen Rentenversicherung Bund habe ich auch nach der Organisationsreform der gesetzlichen Rentenversicherung (vgl. 20. TB Nr.18.1) intensiv weitergeführt.*

Im Zuge ihrer Sicherheitsbemühungen richten Polizeibehörden, Nachrichtendienste, Staatsanwaltschaften und Gerichte in zunehmendem Maße Übermittlungsersuchen an die Rentenversicherungsträger. Zwar liegen mir noch keine aktuellen Zahlen für den Berichtszeitraum vor. Jedoch ergaben sich in den Jahren zuvor (2002: 13 860, 2003: 15 802, 2004: 16 741 Anfragen) jeweils Steigerungen bei der Zahl der Übermittlungsersuchen. Nach meinem Eindruck prüft die Deutsche Rentenversicherung Bund derartige Ersuchen besonnen auf ihre Vereinbarkeit mit den einschlägigen Vorschriften der Sozialgesetzbücher und handhabt die Auskunft über die Sozialdaten ihrer Versicherten eher restriktiv. Ich werde diesem wichtigen Gebiet des Sozialdatenschutzes künftig besondere Aufmerksamkeit widmen.

Auch sonstige wichtige datenschutzrechtliche Themen konnten mit der Deutschen Rentenversicherung Bund vorangebracht werden. Dies betrifft beispielsweise Überlegungen zur Änderung von Abläufen in der Personalverwaltung und damit im Zusammenhang stehende Fragen der elektronischen Personalaktenführung (s. u. Nr. 14.2.). Schließlich konnten in diesen Gesprächen auch besonders gelagerte Einzelfälle im Interesse der Petentinnen und Petenten einer datenschutzgerechten Lösung zugeführt werden.

Die Zusammenarbeit mit der Deutschen Rentenversicherung Bund war dabei stets kooperativ und konstruktiv.

### 13.4.2 Kontrolle einer Rehabilitationsklinik der Deutschen Rentenversicherung Bund

*In den letzten Jahren habe ich mich intensiv mit dem Datenschutz in den Rehabilitationskliniken der Deutschen Rentenversicherung Bund befasst. Ein weiterer Beratungs- und Kontrollbesuch erbrachte ein positives Gesamtergebnis.*

Anknüpfend an verschiedene vorausgegangene Beratungs- und Kontrollbesuche von Rehabilitationseinrichtungen der Deutschen Rentenversicherung Bund (vgl. 19. TB Nr. 25.3, 20. TB Nr. 18.2.2) habe ich im Berichtszeitraum die personenbezogene Datenverarbeitung in einer weiteren Rehabilitationsklinik des Rentenversicherungsträgers kontrolliert. Der Besuch hatte zum Ziel, die Umsetzung der unter meiner Beteiligung erarbeiteten „Richtlinien für den Datenschutz in den Reha-Zentren der Deutschen Rentenversicherung Bund“ (vgl. 19. TB Nr. 25.1) in der Praxis zu überprüfen und insbesondere festzustellen, ob die in der Vergangenheit im Verwaltungsbereich einer anderen geprüften Klinik aufgetretenen Mängel nunmehr abgestellt sind.

Ein weiterer Schwerpunkt der Kontrolle war die Überprüfung der zum Schutz personenbezogener Daten bzw. Sozialdaten getroffenen technischen und organisatorischen Maßnahmen (§ 78a SGB X; § 9 sowie Anlage zu § 9 Satz 1 BDSG) im Verwaltungs- und Personalbereich sowie im ärztlichen Bereich der Klinik. Mein besonderes Augenmerk galt dabei den verschiedenen im ärztlichen Bereich eingesetzten medizinisch-technischen Geräten, mit denen sensible Gesundheitsdaten verarbeitet werden. Nach meinen Feststellungen vor Ort fehlte es hier noch an den notwendigen Datensicherungs- bzw. Datenschutzkonzepten. Ich habe der Deutschen Rentenversicherung Bund daher empfohlen, entsprechende Konzepte einheitlich für die Reha-Zentren zu erstellen und meine Beratung bei der Konzeption angeboten. Meine datenschutzrechtlichen Hinweise und Empfehlungen zu diesen und anderen Gesichtspunkten wurden von der Deutschen Rentenversicherung Bund positiv aufgenommen, so dass ich von einer zügigen Umsetzung ausgehe.

## 13.5 Arbeitsverwaltung

### 13.5.1 Hartz IV und Missbrauchskontrolle

*Das beherrschende Thema im Bereich der Arbeitsverwaltung ist nach wie vor „Hartz IV“. Die Kostenentwicklung führte zur Ausweitung der gesetzlichen Kontrollmaßnahmen gegenüber den Leistungsempfängern.*

Im 20. TB (Nr. 16.1 f.) hatte ich ausführlich über die mit dem „Vierten Gesetz für moderne Dienstleistungen am Arbeitsmarkt“ (Hartz IV) bewirkte Zusammenlegung von Arbeitslosen- und Sozialhilfe für erwerbsfähige Hilfebedürftige zu einer einheitlichen „Grundsicherung für Arbeitsuchende“ und die damit verbundenen vielfältigen datenschutzrechtlichen Probleme berichtet. Auch in diesem Berichtszeitraum hat die Thematik wieder eine große Rolle gespielt. Im Mittelpunkt standen dabei die intensive Suche nach Lösungen für die monierten Mängel und die im Sommer 2005 aufgekommene Missbrauchsdebatte, bei der es um die angeblich massive unberechtigte Inanspruchnahme von Sozialleistungen ging.

Um dies zu untersuchen, startete die Bundesagentur für Arbeit (BA) im Juli 2005 über externe Call-Center eine unangekündigte, breit angelegte Telefonbefragungsaktion bei Alg-II-Empfängern, die zu Recht auf Kritik bei vielen Betroffenen stieß. Ziel dieser Befragung war die aktuelle Bestandsklärung bezüglich des Arbeitslosenstatus. „Cold Calling“, also Telefonanrufe ohne Vorwarnung, sind datenschutzrechtlich aber bedenklich. Ich forderte daher die BA auf, die Befragungsaktion auszusetzen, bis die Betroffenen vorab schriftlich über die geplanten Anrufe informiert worden seien. Ich wies darauf hin, dass erst eine detaillierte Information, in der die Rechtsgrundlage, der Zweck des Verfahrens und die vorgesehene Legitimation und Authentifizierung der anrufenden Mitarbeiter des Call-Centers genannt werden, es dem Betroffenen ermöglicht, nach gründlicher Abwägung über eine Teilnahme zu entscheiden. Nach meiner Prüfung war auf die Freiwilligkeit der telefonischen Auskunftserteilung häufig nicht hingewiesen worden. Auch der Legitimationsnachweis der Interviewer war nicht hinreichend. Eine rechtsmissbräuchliche Beschaffung von Daten durch „Trittbrettfahrer“ war danach nicht auszuschließen. Schließlich forderte ich wegen der Sozialdaten, die bei der Befragung anfielen, dass die BA in den Call-Centern nur eigene Mitarbeiter einsetzt. Die BA griff meine Kritikpunkte erfreulicherweise auf und führte das Verfahren in datenschutzgemäßer Weise fort. Bei der Kontrolle eines Call-Centers in Hamburg habe ich mir hiervon selbst ein Bild gemacht.

Auch wenn die Telefonbefragungsaktion den angeblichen Missbrauch im großen Stil nicht nachweisen konnte, wurden Rufe nach mehr Kontrolle laut. Das am 1. August 2006 in Kraft getretene „Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende“ (Fortentwicklungsgesetz; BGBl. I S. 1706) enthält weit reichende neue Möglichkeiten zur Kontrolle der Leistungsempfänger. Diese Instrumente tangieren das Recht auf informationelle Selbstbestimmung. So ist in Bezug auf die telefonische Befragung über eine Ergänzung des § 51 SGB II die Möglichkeit geschaffen worden, zur Erfüllung der Aufgaben nach dem SGB II einschließlich der Bekämpfung von Leistungsmissbrauch Dritte zu beauftragen und diesen die insoweit erforderlichen Sozialdaten zu übermitteln.

Weiter sollen nach der Neuregelung die Arbeitsgemeinschaften nach dem SGB II (ARGEn) einen Außendienst einrichten (§ 6 Abs. 1 Satz 2 SGB II). Dessen Aufgabe ist, Sachverhalte zu überprüfen, die nicht allein aufgrund der Aktenlage beurteilt werden können. Derartige Hausbesuche tangieren das Grundrecht aus Artikel 13 GG auf Unverletzlichkeit der Wohnung. Sie sind deshalb nur dann zulässig, wenn sie konkret erforderlich, geeignet und verhältnismäßig sind. Keinesfalls dürfen derartige Besuche im Rahmen einer routinemäßigen Überprüfung (z. B. bei Erstantrag) erfolgen. Ich habe in diesem Zusammenhang verbindliche, allgemeine Handlungsanweisungen für die Außendienstmitarbeiter gefordert, damit ein einheitliches, transparentes Vorgehen gewährleistet ist.

Schließlich erweitert das Gesetz die Möglichkeiten zum automatisierten Datenabgleich in § 52 SGB II. So ist nach Abs. 1 Nr. 3 auf der Grundlage der Zinsinformationsverordnung im Wege des Datenabgleichs zu prüfen, ob ALG-II-Empfänger über bislang verschwiegene Konten oder Depots im EU-Ausland verfügen. Solche präventiven Datenabgleiche zum Zwecke der Verdachtsschöp-

fung sind schon aus verfassungsrechtlichen Gründen wegen des hiermit verbundenen Eingriffs in das Recht auf informationelle Selbstbestimmung einer Vielzahl von Betroffenen nur dann gerechtfertigt, wenn sie im vorrangigen öffentlichen Interesse tatsächlich notwendig und verhältnismäßig sind. Hierzu fehlen bislang entsprechende Fakten. Ich hätte eine befristete Regelung mit anschließender Evaluation für angemessener gehalten.

Nennen möchte ich aus dem Maßnahmenpaket noch die Beweislastumkehr bei der Feststellung des Bestehens einer eheähnlichen Gemeinschaft. Gemäß § 7 Abs. 3a SGB II wird ein wechselseitiger Wille, Verantwortung füreinander zu tragen und füreinander einzustehen, nunmehr vermutet, wenn Partner länger als ein Jahr zusammenleben, mit einem gemeinsamen Kind zusammenleben, Kinder oder Angehörige im Haushalt versorgen oder befugt sind, über Einkommen oder Vermögen des anderen zu verfügen. Liegt eines dieser Kriterien vor, muss der Antragsteller umfassend darlegen, warum die gesetzliche Vermutung in seinem Fall nicht zutrifft und dies durch entsprechende Unterlagen nachweisen. Allein die Behauptung, die gesetzliche Vermutung sei nicht erfüllt, reicht dabei nicht aus. Ich halte es für problematisch, dass klare Vorgaben für den Betroffenen, wie er sich „entlasten“ kann, nicht im Gesetz normiert wurden. So ist für mich nur schwer vorstellbar, welche Beweismittel das Nichtbestehen einer Verantwortungs- und Einstehensgemeinschaft im Falle von Zweckwohngemeinschaften belegen können. Ich sehe hier die Gefahr einer exzessiven Erhebung von sensiblen Daten unbeteiligter Dritter.

Ich habe im Gesetzgebungsverfahren in meiner Stellungnahme gegenüber dem Ausschuss für Arbeit und Soziales des Deutschen Bundestags auf diese und weitere Probleme hingewiesen. Unterstützt wurden meine Forderungen auch von den Landesbeauftragten für den Datenschutz (s. Gemeinsame Erklärung – Kasten zu Nr. 13.5.1). Leider hat der Gesetzgeber diesen datenschutzrechtlichen Anliegen nicht Rechnung getragen. Deshalb wird es entscheidend darauf ankommen, in der Praxis sensibel und datenschutzgerecht mit den Neuregelungen umzugehen. Gemeinsam mit den Landesbeauftragten werde ich die Umsetzung der gesetzlichen Vorgaben aufmerksam verfolgen. Aufgabe der Politik wird es sein, die Erforderlichkeit der Regelungen zu evaluieren und diese ggf. zu revidieren.

Kasten zu Nr. 13.5.1

**Gemeinsame Erklärung des Bundesbeauftragten und der Landesbeauftragten für den Datenschutz der Länder Baden-Württemberg, Bayern, Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Sachsen, Sachsen-Anhalt, Schleswig-Holstein und Thüringen**

**Arbeitsuchende unter Generalverdacht**

Die Bundesregierung hat den „Entwurf eines Gesetzes zur Fortentwicklung der Grundsicherung für Arbeitsuchende“ beschlossen, der von den Koalitionsfraktionen in den Deutschen Bundestag eingebracht worden ist (Bundestagsdrucksache 16/1410) und bereits am 1. August 2006 in Kraft treten soll. Ein wesentliches Ziel des Entwurfs ist es, die stark gestiegenen Kosten der Hartz-IV-Reform durch eine verstärkte Kontrolle aller Arbeitsuchenden nennenswert zu begrenzen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat mit Schreiben vom 18. Mai 2006 gegenüber dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages Stellung genommen und auf die datenschutzrechtlichen Probleme hingewiesen. Die Datenschutzbeauftragten unterstützen nachdrücklich die in der Stellungnahme des BfDI enthaltenen Forderungen.

Entgegen den im Sozialrecht geltenden Grundsätzen ist geplant, bei der Frage nach dem Vorliegen einer eheähnlichen Gemeinschaft eine Beweislastumkehr zulasten der Arbeitsuchenden einzuführen. Danach müssten Betroffene selbst nachweisen, dass sie nicht in eheähnlichen Gemeinschaften mit Mitbewohnerinnen oder Mitbewohnern leben. Wie dies in der Praxis geschehen soll, ist unklar. Betroffene könnten sich genötigt sehen, zum einen ihre Hilfsbedürftigkeit Mitbewohnerinnen oder Mitbewohnern und damit Dritten zu offenbaren, zum anderen deren sensible Daten preiszugeben. Dafür gibt es keine Rechtsgrundlage. Eine solche exzessive Datenerhebung wäre datenschutzrechtlich nicht hinnehmbar.

Bedenken bestehen auch gegen die geplante Erweiterung der automatisierten Datenabgleiche. Wegen des hiermit verbundenen massiven Eingriffs in das Recht auf informationelle Selbstbestimmung sind derartige Abgleiche grundsätzlich nur unter sehr engen Voraussetzungen dann zulässig, wenn sie im vorrangigen öffentlichen Interesse tatsächlich notwendig und verhältnismäßig sind. Der Gesetzentwurf enthält aber keine Begründung, weshalb ein regelmäßiger Datenabgleich hinter dem Rücken der Betroffenen erforderlich sein soll. Dass einige von ihnen Leistungen erschleichen wollen, rechtfertigt diese Maßnahme nicht. Belege dafür, dass die vorhandenen Befugnisse zur notwendigen Bekämpfung von Leistungsmissbrauch tatsächlich unzureichend sind, fehlen völlig. Es ist mit dem Menschenbild des Grundgesetzes nicht zu vereinbaren, auf diese Weise alle Arbeitsuchenden, die Grundsicherung beanspruchen, unter Generalverdacht zu stellen.

Gleiches gilt für die Schaffung der diversen Auskunftsmöglichkeiten bei anderen Behörden, beispielsweise beim Kraftfahrtbundesamt. Rein präventive Routineauskunftsersuchen sind als unverhältnismäßig abzulehnen. Es muss deshalb klargestellt werden, dass diese Abfragen nur anlassbezogen, d. h. erst wenn aufgrund der Angaben der Betroffenen tatsächliche Anhaltspunkte für deren Unrichtigkeit oder Unvollständigkeit bestehen, und zielgerichtet im konkreten Einzelfall zulässig sind.

Darüber hinaus regelt der Gesetzentwurf Telefonbefragungen durch private Call Center zur Feststellung von Leistungsmissbrauch. Unabhängig von den rechtlichen Bedenken, diese hoheitliche Aufgabe nichtöffentlichen Stellen zu übertragen, muss die Freiwilligkeit der Teilnahme ausdrücklich klargestellt werden.

Die vorgesehene Verpflichtung der Leistungsträger zur Einrichtung eines Außendienstes für Hausbesuche vermittelt den nicht zutreffenden Eindruck, als würde hierdurch eine Mitwirkungspflicht der Betroffenen begründet. Dass diese Hausbesuche unzweifelhaft wegen des grundgesetzlich geschützten Rechts auf die Unverletzlichkeit der Wohnung (Artikel 13 GG) nur mit vorheriger Zustimmung der Betroffenen möglich sind und die Außendienstmitarbeiter kein Recht zum Betreten haben, ist ausdrücklich zu betonen.

Schließlich beseitigt der Gesetzentwurf nicht die mehrfach von den Datenschutzbeauftragten kritisierten Unklarheiten der Zuständigkeitsverteilung zwischen der Bundesagentur für Arbeit und den Arbeitsgemeinschaften (ARGEn). Im Gegenteil: Die Probleme werden durch den in sich widersprüchlichen Entwurf verfestigt. Einerseits soll die Bundesagentur für Arbeit in Angelegenheiten der ARGEn künftig die datenschutzrechtlich verantwortliche Stelle sein. Andererseits bestimmt der Gesetzentwurf, dass die Länder für die organisatorischen Angelegenheiten und damit auch für den Datenschutz verantwortlich sein sollen. Eine effektive Datenschutzkontrolle wird dadurch unmöglich.

Die Datenschutzbeauftragten fordern den Deutschen Bundestag und den Bundesrat daher auf, den Gesetzentwurf grundlegend mit Blick auf das Recht auf informationelle Selbstbestimmung zu überarbeiten. Dieses Recht muss auch bei denjenigen gewährleistet bleiben, die auf staatliche Grundsicherung angewiesen sind.“

### 13.5.2 Antragsformulare für Alg II jetzt datenschutzfreundlicher

*Die neuen Vordrucke weisen ein wesentlich höheres Datenschutzniveau auf als die Erstauflage.*

Die Erstauflage der Antragsformulare für das Alg II hatte gravierende Mängel aufgewiesen (vgl. 20. TB Nr. 16.1.2). Die unter meiner Mitwirkung entwickelten „Ausfüllhinweise der Bundesagentur für Arbeit zum Antragsvordruck Arbeitslosengeld II“ hatten zunächst für eine Entschärfung der Situation gesorgt. Gleichzeitig war mit Unterstützung der Landesbeauftragten für den Datenschutz an der dringend erforderlichen datenschutzgerechten Neuauflage der Vordrucke gearbeitet worden. Immerhin hat das ursprünglich 16 Seiten lange Hauptantragsformular „Antrag auf Leistungen zur Sicherung des Lebensunterhalts nach dem Zweiten Buch Sozialgesetzbuch (SGB II)“ in der letzten geltenden Fassung „Stand August 2006“ nur noch einen Umfang von 6 Seiten.

Jetzt steht wieder eine Neuauflage an, auch wegen der durch das Fortentwicklungsgesetz bedingten Änderungen. Dieses Mal bin ich erfreulicherweise rechtzeitig, nicht zuletzt auch im eigenen Interesse der BA, beteiligt worden und habe gemeinsam mit den Landesbeauftragten für den Datenschutz die geplanten Änderungen kritisch geprüft. Die BA will meine Forderungen hierzu berücksichtigen. Erhebliche datenschutzrechtliche Mängel sind nicht mehr festzustellen. Die noch vorhandenen Kritikpunkte betreffen überwiegend Detailfragen zur weitergehenden Optimierung der Formulare. Nicht erfolgt ist allerdings die von der BA zugesagte grundlegende Überarbeitung des Zusatzblattes 8 „Antrag auf Gewährung eines Mehrbedarfs für kostenaufwändige Ernährung“ im Zusammenwirken mit dem Verein für öffentliche und private Fürsorge e.V. Ich habe bereits mehrfach darauf hingewiesen, dass die besonders sensiblen Gesundheitsdaten (z. B. eine Aidserkrankung) nicht in den Vermittlungsbereich der Agenturen gelangen dürfen. Auch für die Berechnung des Mehrbedarfs muss der Leistungssachbearbeiter die Diagnose nicht erfahren. Für die Zusammenfassung von Diagnosen, die zur selben Krankenkostzulage führen, ist eine Übergangslösung getroffen worden. Entsprechend der Zusage erwarte ich baldmöglichst einen Vorschlag, wie dauerhaft verfahren werden soll.

Überarbeitet werden musste wegen der Neuregelungen in § 7 SGB II auch das Zusatzblatt 5 „Vorliegen einer Verantwortungs- und Einstehensgemeinschaft“. Nach Abs. 3a wird eine derartige Gemeinschaft nunmehr vermutet, wenn Partner länger als ein Jahr zusammenleben, mit einem gemeinsamen Kind leben, Kinder oder Angehörige im Haushalt versorgen oder befugt sind, über Einkommen oder Vermögen des anderen zu verfügen. Liegt eine dieser Voraussetzungen vor, muss der Antragsteller diese Vermutung widerlegen (Beweislastumkehr). Dies ist datenschutzrechtlich problematisch, weil sensible Daten unbeteiligter Dritter tangiert bzw. Betroffene gezwungen sein könnten, ihre Leistungsbedürftigkeit Mitbewohnern und damit Dritten zu offenbaren. Um hier eine exzessive Datenerhebung zu vermeiden, habe ich mich dafür eingesetzt, dass das Formular als Anhaltspunkt Beispiele für eine mögliche Entkräftung enthält. Wichtig war mir auch der Zusatz, bei Fragen solle sich der Antragsteller an seinen Sachbearbeiter wenden. Auf diese Weise können nicht erforderliche Datenerhebungen vermieden werden. Die Praxis wird zeigen, ob und welche Verbesserungen insoweit zukünftig noch sinnvoll sind.

Weiter muss die BA sicherstellen, dass Vordrucke und Ausfüllhinweise als „Paket“, also gleichzeitig an den Antragsteller ausgegeben werden. Nur so wird es ihm ermöglicht, zu prüfen, ob seine Angaben erforderlich sind. Hier höre ich nach wie vor aus der Praxis, dass dies nicht flächendeckend der Fall sei. Die BA ist in der Pflicht, dies entsprechend organisatorisch umzusetzen.

### 13.5.3 Fortschritte beim Erhebungs- und Leistungssystem A2LL in Sicht

*Die Implementierung eines Zugriffsberechtigungs- und Protokollierungskonzeptes für A2LL steht unmittelbar bevor.*

Über die Implementierung des Software-Programms A2LL, das die BA für die elektronische Datenerfassung aus den Antragsvordrucken für das Arbeitslosengeld II und die Leistungsberechnung verwendet, habe ich bereits berichtet (vgl. 20. TB Nr. 16.1.3). Bei einer Arbeitsagentur hatte ich mir Ende 2004, vor dem Inkrafttreten des SGB II am 11. Januar 2005, die Implementierung der Software angesehen. Wie ich hierbei feststellen musste, waren die bereits seit seinem Einsatz bestehenden Mängel nicht beseitigt worden, was ich beanstandet habe. Insbesondere konnte nach wie vor für die Sachbearbeitung uneingeschränkt bundesweit auf alle Daten zugegriffen werden, die im Rahmen von A2LL erfasst wurden, auch soweit diese für die Sachbearbeitung nicht erforderlich waren. Die Mitarbeiter der Leistungsträger dürfen jedoch nur für ihre Aufgabenerfüllung erforderliche Zugriffsrechte auf die Sozialdaten haben. Ebenso erfolgte noch immer keine Protokollierung der lesenden Zugriffe, so dass missbräuchliche Zugriffe nicht erkannt werden konnten. Den gesetzlichen Vorgaben für ein klar definiertes, abgestuftes Zugriffsberechtigungs- und Protokollierungskonzept entsprach das Verfahren nicht. Darauf habe ich die BA deutlich hingewiesen und Abhilfe angemahnt.

Das endlich im 3. Quartal 2006 von der BA vorgelegte Berechtigungskonzept beschreibt umfassend, welche Personenkreise mit welcher Rollenzuweisung auf welche Daten zugreifen dürfen. Damit ist meine Aufforderung an die BA insoweit grundsätzlich als erfüllt anzusehen. Jetzt kommt es vor allem darauf an, das Berechtigungskonzept zügig im System zu implementieren.

Als weiteres Kernstück der gesetzlich vorgeschriebenen organisatorisch-technischen Maßnahmen hat die BA im 4. Quartal 2006 das von mir geforderte Konzept zur Protokollierung von Suchanfragen im Verfahren A2LL vorgelegt. Darin wird, wie von mir gefordert, das Protokollierungsverfahren vollständig dargelegt. Insbesondere enthält es Aussagen zur Aufbewahrungsdauer der Protokolldaten, zum Auswerte- sowie zum Löschungsverfahren. Mit dem eingereichten Zugriffsberechtigungs- und Protokollierungskonzept verfügt das Programm A2LL nun über die Schutzmechanismen, die eine unkontrollierte bundesweite Personen- und Aktensuche im Datenpool von A2LL verhindern.

Die Umsetzung der Konzepte soll nach Auskunft der BA im 1. Quartal 2007 erfolgen. Die weitere Entwicklung werde ich im Auge behalten und nach Umsetzung der Konzeption vor Ort überprüfen.

### 13.5.4 Datenschutzrechtliche Aufsicht für die Arbeitsgemeinschaften (ARGEn)

*Die Kompetenz für die Datenschutzkontrolle der aus den Leistungsträgern Bundesagentur für Arbeit (BA) und kommunalen Trägern bestehenden ARGEn liegt bei den Landesbeauftragten für den Datenschutz. Im Streitfall muss der Gesetzgeber für eine entsprechende Klarstellung sorgen.*

Die mit dem Hartz-IV-Gesetz zum 1. Januar 2005 ins Leben gerufene Mischkonstruktion „ARGE“ ließ sich unabhängig von den sonstigen organisatorischen, finanziellen und verfahrensmäßigen Schwierigkeiten auch nicht ohne weiteres in das datenschutzrechtliche System integrieren. Denn für die Frage der Kontrollzuständigkeit ist maßgeblich, ob es sich um eine Stelle des Bundes oder der Länder handelt. Nach eingehender rechtlicher Prüfung und Diskussion herrschte schließlich Konsens, dass es sich bei den ARGEn um Stellen der Länder handelt (§ 81 Abs. 1 Nr. 2, Abs. 3 SGB X), weil sie entsprechend § 44b Abs. 3 Satz 4 SGB II der Aufsicht der zuständigen obersten Landesbehörden unterstehen und nicht über den Bereich eines Landes hinaus tätig werden. Sie unterliegen damit uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz. Lediglich soweit die BA zentrale EDV-Programme den ARGEn zur Verfügung gestellt oder generelle Vorgaben getroffen hat, ist meine Zuständigkeit begründet. Die konkrete Anwendung und Umsetzung im Einzelfall obliegen dagegen den ARGEn und dementsprechend der Aufsicht durch die Landesbeauftragten (vgl. hierzu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Kasten a zu Nr. 13.5.4).

Diese im Interesse einer effizienten Datenschutzkontrolle dringend erforderliche einheitliche Aufsichtszuständigkeit für die ARGEn wird im Lichte des Fortentwicklungsgesetzes (Bundestagsdrucksache 16/1410) von einigen Landesbeauftragten aufgrund der Neuregelung in § 50 Abs. 2 SGB II in Frage gestellt, wonach die BA verantwortliche Stelle nach § 67 Abs. 9 SGB X ist, soweit ARGEn die Aufgaben der Agenturen für Arbeit wahrnehmen. Die ARGE sei insoweit nicht mehr für die jeweiligen Verarbeitungsvorgänge verantwortlich. Vielmehr liege eine Verarbeitung durch die BA, mithin durch eine öffentliche Stelle des Bundes vor. Folglich sei nach § 81 Abs. 1 Nr. 1, Abs. 2 Satz 1 SGB X insoweit ausschließlich meine Zuständigkeit für die Datenschutzkontrolle gegeben.

Diese Auffassung teile ich nicht. Eine Datenschutzaufsicht je nach Aufgabenbereich des jeweiligen Leistungsträgers würde die in § 44b Abs. 1 Satz 1 SGB II normierte „einheitliche Wahrnehmung“ der Aufgaben durch die ARGEn außer Acht lassen, insbesondere, dass die ARGE als eigene Stelle handelt und nicht die einzelnen Leistungsträger. Diese bleiben zwar politisch und rechtlich in der sog. Gewährleistungsverantwortung. Soweit sie zur einheitlichen Aufgabenwahrnehmung eine ARGE errichtet haben, handelt diese aber in eigener Aufgabenwahrnehmungszuständigkeit. Dafür spricht auch die nach wie vor bestehende einheitliche Rechtsaufsicht der obersten Landesbehörden über die ARGEn.

Kasten a zu Nr. 13.5.4

**Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. bis 17. März 2006 in Magdeburg**

**Keine kontrollfreien Räume bei der Leistung von ALG II**

Die Datenschutzbeauftragten des Bundes und der Länder haben die Bundesagentur für Arbeit (BA) und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene in ihrer Entschließung vom 27./28. Oktober 2005 aufgefordert, die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Zu diesen Missständen gehört die wiederholte Weigerung der BA, Landesbeauftragten für den Datenschutz zu ermöglichen, ihre Kontrollaufgaben bei den Arbeitsgemeinschaften nach dem SGB II (ARGEn) zu erfüllen. Mit einer „Weisung" vom 31. Januar 2006 versucht die BA, nunmehr alle ARGEn auf diese Linie zu verpflichten. Den Landesdatenschutzbeauftragten soll der für Kontrollzwecke notwendige Zugriff auf die zentralen automatisierten Verfahren verwehrt werden.

Der Bundesbeauftragte für den Datenschutz und die Landesdatenschutzbeauftragten bekräftigen ihre gemeinsame Auffassung, dass es sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen der Länder handelt, die uneingeschränkt der Kontrolle der Landesbeauftragten für den Datenschutz unterliegen. Dass die BA Ressourcen für die Arbeitsgemeinschaften bereitstellt, ändert nichts an diesem Ergebnis.

Es muss gewährleistet sein, dass die Verarbeitung von Sozialdaten in den ARGEn von den jeweils zuständigen Landesbeauftragten umfassend und ohne inhaltliche Beschränkungen datenschutzrechtlich überprüft werden kann. Eine rechtliche Konstellation, durch die die Landesbeauftragten für den Datenschutz von der Kontrolle der ARGEn ausgeschlossen würden, würde gegen die bundesstaatliche Kompetenzordnung verstoßen und wäre einer effektiven Datenschutzkontrolle abträglich. Sie würde den Grundrechtsschutz der betroffenen Bürgerinnen und Bürger empfindlich beeinträchtigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung dazu auf, umgehend einen rechtskonformen Zustand herzustellen.

Dass die Neuregelung in § 50 Abs. 2 SGB II in diesem Kontext zu bewerten ist, wird auch in der Gesetzesbegründung (Bundestagsdrucksache, a. a. O., S. 75) verdeutlicht: „Soweit Arbeitsgemeinschaften gegründet worden sind, ist die Bundesagentur für Arbeit verantwortlich für die Gewährung und Auszahlung der Leistungen zur Sicherung des Lebensunterhalts sowie die Leistungen zur Eingliederung in Arbeit. Die Leistungsgewährung erfolgt mittels einheitlicher, von der Bundesagentur für Arbeit betriebenen und den Arbeitsgemeinschaften zur Verfügung gestellten EDV-Software-Systemen."

Hier bezieht sich der Gesetzgeber eindeutig auf die oben vorgenommene Differenzierung. Soweit die BA zur Erfüllung ihrer Gewährleistungsverantwortung z. B. eine einheitliche Software zur Verfügung stellt, ist sie verantwortliche Stelle. Die mittels dieser Software ausgeführte Aufgabenwahrnehmung vor Ort erfolgt dagegen von der ARGE in eigener Zuständigkeit. Insoweit ist diese verantwortliche Stelle (Aufgabenwahrnehmungsverantwortung). Entsprechendes gilt auch für zentral getroffene Vorgaben wie beispielsweise Antragsvordrucke.

So gehen auch das federführende BMAS ebenso wie die BA von der unveränderten Zuständigkeit der Landesbeauftragten aus. In diesem Sinn hat sich auch die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder durch Beschluss (Kasten b zu Nr. 13.5.4) dafür ausgesprochen, die bisherige Kontrollpraxis zunächst beizubehalten.

Kasten b zu Nr. 13.5.4

**Beschluss der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg**

**Datenschutzkontrollzuständigkeit für die SGB II-Arbeitsgemeinschaften**

Angesichts einer strittigen Rechtslage schließt sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Frage der Datenschutzkontrollzuständigkeit für die SGB II-Arbeitsgemeinschaften im Ergebnis nachfolgendem Vorschlag des BfDI in seinem Schreiben vom 5. September 2006 vorläufig an:

1. Die Kontrollkompetenz der LfD bezieht sich auf alle Leistungen nach dem SGB II.
2. Die ARGEn sind unmittelbar Adressaten von evtl. Beanstandungen der LfD. In Fällen grundsätzlicher Art sollte der BfDI über Beanstandungen informiert werden.
3. Auch wenn der BfDI Kontrollstelle für die zentralen IT-Verfahren der BA ist, sind die ARGEn verpflichtet, den LfD Einblick in oder Auskunft über die technischen Verfahren zu geben, die zu bestimmten Beschwerden Anlass geben. Entsprechendes gilt auch für die Hinweise zu Verfahren, Empfehlungen etc. der BA.

   Die LfD können diese Verfahren/Hinweise selbst nicht datenschutzrechtlich bewerten, aber sie müssen diese zur Kontrolle der datenschutzgemäßen Aufgabenerledigung der ARGEn direkt (vor Ort) zur Kenntnis nehmen können.
4. Die Bestellung von behördlichen Datenschutzbeauftragten in den ARGEn richtet sich nach Landesrecht.
5. Im Einzelfall können sich die LfD auch direkt an die BA wenden.

Der BfDI wird gebeten, auf die Durchsetzung einer entsprechenden Praxis seitens der BA hinzuwirken.

Weiter wird der BfDI gebeten, auf eine zeitnahe gesetzgeberische Klarstellung hinzuwirken.

Allerdings ist den Landesbeauftragten für den Datenschutz insoweit zu Recht wichtig, dass die konkrete Kontrolltätigkeit vor Ort auch tatsächlich ermöglicht wird. In der Vergangenheit hat es nicht akzeptable Behinderungen (z. B. wurde die Einsichtnahme in die von der BA zur Verfügung gestellten EDV-Programme verweigert) gegeben. Die BA hat auf mein Drängen hin die ARGEn noch einmal deutlich auf die Rechtslage und den o. g. Beschluss hingewiesen, der vollinhaltlich vom BMAS geteilt wird. Ich gehe daher davon aus, dass eine wirksame Kontrolle der ARGEn durch die Landesbeauftragten für den Datenschutz gewährleistet ist, wenn auch die Abstimmung hierüber mit einem Landesbeauftragten noch nicht abgeschlossen ist. Sollte es allerdings in der Praxis wider Erwarten rechtliche oder tatsächliche Hindernisse geben, wäre zur Vermeidung kontrollfreier Räume eine gesetzliche Klarstellung notwendig.

### 13.5.5 Einzelfälle

**DALEB-Abgleich nach dem SGB III endlich gesetzlich geregelt**

Mit dem sog. DALEB-Verfahren gleicht die Bundesagentur für Arbeit die ihr von der Datenstelle der Träger der Rentenversicherung übermittelten Beschäftigtendaten (§ 28a SGB IV, § 36 Abs. 3 Datenerfassungs- und Übermittlungsverordnung) automatisiert mit den eigenen Leistungsdaten ab, um die missbräuchliche Inanspruchnahme von Leistungen der Arbeitsförderung zu verhindern. Für diesen präventiven Datenabgleich zum Zwecke der Verdachtsschöpfung fehlte es bislang an einer spezifischen Regelung, die normenklar Inhalt und Umfang der eingeräumten Ermächtigung festlegt. Diese hat das „Gesetz zur Fortentwicklung der Grundsicherung für Arbeitsuchende“ vom 20. Juli 2006 (BGBl. I S. 1706) nun unter meiner Mitwirkung geschaffen. Der neue § 397 SGB III (Artikel 3 Nr. 7 des Fortentwicklungsgesetzes) regelt substantiiert, welche Angaben von welchem Personenkreis zu welchem Zweck mit welchen Daten abgeglichen werden dürfen. Für die Leistungsbezieher entsteht so die notwendige Transparenz über diese Zweckänderung. Nach Absatz 2 dürfen die Daten nur insoweit weiter verwendet werden, als der Verdacht begründet ist, Leistungen seien zu Unrecht beantragt oder bezogen worden. Diese Verdachtsfälle werden den Agenturen für Arbeit zur Überprüfung übermittelt. Die übrigen Daten sind unverzüglich zu löschen.

**BA-interner Datenschutz neu geregelt – auch gestärkt**

Die Reorganisation des Datenschutzes in der BA hatte ich bereits mehrfach, zuletzt im 20. TB (Nr. 16.4), angemahnt. Kernpunkte meiner Kritik waren die an zwei verschiedenen Stellen organisierten Aufgaben des behördlichen Datenschutzbeauftragten – Stabsstelle BfD/BA und Fachreferat IT 3 – und die ungenügende personelle Ausstattung des Bereichs.

Durch Beschluss des Vorstands der BA vom 21. März 2006 wurde der Justitiar der BA in Personalunion zum behördlichen Datenschutz- und Informationsfreiheitsbeauftragten bestellt. Gleichzeitig gingen die dem Fachreferat bisher zugeordneten datenschutzrechtlichen Aufgaben zusammen mit dem entsprechenden Stellen- und Personalansatz auf die Stabsstelle (Datenschutz/Justitiariat) über. Die neu gebildete Organisationseinheit besteht derzeit aus 16 Mitarbeitern und ist dem Vorstand Finanzen zugeordnet.

Meine Erfahrungen mit dieser neuen Organisationsstruktur sind bisher positiv. Die erhofften Synergieeffekte zeichnen sich ab. Gleichwohl wird abzuwarten sein, ob die insgesamt doch sehr anspruchsvollen Zugleichfunktionen des Datenschutzbeauftragten tatsächlich zu leisten sind. Die ordnungsgemäße Erfüllung der gesetzlichen Verpflichtungen nach dem BDSG muss gewährleistet sein. Angesichts der Vielzahl und der Bedeutung der vom BfD/BA in den Rechtskreisen SGB II und III wahrzunehmenden Aufgaben, der über 200 eingesetzten Datenverarbeitungsverfahren und der Zahl der Beschäftigten liegen Zweifel insoweit nicht ganz fern. Grundsätzlich halte ich aber das Konzept für tragfähig und sehe hierin eine erfreuliche Stärkung des Datenschutzes in der BA.

**Mangelnde Diskretion in den Agenturen für Arbeit – nach wie vor ein Thema**

Petenten haben sich darüber beschwert, dass der Vertraulichkeitsschutz in den Kundenservicebereichen der Agenturen für Arbeit im neuen Konzept Kundenzentrum der Zukunft (KuZ) nicht gewährleistet sei. Wesentliches Merkmal der entsprechend dem Konzept gestalteten Arbeitsagenturen ist ein offener Eingangsbereich, um mehr Transparenz in die Abläufe zu bringen. Die Arbeitsbereiche sind als offen gestaltete Großraumbüros mit direkt zugänglichen Arbeitsplätzen eingerichtet. Wie in der Vergangenheit bereits mehrfach betont (vgl. 18. TB Nr. 20.3 und 20. TB Nr. 16.5), sind zur Wahrung der Diskretion geeignete schallhemmende und Sichtschutzmaßnahmen sowie ein entsprechender Abstand zwischen den Arbeitsplätzen erforderlich, um ein „Mithören“ nahezu auszuschließen; weiter müssen die Betroffenen die Möglichkeit haben, das Beratungsgespräch in einem separaten Büro zu führen. Auf diese Alternative ist durch ein ausreichend großes und an auffälliger Stelle angebrachtes Schild hinzuweisen. Ich habe die BA aufgefordert, die Defizite durch geeignete Maßnahmen zu beheben. Die BA hat zugesagt, diesen Forderungen zu entsprechen. Ich werde mich von der Umsetzung dieser Zusage überzeugen.

**Unzulässige Datensammlung über die Nutzer der BA-Internetplattform**

Ein Petent wollte im Internet-Center des Berufsinformationszentrums der BA (BIZ) Recherchen nach Stellenangeboten durchführen. Ihm wurde mitgeteilt, dass für die erweiterte Nutzung bzw. Stellensuche über das freigegebene Internetangebot der BA hinaus eine Zugangsberechtigung in Form eines Benutzernamens und eines Kennwortes vom BIZ erforderlich sei. Nach Erfassung der persönlichen Daten und Vorlage des Personalausweises erhielt er die entsprechende Zugangsberechtigung. Ihm wurde weiter mitgeteilt, dass der Verlauf der

Nutzung für den Zeitraum von 180 Tagen gespeichert werde und Stichprobenkontrollen durchgeführt würden, ob rechtlich unzulässige Nutzungen erfolgt seien. Der Petent sah in der Speicherung der Internetnutzung in Verbindung mit der Aufnahme seiner persönlichen Daten einen datenschutzrechtlich unzulässigen Eingriff in seine Persönlichkeitsrechte und das Recht auf informationelle Selbstbestimmung.

Die BA wies darauf hin, dass ihr freigegebenes Internetangebot auch ohne personenbezogene Registrierung genutzt werden könne, lediglich für die darüber hinausgehende Nutzung müssten sich die Nutzer persönlich anmelden. Hierbei beruft sich die BA auf wiederholte Verstöße gegen die Nutzerordnung. Diese seien teilweise so schwerwiegend gewesen, dass die Einleitung polizeilicher Ermittlungen wegen Verdachts einer strafbaren Handlung notwendig gewesen sei.

Eine Befugnis zur vorsorglichen Speicherung sämtlicher Verkehrs- und Nutzungsdaten für Zwecke der Strafverfolgung besteht nicht. Die BA ist als Anbieterin gemäß § 9 Teledienstegesetz (TDG) für fremde Informationen nicht verantwortlich, die über ihr System übermittelt werden oder zu denen sie den Zugang vermittelt. Der BA steht es zwar frei, die Bedingungen für die Nutzung ihrer Internet-Center festzulegen und Identifizierungs- und Nutzungsdaten für einen begrenzten Zeitraum zu speichern. Der Umfang der von der BA erhobenen Daten ging darüber jedoch weit hinaus. Deshalb habe ich die BA auf die Einhaltung der datenschutzrechtlichen Vorschriften hingewiesen. So muss z. B. eine schriftliche Unterrichtung des Nutzers über Umfang, Dauer und Zweck der Erhebung, Verarbeitung und Nutzung seiner Daten erfolgen. Die Einwilligung in die Speicherung ist schriftlich einzuholen. Zudem habe ich eine Neufassung der Nutzerordnung angeregt, um derartige Vorkommnisse für die Zukunft zu verhindern. Da die BA meiner Forderung entsprechend die Nutzerdaten nur noch mit schriftlicher Einwilligung nach vorheriger Unterrichtung erheben und speichern will, habe ich von einer förmlichen Beanstandung abgesehen.

**Personalausweiskopien bei den Agenturen für Arbeit**

Ein Petent beschwerte sich darüber, dass sowohl von ihm als auch von anderen Antragstellern auf Arbeitslosengeld I Kopien der Personalausweise gefertigt und zur Akte genommen wurden. Zur Feststellung der Anspruchsvoraussetzungen ist es zwar erforderlich, die Identität des Antragstellers zu überprüfen. Zur Kontrolle der Personalien können Mitarbeiter der Arbeitsagenturen deshalb verlangen, dass Kunden einen gültigen Pass oder Personalausweis vorlegen (vgl. § 1 Abs. 1 Satz 1 Personalausweisgesetz – PersAuswG), um Verwechslungen auszuschließen. Allerdings ist eine Kopie des Dokuments – auch wegen der zusätzlichen Daten im Ausweis – nicht erforderlich, vielmehr genügt ein kurzer Vermerk, dass der gültige Pass bzw. Personalausweis vorgelegen hat. Von einer förmlichen Beanstandung habe ich abgesehen, weil die Bundesagentur für Arbeit meiner Rechtsauffassung gefolgt ist und die Agenturen nachdrücklich auf die Einhaltung der Datenschutzbestimmungen hingewiesen hat.

**Datenweitergabe nach sog. Kompetenzchecks zur Berufswahl Jugendlicher**

Ein Petent, der einen Ausbildungsplatz suchte, erhielt von der Agentur für Arbeit eine Einladung zu einem sog. Kompetenzcheck. Im Rahmen des Ausbildungskonsenses NRW II hatten die Agenturen für Arbeit in Nordrhein-Westfalen im Herbst 2005 allen Jugendlichen, die noch keinen Ausbildungsplatz gefunden hatten, die Durchführung eines kostenlosen und freiwilligen Kompetenzchecks angeboten. Hierbei sollten individuelle Fähigkeiten und Interessen festgestellt und gemeinsam mit dem Interessenten berufliche Perspektiven entwickelt werden. Die praktische Durchführung des Kompetenzchecks wurde privaten Trägern übertragen, die danach eine schriftliche Potentialbilanz anfertigten, die z. B. Kompetenzen und Stärken berücksichtigen sollte. Diese Potentialbilanz wurde nicht nur dem Jugendlichen sondern auch – zum Zwecke der Vermittlung einer Ausbildungsstelle – der Berufsberatung der örtlichen Agentur für Arbeit und der regionalen Koordinierungsstelle bei der jeweils zuständigen Industrie- und Handelskammer (IHK) zugeleitet.

Für diese Übermittlung der Potentialbilanz war eine vorherige schriftliche Einwilligungserklärung des Jugendlichen bzw. seines gesetzlichen Vertreters erforderlich. Ohne diese konnte eine Teilnahme am Kompetenzcheck nicht erfolgen. Hiergegen hat sich der Petent gewandt, da er keine Kenntnis darüber hätte, was mit seinen Daten bei der IHK geschähe. Insbesondere befürchtete er, dass mit der Potentialbilanz eine Art „Intelligenztest“ bei der IHK zu für ihn nicht bekannten Zwecken gespeichert werde.

Nach meiner datenschutzrechtlichen Überprüfung kann eine Einwilligungserklärung im Vorfeld des Kompetenzchecks nicht erfolgen, weil sich, wie die Bundesagentur für Arbeit (BA) dazu schreibt, die jugendlichen Ratsuchenden zu diesem Zeitpunkt noch nicht über die mögliche Tragweite einer solchen Erklärung bewusst sind. Die BA hat das Verfahren daraufhin abgeändert und die Zugriffsrechte sowohl der regionalen Agenturen als auch der IHK gesperrt. Nur wenn die Personensorgeberechtigten der Jugendlichen in Kenntnis der Ergebnisse, also nach Durchführung des Kompetenzchecks, der Datenweitergabe zustimmen, dürfen die Daten weitergegeben werden. Da die BA meine Rechtsauffassung teilt und der Mangel bei der Einverständniserklärung beseitigt worden ist, habe ich von einer förmlichen Beanstandung abgesehen.

**Unzulässige Weitergabe von Kundendaten der BA an private Krankenversicherungsunternehmen**

Einem Petenten, der Arbeitslosengeld I erhielt, bewilligte die zuständige Agentur für Arbeit die Übernahme der Beiträge nach § 207a Abs. 3 SGB III zur Weiterführung seiner privaten Krankenversicherung. Die Beiträge wur-

den auf seinen Wunsch hin direkt an ihn und nicht an die private Krankenversicherung ausgezahlt.

Trotz der Direktauszahlung übersandte die Agentur für Arbeit eine Kopie des Leistungsbescheids an die private Krankenversicherung. Der Bescheid enthielt die Kundendaten des Petenten bei der Agentur für Arbeit sowie Angaben über die Höhe der übernommenen Beiträge sowie die voraussichtliche Dauer der Beitragsübernahme. Die Arbeitsagentur begründete die Übermittlung u. a. damit, sie sei dazu durch die gesetzliche Regelung in § 207a SGB III verpflichtet.

Ich halte die Übermittlung des Bescheids an die private Krankenversicherung für unzulässig, da der Petent selbst die Beiträge zahlte. Die BA erklärte dazu, dass im Leistungsbearbeitungsprogramm „Colibri“ automatisch ein Schreiben an den Versicherungsträger erzeugt werde. Der Bearbeiter habe jedoch die Möglichkeit, die Versendung der Kopie manuell zu unterdrücken, wenn die Zahlung nicht an die private Krankenversicherung, sondern an den Kunden erfolge. Im vorliegenden Fall sei die Unterdrückung versehentlich unterlassen worden. Um versehentliche Meldungen an private Krankenversicherungen in Zukunft zu vermeiden, beabsichtigt die BA auf meine Anregung hin, eine entsprechende Änderung in der nächsten Programmversion voraussichtlich April 2007 vorzunehmen. Die Erstellung einer Kopie soll dann nicht mehr automatisch erfolgen, sondern vom Bearbeiter manuell angestoßen werden. Von einer förmlichen Beanstandung habe ich deshalb abgesehen. Die Umsetzung der Programmumstellung werde ich begleiten.

## 14 Mitarbeiterdatenschutz

### 14.1 Zugang von Vorgesetzten zu Personal- und Personalaktendaten

*Die Frage, ob und ggf. in welchem Umfang (Fach-)Vorgesetzten bzw. Fachabteilungen Mitarbeiterdaten zur Verfügung gestellt und dort genutzt werden dürfen, ist immer wieder Gegenstand von Anfragen und Beratungsersuchen.*

Im Berichtszeitraum hatte ich mich verstärkt mit der Frage, welche personenbezogenen Mitarbeiterdaten den (Fach-)Vorgesetzten zur Verfügung gestellt werden dürfen, auseinanderzusetzen. Gegenstand verschiedener Beratungsersuchen war dabei insbesondere, ob und ggf. in welchem Umfang den Fachvorgesetzten auch Personalaktendaten überlassen werden dürfen. Die wiederkehrenden Anfragen, meine früheren Feststellungen (vgl. z. B. 20. TB Nrn. 10.4.3, 10.4.4) und die neue Entwicklung in den Personalverwaltungen geben Veranlassung, die Thematik unter verschiedenen Gesichtspunkten nochmals zusammenfassend darzustellen.

Die Führung von Unterlagen zu einzelnen Mitarbeitern – unabhängig, ob in automatisierter oder in manueller Form – ist grundsätzlich Aufgabe der Personalabteilung. So bestimmt § 90 Abs. 3 BBG, dass Zugang zur Personalakte nur Beschäftigte haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind und dies zu Zwecken der Personalverwaltung oder Personalwirtschaft erforderlich ist. Demnach dürfen Fachvorgesetzte im Grundsatz keinen Zugang zu Personalaktendaten ihrer Mitarbeiterinnen und Mitarbeiter haben; ebenso dürfen in den Fachabteilungen keine Personalteil- oder Personalnebenakten geführt werden.

**Arbeitsorganisation und personelle Führung**

In den verschiedensten Fällen sind Vorgesetzte im Rahmen der täglichen Arbeitserledigung allerdings darauf angewiesen, personenbezogene Daten ihrer Mitarbeiterinnen und Mitarbeiter zu verwenden. Aus datenschutzrechtlicher Sicht bestehen keine Bedenken dagegen, wenn Fachvorgesetzte personenbezogene Angaben zu ihren Mitarbeitern nutzen, soweit dies für die organisatorische und personelle Führung der jeweiligen Organisationseinheit erforderlich ist. Im Hinblick auf die Steuerung der Aufgabenerledigung kann sich der Leiter einer Organisationseinheit beispielsweise erteilte Arbeitsaufträge und terminliche Vorgaben notieren (vgl. 17. TB Nr. 18.3.5).

**Abwesenheitszeiten**

Zu den organisatorischen Aufgaben eines Vorgesetzten gehört auch die Führung eines Abwesenheits- und Urlaubsplanes. Es bestehen keine datenschutzrechtlichen Bedenken dagegen, wenn sich Fachvorgesetzte Angaben über geplante Abwesenheitszeiten für einen gewissen Zeitraum – z. B. Urlaubsjahr – notieren, um so die Funktionsfähigkeit ihrer Organisationseinheit im Hinblick auf Abwesenheitszeiten von Beschäftigten steuern und sicherstellen zu können. Soweit dies in automatisierter Form geschieht, sind unter anderem die Beteiligung des behördlichen Datenschutzbeauftragten und die Mitbestimmungsrechte der Personalvertretung zu beachten.

Wichtig ist, dass die zur Arbeitsorganisation und zur personellen Führung genutzten Mitarbeiterdaten bei den Vorgesetzen wieder gelöscht werden, wenn sie für deren konkrete Aufgaben nicht mehr benötigt werden.

**Beurteilungsdaten**

Außer Frage steht, dass Vorgesetzte bzw. Beurteiler im Entwurfsstadium von Beurteilungen Mitarbeiterdaten nutzen und entsprechende Entwürfe – allerdings ohne auf frühere Beurteilungen zurückzugreifen – erstellen dürfen. Ebenso ist es zulässig, im Hinblick auf die künftige Beurteilung von Beschäftigten hierfür erforderliche Angaben – zur Gedächtnisstütze – zu notieren (siehe 17. TB Nr. 18.3.5).

Nach Abschluss des Beurteilungsverfahrens sind die den Beschäftigten eröffneten Beurteilungen in die Personalakte aufzunehmen; sie unterliegen dem Personalaktengeheimnis und dürfen – auch in Ablichtungen – bei Fachvorgesetzten nicht weiter aufbewahrt werden. Dies gilt insbesondere auch für etwaige Entwurfsfassungen, die vielfach in elektronischer Form gespeichert sind. Dementsprechend sind Entwürfe und vorbereitende Notizen zu löschen.

Leider ist anlässlich von Kontrollen immer wieder festzustellen, dass hiergegen verstoßen wird und eröffnete Beurteilungen zum Teil über Jahre sowohl in Papier- als auch in elektronischer Form bei Vorgesetzten/Beurteilern vorgehalten werden (vgl. 18. TB Nr. 18.3.2, 19. TB Nr. 21.3.4, 20. TB Nrn. 10.4.3 und 10.4.4).

**Arbeits- und Gleitzeitkonten**

Ein beständiges Thema ist auch, inwieweit Vorgesetzten Arbeits- bzw. Gleitzeitdaten ihrer Mitarbeiterinnen und Mitarbeiter zur Verfügung zu stellen sind. Hierzu hatte ich im 20. Tätigkeitsbericht (Nr. 10.3.5) ausgeführt, dass der Entwurf einer Arbeitszeitverordnung für die Beamtinnen und Beamten des Bundes (AZV) vorsah, Vorgesetzten einen (vollständigen) Einblick in die Gleitzeitkonten der ihnen zugewiesenen Mitarbeiterinnen und Mitarbeiter zu gewähren. Bereits damals hatte ich die Auffassung vertreten, dass ein eigener und vollständiger – ggf. elektronischer – Zugriff von Fachvorgesetzten auf Arbeits- oder Gleitzeitkonten nicht erforderlich sei. Auf Grund auch meiner Hinweise wurde von der Aufnahme eines solchen unbeschränkten Einsichtnahmerechts der Vorgesetzten zunächst abgesehen. Auch im Rahmen einer erneuten Novellierung der AZV im Berichtszeitraum wurde ein generelles Einblicksrecht von Fachvorgesetzten nicht eingeführt. Den unmittelbaren Vorgesetzten sind aber für Zwecke des gezielten Personaleinsatzes die Gleitzeitsalden ihrer Mitarbeiterinnen und Mitarbeiter mitzuteilen, sofern sich positive Salden von mehr als 20 Stunden oder negative Salden von mehr als 10 Stunden ergeben. Diese Informationen sollen den Vorgesetzten die Planung und einen sinnvollen Einsatz der Mitarbeiterinnen und Mitarbeiter in Belastungsspitzen und das Hinwirken auf den erforderlichen Saldenausgleich in Zeiten geringerer Belastung der Arbeitseinheit ermöglichen. Die Daten dürfen nach der Vorgabe der AZV jedoch auf keinen Fall für eine Kontrolle oder Bewertung der Leistung oder des Verhaltens der Beschäftigten verwendet werden. Ich werde im Rahmen künftiger Beratungs- und Kontrollbesuche ein besonderes Augenmerk auf eine der Zweckbindung entsprechende Verwendung der Arbeitszeitdaten legen.

**Neue Organisationsformen in der Personalverwaltung**

Neue Organisationsformen in der Bundesverwaltung mit einer Übertragung bestimmter Aufgaben der Personalverwaltung/Personalplanung von der Personalabteilung auf Fachvorgesetzte lassen unter bestimmten Voraussetzungen auch eine Nutzung von Personalaktendaten durch Fachabteilungen bzw. durch Fachvorgesetzte zu. Dies kann dann als datenschutzgerecht angesehen werden, wenn die wesentlichen Vorgaben der §§ 90 ff. BBG weiterhin erfüllt sind; dies bedeutet insbesondere,

– dass die in einer Fachabteilung wahrzunehmenden Personalverwaltungsaufgaben konkret definiert, festgelegt und die Zuständigkeit hierfür schriftlich übertragen werden müssen,
– die Zweckbindung der Personalaktendaten für eine bestimmte Nutzung festgelegt und (organisatorisch) umgesetzt ist,
– der Zugang und Zugriff zu den Personalaktendaten weiterhin auf möglichst wenige Beschäftigte begrenzt wird und
– sichergestellt ist, dass keine doppelte oder parallele Personalaktenführung in den Fachabteilungen stattfindet.

Die vorstehend aufgeführten Grundsätze habe ich im Berichtszeitraum im Rahmen der Beratung mehrer Bundesbehörden und Institutionen, u. a. der Deutschen Bundesbank und der Deutschen Rentenversicherung Bund, vertreten. Die hierbei gewonnenen Erfahrungen zeigen, dass es in allen Fällen möglich war, datenschutzgerechte und den Bedürfnissen einer modernen Personalverwaltung entsprechende Lösungen zu finden.

Meine datenschutzrechtliche Empfehlung zur Umsetzung der oben genannten Grundsätze wurde auch bei der Konzeption eines sog. Rotationsverfahrens für Referentinnen und Referenten im Bundesministerium für Verkehr, Bau und Stadtentwicklung, unter Nutzung von Personalaktendaten durch die Fachabteilungen bzw. die Fachvorgesetzten berücksichtigt.

## 14.2 Neuordnung des Beamtenrechts in Bund und Ländern

*Die mit der Föderalismusreform einhergehende Neuordnung des Beamtenrechts berührt auch Fragen des Datenschutzes.*

In den Berichtszeitraum fiel der Entwurf eines Gesetzes zur Reform der Strukturen des öffentlichen Dienstrechts (Strukturreformgesetz, Bundesratsdrucksache 615/05 v. 12. August 2005). Die im Gesetzentwurf enthaltenen Neuregelungen bleiben weiterhin aktuell, da die Reform nunmehr unter den durch die Föderalismusreform veränderten Bedingungen fortgesetzt werden soll.

Bedeutsam war insbesondere, dass die Möglichkeit eingeführt werden sollte, Personalakten in Teilen oder vollständig automatisiert zu führen (sog. elektronische Personalakte). Aus datenschutzrechtlicher Sicht bestehen gegen die Einführung einer elektronischen Personalakte keine grundsätzlichen Bedenken. Im Rahmen meiner Beteiligung hatte ich jedoch empfohlen, entsprechend der bisherigen Rechtslage sicherzustellen, dass über jede Beamtin bzw. jeden Beamten nur eine Personalakte geführt wird. Eine doppelte oder parallele Aktenführung sollte – abgesehen von bestimmten zulässigen Fällen der Führung von Nebenakten – weiterhin ausgeschlossen bleiben. Insbesondere darf die mit dem Gesetzentwurf vorgesehene Einführung einer teilweisen elektronischen Personalaktenführung (sog. Hybrid-Akte) im Ergebnis nicht dazu führen, dass die für die Beamtinnen und Beamten zu führenden Personalakten teilweise sowohl in Papierform als auch in elektronischer Form vorgehalten werden. Bei einer solchen „parallelen Aktenführung“ würde sich zudem die Frage stellen, welche der Akten – elektronische

oder Papierform – maßgebend ist. Ebenso bestünde die Gefahr, dass die Inhalte der parallel geführten Akten in der Praxis unter Umständen voneinander abweichen könnten, was zu Zweifeln an der Eindeutigkeit der Personalakte führen würde. Den vorgenannten Gesichtspunkten wurde im Rahmen des Strukturreformgesetzentwurfs durch die Aufnahme einer Regelung Rechnung getragen, wonach die personalverwaltende Stelle jeweils schriftlich festlegt, welche Teile in welcher Form geführt werden. Eine solche eindeutige Festlegung durch die aktenführende Stelle erschien zudem für eine effektive Gewährleistung der Rechte der Beamtinnen und Beamten – insbesondere zur Gewährleistung eines vollständigen Einsichtsrechts – notwendig. Um bei Einführung einer elektronischen Personalakte die Beweiskraft sicherzustellen, bedarf es zudem einer Regelung zur Verwendung der qualifizierten Signatur (vgl. Nr. 4.4). Entsprechend heißt es in der Begründung zum Strukturreformgesetzentwurf, dass die Personalakte vollständig in elektronischer Form geführt werden kann, sobald die erforderlichen technischen Voraussetzungen vorliegen, insbesondere die Beweiskraft elektronisch gespeicherter Urkunden durch eine qualifizierte elektronische Signatur gewährleistet wird.

Wenn auch der Strukturreformgesetzentwurf nach den Neuwahlen des Deutschen Bundestages nicht mehr weiter verfolgt wurde, erwarte ich, dass die in diesem Rahmen mit mir abgestimmten Punkte im Hinblick auf die Einführung einer elektronischen Personalakte auch im Rahmen einer künftigen Neufassung des Bundesbeamtengesetzes Berücksichtigung finden werden. Gleiches gilt für die weiteren mit mir abgestimmten Änderungen und Ergänzungen der Vorschriften des Personalaktenrechts für die Bundesbeamtinnen und Bundesbeamten.

In den Berichtszeitraum fiel ferner der Entwurf eines Gesetzes zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern (Beamtenstatusgesetz, Bundesratsdrucksache 780/06 v. 3. November 2006). Mit der Föderalismusreform werden wichtige Gesetzgebungskompetenzen für das Beamtenrecht auf die Länder übertragen. Lediglich eine eng begrenzte Kompetenz des Bundes für die Statusrechte und -pflichten von Landesbeamtinnen und -beamten bleibt weiterhin bestehen. Zum Personalaktenrecht enthielt der Ausgangsentwurf des Gesetzes ursprünglich nur die Festlegung, dass für jede Beamtin und jeden Beamten eine Personalakte zu führen ist, und dass zur Personalakte alle Unterlagen gehören sollen, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Damit fehlten zunächst Regelungen zu den grundlegenden datenschutzrechtlichen Rechten der Beamtinnen und Beamten in den Ländern. Im Rahmen meiner Beteiligung konnte ich noch die Aufnahme der das Personalaktenrecht prägenden Grundsätze der Vertraulichkeit (Personalaktengeheimnis) und der Zweckbindung von Personalaktendaten in den Gesetzentwurf erreichen. Ferner wird in der Begründung nunmehr auf mein Betreiben hin aufgeführt, dass den Beamtinnen und Beamten ein Recht auf Einsicht in ihre Personalakte zusteht und dass unrichtige Inhalte aus der Personalakte zu entfernen sind. Aus datenschutzrechtlicher Sicht grundlegend ist ferner, Beihilfeakten von der übrigen Personalakte getrennt zu führen und aufzubewahren. Das besondere Schutzbedürfnis der Beamtinnen und Beamten in Bezug auf Beihilfevorgänge ergibt sich hier daraus, dass sie im Beihilfeantrag und den beizufügenden Belegen notwendigerweise Angaben über ihren Gesundheitszustand und den ihrer Familienangehörigen sowie die entsprechenden Heilbehandlungen offenbaren müssen. Diese Angaben sind in besonders hohem Maße dem persönlichen Bereich zuzurechnen, was einen besonderen einheitlichen Vertraulichkeitsschutz – insbesondere auch gegenüber der übrigen Personalverwaltung – bei jedem Dienstherren gleichermaßen notwendig macht.

Der weitere Fortgang dieses Gesetzgebungsverfahrens, das im Berichtszeitraum noch nicht abgeschlossen war, bleibt abzuwarten.

## 14.3 Automatisierte Personaldatenverarbeitung

*Im Zusammenhang mit dem verstärkten Einsatz automatisierter Verfahren der Personaldatenverarbeitung in der Bundesverwaltung werden mir immer wieder datenschutzrechtliche Fragen von grundsätzlicher Bedeutung gestellt.*

Der Einsatz automatisierter Verfahren in der Personalwirtschaft nimmt auch in der Bundesverwaltung weiter zu. Neben Großverfahren (Personalinformations- und Personalverwaltungssystemen) kommen computergestützte Verfahren auch in vielen anderen Bereichen des Personalwesens zum Einsatz. Dies bleibt nicht ohne Folgen für den Datenschutz. Deshalb hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Handlungsempfehlung zum Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung erarbeitet, die von meiner Website abgerufen werden kann (http://www.bfdi.bund.de). Kern dieser Handlungsempfehlung sind die im Kasten zu Nr. 14.3 wiedergegebenen „Allgemeinen datenschutzrechtlichen Leitplanken“. Im Folgenden sollen einige der an mich herangetragenen Fragen näher erörtert werden:

### Gleichstellungsbeauftragte und Personalvertretung: Zugriffsrechte auf ein Personalinformationssystem

Bei der Einführung von Personalinformations-/Personalverwaltungssystemen taucht wiederholt die Frage auf, ob bzw. ggf. in welchem Umfang der Gleichstellungsbeauftragten und dem Personalrat Zugriffsrechte im Rahmen der elektronischen Personaldatenverarbeitung eingeräumt werden können. Rechtsgrundlage für den Zugang der Gleichstellungsbeauftragten zur Personalakte und damit auch auf die automatisiert gespeicherten Personalaktendaten ist § 90 Abs. 3 Satz 2 BBG. Danach haben Gleichstellungsbeauftragte Zugang zu entscheidungsrelevanten Teilen der Personalakte, soweit dies zur Wahrnehmung ihrer Aufgaben erforderlich ist. Auch § 20 Abs. 1 Bundesgleichstellungsgesetz (BGleiG) räumt Gleichstellungsbeauftragten insofern ein Einsichtsrecht in die entscheidungsrelevanten Teile von Personalakten ein. Welche Personalaktendaten dies konkret sind, muss – ggf.

im Einzelfall – nachvollziehbar dargelegt werden. Losgelöst vom jeweiligen Einzelvorgang kann es zur Aufgabenerfüllung der Gleichstellungsbeauftragten unter Umständen auch erforderlich sein, ihr einen eingeschränkten Lesezugriff auf den Stammdatensatz in einem Personalverwaltungs-/Personalinformationssystem einzuräumen. Dies setzt jedoch eine konkrete Festlegung der einzelnen Datenfelder voraus und sollte auch in einer Dienstvereinbarung dokumentiert werden.

Hinsichtlich der Zugriffsrechte der Personalvertretung stellt sich die Rechtslage anders dar, da es für diese kein eigenes Recht auf Zugang zur Personalakte bzw. Personalaktendaten nach dem BBG gibt. Vielmehr dürfen nach § 68 Abs. 2 Satz 3 und 4 Bundespersonalvertretungsgesetz (BPersVG) Personalakten nur mit Zustimmung des Beschäftigten und nur von den von ihm bestimmten Mitgliedern der Personalvertretung eingesehen werden. Meine Auffassung zur Thematik „Zugriffsrechte der Mitarbeitervertretung auf Personaldaten“ habe ich in meinem 15. Tätigkeitsbericht (Nr. 9.6.1) dargestellt. Im Tenor können dem Personalrat danach ebenfalls bestimmte Grunddaten, die er auf Dauer zur sachgemäßen Aufgabenerfüllung, insbesondere zur Wahrnehmung seiner Beteiligungsrechte nach dem BPersVG benötigt, zur Verfügung gestellt werden. Dies kann, unabhängig von Beteiligungsverfahren, auch durch Einräumung eines lesenden Zugriffs auf ein Personalinformations-/Personalverwaltungssystem geschehen.

**Personalmanagementsystem EPOS 2.0: IT-Hosting**

In meinem 20. Tätigkeitsbericht (Nr. 10.3.2) hatte ich über die Entwicklung und Einführung des neuen elektronischen Personal-, Organisations- und Stellenmanagementsystems EPOS 2.0 im BMI bzw. im Bundesverwaltungsamt (BVA) berichtet. Im Zusammenhang mit der Einführung von EPOS 2.0 im BMU und dessen Geschäftsbereich wurde erstmals auch die Thematik eines IT-Hostings an mich herangetragen. Hierbei soll das BVA für das BMU IT-Dienstleistungen bei Bereitstellung und Betrieb von EPOS 2.0 übernehmen. Bei dieser Übertragung von Service-Aufgaben für den technischen Betrieb sowie der technischen und fachlichen Administration dieses Systems handelt es sich um eine Datenverarbeitung im Auftrag (§ 11 BDSG). Ich habe zum Ausdruck gebracht, dass hierbei sowohl die in § 11 BDSG genannten Voraussetzungen gewährleistet als auch die Zugangsbeschränkungen des § 90 Abs. 3 BBG hinsichtlich der in EPOS 2.0 gespeicherten Personalaktendaten eingehalten werden müssen. Zur Zulässigkeit eines solchen IT-Hostings im Personalbereich hat das BVA auf meine Anregung hin eine grundsätzliche Stellungnahme des BMI aus personalaktenrechtlicher Sicht eingeholt. Darin führt das BMI aus, dass die Personalakten physisch auch an einer anderen Stelle aufbewahrt werden können. Entscheidend sei, dass kein gezielter Einblick im Sinne eines inhaltlichen Zur-Kenntnis-Nehmens in Personalaktendaten erfolge. Solange lediglich eine – aus technischen Gründen nicht auszuschließende – kurzfristige optische Wahrnehmungsmöglichkeit im Zuge der Sicherung der Betriebsfähigkeit von EPOS 2.0 erfolge, liege nach dem Schutzzweck des § 90 Abs. 3 BBG noch kein „Zugang“ im personalaktenrechtlichen Sinne vor.

In die daraufhin zwischen BMU und BVA abgeschlossene Service-Vereinbarung zur Wahrnehmung von IT-Dienstleistungen im Rahmen der Bereitstellung und des Betriebs von EPOS 2.0 sind auf meine Empfehlung auch umfassende datenschutzrechtliche Regelungen aufgenommen worden. Unter diesen Bedingungen habe ich aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken gegen eine solche Datenverarbeitung im Auftrag bei einem Personalmanagementsystem.

Kasten zu Nr. 14.3

**Handlungsempfehlungen Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung**

**II. Allgemeine datenschutzrechtliche Leitplanken**

Personenbezogene Daten fallen bei der Nutzung dieser technisch unterstützten Verfahren als Inhaltsdaten (Personaldaten bzw. Personalaktendaten) und als Protokolldaten (mit besonderer Zweckbindung) an.

Für den Umgang mit diesen Daten gelten die folgenden allgemeinen Grundsätze:

1. Personenbezogene Daten der Beschäftigten dürfen in technikgestützten Verfahren nur in dem Umfang gespeichert, übermittelt und genutzt werden, in dem dies rechtlich zulässig und im Rahmen der festgelegten Zwecke zur Durchführung der der jeweiligen Stelle obliegenden personalwirtschaftlichen, organisatorischen und sozialen Aufgaben erforderlich ist (Grundsatz der Zulässigkeit, Zweckbindung und Erforderlichkeit).
2. In einem Berechtigungskonzept ist festzulegen, welche Stellen und/oder Funktionsträgerinnen oder Funktionsträger im Rahmen der ihnen übertragenen Aufgaben für welche Zwecke und in welcher Form (lesend/verändernd) befugt sind, auf Daten zuzugreifen oder Auswertungen vorzunehmen. Das Berechtigungskonzept ist fortzuschreiben und mindestens so lange zu speichern wie die zugehörigen Protokolldaten.
3. Es ist schon im Vorfeld bei der Auswahl und Gestaltung der automatisierten Verfahren darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet werden (Grundsatz der Datenvermeidung und Datensparsamkeit).

4. Die Betroffenen sind über ihren persönlichen Datenbestand, die Zwecke der Verarbeitung und Zugriffsberechtigungen zu unterrichten. Ihre Rechte auf Auskunft, Sperrung und Löschung sind zu wahren (Transparenzgebot und Betroffenenrechte).
5. Arbeits- und dienstrechtliche Entscheidungen, die für die Betroffenen eine rechtliche Folge nach sich ziehen oder sie erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient (Verbot der automatisierten Einzelentscheidung).
6. Zulässige dienststellenübergreifende Auswertungen der in den Verfahren verarbeiteten Personaldaten sollten soweit möglich anonym oder pseudonym erfolgen; dies gilt nicht für Auswertungen, Abgleiche oder Zusammenführungen, die sich auf wenige Merkmale (Informationen zur dienstlichen Funktion und Erreichbarkeit = so genannte Funktionsträgerdaten) beschränken.
7. Die Sicherungsziele Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit sind – ausgerichtet am Schutzbedarf der Daten – durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten; das Grundschutz-Handbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gibt dazu zahlreiche Hilfestellungen.

   Für die Ausgestaltung der Datenschutz- und Datensicherungsmaßnahmen ist – ggf. aus einer Vorabkontrolle (vgl. Ziffer 9) – ein Sicherheitskonzept zu entwickeln und entsprechend dem Stand der Technik fortzuschreiben. Die für das jeweilige Verfahren fachlich Verantwortlichen sind verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen spätestens mit dem Einsatz des Verfahrens umzusetzen und zu dokumentieren, falls dies noch nicht im Sicherheitskonzept enthalten ist. Insbesondere mit Protokollierungsverfahren ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, wer welche Beschäftigtendaten zu welcher Zeit eingegeben, verändert, übermittelt und/oder abgerufen hat; entsprechendes gilt auch für die Systemadministration.
8. Protokolldaten von Anwenderinnen und Anwendern sowie Administratorinnen und Administratoren, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs gespeichert werden, dürfen grundsätzlich nicht für andere Zwecke, insbesondere nicht für eine Verhaltens- und Leistungskontrolle, verarbeitet werden. Die Zweckbindung muss daher technisch und organisatorisch (z.B. durch Dienstanweisung) sichergestellt werden. Für Art, Umfang und Aufbewahrung der Protokollierung gilt der Grundsatz der Erforderlichkeit. Soweit technisch möglich und ausreichend sollte auf personenbezogene Daten verzichtet werden. Die Beteiligungsrechte des Personalrates sind zu beachten.
9. Vor der Einführung und Anwendung neuer Verfahren oder im Falle einer wesentlichen Veränderung der Verfahren ist eine Vorabkontrolle (auch „Technikfolgenabschätzung“ genannt) durchzuführen, wenn dies durch eine Rechtsvorschrift vorgesehen ist.
10. Die Verfahren sind in inhaltlicher und technischer Hinsicht ausreichend und nachvollziehbar zu dokumentieren.
11. Die behördlichen Beauftragten für den Datenschutz sind bei der Entwicklung und Implementierung der Verfahren frühzeitig zu beteiligen.
12. Um die Akzeptanz zu fördern, wird empfohlen, über Einführung und Anwendung der Verfahren eine Dienstvereinbarung mit dem Personalrat abzuschließen, in der insbesondere die Fragen der Zugriffsberechtigungen, der Zulässigkeit und Zweckbestimmung von Auswertungen und die Durchführung von Kontrollen für alle Beteiligten eindeutig und klar geregelt werden. Soweit die Verfahren geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, sind die Mitbestimmungs- bzw. Mitwirkungsrechte der Personalvertretung zu berücksichtigen.

### 14.4 Behördeninterne Veröffentlichung von Mitarbeiterdaten

*Bei Veröffentlichungen in Hausmitteilungen oder im Intranet müssen das Personalaktengeheimnis und der Mitarbeiterdatenschutz beachtet werden.*

Immer wieder erreichen mich Eingaben von Mitarbeiterinnen und Mitarbeitern der Verwaltung, in denen es um die Veröffentlichung personenbezogener Daten geht. Ich habe mich deshalb wiederholt hierzu geäußert (vgl. z. B. 17. TB Nr. 18.3.1 und Nr. 18.4, 20. TB Nr. 10.2.2). Gegen eine Veröffentlichung von personenbezogenen Mitarbeiterdaten bestehen keine Bedenken, soweit die Bekanntgabe zur Durchführung des Dienstbetriebes notwendig ist und einem dienstlichen Bedürfnis entspricht (sog. Organisations- und Funktionsangaben wie z. B. Name, Dienstzimmer, Funktionsbezeichnung/-übertragung, Dienststellung, Organisationseinheit, Einstellung). Dagegen sollte die Angabe personenbezogener Daten mit sensiblem Charakter und solcher, die Rückschlüsse auf die persönlichen und privaten Verhältnisse von Mitarbeitern zulassen (z. B. die Angabe der Gründe für eine Kündigung oder längere Abwesenheitszeiten, etwa Mutterschutz) vermieden werden. In Zweifelsfragen sollte das Persönlichkeitsrecht der Betroffenen vor Veröffentlichung durch Einwilligung oder zumindest

Einräumung einer Widerspruchsmöglichkeit angemessen berücksichtigt werden. Dies gilt auch für sog. Geburtstagslisten, die oftmals in Dienststellen verbreitet werden (vgl. 16. TB Nr. 18.3).

Von besonderer Brisanz ist die Veröffentlichung von Entscheidungen im Rahmen der Leistungsbezahlung. Dies gilt beispielsweise für die namentliche Bekanntgabe derjenigen Beschäftigten, denen ein Leistungselement, z. B. eine Leistungsprämie, gewährt wurde. Die personenbezogene Veröffentlichung in Hausmitteilungen oder im Intranet darf hier grundsätzlich nur mit Einwilligung der betroffenen Beschäftigten erfolgen (vgl. 20. TB Nr. 10.2.2). Leider wird diese Auffassung bislang nicht von allen Ressorts geteilt. Das BMI beabsichtigt, seine bisher praktizierte personenbezogene Veröffentlichung von Leistungselementen in den Hausmitteilungen auch künftig fortzusetzen. Auch die von mir vorgeschlagene Widerspruchsmöglichkeit im Einzelfall lehnt es ab. Ich habe die fortgesetzte namentliche Bekanntgabe der Empfänger von Leistungselementen in den Hausmitteilungen gegenüber dem BMI als Verstoß gegen das Personalaktengeheimnis förmlich beanstandet.

Obwohl auch ich das Ziel, im Bereich der Beschäftigten eine höchstmögliche Transparenz der Vergabepraxis im Rahmen der Leistungsbezahlung herzustellen, grundsätzlich positiv beurteile, darf das Persönlichkeitsrecht der Beschäftigten im Einzelfall nicht unberücksichtigt bleiben. Ich werde mich bei der künftigen Ausgestaltung einer leistungsorientierten Bezahlung bzw. Besoldung im öffentlichen Dienst weiter dafür einsetzen, dass auch hier das Persönlichkeitsrecht der Beschäftigten – zumindest durch Einführung einer Widerspruchsmöglichkeit im Einzelfall – gewahrt wird.

### 14.5 Personaldatenschutz und Verwaltungsermittlungen

*Bei der Durchführung behördeninterner Verwaltungsermittlungen vor Einleitung eines Disziplinar- oder Strafverfahrens ist den Datenschutzrechten der betroffenen Mitarbeiterinnen und Mitarbeiter angemessen Rechnung zu tragen. Das gilt auch für behördeninterne Ermittlungsmaßnahmen „gegen Unbekannt“.*

Im Berichtszeitraum hatte ich mich mit der Frage zu befassen, welche behördeninternen Maßnahmen mit Blick auf die Datenschutzrechte der Beschäftigten im Vorfeld von möglichen Disziplinar- oder Strafverfahren durchgeführt werden dürfen.

Dass die Behörde sog. Verwaltungsermittlungen in Fällen durchführen kann, in denen Verdachtsmomente bereits gegen namentlich bekannte Beschäftigte gerichtet sind, steht außer Frage. Es ist anerkanntermaßen Ausfluss des Informationsrechts und der Aufsichtspflicht des Dienstvorgesetzten, sich zunächst formlos die nötige Aufklärung zu verschaffen. Diese können auch dann gerechtfertigt sein, wenn die Person (noch) nicht bestimmbar ist, gegen die der konkrete Verdacht gerichtet werden könnte. Auch wenn hiernach Verwaltungsermittlungen „gegen Unbekannt“ grundsätzlich zulässig sind, dürfen sie nicht schrankenlos durchgeführt werden. Dies gilt insbesondere dann, wenn davon ein großer Kreis von Mitarbeiterinnen und Mitarbeitern betroffen ist.

Vor der Durchführung konkreter interner Maßnahmen zur Ermittlung von Beschäftigten, die möglicherweise für Unregelmäßigkeiten verantwortlich sein können, ist daher jeweils die Erforderlichkeit und Verhältnismäßigkeit der konkret beabsichtigten Maßnahme im Hinblick auf die damit verbundene Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Mitarbeiterinnen und Mitarbeitern zu prüfen. Sofern beispielsweise eine notwendige Recherche in einem Personalverwaltungs- oder Personalinformationssystem durchgeführt werden soll, ist sicherzustellen, dass Auswertungen auf den in Frage kommenden Personenkreis und den notwendigen Datenumfang beschränkt sind und nur den mit den internen Ermittlungen konkret beauftragten Personen oder Stellen zur Verfügung gestellt werden. Welche Maßnahmen als erforderlich und verhältnismäßig angesehen werden können, kann allerdings nur im jeweiligen Einzelfall aufgrund der vorhandenen Informationen und der bestehenden Sachlage beurteilt werden.

Die von „Ermittlungsmaßnahmen gegen Unbekannt“ betroffenen Mitarbeiterinnen und Mitarbeiter sind im Hinblick auf ihr Recht auf informationelle Selbstbestimmung über den Umgang mit ihren personenbezogenen Daten zumindest in allgemeiner Form zu informieren, um die nötige Transparenz zu schaffen. Nach Abschluss der Verwaltungsermittlung und der Beendigung etwaiger weiterführender Verfahren sind die erhobenen Daten zu löschen, sofern sie nicht Bestandteil z. B. der Disziplinarakten oder staatsanwaltschaftlichen Ermittlungsakten geworden sind.

Die Durchführung verwaltungsinterner Ermittlungsmaßnahmen habe ich im Berichtszeitraum unter dem Gesichtspunkt des Mitarbeiterdatenschutzes im Rahmen eines Beratungs- und Kontrollbesuches beim BKA geprüft. Die vom BKA intern zur Ermittlung eines unbekannten Mitarbeiters und möglichen Täters vor Einleitung eines Strafverfahrens durchgeführten „Ermittlungsmaßnahmen“ – insbesondere in den Bürokommunikationssystemen – habe ich als grundsätzlich verhältnismäßig und datenschutzrechtlich zulässig bewertet.

## 15 Deutscher Bundestag

### 15.1 Online-Angebot „Öffentliche Petitionen“

*Seit dem 1. September 2005 können für öffentliche Diskussionen bestimmte Petitionen auch ins Internet eingestellt werden. Die Mitzeichnung einer solchen Eingabe ist online möglich, sofern sie vom Petitionsausschuss als öffentliche Petition angenommen worden ist.*

Der auf zwei Jahre befristete Modellversuch zur Mitzeichnung von Petitionen im Internet (sog. „öffentliche Petition“) basiert auf einem seit 2001 mit Erfolg operierenden Verfahren des schottischen Regionalparlaments. Der Petitionsausschuss des Deutschen Bundestages will mit dem neuen, interaktiv angelegten Online-Diskussionsangebot die Intensivierung der Kommunikation zwi-

schen Bürgern untereinander und zwischen Bürgern und Deutschem Bundestag ermöglichen.

„Öffentliche“ Petitionen werden nur mit Einverständnis der Petentin bzw. des Petenten und nach Maßgabe des Persönlichkeitsrechtsschutzes in das Internet eingestellt. Die Bitte oder Beschwerde muss zunächst in den Zuständigkeitsbereich des Deutschen Bundestages fallen und ein Anliegen von allgemeinem Interesse betreffen. Ob eine Eingabe als öffentliche Petition ins Netz gestellt wird, entscheidet der Petitionsausschuss auf der Grundlage von veröffentlichten Verfahrensgrundsätzen sowie einer diese Grundsätze konkretisierenden Richtlinie. Wird die Petition online veröffentlicht, kann jeder sie unterstützen bzw. sich dazu in einem Diskussionsforum äußern. Im Übrigen kann der Verlauf von öffentlichen Petitionsverfahren über die Website des Deutschen Bundestages verfolgt werden (www.bundestag.de/Petitionen).

Mittlerweile haben mich mehrere Beschwerden erreicht, die dieses neue Online-Angebot betreffen. Die Beschwerde, dass eine Petition – nicht wie gewünscht – als öffentliche Petition angenommen wurde, griff allerdings nicht durch, weil gerade kein Rechtsanspruch auf Annahme einer Petition als öffentliche Petition besteht. Sofern am selben Tage mehrere Petenten zum selben Thema die Einstellung einer öffentlichen Petition beantragt haben, kann die Annahme als öffentliche Petition aus Gründen der Gleichbehandlung verweigert werden. Allerdings könnte der Petitionsausschuss in solchen Fällen erwägen, einen Hauptpetenten – etwa im Losverfahren – zu bestimmen und die weiteren Petenten als Unterstützer zu behandeln.

Weitere Beschwerden von Mitzeichnern öffentlicher Petitionen richten sich dagegen, dass die Namen der Mitzeichner über Suchmaschinen gefunden werden können. Der Deutsche Bundestag habe dafür zu sorgen, dass die auf seinen Internetseiten veröffentlichten Listen von Diskutanten und Mitzeichnern für Suchmaschinen gesperrt werden. Es liegt in der Natur einer im Internet platzierten öffentlichen Petition, dass sie allgemein einsehbar ist und auch von Suchmaschinen gefunden werden kann. Zudem werden die Petenten, Mitzeichner und Diskutanten auf der Internet-Plattform darüber aufgeklärt, dass mit der Beteiligung an einer öffentlichen Petition die Veröffentlichung unter anderem des eigenen Namens verbunden ist. Gleichwohl begrüße ich das aktuelle Vorhaben des Petitionsausschusses des Deutschen Bundestages, Mechanismen zu erarbeiten, die verhindern, dass Diskutanten und Mitzeichner öffentlicher Petitionen von Suchmaschinen erfasst werden.

### 15.2 Wahrung der Vertraulichkeit von Petitionen

*An Bundesministerien zum Zwecke der Abgabe von Stellungnahmen übersandte Petitionen dürfen nicht im Rahmen eines anhängigen Gerichtsverfahrens verwendet werden.*

Ein Petent beschwerte sich darüber, dass seine Petition nicht vertraulich behandelt worden war. Die Eingabe, bei der es im Wesentlichen um eine Änderung des Einkommensteuergesetzes ging, war durch den Petitionsausschuss des Deutschen Bundestages dem Bundesfinanzministerium zur Stellungnahme übersandt worden. Ohne Einwilligung des Petenten übersandte das Ministerium sodann seine Stellungnahme nebst Petition an eine Landesfinanzbehörde, die beide Schriftstücke unaufgefordert in ein laufendes, vom Petenten angestrengtes Gerichtsverfahren einbrachte.

Zwar muss ein Bürger, der sich an den Petitionsausschuss wendet, damit rechnen, dass dem zuständigen Ressort Gelegenheit gegeben wird, seine Position darzulegen. Dies entspricht auch den Verfahrensgrundsätzen des Petitionsausschusses über die Behandlung von Bitten und Beschwerden (vgl. dort Ziffer 7.7). Jedoch darf die Petition nur entsprechend dem Zweck der Übermittlung, also zur Anfertigung einer Stellungnahme für den Petitionsausschuss bzw. zur Erarbeitung einer eigenen Antwort verwandt werden. Petitionen zeichnen sich gerade dadurch aus, dass nur bestimmte Personen und Institutionen von ihr Kenntnis erhalten, die im Außenverhältnis zur Verschwiegenheit verpflichtet sind. Deshalb hätte die Petition nicht im Rahmen des anhängigen Gerichtsverfahrens verwendet werden dürfen. Meine Auffassung habe ich dem Bundesfinanzministerium dargelegt und es aufgefordert, fortan die Vertraulichkeit von Petitionen sicherzustellen.

## 16 Bundeswehr

### 16.1 Das Großprojekt HERKULES

*Das Bundesministerium der Verteidigung (BMVg) will mit dem Projekt HERKULES seine nahezu gesamte Informationstechnik outsourcen.*

Auch in der Bundesverwaltung werden zunehmend Dritte mit der Abwicklung von bestimmten Aufgaben beauftragt. Meist betrifft das Outsourcing IT-Verfahren. Das bereits vor rund sechs Jahren begonnene Milliarden-Projekt HERKULES hebt sich allein durch seine Größenordnung von vergleichbaren Vorhaben anderer Behörden ab. Es umfasst im Wesentlichen die Auslagerung der Bereitstellung und Betreuung nahezu der gesamten IT-Ausstattungen und -Dienstleistungseinrichtungen des BMVg im Inland im Wege einer „Öffentlich-privaten Partnerschaft“ auf eine neu zu gründende IT-Gesellschaft in der Rechtsform einer GmbH. An dieser bleibt der Bund in Höhe von 49,9 Prozent beteiligt, während die Mehrheit der Geschäftsanteile von einem privatwirtschaftlichen Konsortium aus zwei in Deutschland ansässigen Unternehmen der IT-Branche gehalten wird. Ziel dieser Außenvergabe ist die Modernisierung und Vereinheitlichung der IT-Ausstattung der Bundeswehr, zu der u. a. auch die Konzentration der bisher noch auf mehrere Standorte innerhalb des Bundesgebietes verteilten Rechenzentren zählt. Ungeachtet der dadurch erhofften positiven Auswirkungen auf die Wirtschaftlichkeit der Aufgabenerledigung beinhaltet der zunächst auf 10 Jahre festgeschriebene Auftrag ein jährliches Leistungsvolumen in Höhe von 665 Mio. Euro.

Die mir im Entwurf zur Verfügung gestellten Vertragselemente, die den Umgang mit personenbezogenen Daten

bei der Übertragung der Aufgaben auf die künftige IT-Gesellschaft und deren Wahrnehmung dort regeln, verdeutlichen die Dimension des Gesamtvertragswerkes, das sich vor allem durch die darin vorgesehene Zulassung von weiteren rechtlich selbstständigen Auftragnehmern neben der IT-Gesellschaft sowie von – teilweise mehrfach untereinander abgestuften – Subauftragsverhältnissen als sehr komplex erweist. Nach mündlichen und schriftlichen erläuternden Stellungnahmen des BMVg konnte ich diesem in einer ersten rechtlichen Einschätzung signalisieren, dass ich die der vertraglichen Ausgestaltung zugrunde gelegte Annahme einer Datenverarbeitung im Auftrag gemäß § 11 BDSG grundsätzlich teile. Ich habe allerdings auch darauf hingewiesen, dass es angesichts der vorgesehenen Verschachtelung von Auftragsverhältnissen bis hin zur Unterbeauftragung von ausländischen Unternehmen von besonderer Bedeutung sein wird, wie die für § 11 BDSG maßgebliche Weisungsgebundenheit und damit die datenschutzrechtliche Kontrollmöglichkeit über die insoweit ausschließlich als Auftragnehmerin zu qualifizierende IT-Gesellschaft zum Auftraggeber Bund/BMVg sowohl vertraglich als auch praktisch durch entsprechende technisch-organisatorische Maßnahmen sichergestellt werden kann. Dieses wird das BMVg im Rahmen des noch zu erarbeitenden Datenschutz- und des IT-Sicherheitskonzeptes, in dem auch auf die noch offene Frage einer Verschlüsselung personenbezogener Daten einzugehen ist, darzulegen haben. Eine abschließende datenschutzrechtliche Bewertung ist daher zur Zeit noch nicht möglich.

### 16.2 Einhaltung von Datenschutzbestimmungen durch die Kleiderkasse der Bundeswehr

*Undifferenzierte Übermittlung von personenbezogenen Daten an den privatrechtlichen Nachfolger der Kleiderkasse der Bundeswehr.*

Ein Petent beschwerte sich darüber, dass er viele Jahre nach Ende seiner Dienstzeit in der Bundeswehr Post von einer privaten Firma erhalten hatte, der Nachfolgerin der Kleiderkasse der Bundeswehr. Weder hatte der Petent dieser Firma seine Anschrift zur Verfügung gestellt, noch in die Weitergabe seiner Daten an diese Firma eingewilligt. Offenbar sind bei der Privatisierung der bundeseigenen Kleiderkasse für die Bundeswehr umfangreiche Datenbestände von aktiven und ehemaligen Bundeswehrangehörigen sowie in geringem Umfang auch von Privatpersonen mit personenbeziehbaren Inhalten an die privatrechtlich organisierte Nachfolgegesellschaften übermittelt worden, ohne im Vorfeld die Erforderlichkeit sorgfältig zu prüfen. Das BMVg hat mir zugesichert, dass der privatrechtliche Nachfolger der Kleiderkasse der Bundeswehr künftig die übernommenen Kundendaten entsprechend der mit ihm getroffenen Vereinbarung ausschließlich für die Zwecke der ordnungsgemäßen Verwaltung und nicht zu anderen Zwecken, wie z. B. Werbung, einsetzen wird, es sei denn, die Betroffenen hätten ausdrücklich zugestimmt. Ich habe das BMVg aufgefordert, die offenbar noch bestehenden Mängel im Umgang mit den Kundendaten der ehemaligen Kleiderkasse kurzfristig zu beheben und insbesondere für eine zeitnahe Erstellung und Umsetzung eines schlüssigen Datenschutzkonzeptes zu sorgen. Von einer förmlichen Beanstandung habe ich abgesehen, weil das BMVg Abhilfe zugesagt hat.

## 17 Auswärtige Angelegenheiten

### 17.1 Urkundenüberprüfungsverfahren bei unzuverlässigem Beurkundungswesen

*Um ausländische öffentliche Urkunden überprüfen zu können, bedient sich das Auswärtige Amt in bestimmten Ländern lokaler Vertrauensanwälte. Diese Praxis ist datenschutzrechtlich grundsätzlich zulässig.*

Das Auswärtige Amt hat feststellen müssen, dass aus einer Reihe von Ländern stammende öffentliche Urkunden nicht ohne weiteres in Deutschland legalisiert werden können. Grund dafür ist, dass ein hoher Prozentsatz solcher Urkunden verfälscht bzw. vollständig gefälscht oder zwar formal echt, aber inhaltlich falsch ist. Dies gilt vor allem für Personenstandsurkunden (z. B. Geburtsurkunden). Da die vor Ort notwendigen Überprüfungen nicht mit eigenem Personal durchgeführt werden können, bedienen sich die deutschen Auslandsvertretungen örtlicher Vertrauensanwälte. Die mit deren Hilfe durchgeführten Überprüfungen von Urkunden zielen auf die Klärung der Identität und des Personenstands, beispielsweise in Visa- und Eheschließungsangelegenheiten. Um die Schlüssigkeit der Angaben in den vorgelegten Dokumenten und der Angaben der Referenzpersonen zu bewerten, werden mancherorts auch Auskünfte zum Lebenslauf des Urkundsinhabers eingeholt.

Mich haben hierzu mehrere Beschwerden erreicht. In einem Fall hatte die Rüge zwar insoweit Erfolg, als der vom lokalen Vertrauensanwalt eingeschaltete Mitarbeiter in Bezug auf sensible personenbezogene Daten des Petenten nicht die notwendige Vertraulichkeit walten ließ; dieser Mitarbeiter wird deshalb nicht weiter mit Recherchecaufgaben betraut. Aus datenschutzrechtlicher Sicht sehe ich jedoch keinen Anlass zur grundsätzlichen Beanstandung des Urkundenüberprüfungsverfahrens, jedenfalls in Ländern mit erwiesenermaßen unzuverlässigem Urkunds- bzw. Personenstandswesen. Das Auswärtige Amt hat mir glaubhaft versichert, durch vielfältige Maßnahmen die kontinuierliche Überprüfung der Zuverlässigkeit seiner externen Ermittler vor Ort sicherzustellen, so dass die einschlägigen Bestimmungen des Bundesdatenschutzgesetzes beachtet werden (siehe die §§ 11, 13, 14 Abs. 2 Nr. 4 und 16 Abs. 1 Nr. 1).

### 17.2 Vertragsloser Zustellungsverkehr

*Die Zustellung ausländischer Gerichtspost bedarf einer gesetzlichen Grundlage.*

Ein Petent beschwerte sich darüber, dass das Auswärtige Amt und das Bundesministerium der Justiz ein für ihn bestimmtes amtliches Schriftstück aus der Schweiz mitgelesen und kontrolliert hätten. Das dem Petenten letztlich durch das Ordnungsamt der Stadt Dresden zuzustellende Schriftstück durchlief zudem noch die sächsischen Minis-

terien für Justiz und Inneres. Diese Form der „offenen“ Zusendung betrifft Fälle, in denen die beteiligten Staaten keine Regelung über die Zustellung amtlicher Schriftstücke getroffen haben. Das trifft im Verhältnis zwischen der Bundesrepublik Deutschland und der Schweiz zu, weil Letztere nicht zu den Parteien des Europäischen Übereinkommens über die Zustellung von Schriftstücken in Verwaltungssachen gehört. In solchen Fällen wird dann im Wege der sog. vertragslosen Rechtshilfe zugestellt. Jede beteiligte nationale Stelle kann hier eine Prüfung der versandten Dokumente nach außenpolitischen Erwägungen bzw. innenpolitischen Wertentscheidungen vornehmen.

Das Verfahren der vertragslosen Rechtshilfe greift in das Recht auf informationelle Selbstbestimmung der Betroffenen ein und bedarf deshalb einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang des zulässigen Grundrechtseingriffs klar und für den Bürger erkennbar ergeben. Das EGGVG enthält solche Rechtsgrundlagen nicht. Verwaltungsvorschriften, die den vertragslosen Zustellungsverkehr betreffen, stellen keine eigenständige Ermächtigungsgrundlage dar.

## 18 Aus meiner Dienststelle

### 18.1 Neuer Internetauftritt

*Mit der Erweiterung des Aufgabenkreises um die Informationsfreiheit ging auch eine grundlegende Überarbeitung des Internetauftritts zum 1. Januar 2006 online einher.*

Der Internetauftritt meiner Dienststelle wurde grundlegend umgestaltet und entspricht nun dem aktuellen Aufgabenkreis. Unter der neuen Internetadresse http://www.bfdi.bund.de kann der Besucher zwischen den Beiträgen zum Datenschutz oder zur Informationsfreiheit wählen.

So bietet die Datenschutz–Seite eine Auswahl an Schwerpunktthemen von besonderer Aktualität oder Bedeutung an. Eng verknüpft mit den Schwerpunktthemen dokumentieren rund 450 Themenbeiträge die Inhalte meiner datenschutzrechtlichen Tätigkeit. Der neue Internetauftritt hält zudem eine Sammlung bedeutsamer Rechtsprechung zum Datenschutz und zur Informationsfreiheit vor. Wie bisher lassen sich auch Informationen wie Pressemitteilungen, Reden, Arbeitshilfen oder die Tätigkeitsberichte nachlesen. Ebenso können die von mir herausgegebenen Informationsbroschüren und Faltblätter (s. u. Nr. 18.2) online abgerufen werden. Alle Beiträge können über eine Suchmaschine gefunden werden. Den Anforderungen der Barrierefreien Informationstechnik-Verordnung (BITV) wurde weitestgehend genüge geleistet.

### 18.2 Öffentlichkeitsarbeit

*Neues Informationsmaterial: Unterrichtung von Bürgerinnen und Bürgern durch Herausgabe von weiteren, neuen Faltblättern.*

Meine Öffentlichkeitsarbeit hat zum Ziel, die datenschutzrechtlichen Bestimmungen bekannt zu machen und zu erläutern, interessierte Bürgerinnen und Bürger über ihre Rechte zu informieren und ihnen damit zu helfen, ihr Recht auf informationelle Selbstbestimmung wahrzunehmen. Darüber hinaus informiere ich die Öffentlichkeit über wichtige Entwicklungen mit Bezug zum Datenschutz und nehme zu datenschutzpolitischen Fragen Stellung.

Über den Internetauftritt, das inzwischen wichtigste Informationsmittel, habe ich bereits gesondert berichtet (s. o. Nr. 18.1). Daneben wurden weiterhin die Informationsbroschüren „BfD-Info 1 (Bundesdatenschutzgesetz – Text und Erläuterung)“, „BfD-Info 4 (Die Datenschutzbeauftragten in Behörde und Betrieb)“ und „BfD-Info 5 (Datenschutz in der Telekommunikation)“ angeboten, die z. T. bei notwendig werdenden Neuauflagen aktualisiert wurden und allesamt großen Zuspruch gefunden haben.

Zusätzlich habe ich im Berichtszeitraum auch verschiedene neue Faltblätter zu aktuellen datenschutzrechtlichen Themen herausgegeben:

- Das Faltblatt „Datenschutz beim Telefonieren – was mit Ihren Daten passiert“ informiert darüber, was beim Abschluss eines Vertrages mit einem Telekommunikationsunternehmen mit den angegebenen Daten geschieht und welche Wahlmöglichkeiten der Kunde hat.
- Das Faltblatt „Surfen am Arbeitsplatz – Datenschutz-Wegweiser“ gibt Hinweise, was im Falle einer dienstlichen und/oder privaten Nutzung des Internets am Arbeitsplatz zu beachten ist und was mit den Daten der Nutzer passiert.
- Das Faltblatt „RFID-Funkchips für jede Gelegenheit?“ informiert über Radio Frequency Identification-Systeme, insbesondere zu Gefahren, Schutzmaßnahmen und zum transparenten Einsatz dieser Technologie.
- Das Faltblatt „Datenschutz bei der Polizei“ dient dazu, über die Informationsverarbeitung bei der Polizei und über die Wahrnehmung der Rechte der Bürgerinnen und Bürger gegenüber der Polizei aufzuklären.
- Das Faltblatt „Datenschutz bei der Internet-Telefonie – Moderne Technik mit Risiken“ bietet Informationen über die neue Technik des Telefonierens über das Internet (Voice over Internet Protocol – VoIP) und die damit verbundenen Risiken und datenschutzrechtlichen Probleme.

Im Jahr 2005 war meine Dienststelle auf der CeBIT vertreten, dieses Mal auf einem gemeinsamen Stand mit dem Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein. Zeitweise haben sich daneben auch vier weitere Landesbeauftragte für den Datenschutz an der Präsentation beteiligt. Dort wurde den Messebesuchern die Möglichkeit geboten, sich umfassend über datenschutzrechtliche Fragen zu informieren und mit den Datenschutzbeauftragten zu diskutieren. Das Themenspektrum reichte von Biometrie über die elektronische Signatur bis hin zur IT-Sicherheit.

## 18.3 Twinning-Projekt Malta

*Im Rahmen eines Twinning-Projekts wurden die Regierung und der Datenschutzbeauftragte der Republik Malta beraten.*

Die neuen EU-Mitgliedstaaten haben auch nach ihrem Beitritt die Möglichkeit, Defizite bei der Umsetzung von EU-Recht in nationales Recht im Rahmen von sog. Twinning-Projekten zu beheben. Die Republik Malta entschied sich im Bereich des Datenschutzes für Deutschland als Twinning-Partner. Diese Projektträgerschaft habe ich gerne übernommen, zumal es bereits im Vorfeld des Twinnig-Projekts eine enge Zusammenarbeit mit der maltesischen Datenschutzbehörde gab.

Die Beratung wurde gemeinsam von Mitarbeitern meines Hauses sowie einzelnen Landesdatenschutzbehörden in vorbildlicher Zusammenarbeit ausgeführt. Zwar hat Malta mit seinem Beitritt zur EU die EG-Datenschutzrichtlinien vollständig übernommen, allerdings fehlte es noch an praktischer Erfahrung, wie diese Vorgaben konkret bei einzelnen Gesetzesvorhaben, etwa im Gesundheitsbereich oder im Telekommunikationssektor, in die Praxis umgesetzt werden können. Neben dem Austausch von Erfahrungen stand bei den einzelnen Beratungen auch die Durchsetzung geltenden Rechts durch die maltesische Aufsichtsbehörde, zum Beispiel bei der Bearbeitung von Bürgereingaben, im Vordergrund.

Bei einem Besuch in Deutschland konnten sich anschließend hochrangige Vertreter verschiedener Ministerien sowie der Datenschutzbeauftragte davon überzeugen, wie datenschutzrechtliche Regelungen, vor allem im Bereich der polizeilichen und justiziellen Zusammenarbeit und im Rahmen des Schengener Abkommens, konkret angewandt werden.

## 18.4 Besuche ausländischer Delegationen

*Im Berichtszeitraum konnte ich zahlreiche Besucher begrüßen und über den Datenschutz in Deutschland informieren.*

Schon seit Jahren gibt es einen regelmäßigen Informationsaustausch mit Japan. So unterrichtete sich ein japanischer Hochschullehrer anlässlich seines Besuchs in meiner Dienststelle über die Modernisierung des deutschen Datenschutzrechts.

Eine rumänische Delegation unter Leitung der Datenschutzbeauftragten besuchte für mehrere Tage meine Dienststelle, um die Aufgaben meines Hauses kennen zu lernen. Dabei interessierte sie sich insbesondere für meine Öffentlichkeits- und Pressearbeit sowie für Fragen der Beratungs- und Kontrolltätigkeit im Bereich Post und Telekommunikation und Themen der inneren Sicherheit.

Die Gesellschaft für technische Zusammenarbeit (GTZ) hat mich mehrfach um Gespräche mit ausländischen Delegationen gebeten, darunter eine Delegation aus China, die grundlegende Informationen zum Datenschutz und zur Informationsfreiheit in Deutschland wünschte. Aus Indonesien konnte ich zwei Besuchergruppen begrüßen, wovon eine vom Innenminister geleitet wurde. Bei beiden Besuchen ging es um allgemeine Datenschutzfragen, Datenschutz in Europa und um besondere Fragen zum Melderecht.

Auch in Zukunft sehe ich es als wichtige Aufgabe an, den Kontakt mit ausländischen Datenschutzbeauftragten und Vertretern der Wissenschaft zu pflegen, um auch auf diese Weise das Verständnis für datenschutzrechtliche Anliegen weltweit zu fördern.

## 18.5 BfDI als Ausbildungsbehörde

*Referendare und Praktikanten.*

Auch in diesem Berichtszeitraum konnte ich eine große Zahl von Anfragen nach Praktika in meiner Dienststelle verzeichnen. Vor allem interessierten sich Studierende der Rechtswissenschaften und Rechtsreferendare für Themen des Datenschutzes.

In den Jahren 2005 und 2006 haben insgesamt 15 Studierende und Referendare Teile ihrer Ausbildung in meinem Hause absolviert. Darüber hinaus haben vier Anwärterinnen und Anwärter des gehobenen Dienstes in der allgemeinen inneren Verwaltung ihr Pflichtpraktikum in meiner Dienststelle abgeleistet.

Die uneingeschränkt positiven Erfahrungen auf beiden Seiten sind Anlass, auch künftig – trotz begrenzter Kapazitäten – alle Möglichkeiten zu nutzen, um an der Ausbildung junger Menschen mitzuwirken.

## 18.6 Künftig mehr Präsenz in der Bundeshauptstadt

*Mein Verbindungsbüro in Berlin nimmt 2007 seine Arbeit auf.*

Auf Grund der räumlichen Distanz zwischen meiner Dienststelle in Bonn und der Bundeshauptstadt Berlin und der damit verbundenen Notwendigkeit von Dienstreisen, der häufig kurzfristigen Termine in den Ausschüssen des Deutschen Bundestages und bei Ressortbesprechungen sowie der begrenzt zur Verfügung stehenden Mitarbeiterzahl konnte ich seit dem Regierungsumzug meine gesetzlichen Aufgaben und Befugnisse nicht immer im notwendigen und angemessenen Umfang realisieren. Um künftig eine wirkungsvollere und direktere Teilnahme am politischen Geschehen in der Bundeshauptstadt zu erreichen, werde ich deshalb im Laufe des Jahres 2007 ein Verbindungsbüro in Berlin einrichten.

Die Mitarbeiter/innen dieses Verbindungsbüros sollen künftig insbesondere für die Koordinierung und Wahrnehmung der Termine in den Ausschüssen des Deutschen Bundestages sowie in den Sitzungen der Bundesressorts in Berlin in Abstimmung mit den Fachreferaten verantwortlich sein. Darüber hinaus nehmen die Mitarbeiter/innen des Verbindungsbüros weiterhin ihre originären Referatsaufgaben wahr. Durch die Einrichtung des Verbindungsbüros in Berlin sollen keine neuen Planstellen bzw. Stellen beim BfDI geschaffen werden. Vielmehr werden bestimmte bislang in Bonn wahrgenommene Funktionen mit besonderem Berlinbezug mittelfristig verlagert und um die o. a. Koordinierungsaufgaben ergänzt.

### 18.7 Folgen des neuen Informationsfreiheitsgesetzes für meine Dienststelle

*Datenschützer sind künftig auch für Informationsfreiheit zuständig.*

Am 1. Januar 2006 trat das Informationsfreiheitsgesetz des Bundes (IFG) in Kraft (s. o. Nr. 2.8), das mir die Aufgabe des Bundesbeauftragten für die Informationsfreiheit in Zugleichfunktion übertragen hat. Im Hinblick auf diese Aufgabenerweiterung habe ich zunächst eine zeitlich befristete Projektgruppe „Aufbaustab Informationsfreiheitsgesetz – PG IFG“ errichtet.

Sofort nach Inkrafttreten des IFG ergab sich erheblicher Beratungs- und Koordinierungsbedarf bei vielen Bundesbehörden, insbesondere zu Fragen grundsätzlicher Art, etwa zum Anwendungsrahmen des Gesetzes von Behörden mit sehr unterschiedlichen Aufgabenstellungen. Im Jahr 2006 haben sich Bürgerinnen und Bürger in 196 Fällen schriftlich und in 317 telefonischen Beratungsersuchen an mich gewandt. Diese Eingaben betreffen sehr unterschiedliche Rechtsgebiete mit zum Teil sehr schwierigen juristischen Fragestellungen.

Durch den durch das IFG bewirkten Aufgabenzuwachs und die zudem ständig anwachsenden Anforderungen im Datenschutzbereich – so hat sich z. B. die Zahl der Bürgereingaben seit 2002 nahezu verdoppelt – hat sich die Arbeitsbelastung meiner Mitarbeiterinnen und Mitarbeiter erheblich erhöht. Zwar ist es durch strikte Prioritätensetzung, organisatorische Änderungen und verstärkten Technikeinsatz teilweise gelungen, den weiteren Anstieg des Arbeitsrückstaus zu begrenzen. Trotzdem halte ich es für unabdingbar, die Personal- und Sachausstattung meiner Dienststelle zu verbessern, damit die dem BfDI übertragenen Aufgaben sachgerecht erfüllt werden können.

Der 15. Deutsche Bundestag hatte bereits im Gesetzgebungsverfahren zum IFG festgestellt, dass in meiner Dienststelle für die neuen Aufgaben zusätzliche Personalkosten entstehen werden; er ging dabei für die Anfangszeit von fünf bis sechs neuen Stellen aus (Bundestagsdrucksache 15/4493). Über die Ausbringung und Finanzierung sollte im Haushaltsaufstellungsverfahren entschieden werden. Nachdem mir im Haushaltsjahr 2002 im Vorwege zwei neue Planstellen für Aufgaben nach dem IFG bewilligt worden waren, blieben die Forderungen nach den restlichen Planstellen jedoch bislang erfolglos. Im Haushaltsaufstellungsverfahren 2008 werde ich erneut darauf hinwirken, die noch ausstehenden vier neuen Planstellen zu erhalten, um so die Wahrnehmung meiner gesetzlichen Aufgaben in Zukunft zu gewährleisten und um Mitarbeiter ihrer eigentlichen Datenschutzaufgabe nicht zu entziehen.

## 19 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. In meinem letzten Tätigkeitsbericht (20. TB Nr. 6.1.3) habe ich über das Vorhaben der Bundesregierung informiert, beim BVA eine **Fundpapierdatenbank** einzurichten; eine entsprechende Regelung findet sich nunmehr im Aufenthaltsgesetz (§§ 49a, 49b). Zweck der Fundpapierdatenbank ist es, die sich in Deutschland aufhaltenden Ausländer, deren Herkunft auf Grund fehlender Ausweisdokumente unklar ist und die daher nicht abgeschoben werden können, durch die aufgefundenen Ausweisdokumente aus visumspflichtigen Staaten mittels biometrischer Verfahren (Lichtbilder-Abgleich) zu identifizieren. Bei einem Beratungs- und Kontrollbesuch im BVA im Oktober 2006 habe ich zwar keine gravierenden datenschutzrechtlichen Mängel festgestellt. Bestimmte Verfahrensabschnitte wie das Einscannen der Funddokumente und behördlichen Anschreiben in das elektronische Vorgangsverarbeitungssystem sowie deren Speicherung könnten jedoch datenschutzgerechter ausgestaltet werden. Ich habe beim BVA angeregt, das Verfahren entsprechend zu verbessern.

2. Die Verordnung über das **Zentrale Vorsorgeregister** bei der **Bundesnotarkammer** ist am 1. März 2005 in Kraft getreten. Entgegen meiner im 20. TB (Nr. 7.11) geäußerten Bedenken ist dort in § 4 vorgesehen, dass die Eintragung auch ohne Vorlage einer schriftlichen Einwilligungserklärung des Bevollmächtigten vorgenommen werden kann. Dieser wird vielmehr erst nachträglich über die Eintragung und sein Löschungsrecht informiert (sog. Benachrichtigungslösung). Ich halte dies nach wie vor nicht für die datenschutzrechtlich beste Lösung. Da in den Musteranträgen zur Eintragung aber auch eine Einwilligungserklärung des Bevollmächtigten enthalten ist, wird wohl die vorherige Einwilligung in der Praxis der Regelfall sein. Ein etwaiger Missbrauch der Daten von Vollmachtgebern war bislang noch nicht Gegenstand von Eingaben. Ich werde das Verfahren aber im Rahmen meiner Kontrollfunktion weiterhin im Blick behalten.

3. Das **Gesetz über Musterverfahren in kapitalmarktrechtlichen Streitigkeiten** (KapMuG) (vgl. 20. TB Nr. 7.13) ist am 1. November 2005 in Kraft getreten (BGBl. I S. 2437). Das hierdurch geschaffene Klageregister ermöglicht einem potentiell geschädigten Kapitalanleger, sich ohne größeren Aufwand im Internet darüber zu informieren, ob bereits seinem eigenen Anliegen entsprechende, gleichgerichtete Verfahren anhängig sind. Zu diesem Zweck enthält das Register unter anderem die vollständige Bezeichnung der beklagten Partei und ihres gesetzlichen Vertreters (§ 2 Abs. 1 Satz 4 Nr. 1 KapMuG). Ich hatte angeregt, in den Fällen, in denen nicht die Bank oder ein sonstiges Unternehmen des Kapitalmarktes, sondern der Kapitalanleger selbst in der Rolle des Beklagten ist, von der Veröffentlichung seiner personenbezogenen Daten Abstand zu nehmen. Dies ist trotz meiner Bemühungen nicht vom BMJ in der Klageregisterverordnung (KlagRegV vom 26. Oktober 2005, BGBl. I S. 3092) umgesetzt worden, die die näheren Bestimmungen über Inhalt und Aufbau des Klageregisters enthält. Vielmehr heißt es in § 1 Abs. 2 Satz 1 KlagRegV, dass zur vollständigen Bezeichnung der beklagten Partei und ihres gesetzlichen Vertreters das Klagere-

gister Angaben zu Name oder Firma und Anschrift zu enthalten hat. Ich halte daran fest, dass diese Daten des Anlegers nicht erforderlich sind, so dass ich nach wie vor Nachbesserungsbedarf sehe.

4. In meinem 20. TB (Nr. 8.11) hatte ich darüber berichtet, dass die **Zinsinformationsverordnung** – ZIV – vom 26. Januar 2004 (BGBl. I S. 128) ohne meine vorherige Beteiligung in Kraft getreten war. Die Verordnung enthielt eine Reihe unzureichender Regelungen zur Übermittlung personenbezogener Daten. Insbesondere fehlten in §§ 8 und 9 ZIV Zweckbestimmungen für die Mitteilungspflichten der inländischen Zahlstelle und des Bundesamtes für Finanzen (BfF – jetzt: Bundeszentralamt für Steuern – BZSt) sowie Fristen für die Löschung der Daten beim BfF.

   Diese datenschutzrechtlichen Defizite wurden mit Unterstützung des BMJ mit der Novellierung der ZIV vom 22. Juni 2005 (BGBl. I S. 1692) beseitigt (s. § 9 Abs. 1 und Abs. 4 ZIV).

5. Mit der **Steuerdatenabrufverordnung (StDAV)** sollen Daten, die unter das Steuergeheimnis fallen (§ 30 AO), durch technische und organisatorische Maßnahmen gegen einen unbefugten Abruf im automatisierten Verfahren geschützt werden. Nach intensiven Verhandlungen hatte das BMF den Entwurf einer entsprechenden Verordnung vorgelegt, der datenschutzrechtlich nicht zu bestanden war. Überraschend wurde dieser Entwurf jedoch zurückgezogen und ein neuer Entwurf vorgelegt, gegen den ich wiederum datenschutzrechtliche Bedenken erheben musste (vgl. 20. TB Nr. 8.8). Diese wurden im Rahmen der Beratungen berücksichtigt, so dass ich der StDAV vom 13. Oktober 2005 zustimmen konnte. Die Verordnung ist am 27. Oktober 2005 in Kraft getreten.

6. In meinem 20. TB (Nr. 16.3) hatte ich über die von der Bundesagentur für Arbeit (BA) geplante **Nutzung** der für die Arbeitsmarktstatistik übermittelten **Daten der Rentenversicherungsträger für andere Zwecke** berichtet. Die BA prüfte einen Datenabgleich ihrer Schuldnerdatei mit den von der Datenstelle der Rentenversicherungsträger übermittelten Daten. Wie die BA mir inzwischen mitgeteilt hat, hat sie von der geplanten Nutzung der o. g. Daten abgesehen. Zu einem entsprechenden Datenabgleich ist es infolge dessen nicht gekommen.

7. Mit dem Bestreben von **Personalvertretungen**, **Arbeitszeitdaten** von Mitarbeiterinnen und Mitarbeitern personenbezogen von der Dienststelle zu erhalten (vgl. 20. TB Nr. 10.3.5), hat sich das Oberverwaltungsgericht Nordrhein-Westfalen näher auseinandergesetzt (OVG NRW, Beschluss vom 4. November 2005 – Az.: 1 A 4935/04.PVB –). Danach genügt es zu einer ausreichenden Unterrichtung der Personalvertretung im Rahmen ihrer Aufgabenerfüllung, die Arbeitszeitdaten der Beschäftigten in pseudonymisierter Form, d.h. mit Kennziffern versehen, zur Verfügung zu stellen.

8. In meinem 20. TB (Nr. 21.2) hatte ich über den Entwurf des Gemeinsamen Bundesausschusses (vgl. § 91 Abs. 5 SGB V) zur Ergänzung der Richtlinie über die **Früherkennung von Krankheiten bei Kindern** bis zur Vollendung des 6. Lebensjahres berichtet. In der Zwischenzeit ist die sog. „Einführung des erweiterten Neugeborenen–Screenings“ in Kraft getreten. Die Richtlinie sieht erfreulicherweise u. a. eine schriftliche Einwilligung der Eltern (Personensorgeberechtigten), eine detaillierte Aufzählung der Zielkrankheiten sowie die Vernichtung der Restblutproben spätestens nach drei Monaten vor. Unabhängig von dieser Richtlinie lassen einzelne Bundesländer weitergehende Untersuchungen und längere Aufbewahrungszeiten der Restblutproben zu, wenn eine entsprechende Einwilligung der Personensorgeberechtigten vorliegt.

9. Im 20. TB (Nr. 5.6.1) hatte ich darüber berichtet, dass mir das BMVg nach vorangegangener Änderung des MADG den Entwurf einer Dienstvorschrift zur Anhörung vorgelegt hatte, die den **Zugriff des MAD** auf einen festgelegten Datenkranz des Personal- und Führungssystems der Bundeswehr (**PERFIS**) regeln sollte, den Vorgaben des Gesetzes jedoch nicht entsprach. Nach Erörterungen mit dem BMVg und dem MAD-Amt hat das BMVg inzwischen eine Dienstvorschrift erlassen, die den Vorgaben des Gesetzes entspricht und gegen die ich im Anhörungsverfahren keine Einwendungen mehr erhoben habe.

10. An der Durchführung des **Konsultationsverfahrens nach Artikel 17 Abs. 2 SDÜ** durch das BKA hatte ich insbesondere kritisiert, dass das BKA die ihm obliegende Pflicht zur Prüfung der Validität der Daten, auf die es ein ablehnendes Votum stützt, vermissen lässt (vgl. 20. TB Nr. 5.2.6). Nach einem Gespräch mit dem BMI und dem BKA sowie einer danach vorgenommenen Kontrolle im BKA prüft dieses nunmehr im Konsultationsverfahren in jedem Einzelfall, ob die vorhandenen Erkenntnisse ein ablehnendes Votum rechtfertigen.

    Allerdings bestehen weiterhin unterschiedliche Auffassungen zum von mir kritisierten Umfang der Informationen, die das BKA zur Prüfung von Visumanträgen im Konsultationsverfahren beizieht und die weit über den mit dem Verfahren verfolgten Zweck hinausgehen.

11. Das **I**nteraktive **Fo**rtbildungs**s**ystem des Bundes (**IFOS Bund**), über das ich in meinem 20. Tätigkeitsbericht unter Nr. 6.5 berichtet habe, wurde inzwischen um eine virtuelle Lernplattform erweitert. Die Gesamtkonzeption und die Weiterentwicklung des Systems habe ich begleitet. Nach einem erfolgreichen Pilotbetrieb ist die Lernplattform seit 1. September 2005 online. Die E-Learning-Objekte der Bundesakademie für öffentliche Verwaltung (BAköV) stehen nunmehr allen Bundesbediensteten

in 13 Themenbereichen zur Verfügung. Mit IFOS-Bund hat die BAköV ein System entwickelt, das nicht nur den am Fortbildungsprozess Beteiligten die Arbeit und den Informationsaustausch erleichtert, sondern auch die Teilnehmer an Fortbildungsveranstaltungen unterstützt.

12. Das BMJ hatte 2004 einen Gesetzentwurf vorgelegt, der den **Jugendstrafvollzug** erstmals zusammenfassend regeln sollte (vgl. 20. TB Nr. 7.6). Dieser Entwurf wurde aufgrund der Auflösung des Bundestages und der Neuwahlen im November 2005 nicht mehr dem Kabinett vorgelegt und unterlag somit der Diskontinuität. Aufgrund der Verfassungsänderungen im Zuge der Föderalismusreform sind nunmehr für die Gesetzgebung im Strafvollzug die Länder zuständig. Bislang sind mir allerdings aus keinem Land Gesetzesinitiativen für eine Neufassung bekannt. Ich hoffe, dass der Jugendstrafvollzug einheitlich in allen Ländern reformiert wird und dabei die Belange des Datenschutzes hinreichend berücksichtigt werden.

13. Bereits mehrfach (18. TB Nr. 14.1, 20. TB Nr. 5.5.2) habe ich über die **Einführung der elektronischen Akte beim BfV** berichtet. Es bestand Einvernehmen, dass dies eine – möglichst zeitnahe – Änderung der §§ 10 und 11 BVerfSchG erforderlich macht. Das ist bislang aber noch nicht geschehen. Änderungen dieses Gesetzes sind aber auch aus einem anderen Grund erforderlich. Nach § 45 BDSG sind Vorschriften über Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 binnen fünf Jahren nach Inkrafttreten des BDSG (18. Mai 2001) mit den Vorschriften des BDSG in Übereinstimmung zu bringen. Eine Anpassung des BVerfSchG – wie auch des BNDG und des MADG – ist insbesondere deswegen notwendig, weil das BDSG vom 18. Mai 2001 nicht mehr zwischen den Begriffen „Datei“ und „Akte“ differenziert, wie dies in § 3 BDSG – alt – der Fall war.

    Da die angemahnten Gesetzesänderungen wegen des Ablaufs der in § 45 BDSG gesetzten Frist nunmehr dringlich sind, erwarte ich von der Bundesregierung die baldige Vorlage eines entsprechenden Referentenentwurfs.

14. Im 20. TB (Nr. 5.5.5) habe ich über Probleme bei einer datenschutzrechtlichen **Kontrolle beim BfV** in Bezug auf Daten, die dem Quellenschutz unterliegen, berichtet. Danach darf eine Beschränkung meiner Kontrollbefugnis unter Berufung auf Quellenschutz nur zum Schutz der Anonymität natürlicher Personen erfolgen, nicht jedoch zum Schutz von Organisationen. Eine Lösung des Konflikts sollte in Gesprächen mit dem BMI und dem BfV gefunden werden. Nach mehrfachen Versuchen soll nun endlich dieses Thema erörtert werden. Ich hoffe, hierbei eine einvernehmliche Lösung zu finden, die einen Ausgleich zwischen den Geheimhaltungsinteressen des BfV und meinem gesetzlichen Kontrollauftrag schafft, ohne dass letzterer in Frage gestellt wird.

Anlage 1

**Hinweis für die Ausschüsse des Deutschen Bundestages**

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von *besonderem Interesse* sein könnten:

| | |
|---|---|
| Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung | 4.4; 15.1 bis 15.2; |
| Auswärtiger Ausschuss | 3.3.2; 9.5; 17.1 bis 17.2; |
| Innenausschuss | 2.1 bis 2.8; 3.2; 4.2; 4.4; 4.4.3; 4.5; 4.7; 4.9; 4.13; 5; 7.1.1 bis 7.1.3; 7.1.5; 7.3; 7.5 bis 7.6; 9.1 bis 9.2; 9.5 bis 9.7; 10.1; 10.8; 12.1; 14.1 bis 14.5; 18.1 bis 18.2; 19.1; 19.7; |
| Sportausschuss | 5.3.2; |
| Rechtsausschuss | 2.1; 3.2; 4.2; 4.5; 4.11; 4.13; 5.1.1 bis 5.1.2; 6.1 bis 6.8; 7.3; 7.5; 9.5 bis 9.7; 10.1; 10.8; 12.1; 19.2 bis 19.3; |
| Finanzausschuss | 4.4; 5.2.7; 5.4; 8; 9.2; 9.4 bis 9.5; 19.4 bis 19.5 |
| Ausschuss für Wirtschaft und Technologie | 2.3 bis 2.4; 4.2 bis 4.3; 4.5 bis 4.6; 4.11; 4.13; 5.8.3.2; 8.3; 10.8 bis 10.9; 14; |
| Ausschuss für Ernährung, Landwirtschaft und Verbraucherschutz | 4.2 bis 4.5; 4.8; 8.2; 8.4; 9.2; |
| Ausschuss für Arbeit und Soziales | 2.7; 13.4; 19.6 bis 19.7; |
| Verteidigungsausschuss | 5.6; 16; |
| Ausschuss für Familie, Senioren, Frauen und Jugend | 4.7 |
| Ausschuss für Gesundheit | 4.1; 4.6; 10.8; 13.1 bis 13.3; |
| Ausschuss für Verkehr, Bau und Stadtentwicklung | 3.3.2; 4.2; 12.1 bis 12.2; |
| Ausschuss für Menschenrechte und Humanitäre Hilfe | 4.5; |
| Ausschuss für Bildung, Forschung und Technikfolgenabschätzung | 2.4; 4.1 bis 4.13; 7.6; |
| Ausschuss für Tourismus | 3.3.2; |
| Ausschuss für die Angelegenheiten der Europäischen Union | 3.2; 6.5; 7.1.3; |
| Ausschuss für Kultur und Medien | 4.2 bis 4.5; 4.8 bis 4.11; 4.13; 6.5 bis 6.6; 7.2.1; |
| Ausschuss für Kultur und Medien<br>– Unterausschuss „Neue Medien“ – | 4.2 bis 4.5; 4.8 bis 4.11; 4.13; 10.9; |

Anlage 2

**Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche**

**Deutscher Bundestag**

- Liegenschaften des Deutschen Bundestages (Videoüberwachung)

**Bundeskanzleramt (einschließlich Beauftragter für Kultur und Medien)**

- Bundesnachrichtendienst
- Stiftung Preußischer Kulturbesitz
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (Zentrale und zwei Außenstellen)

**Bundesministerium des Innern**

- Ministerium
- Bundesamt für Migration und Flüchtlinge
- Bundesverwaltungsamt
- Bundeskriminalamt
- Bundesamt für die Sicherheit in der Informationstechnik
- Statistisches Bundesamt
- Bundespolizeipräsidium Mitte
- Bundespolizeiamt Köln
- Bundesamt für Verfassungsschutz
- Beschaffungsamt beim Bundesministerium des Innern
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- Bundeszentrale für politische Bildung
- Technisches Hilfswerk

**Bundesministerium der Justiz**

- Dienststelle Bundeszentralregister beim Generalbundesanwalt beim Bundesgerichtshof

**Bundesministerium der Finanzen**

- Ministerium
- Bundeszentralamt für Steuern
- zwei Oberfinanzdirektionen
- ein Hauptzollamt
- Bundesanstalt für Finanzdienstleistungsaufsicht
- Zollkriminalamt

**Bundesministerium für Arbeit und Soziales**

- Ministerium
- drei Agenturen für Arbeit
- eine Arbeitsgemeinschaft (zusammen mit LDI NRW)
- Bundesversicherungsamt
- Deutsche Rentenversicherung Bund
- Barmer Ersatzkasse
- Techniker Krankenkasse
- Künstlersozialkasse
- Berufsgenossenschaft Druck und Papierverarbeitung
- Steinbruchsberufsgenossenschaft

**Bundesministerium der Verteidigung**

- Ministerium
- Amt für den Militärischen Abschirmdienst

**Bundesministerium für Familie, Senioren, Frauen und Jugend**

- Ministerium
- Bundesamt für den Zivildienst
- zwei Zivildienstgruppen
- eine Zivildienstschule
- eine Verwaltungsstelle eines Wohlfahrtsverbandes

**Bundesministerium für Gesundheit**

- Ministerium
- Robert-Koch-Institut

**Bundesministerium für Verkehr, Bau und Stadtentwicklung**

- Ministerium
- Luftfahrt-Bundesamt
- Kraftfahrt-Bundesamt
- Fa. Toll Collect GmbH
- Bundesamt für Güterverkehr

**Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit**

- Ministerium
- Bundesamt für Naturschutz

noch Anlage 2

**Deutsche Post AG**

- Zentrale
- Niederlassung Brief und Zustellstützpunkte Berlin und Stahnsdorf
- Betriebseigene Agenturen und Partnerfilialen im Großraum Bonn
- Nachsendezentrum INA München
- Paketfrachtzentrum München
- Zustellstützpunkt Sankt Augustin
- Internationales Postfrachtzentrum (IPZ) Frankfurt

**Telekommunikationsunternehmen**

- E-Plus Mobilfunk GmbH & Co. KG
- Indigo networks GmbH
- OneTel Telecommunication GmbH
- Versatel Süd-Deutschland GmbH
- Deutsche Telekom AG-T-Com
- Merkur Telecomservices GmbH
- debitel AG
- Kabel Deutschland GmbH
- Vodafone D2 GmbH

**Sonstige**

- Deutsche Bundesbank
- Gemeinsamer Bundesausschuss
- Verband der Angestellten-Krankenkassen (VdAK)
- eine Rehabilitationsklinik
- Wirtschaftsunternehmen wegen Verfahren zur Sicherheitsüberprüfung
- Bundesdruckerei GmbH
- Stadt Siegburg zusammen mit LDI NRW
- Internationaler Suchdienst Arolsen

Anlage 3

**Übersicht über Beanstandungen nach § 25 BDSG**

**Bundesministerium des Innern**

- Verstoß des Bundeskriminalamtes gegen § 18 Abs. 1 Satz 1 BVerfSchG wegen unterlassener Einzelprüfung in zahlreichen Fällen (s. Nr. 5.1.4).

- Verstoß der Bundespolizei gegen § 18 Abs. 1 Satz 1 BVerfSchG wegen unterlassener Einzelfallprüfung in zahlreichen Fällen (s. Nr. 5.1.4).

- Verstoß des Bundeskriminalamtes gegen §§ 4 Abs. 1, 4a Abs. 1 BDSG wegen Übermittlung personenbezogener Daten, obwohl eine Einwilligungserklärung hierfür fehlte (s. Nr. 5.2.5).

**Bundeskanzleramt**

- Verstoß des Bundesnachrichtendienstes gegen § 5 Abs. 1 BNDG i.V.m. § 12 Abs. 3 BVerfSchG wegen unterlassener Einzelfallprüfung in zahlreichen Einzelfällen (s. Nr. 5.7.6).

**Bundesministerium für Wirtschaft und Technologie**

- Verstoß der Deutschen Post AG gegen das Postgeheimnis nach § 39 Postgesetz (s. Nr. 11.1).

**Bundesministerium für Arbeit und Soziales**

- Verstoß der City-BKK, Hamburg, wegen fortlaufender rechtswidriger Erhebung von Sozial-/Gesundheitsdaten der Versicherten ohne gesetzliche Grundlage (s. Nr. 13.1.8)

Anlage 4 (zu Nr. 3.5)

**27. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2005**

**Erklärung von Montreux:**
**„Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“**

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. Entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung,

2. Erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschließung über den Datenschutz und die internationalen Organisationen,

3. Stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmassnahmen beherrscht wird,

4. Sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt,

5. Verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien,

6. Sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt,

7. Sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten überhaupt werden können, und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt,

8. Erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen,

9. Anerkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann,

10. Sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehrs und einer offenen Marktwirtschaft ist,

11. Sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist,

12. Sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen,

13. Sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen,

14. Erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat,

15. Erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten Zehn Geboten zum Schutz der Privatheit Rechnung zu tragen,

16. Anerkennen, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezo-

noch Anlage 4 (zu Nr. 3.5)

gener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC),

17. Erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:

- Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,
- Prinzip der Richtigkeit,
- Prinzip der Zweckgebundenheit,
- Prinzip der Verhältnismäßigkeit,
- Prinzip der Transparenz,
- Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,
- Prinzip der Nicht-Diskriminierung,
- Prinzip der Sicherheit,
- Prinzip der Haftung,
- Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,
- Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierungen und den internationalen und supranationalen Organisationen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragen

a. die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;

b. sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäß den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;

c. den Europarat, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern;

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16. bis 18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a. die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzuhalten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;

b. die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;

c. die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten.

Die Datenschutzbeauftragten kommen außerdem überein

a. namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschließungen der Konferenz zu verstärken;

b. die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;

c. den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;

d. mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;

e. eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragten für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

Anlage 5 (zu Nr. 3.5)

**27. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2005**

**Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten**

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschließt:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zur Zeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum andern Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

Wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

Unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

Im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar“ machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

Unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weit reichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

1. wirksame Schutzmassnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) gesammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technische Beschränkungen der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumentinhabers im Moment der Dokumentvorlage.

Anlage 6 (zu Nr. 3.5)

**27. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2005**

**Resolution zur Verwendung von Personendaten für die politische Kommunikation**

**Die Konferenz**

In Erwägung, dass politische Kommunikation ein grundlegendes Instrument für die Beteiligung der Bürgerinnen und Bürger, der politischen Kräfte und der Kandidatinnen und Kandidaten am Leben einer Demokratie ist, und in Anerkennung der Wichtigkeit der Freiheit der politischen Meinungsäußerung als ein Grundrecht;

In Erwägung, dass gelebte Staatsbürgerschaft das Recht der Bürgerinnen und Bürger voraussetzt, im Rahmen von Wahlkampagnen von Politik und Verwaltung Informationen zu erhalten und angemessen informiert zu werden; in Erwägung, dass diese Rechte auch geeignet sind um bei weiteren Themen, Ereignissen und politischen Positionen in Kenntnis der Sachlage seine Wahl zu anderen Themen des politischen Lebens treffen zu können, sei es bei Referenden, bei der Wahl von Kandidatinnen und Kandidaten oder beim Zugang zu Informationen innerhalb politischer Organisationen oder von gewählten Amtsträgern;

In Erwägung, dass die politischen Kräfte und politische Organisationen im Allgemeinen sowie gewählte Abgeordnete sich verschiedener Formen der Kommunikation und der Geldmittelbeschaffung bedienen und Informationsquellen und neue Technologien nutzen, um direkte und persönliche Kontakte mit verschiedensten Kategorien von betroffenen Personen zu knüpfen;

In Erwägung, dass in einer wachsenden Zahl von Ländern ein Trend hin zu immer stärkerer institutioneller Kommunikation gewählter Kandidatinnen und Kandidaten und Körperschaften zu beobachten ist, ebenfalls auf lokaler Ebene und mittels E-Government; in der Erwägung, dass diese Aktivitäten, die die Verarbeitung von Personendaten voraussetzen können, in Einklang stehen mit dem Recht der Staatsbürgerinnen und -bürger, über die Tätigkeiten der gewählten Kandidatinnen und Kandidaten und Körperschaften informiert zu werden;

In Erwägung, dass in diesem Rahmen von politischen Organisationen fortlaufend eine große Menge von Personendaten gesammelt und manchmal in aggressiver Art und Weise verwendet werden, unter Anwendung verschiedener Techniken wie Umfragen, Sammlung von E-Mail-Adressen mittels geeigneter Software oder Suchmaschinen, flächendeckender Stimmenwerbung in Städten oder Formen politischer Entscheidbildung durch interaktives Fernsehen oder Computerdateien, die die Herausfilterung einzelner Stimmenden erlauben; in Erwägung, dass in diesen Daten – zusätzlich zu elektronischen Adressen, Telefonnummern, E-Mail-Konten, Informationen über berufliche Tätigkeiten und familiäre Verhältnisse – zuweilen unrechtmäßig auch sensible Daten enthalten sein können wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten;

In Erwägung, dass von verschiedenen Personen invasive Profile erstellt und sie klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen, ihr angehören oder gar Parteimitglieder sind, um so mit bestimmten Gruppen von Bürgerinnen und Bürgern vermehrt persönlich kommunizieren zu können;

In Erwägung, dass diese Aktivitäten gesetzeskonform und ordnungsgemäß ausgeübt werden müssen; In Erwägung, dass es nötig ist, die Grundrechte und Grundfreiheiten der betroffenen Personen zu schützen und mit geeigneten Maßnahmen zu verhindern, dass diese Personen ungerechtfertigtes Eindringen in ihre Privatsphäre erfahren, Schaden erleiden oder ihnen Kosten entstehen, dass sie namentlich negative Auswirkungen und mögliche Diskriminierungen erleiden oder auf die Ausübung bestimmter Formen der politischen Beteiligung verzichten müssen;

In Erwägung, dass es möglich sein sollte, das Schutzziel zu erreichen, indem sowohl die Interessen der Öffentlichkeit an bestimmten Formen politischer Kommunikation als auch angemessene Modalitäten und Garantien in Bezug auf die Kommunikation mit Parteimitgliedern und mit andern Bürgerinnen und Bürgern in Betracht gezogen werden;

In Erwägung, dass in diesem Sinne ein verantwortungsbewusstes Marketing gefördert werden kann, ohne dass der Austausch politischer Ideen und Vorschläge behindert zu werden braucht, und dass die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten hat, die sie vom kommerziellem Marketing unterscheiden;

In Erwägung, dass Datenschutzgesetze bereits in vielen Gerichtsbarkeiten auf politische Kommunikation anwendbar sind;

In Erwägung, dass es nötig ist, die Einhaltung der Datenschutzesgrundsätze zu garantieren und dazu einen weltweiten Minimalstandard zu schaffen, der dazu beitragen könnte, dass das Schutzniveau für Personen, von denen Daten gesammelt werden können, zu harmonisieren, indem zum einen nationale und internationale Verhaltensregeln zur Grundlage genommen und zum andern spezifische Lösungen und Regelungen einzelner Länder berücksichtigt werden;

In Erwägung, dass die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen könnten, auch in Zusammenarbeit mit anderen Auf-

sichtsbehörden in den Bereichen des Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren;

**verabschiedet folgende Resolution**

Jede Aktivität politischer Kommunikation, die die Verarbeitung von Personendaten voraussetzt – auch diejenige, die nicht im Zusammenhang mit Wahlkampagnen steht – muss die Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen respektieren, einschließlich des Rechts auf Schutz der persönlichen Daten, und muss im Einklang stehen mit den anerkannten Grundsätzen des Datenschutzes, namentlich:

*Datenminimierung*

Personendaten sollen nur so weit verarbeitet werden, als es zur Erreichung des spezifischen Zwecks, zu welchem sie gesammelt werden, erforderlich ist.

*Erhebung auf rechtmäßige Weise und nach Treu und Glauben*

Personendaten sollen aus erkennbaren Quellen rechtmäßig erhoben werden und sie sollen nach Treu und Glauben verarbeitet werden. Es soll sichergestellt werden, dass die Quellen, im Einklang mit dem Gesetz, entweder öffentlich zugänglich sind, oder dass andernfalls respektiert wird, dass sie nur zu bestimmten Zwecken, unter bestimmten Modalitäten, für einen begrenzten Anlass oder Zeitraum genutzt werden dürfen.

Besondere Aufmerksamkeit soll jenen Fällen geschenkt werden, in denen aggressive Methoden für die Kontaktaufnahme mit den betroffenen Personen gewählt werden.

*Datenqualität*

Bei der Verarbeitung sollen die anderen Grundsätze zur Sicherung der Datenqualität beachtet werden. Die Daten müssen insbesondere richtig, relevant und auf das notwendige Minimum beschränkt sein und à jour gehalten werden im Hinblick auf den bestimmten Zweck, zu dem sie erhoben wurden, besonders wenn sich die Informationen auf gesellschaftliche oder politische Anschauungen oder ethische Überzeugungen der betroffenen Person beziehen.

*Zweckmäßigkeit*

Personendaten aus privaten oder öffentlichen Informationsquellen, Institutionen oder Organisationen dürfen für die politische Kommunikation verwendet werden, wenn ihre Weiterverarbeitung im Einklang steht mit dem Zweck, zu dem sie ursprünglich erhoben wurden, und den betroffenen Personen zur Kenntnis gebracht wird; dies gilt insbesondere für sensible Daten. Gewählte Abgeordnete müssen diese Grundsätze beachten, wenn sie Daten, die zur Ausübung der amtlichen Funktionen gesammelt wurden, für die politische Kommunikation benützen wollen.

Personendaten, die ursprünglich mit aufgeklärter Einwilligung der betroffenen Person zu Marketingzwecken erhoben wurden, dürfen für die politische Kommunikation verwendet werden, wenn der Zweck der politischen Kommunikation in der Zustimmungserklärung ausdrücklich genannt wird.

*Verhältnismäßigkeit*

Personendaten dürfen nur auf die Art und Weise verarbeitet werden, die dem Zweck der Datensammlung entspricht, insbesondere wenn es um Daten zu potenziellen Wählerinnen und Wählern oder um den Vergleich von Daten geht, die aus verschiedenen Archiven oder Datenbanken stammen.

Personendaten, insbesondere solche, die über den Anlass hinaus, zu dem sie erhoben wurden, aufbewahrt werden, dürfen weiter verwendet werden, bis die Ziele der politischen Kommunikation erreicht sind.

*Information der betroffenen Person*

Den betroffenen Personen muss eine dem gewählten Kommunikationsmittel entsprechende Informationsnotiz zugestellt werden, bevor von ihnen Daten gesammelt werden; die Notiz hat den für die Datensammlung Verantwortlichen zu bezeichnen (die einzelne kandidierende Person; den externen Kampagnenleiter; die lokale Unterstützungsgruppe; lokale oder assoziierte Vereinigungen; die Partei insgesamt) sowie den zu erwartenden Datenaustausch zwischen diesen Instanzen.

Die Person, von der Daten gesammelt werden, muss informiert werden, wenn diese Daten ohne ihr Zutun gesammelt werden, zumindest wenn die Daten nicht nur vorübergehend aufbewahrt werden.

*Einwilligung*

Es muss sichergestellt sein, dass die Verarbeitung von Personendaten auf der Einwilligung der betroffenen Person oder auf einen anderen gesetzlich vorgesehen Grund beruht. Die Verarbeitung muss die im jeweiligen Staat geltenden, den spezifischen Informationsquellen und -mitteln entsprechenden Regelungen beachten, namentlich im Falle von E-Mail-Adressen, Faxnummern, SMS oder andern Text/Bild/Video-Mitteilungen oder von aufgezeichneten Telefonkontakten.

*Datenaufbewahrung und Datensicherheitsmaßnahmen*

Jede für eine Datensammlung verantwortliche Person, sei es eine politische Gruppierung oder eine einzelne kandidierende Person, muss alle technischen und organisatorischen Maßnahmen treffen, die nötig sind, um die Integrität der Daten zu schützen und um zu verhindern, dass die Daten verloren gehen oder von unbefugten Personen oder Stellen benutzt werden.

*Rechte der betroffenen Person*

Die betroffene Person hat das Recht auf Zugang, Berichtigung, Sperrung und Löschung ihrer Daten; sie hat das Recht, sich gegen unerwünschte Kommunikation zu wehren und – kostenlos sowie auf einfache Weise – zu verlangen, keine neuen Mitteilungen mehr zu erhalten. Diese Rechte müssen in der an sie gerichteten Informationsnotiz ausdrücklich genannt werden.

Für den Fall, dass diese Rechte verletzt werden, sind angemessene Maßnahmen und Sanktionen vorzusehen.

Anlage 7 (zu Nr. 3.5 und Nr. 10.10)

**28. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre am 2. und 3. November 2006**

**Entschließung zum Datenschutz bei Suchmaschinen (Übersetzung aus dem Englischen)**

Vorgeschlagen von: Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützer: Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit), Irland (Datenschutzbeauftragter), Neuseeland (Datenschutzbeauftragter), Norwegen (Datatilsynet), Polen (Generalinspektor für den Schutz personenbezogener Daten)

**Entschließung**

Heutzutage sind Suchmaschinen der Schlüssel zum „cyberspace" geworden, um in der Lage zu sein, Informationen im Internet aufzufinden, und damit ein unverzichtbares Werkzeug.

Die steigende Bedeutung von Suchmaschinen für das Auffinden von Informationen im Internet führt zunehmend zu erheblichen Gefährdungen der Privatsphäre der Nutzer solcher Suchmaschinen.

Anbieter von Suchmaschinen haben die Möglichkeit, detaillierte Interessenprofile ihrer Nutzer aufzuzeichnen. Viele IP-Protokolldaten, besonders wenn sie mit den entsprechenden Daten kombiniert werden, die bei Zugangsdiensteanbietern gespeichert sind, erlauben die Identifikation von Nutzern. Da die Nutzung von Suchmaschinen heute unter den Internet-Nutzern eine gängige Praxis ist, erlauben die bei den Anbietern populärer Suchmaschinen gespeicherten Verkehrsdaten, ein detailliertes Profil von Interessen, Ansichten und Aktivitäten über verschiedene Sektoren hinweg zu erstellen (z. B. Berufsleben, Freizeit, aber auch über besonders sensitive Daten, z. B. politische Ansichten, religiöse Bekenntnisse, oder sogar sexuelle Präferenzen).

Die Datenschutzbeauftragten sind bereits in der Vergangenheit hinsichtlich der Möglichkeit zur Erstellung von Profilen über Bürger besorgt gewesen. Die im Internet verfügbare Technologie macht diese Praxis jetzt in einem gewissen Umfang auf globaler Ebene technisch möglich.

Es ist offensichtlich, dass diese Informationen unter Umständen auf einzelne Personen zurückgeführt werden können. Deswegen sind sie nicht nur für die Betreiber von Suchmaschinen selbst von Nutzen, sondern auch für Dritte. So hat zum Beispiel vor kurzem ein Ereignis das Interesse unterstrichen, dass Strafverfolgungsbehörden an diesen Daten haben: Im Frühjahr 2006 forderte das Justizministerium der Vereinigten Staaten von Amerika von Google, Inc. die Herausgabe von Millionen von Suchanfragen für ein Gerichtsverfahren, das unter anderem den Schutz vor der Verbreitung von kinderpornographischen Inhalten im Internet zum Gegenstand hatte. Google weigerte sich, dieser Aufforderung nachzukommen und gewann letztendlich das Verfahren. Im weiteren Verlauf desselben Jahres publizierte AOL eine Liste von beinahe 20 Millionen scheinbar anonymisierten Suchanfragen, die ungefähr 650.000 AOL-Nutzer über einen Zeitraum von drei Monaten in die AOL-Suchmaschine eingegeben hatten. Laut Presseberichten konnten daraus einzelne Nutzer auf der Basis des Inhalts ihrer kombinierten Suchanfragen identifiziert werden. Diese Liste war – obwohl sie von AOL umgehend zurückgezogen wurde, als der Fehler dort erkannt worden war – zum Zeitpunkt des Zurückziehens Berichten zufolge bereits vielfach heruntergeladen und neu publiziert, und in durchsuchbarer Form auf einer Anzahl von Websites verfügbar gemacht worden.

Es muss darauf hingewiesen werden, dass nicht nur die Verkehrsdaten, sondern auch der Inhalt von Suchanfragen personenbezogene Informationen darstellen können.

Diese Entwicklung unterstreicht, dass Daten über zurückliegende Suchvorgänge, die von Anbietern von Suchmaschinen gespeichert werden, bereits jetzt in vielen Fällen personenbezogene Daten darstellen können. Insbesondere in Fällen, in denen Anbieter von Suchmaschinen gleichzeitig auch andere Dienste anbieten, die zur einer Identifikation des Einzelnen führen (z. B. E-Mail), können Verkehrs- und Inhaltsdaten über Suchanfragen mit anderen personenbezogenen Informationen kombiniert werden, gewonnen aus diesen anderen Diensten innerhalb derselben Sitzung (z. B. auf der Basis des Vergleichs von IP-Adressen). Der Prozentsatz von Daten über Suchanfragen, die auf Einzelpersonen zurückgeführt werden können, wird vermutlich in der Zukunft weiter ansteigen wegen der Zunahme der Nutzung fester IP-Nummern in Hochgeschwindigkeits-DSL oder anderen Breitbandverbindungen, bei denen die Computer der Nutzer ständig mit dem Netz verbunden sind. Er wird noch weiter ansteigen, sobald die Einführung von Ipv6 abgeschlossen ist.

**Empfehlungen**

Die Internationale Konferenz fordert die Anbieter von Suchmaschinen auf, die grundlegenden Regeln des Datenschutzes zu respektieren, wie sie in der nationalen Gesetzgebung vieler Länder sowie auch in internationalen Richtlinien und Verträgen (z. B. den Richtlinien der Vereinten Nationen und der OECD zum Datenschutz, der Konvention 108 des Europarates, dem APEC Regelungsrahmen zum Datenschutz, und den Datenschutzrichtlinien der Europäischen Union) niedergelegt sind, und gegebenenfalls ihre Praktiken entsprechend zu ändern:

1. Unter anderem sollten Anbieter von Suchmaschinen ihre Nutzer im Vorhinein in transparenter Weise über die Verarbeitung von Daten bei der Nutzung der jeweiligen Dienste informieren.
2. Im Hinblick auf die Sensitivität der Spuren, die Nutzer bei der Nutzung von Suchmaschinen hinterlassen, sollten Anbieter von Suchmaschinen ihre Dienste in einer datenschutzfreundlichen Art und weise anbieten. Insbesondere sollten sie keine Informationen über eine Suche, die Nutzern von Suchmaschinen zugeordnet werden können, oder über die Nutzer von Suchmaschinen selbst aufzeichnen. Nach dem Ende eines Suchvorgangs sollten keine Daten, die auf einen einzelnen Nutzer zurückgeführt werden können, gespeichert bleiben, außer der Nutzer hat seine ausdrückliche, informierte Einwilligung dazu gegeben, Daten, für die Erbringung eines Dienstes die notwendig sind, speichern zu lassen (z.B. zur Nutzung für spätere Suchvorgänge).
3. In jedem Fall kommt der Datenminimierung eine zentrale Bedeutung zu. Eine solche Praxis würde sich auch zugunsten der Anbieter von Suchmaschinen auswirken, indem die zu treffenden Vorkehrungen bei Forderungen nach der Herausgabe nutzerspezifischer Informationen durch Dritte vereinfacht würden.

Anlage 8 (zu Nr. 3.5)

**28. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre am 2. und 3. November 2006**

**„Datenschutz vermitteln und effektiver gestalten“**

**Ursprung dieser Initiative**

Dieser Bericht hat seinen Ursprung in der Rede von Alex Türk, dem Vorsitzenden der französischen Datenschutzbehörde (CNIL), anlässlich einer im Mai 2006 vom polnischen Generalinspektor für Datenschutz in Warschau abgehaltenen Konferenz zum Thema „Öffentliche Sicherheit und Schutz der Privatsphäre“. Alex Türk sprach über seine ernste Besorgnis angesichts der Herausforderungen, denen die Datenschutzbehörden zurzeit gegenüberstehen. Er betonte, dass die Datenschutzbehörden ihre Aktivitäten dringend auf diese Herausforderungen ausrichten müssten, da andernfalls Gefahr bestehe, dass die den Datenschutzbestimmungen zugrunde liegende Philosophie in kürzester Zeit an Gehalt verliere.

Im Anschluss an die Konferenz lud der Europäische Datenschutzbeauftragte (EDPS) den CNIL ein, eine gemeinsame Initiative ins Leben zu rufen, um die Notwendigkeit dieser dringlichen Maßnahmen bei der Konferenz in London zu präsentieren. Der britische Datenschutzbeauftragte gab der Initiative sofort volle Unterstützung. Vorliegender Bericht wurde in enger Zusammenarbeit der drei genannten Datenschutzbehörden erstellt.

Durch ihren Beitritt zu dieser Initiative verpflichten sich die teilnehmenden Datenschutzbehörden, ihre Aktivitäten im Hinblick auf die folgenden Ziele zu koordinieren:

- Entwicklung von Kommunikationsaktivitäten auf der Grundlage gemeinsamer Ideen, von denen einige in beigefügtem Text zum Ausdruck gebracht werden
- Anpassung der eigenen Verfahrensweisen und Methoden durch eingehende Beurteilung ihrer Effektivität und Effizienz sowie durch Ausweitung ihrer Kapazitäten in den Bereichen technische Kompetenz, Trendprognose und Intervention im technologischen Bereich
- Beitrag zur institutionellen Anerkennung von Datenschutzbehörden auf internationaler Ebene und Förderung der Einbeziehung anderer relevanter Interessenvertreter auf nationaler und internationaler Ebene

Zum gegenwärtigen Zeitpunkt haben die folgenden Datenschutzbehörden bestätigt, diese Initiative grundsätzlich zu unterstützen:

- Commission nationale de l’informatique et des libertés (Frankreich)
- European Data Protection Supervisor (Europäische Union)
- Information Commissioner (Großbritannien und Nordirland)
- Privacy Commissioner of Canada (Kanada)
- Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (Deutschland)
- Agencia Española de Protección de Datos (Spanien)
- Garante per la Protezione dei Dati Personali (Italien)
- College Bescherming Persoonsgegevens (Niederlande)
- Privacy Commissioner (Neuseeland)
- Préposé fédéral à la protection des données et à la transparence (Suisse)/Eidgenössische Datenschutz und Öffentlichkeitsbeauftragte (Switzerland)

Anlage 9 (zu Nr. 3.3)

**Von der Artikel 29-Gruppe im Berichtszeitraum verabschiedete Dokumente**

| | |
|---|---|
| WP 103 (1112/05) | Stellungnahme 1/2005<br>zu dem in Kanada gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdatensätzen (Passenger Name Records – PNR) und erweiterte Passagierdaten (Advanced Passenger Information – API) von Fluggesellschaften<br>Angenommen am 19. Januar 2005 |
| WP 104 (10092/05) | Arbeitsdokument<br>„Datenschutz und geistiges Eigentum“<br>Angenommen am 18. Januar 2005 |
| WP 105 (10107/05) | Arbeitsdokument<br>„Datenschutz und RFID-Technologien“<br>Angenommen am 19. Januar 2005 |
| WP 106 (1227/05) | Bericht der Art. 29-Datenschutzgruppe über die Meldepflicht an die nationalen Kontrollstellen, die bestmögliche Nutzung von Ausnahmen und Vereinfachungen und über die Rolle der Datenschutzbeauftragten in der Europäischen Union<br>Angenommen am 18. Januar 2005 |
| WP 107 (05) | Arbeitsdokument über ein Verfahren der Zusammenarbeit zur Abgabe gemeinsamer Stellungnahmen zu den sich aus verbindlichen unternehmensinternen Vorschriften ergebenden angemessenen Garantien<br>Angenommen am 14. April 2005 |
| WP 108 (05) | Arbeitsdokument über die Einführung eines Prüfkatalogs für einen Antrag auf Genehmigung verbindlicher unternehmensinterner Vorschriften<br>Angenommen am 14. April 2005 |
| WP 109 (00862/05) | Arbeitsprogramm 2005<br>Angenommen am 14. April 2005 |
| WP 110 (1022/05) | Stellungnahme 2/2005 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visen für einen kurzfristigen Aufenthalt (KOM (2004) 835 endg.)<br>Angenommen am 23. Juni 2005 |
| WP 111 (1670/05) | Ergebnisse der öffentlichen Anhörung zum Arbeitspapier 105 der Artikel 29-Gruppe zum Thema Datenschutz und RFID-Technologie<br>Angenommen am 28. Juni 2005 |
| WP 112 (1710/05) | Stellungnahme 3/2005 zur Anwendung der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten<br>Angenommen am 30. September 2005 |
| WP 113 (1868/05) | Stellungnahme 4/2005 zum Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (KOM (2005) 438 endgültig; 21. September 2005)<br>Angenommen am 21. Oktober 2005 |

noch Anlage 9 (zu Nr. 3.3)

| | |
|---|---|
| WP 114 (2093-01/05) | Arbeitspapier über eine gemeinsame Auslegung des Artikels 26 Abs. 1 der Richtlinie 95/46/EG vom 24. Oktober 1995<br>Angenommen am 25. November 2005 |
| WP 115 (2130/05) | Stellungnahme 5/2005 der Artikel 29-Gruppe zur Nutzung von Standortdaten für die Bereitstellung von Diensten mit Zusatznutzen<br>Angenommen am 25. November 2005 |
| WP 116 (2067/05) | Stellungnahme 6/2005 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates (KOM (2005) 236 endg.) bzw. für einen Beschluss des Rates (KOM (2005) 230 endg.) über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) und zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über den Zugang von für die Ausstellung von Kfz-Zulassungsbescheinigungen zuständigen Dienststellen der Mitgliedstaaten zum Schengener Informationssystem der zweiten Generation (SIS II) (KOM (2005) 237 endg.)<br>Angenommen am 25. November 2005 |
| | Achter Jahresbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten in der Europäischen Union und in Drittländern im Berichtsjahr 2004 |
| WP 117 (00195/06) | Stellungnahme 1/2006 über die Anwendung von EU-Datenschutzvorschriften auf innerbetriebliche Maßnahmen zur Unterstützung von Hinweisgebern (Whistleblowing) in den Bereichen Buchhaltung, Rechnungsprüfung, Buchprüfung und Kampf gegen Bestechung sowie Banken- und Finanzkriminalität<br>Angenommen am 1. Februar 2006 |
| WP 118 (00451/06) | Stellungnahme 2/2006 der Art. 29-Datenschutzgruppe zu Datenschutzfragen bei Filterdiensten für elektronische Post<br>Angenommen am 21. Februar 2006 |
| WP 119 (654/06) | Stellungnahme 3/2006 zur Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG<br>Angenommen am 25. März 2006 |
| WP 120 (00744/06) | Arbeitsprogramme 2006 bis 2007<br>Angenommen am 5. April 2006 |
| WP 121 (1014/06) | Stellungnahme 4/2006 zu der Mitteilung eines Regelungsvorschlags des US Department of Health and Human Services (Gesundheitsministerium der Vereinigten Staaten) zur Kontrolle übertragbarer Krankheiten und zur Erhebung von Daten über Passagiere vom 20. November 2005 (Control of Communicable Disease Proposed 42 CFR Parts 70 and 71)<br>Angenommen am 14. Juni 2006 |
| WP 122 (1015/06) | Stellungnahme 5/2006 zum Urteil des Europäischen Gerichtshofs vom 30. Mai 2006 in den verbundenen Rechtssachen C-317/04 und C-318/04 zur Übermittlung von Fluggastdaten an die USA<br>Angenommen am 14. Juni 2006 |
| WP 123 (01313/06) | Stellungnahme 6/2006 zu dem Vorschlag für eine Verordnung des Rates über die Zuständigkeit und das anwendbare Recht in Unterhaltssachen, die Anerkennung und Vollstreckung von Unterhaltsentscheidungen und die Zusammenarbeit im Bereich der Unterhaltspflichten<br>Angenommen am 9. August 2006 |

noch Anlage 9 (zu Nr. 3.3)

| | |
|---|---|
| WP 124 (01612/06) | Stellungnahme 7/2006 zum Urteil des Europäischen Gerichtshofs vom 30. Mai 2006 in den verbundenen Rechtssachen C-317/04 und C-318/04 über die Übermittlung von Fluggastdaten an die USA und zur Dringlichkeit eines neuen Abkommens<br>Angenommen am 27. September 2006 |
| WP 125 (1609/06) | Arbeitsdokument zum Datenschutz und Auswirkungen auf die Privatsphäre der eCall Initiative<br>Angenommen am 26. September 2006 |
| WP 126 (1611/06) | Stellungnahme 8/2006 zur Überprüfung des regulierenden Rahmenwerks für die elektronische Kommunikation und Dienste mit dem Schwerpunkt auf der Datenschutzrichtlinie für elektronische Kommunikation<br>Angenommen am 26. September 2006 |
| WP 127 (1613/06) | Stellungnahme 9/2006 zur Umsetzung der Richtlinie 2004/82/EG des Rates vom 29. April 2004 über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln<br>Angenommen am 27. September 2006 |
| WP 128 (01935/06) | Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunications (SWIFT)<br>Angenommen am 22. November 2006 |

Anlage 10 (zu Nr. 4.5.3)

**Entschließung zwischen der 69. und 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur**

**Einführung biometrischer Ausweisdokumente vom 1. Juni 2005**

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützter Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

- dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,
- dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,
- dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,
- dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,
- dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,
- dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,
- dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

Anlage 11 (zu Nr. 2.1)

**Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27./28. Oktober 2005 in der Hansestadt Lübeck**

**Appell der Datenschutzbeauftragten des Bundes und der Länder:**
**Eine moderne Informationsgesellschaft braucht mehr Datenschutz**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in der kommenden Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Auditgesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem ein adäquater Sicherheitsgewinn gegenübersteht. Nur eine freie Gesellschaft kann eine sichere Gesellschaft sein. Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müssen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Eingriffsbefugnisse, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen kann zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

noch Anlage 11 (zu Nr. 2.1)

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle vielerorts durch nachgeordnete Stellen mit unzureichender Personalkapazität ohne adäquate technische Ausstattung statt. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird. Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten für die Zwecke setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

Anlage 12 (zu Nr. 4.7)

**Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zwischen der 70. und 71. Konferenz**

**Sicherheit bei eGovernment durch Nutzung des Standards OSCI**
(Stand: 15. Dezember 2005)

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheits-Standard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von so genannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Anlage 13 (zu Nr. 4.3)

**Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. bis 27. Oktober 2006 in Naumburg**

**Verbindliche Regelungen für den Einsatz von RFID-Technologien**

Der Einsatz von RFID-Tags (Radio Frequency Identification) hält unaufhaltsam Einzug in den Alltag. Schon jetzt werden sowohl im öffentlichen als auch im privatwirtschaftlichen Bereich viele Gegenstände mit diesen miniaturisierten IT-Systemen gekennzeichnet. Es ist zu erwarten, dass neben bereits jetzt mit RFID-Technik gekennzeichneten Lebensmitteln künftig auch Personalausweise, Geldscheine, Kleidungsstücke und Medikamentenpackungen mit RFID-Tags versehen werden. In wenigen Jahren könnten somit praktisch alle Gegenstände des täglichen Lebens weltweit eindeutig gekennzeichnet sein.

Die flächendeckende Einführung derart gekennzeichneter Gegenstände birgt erhebliche Risiken für das Recht auf informationelle Selbstbestimmung in sich. Die RFID-Kennungen verschiedenster Gegenstände können sowohl miteinander als auch mit weiteren personenbezogenen Daten der Nutzenden – in der Regel ohne deren Wissen und Wollen – zusammengeführt werden. Auf diese Weise werden detaillierte Verhaltens-, Nutzungs- und Bewegungsprofile von Betroffenen ermöglicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet von allen Stellen, in deren Verantwortungsbereich RFID-Tags verwendet werden, insbesondere von Herstellern und Anwendern im Handels- und Dienstleistungssektor, alle Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie zu entwickeln und zu nutzen, und vor allem die Prinzipien der Datensparsamkeit, Zweckbindung, Vertraulichkeit und Transparenz zu gewährleisten. Der schnellen Umsetzung dieser Forderungen kann auch eine verbindliche Selbstverpflichtung von Herstellern und Anwendern der RFID-Technologie im Handels- und Dienstleistungssektor dienen.

Das Bundesverfassungsgericht hat den Gesetzgeber mehrfach darauf hingewiesen, dass wegen des schnellen und für den Grundrechtsschutz riskanten informationstechnischen Wandels die technischen Entwicklungen aufmerksam zu beobachten sind und notfalls durch ergänzende Rechtsetzung korrigierend einzugreifen ist. Daher sind die besonderen Gegebenheiten, die mit dem Einsatz der RFID-Technologie verbunden sind, vom Gesetzgeber daraufhin zu untersuchen, ob für alle Risiken adäquate und rechtliche Schutzmechanismen vorhanden sind. In den Bereichen, in denen diese fehlen, hat der Gesetzgeber einzugreifen. Dies gilt insbesondere für den Fall, dass die Hersteller und Anwender sich auf eine verbindliche Selbstverpflichtung nicht einlassen.

Für den Schutz der Persönlichkeitsrechte Betroffener sind generell folgende Forderungen zu berücksichtigen:

- Transparenz
  Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.
- Kennzeichnungspflicht
  Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.
- Keine heimliche Profilbildung
  Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.
- Vermeidung der unbefugten Kenntnisnahme
  Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.
- Deaktivierung
  Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren, bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Anlage 14 (zu Nr. 4.4.1, Nr. 4.7 und Nr. 8.4)

**Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006**
(bei Enthaltung von Schleswig-Holstein)

**Sachgemäße Nutzung von Authentisierungs- und Signaturverfahren**

Die Datenschutzbeauftragten des Bundes und der Länder beobachten einen Trend, abweichend von den bislang geltenden Vorgaben zur Nutzung der qualifizierten elektronischen Signatur in der öffentlichen Verwaltung zunehmend ungeeignete oder weniger sichere Verfahren zuzulassen. So soll beispielsweise infolge des Gesetzentwurfes der Bundesregierung zum Jahressteuergesetz 2007 (Bundesratsdrucksache 622/06) beim Verfahren Elster Online der Finanzverwaltung das in § 87a AO Abs. 3 geforderte Verfahren zur qualifizierten elektronischen Signatur durch ein Verfahren ersetzt werden, das lediglich zur Authentisierung der Datenübermittler geeignet ist. Auch die Planungen zum Verfahren für den elektronischen Einkommensnachweis ELENA sehen zumindest für einen Übergangszeitraum den Verzicht auf die qualifizierte elektronische Signatur vor. Einer derartigen Fehlentwicklung muss mit Nachdruck entgegengetreten werden.

Obwohl Signatur- und Authentisierungsverfahren mit der asymmetrischen Verschlüsselung vergleichbare technische Verfahren nutzen, unterscheiden sie sich im Inhalt ihrer Aussagen und müssen unterschiedliche Rechtsfolgen für die Nutzenden nach sich ziehen. Der grundlegende Unterschied dieser Verfahren muss sowohl bei der Planung als auch bei ihrem Einsatz in Verwaltungsverfahren berücksichtigt werden.

Elektronische Signaturen liefern Aussagen über elektronische Dokumente, insbesondere über deren Authentizität und Integrität. Ausschließlich die qualifizierte elektronische Signatur ist durch rechtliche Regelungen der eigenhändigen Unterschrift in weiten Bereichen gleichgestellt und dient dem Nachweis der Echtheit elektronischer Dokumente. Zudem sind nur Verfahren zur Erzeugung elektronischer Signaturen rechtlich geregelt und sicherheitstechnisch genau definiert.

Authentisierungsverfahren liefern hingegen lediglich eine Aussage über die Identität einer Person oder einer Systemkomponente. Solche Verfahren sind beispielsweise zur Authentifizierung einer Person oder eines IT-Systems gegenüber Kommunikationspartnern oder zur Anmeldung an einem IT-System geeignet. Die hierbei ausgetauschten Informationen unterliegen in der Regel nicht dem Willen und dem Einfluss der Rechnernutzenden bzw. der Kommunikationspartner und beziehen sich ausschließlich auf den technischen Identifizierungsprozess. Daher dürfen an die Authentizität und Integrität solcher Daten nicht die gleichen Rechtsfolgen geknüpft werden wie an eine qualifizierte elektronische Signatur.

Die Aufrechterhaltung der unterschiedlichen Funktionalität und Verbindlichkeit von Signatur und Authentisierung liegt sowohl im Interesse von Bürgerinnen und Bürgern als auch der Verwaltung und ist rechtlich geboten. Die unsachgemäße Anwendung oder in Kauf genommene Funktionsvermischung dieser Verfahren mindert die Transparenz, die Sicherheit und die Verlässlichkeit bei der elektronischen Datenverarbeitung. Darüber hinaus sind erhebliche Nachteile für die Nutzenden zu erwarten.

Wird ein Authentisierungsschlüssel zum Signieren verwendet,

- kann fälschlicher Weise behauptet werden, dass Nutzende elektronische Dokumente signiert haben; da sie das Gegenteil nicht beweisen können, müssen sie befürchten, die damit verbundenen Rechtsfolgen tragen zu müssen,
- besteht die Möglichkeit, dass Authentisierungsverfahren (Single Sign On, Challenge Response etc.) gezielt missbräuchlich verwendet werden,
- wird den Nutzenden keine „Warnfunktion“ mehr angeboten wie bei der ausschließlichen Verwendung des Signaturschlüssels zum Signieren und
- sind die Verfahren und die daraus resultierenden Konsequenzen für die Nutzenden nicht mehr transparent.

Vor diesem Hintergrund fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass der Gesetzgeber weder ungeeignete noch weniger sichere Verfahren zulässt. Dies bedeutet, dass

- Nutzenden die Möglichkeit eröffnet werden muss, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern,
- immer dann Signaturverfahren eingesetzt werden müssen, wenn Aussagen über Dokumente oder Nachrichten gefordert sind und Authentisierungsverfahren nur dort verwendet werden dürfen, wo es um Aussagen über eine Person oder eine Systemkomponente geht,
- die Transparenz der Verfahren und die Nutzbarkeit der Authentisierungsfunktion erhalten bleiben müssen.

Die Datenschutzbeauftragten appellieren darüber hinaus an die Verantwortlichen in der Verwaltung und bei den Projektträgern, gemeinsam die offenen Fragen beim Ein-

satz der qualifizierten elektronischen Signatur zu lösen und insbesondere die Entwicklung interoperabler, ökonomischer Verfahren zur Prüfung qualifizierter elektronischer Signaturen zu unterstützen. Hierfür ist die konstruktive Zusammenarbeit der Verantwortlichen von großen Anwendungsverfahren wie Elster Online, ELENA und Elektronische Gesundheitskarte unabdingbar.

Die Bundesregierung sollte verstärkt die Einführung von Verfahren mit qualifizierter elektronischer Signatur unterstützen, weil diese Verfahren für die sichere und authentische Kommunikation zwischen Bürgerinnen und Bürgern und der Verwaltung besonders geeignet sind. Die qualifizierte elektronische Signatur muss eine zentrale Komponente in eGovernment-Anwendungen sein, und darf nicht durch ungeeignete oder weniger sichere Verfahren ersetzt werden. Die Bundesregierung sollte daher die Verbreitung von Chipkarten mit qualifiziertem Zertifikat fördern. Erst der flächendeckende Einsatz von qualifizierten elektronischen Signaturen ermöglicht niedrige Kosten bei der Bereitstellung der Karten und führt darüber hinaus zu rationellen und somit kostengünstigen Verwaltungsabläufen.

Anlage 15 (zu Nr. 4.3)

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006 in Bremen**

**Empfehlung der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich: Die Entwicklung und Anwendung von RFID-Technologie ist insbesondere im Handel und im Dienstleistungssektor datenschutzkonform zu gestalten!**

Die gegenwärtige Entwicklung der RFID-Technologie (Radio Frequency Identification) und ihr Einsatz im Handel und im Dienstleistungssektor kann Kosteneinsparungspotenziale beispielsweise im Rahmen von Logistik- und Produktionsprozessen eröffnen. Sie birgt allerdings auch erhebliche Risiken für das Persönlichkeitsrecht von Verbraucherinnen und Verbrauchern. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es deswegen für erforderlich, dass die RFID-Technologie datenschutzkonform entwickelt und eingesetzt wird. Bereits jetzt sollten Hersteller und Anwender im Handel und im Dienstleistungssektor die Möglichkeiten der datenschutzgerechten Gestaltung dieser Technologie nutzen.

RFID ist eine Technik, um Daten mit Hilfe von Funkwellen auf einem Chip berührungslos und ohne Sichtkontakt lesen, speichern und gegebenenfalls verarbeiten zu können. Mit RFID-Chips gekennzeichnete Gegenstände können mit einem Lesegerät abhängig von der Reichweite bzw. Sendestärke identifiziert und lokalisiert werden. Ungeachtet der zahlreichen Vorteile des Einsatzes von RFID-Chips ist zu befürchten, dass zukünftig massenhaft personenbezogene Daten verarbeitet werden, indem nahezu alle Gegenstände des täglichen Lebens (einschließlich Kleidung, Lebensmittel- und andere Verpackungen, Medikamente usw.) über Hintergrundsysteme dauerhaft den Betroffenen zugeordnet werden können. RFID ermöglicht damit technisch die von den Verbraucherinnen und Verbrauchern unbemerkte Ausforschung ihrer Lebensgewohnheiten und ihres Konsumverhaltens etwa zu kommerziellen Zwecken.

Diese technologische Entwicklung stellt den Datenschutz vor neue Herausforderungen. Ob auf RFID-Chips gespeicherte Daten einen Personenbezug aufweisen, wird häufig von den konkreten Umständen des Einzelfalls abhängen. Selbst Informationen, die zunächst keinen Personenbezug haben, weil sie allein ein Produkt kennzeichnen, könnten über die Lebensdauer des Chips gesehen – zum Beispiel mit Hilfe von Hintergrundsystemen – später einer konkreten Person zugeordnet werden. Damit würden rückwirkend alle gespeicherten Daten über einen mit einem RFID-Chip gekennzeichneten Gegenstand zu personenbezogenen Daten. Ein datenschutzkonformer Einsatz der RFID-Technologie wird deshalb immer schwerer kontrollierbar sein. Die Ausübung der verfassungsrechtlich begründeten, datenschutzrechtlich unabdingbaren Rechte der Verbraucherinnen und Verbraucher auf Auskunft sowie auf Löschung und Berichtigung von unrichtigen personenbezogenen Daten wird – insbesondere wegen der geringen Größe der RFID-Chips – künftig erheblich erschwert.

Angesichts dieses Gefährdungspotenzials der RFID-Technologie erscheint es fraglich, ob die bestehenden gesetzlichen Regelungen ausreichen, den wirksamen Schutz der Persönlichkeitsrechte der Betroffenen zu gewährleisten.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich halten es für erforderlich, dass bereits bei der technologischen Ausgestaltung von RFID das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt wird. Dazu gehört vor allem, dass Verbraucherinnen und Verbrauchern nach dem Kauf von Produkten die RFID-Chips auf einfache Weise unbrauchbar machen können. Daneben sind auch die Datenschutzrechte der betroffenen Arbeitnehmerinnen und Arbeitnehmer im Produktions- und Logistikprozess zu wahren. Zugleich sind unter anderem der Handel und der Dienstleistungssektor und insbesondere die entsprechenden Verbände aufgerufen, umfassende, verbindliche und nachprüfbare Selbstverpflichtungen für eine datenschutzfreundliche Ausgestaltung der RFID-Technologie abzugeben.

Für den Schutz der Persönlichkeitsrechte der betroffenen Verbraucherinnen und Verbraucher sind dabei folgende Regeln unabdingbar:

Transparenz/Benachrichtigungspflicht

Die Verbraucherinnen und Verbraucher müssen wegen des möglichen Personenbezugs der auf RFID-Chips gespeicherten Daten umfassend über den Einsatz, Verarbeitungs- und Verwendungszweck und Inhalt von RFID-Chips informiert werden. Werden durch ihren Einsatz personenbezogene Daten gespeichert, sind die Betroffenen hiervon zu benachrichtigen.

Kennzeichnungspflicht

Nicht nur die eingesetzten RFID-Chips selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips, Lesegeräte bzw. dazugehörige Hintergrundsysteme ausgelöst werden, müssen für die Verbraucherinnen und Verbraucher transparent und leicht zu erkennen sein. Eine heimliche Anwendung „hinter dem Rücken“ der Betroffenen darf es nicht geben.

Deaktivierung

Den betroffenen Verbrauchern muss ab dem Kauf von mit RFID-Chips versehenen Produkten die Möglichkeit eröffnet werden, die RFID-Chips jederzeit dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die ursprünglichen Speicherzwecke nicht mehr erforderlich sind. Dieses Recht darf nicht durch Gewährleistungsbeschränkungen in Allgemeinen Geschäftsbedingungen beeinträchtigt werden.

Datensicherheit

Die Vertraulichkeit der gespeicherten und der übertragenen Daten ist durch Sicherstellen der Authentizität der beteiligten Geräte (Peripherie) und durch Verschlüsselung zu gewährleisten. Das unbefugte Auslesen der gespeicherten Daten muss wirksam verhindert werden.

Keine heimliche Profilbildung

Daten von RFID-Chips aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Einwilligung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Chips verzichtet werden.

Anlage 16 (zu Nr. 9.4)

**Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 8./9. November 2006**

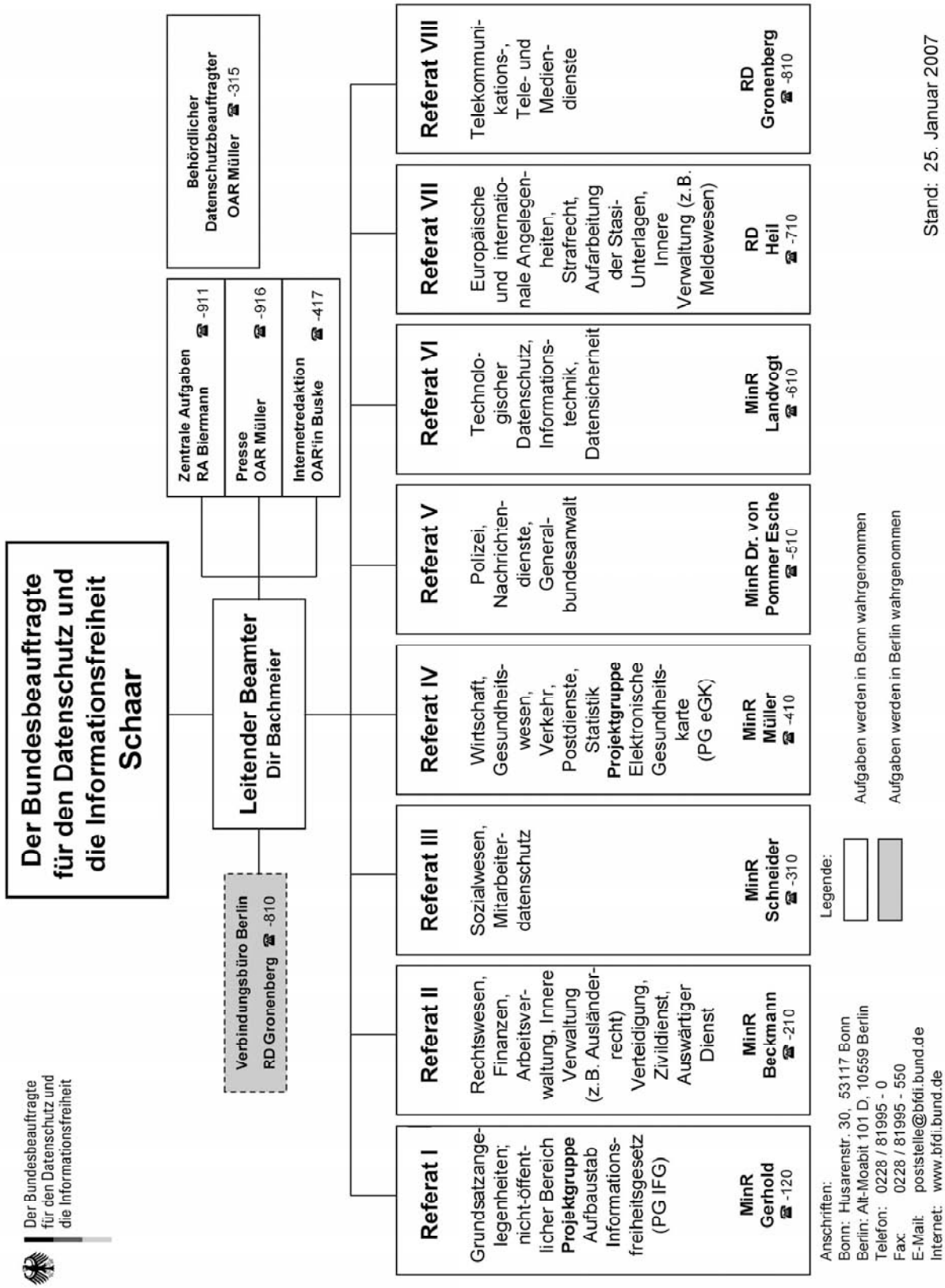
**SWIFT: Datenübermittlung im SWIFT–Verfahren in die USA**

Es wird festgestellt, dass die gegenwärtige Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA und die anschließende Herausgabe von dort gespeicherten Daten an US–amerikanische Behörden wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG–Datenschutzrecht unzulässig ist. Insbesondere verfügen die USA über kein angemessenes Datenschutzniveau im Sinne des Artikel 25 Abs. 1 und Abs. 2 der EG–Datenschutzrichtlinie. Rechtlich verantwortlich für die Übermittlung der Daten in die USA sind sowohl die in Belgien ansässige SWIFT, als auch die deutschen Banken, die sich trotz des Zugriffs der amerikanischen Behörden auf die bei SWIFT/USA gespeicherten Datensätze auch weiterhin der Dienstleistungen von SWIFT bedienen.

Die Banken werden aufgefordert, unverzüglich Maßnahmen vorzuschlagen, durch die im SWIFT-Verfahren entweder eine Übermittlung von Daten in die USA unterbunden werden kann oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden, damit der bislang mögliche Zugriff der US-amerikanischen Sicherheitsbehörden künftig ausgeschlossen ist. Eine Möglichkeit besteht nach Ansicht der Aufsichtsbehörden in der Verlagerung des zur Zeit in den USA gelegenen Servers in einen Staat mit einem angemessenen Datenschutzniveau. Eine weitere Möglichkeit besteht in einer wirksamen Verschlüsselung der in die USA übermittelten Zahlungsverkehrsinformationen. Es muss ausgeschlossen sein, dass die US-amerikanischen Behörden in die Lage versetzt sind, die auf dem dortigen Server gespeicherten Datensätze zu dechiffrieren. Die Aufsichtsbehörden erwarten eine ernsthafte Auseinandersetzung der Banken mit den aufgezeigten Möglichkeiten. Allgemeine Hinweise auf eine faktische oder ökonomische Unmöglichkeit sind nicht akzeptabel. Der Verweis auf einen in der Zukunft liegenden und noch keinesfalls feststehenden Abschluss eines völkerrechtlichen Abkommens zwischen dem EU-Rat und der US-Regierung vermag nicht den gegenwärtigen Handlungsbedarf zu beseitigen.

Unabhängig davon müssen die Banken gemäß § 4 Abs. 3 Bundesdatenschutzgesetz ihre Kundinnen und Kunden darüber informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges SWIFT Operating Center übermittelt werden. Dabei bleibt es den Banken überlassen, ob sie alle Kundinnen und Kunden über die Übermittlung der Datensätze an SWIFT/USA informieren oder nur diejenigen, für die die Dienste von SWIFT genutzt werden. Die Unterrichtung der Kundinnen und Kunden ist eine notwendige, wenn auch nicht hinreichende Mindestvoraussetzung für die Zulässigkeit der Übermittlung der Daten an SWIFT/USA. Sie ist unverzüglich umzusetzen.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht–öffentlichen Bereich nehmen das Anliegen der deutschen Banken zur Kenntnis, aus Gründen des Wettbewerbs eine europaweit einheitliche Lösung zu erreichen. Es soll in Zusammenarbeit mit den übrigen europäischen Datenschutz-Aufsichtsbehörden eine einheitliche Handhabung angestrebt werden.


Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Schaar
Leitender Beamter
Dir Bachmeier
Verbindungsbüro Berlin
RD Gronenberg ☎ -810
Behördlicher Datenschutzbeauftragter
OAR Müller ☎ -315
Zentrale Aufgaben
RA Biermann ☎ -911
Presse
OAR Müller ☎ -916
Internetredaktion
OAR'in Buske ☎ -417
Referat I
Grundsatzangelegenheiten; nicht-öffentlicher Bereich Projektgruppe Aufbaustab Informationsfreiheitsgesetz (PG IFG)
MinR Gerhold ☎ -120
Referat II
Rechtswesen, Finanzen, Arbeitsverwaltung, Innere Verwaltung (z.B. Ausländerrecht) Verteidigung, Zivildienst, Auswärtiger Dienst
MinR Beckmann ☎ -210
Referat III
Sozialwesen, Mitarbeiterdatenschutz
MinR Schneider ☎ -310
Referat IV
Wirtschaft, Gesundheitswesen, Verkehr, Postdienste, Statistik Projektgruppe Elektronische Gesundheitskarte (PG eGK)
MinR Müller ☎ -410
Referat V
Polizei, Nachrichtendienste, Generalbundesanwalt
MinR Dr. von Pommer Esche ☎ -510
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherheit
MinR Landvogt ☎ -610
Referat VII
Europäische und internationale Angelegenheiten, Strafrecht, Aufarbeitung der Stasi-Unterlagen, Innere Verwaltung (z.B. Meldewesen)
RD Heil ☎ -710
Referat VIII
Telekommunikations-, Tele- und Mediendienste
RD Gronenberg ☎ -810
Legende:
Aufgaben werden in Bonn wahrgenommen
Aufgaben werden in Berlin wahrgenommen
Stand: 25. Januar 2007
Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Anschriften:
Bonn: Husarenstr. 30, 53117 Bonn
Berlin: Alt-Moabit 101 D, 10559 Berlin
Telefon: 0228 / 81995 - 0
Fax: 0228 / 81995 - 550
E-Mail: poststelle@bfdi.bund.de
Internet: www.bfdi.bund.de

**Sachregister**

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.


@rtus 5.3.1

A2LL 13.5.3

Abgabenordnung (AO) 8.2

Abwesenheitszeiten 14.1

Adress- und Gebäuderegister 7.5

Ahnenforschung 7.4

Akustische Wohnraumüberwachung 6.2

Altdatenbereinigung 5.7.5

Altdatenbestände 5.7.5

Anhörung 5.8.3.1

Antiterrordateigesetz 5.1.1

Antragsformulare für Alg II 13.5.2

API-Richtlinie 3.3.3

Arbeitnehmerdatenschutz 2.7

Arbeits- und Gleitzeitkonten 14.1

Arbeitsgemeinschaften nach dem SGB II (ARGEn) 13.5.1; 13.5.4

Arbeitsverwaltung 13.5

Arbeitszeitdaten 19.7

Artikel 29-Gruppe 3.3; 3.3.1; 3.3.2; 3.3.3; 3.3.4; 3.3.6

Artikel 10-Gesetz 5.7.1

Audit 2.4

Auditverfahren 4.13

Aufsichtsbehörden 2.2

Aufsichtszuständigkeit für die ARGEn 13.5.4

Ausbildung 18.5

Auskunft 5.7.7

Auskunftsersuchen 13.1.3

Auskunftsverpflichtung 5.7.7

Ausländerrecht 7.1

Ausländerzentralregister (AZR) 7.1.1; 7.1.3

Ausschreibungen zur verdeckten Registrierung 3.2.4.2

Aussonderungsprüffrist 5.2.4.1

Auswärtiges Amt 17.1; 17.2

Ausweisdokumente 19.1

Ausweispflicht 11.1

Authentisierungsverfahren 4.4.1; 8.4

automatisierte Personaldatenverarbeitung 14.3

automatisiertes Fingerabdruck-Identifizierungs-System 5.2.4.2

autonome Systeme 4.12

Bahnhof 4.2.2

„Barmer Hausarzt und Hausapotheke“ 13.1.7

Basel II 9.2

Beamtenstatusgesetz 14.2

Bekämpfung der Schwarzarbeit 8.3

Beobachtung von Journalisten 5.7.2

Berufswahl Jugendlicher 13.5.5

Bestandsdaten 10.6

Bestellung betrieblicher Datenschutzbeauftragter 2.3

Betreuungsbehörde 6.8

Beurteilungsdaten 14.1

Binding Corporate Rules 3.3.6

Biometrie 4.5

biometrische Ausweisdokumente 4.5.3

biometrische Daten 7.1.4

biometrische Merkmale 4.5.4

biometrische Verfahren 19.1

Bonität 9.1

branchenspezifische Auskunftssysteme 9.1

Bundesagentur für Arbeit (BA) 19.6, 13.5; 13.5.5

Bundesamt für Güterverkehr (BAG) 12.1

Bundesamt für Migration und Flüchtlinge (BAMF) 7.1.2; 7.1.3

Bundesanstalt für Finanzdienstleistungen (BaFin) 9.3

Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) 7.2

Bundesamt für Verfassungsschutz (BfV) 5.5; 5.5.2; 19.13; 19.14

Bundeskriminalamt (BKA) 5.2; 5.2.4.1; 5.2.4.2; 5.2.5; 5.2.6; 19.10

Bundesmeldegesetz 7.3

Bundesmelderegister 7.3

Bundesnachrichtendienst (BND) 5.7; 5.7.4
Bundesnotarkammer 19.2
Bundespolizei 5.3; 5.8.3.1
Bundesrechtsanwaltskammer 9.7
Bundestag 4.2.3; 15;
Bundesverwaltungsamt (BVA) 14.3
Bundeswehr 16

Call-Center 10.3
Common Criteria 4.2.1

DALEB 13.5.5
Datei „Gewalttäter Sport“ 5.3.2
Datenabgleich 19.6
Datenlöschung 4.8
Datenschutz bei Rechtsanwälten 9.7
Datenschutz in der 3. Säule 3.2.1
Datenschutzaudit 2.4
Datenschutzaufsicht 2.2
Datenschutzbeauftragte der obersten Bundesbehörden 2.6
Datenschutzgütesiegel 4.13
datenschutzkonformer Betrieb 4.13
Datenschutzniveau 5.1.5; 11.2
Datenschutzrichtlinie 3
Datenschutz-Werkzeuge 4.13
Datensparsamkeit 4.13
Datenverarbeitung im Auftrag 2.5
Datenvermeidung 4.13
DDR 7.2.1
Deutsche Post AG 11.1
Deutsche Rentenversicherung Bund 13.4.1; 13.4.2
3Dface 4.5.1
Digital Rights Management 4.11
Digitales Rechtemanagement (DRM) 4.11; 6.6
digitalisiertes Lichtbild 4.5.3
Direktauszahlung 13.5.5
DNA-Analyse 6.3
DNA-Analyse-Dateien 3.2.2
Dokumentenmanagementsystem 5.6.1
Drittlandtransfer 3.3.6

e-Akte 4.7
eCall 12.2
eCard 4.4
EC-Karte 4.4.3
eGovernment 2.5; 4.7
Eigensicherung 5.7.2
Einwilligungserklärung 9.6
Einzelverbindungsnachweis 10.4; 10.5
EIS 3.2.3.1
elektronische Akte 19.13
elektronische Gesundheitskarte 4.1
elektronische Personalakte 4.7; 14.2
elektronische Personaldatenverarbeitung 14.3
elektronische Signaturverfahren 4.4
ELENA 4.6
ELSTER-Portal 4.4.1
ELSTER-Verfahren 8.4
E-Mail 10.4
Empfängerdateien 11.1
Entscheidungsfreiheit 4.13
ePass 4.3; 4.5.3
EPOS 2.0 14.3
Erhebungs- und Leistungssystem A2LL 13.5.3
erkennungsdienstliche Daten 5.2.4; 5.2.4.1
eSafety 12.2
Eurodac 3.2.8
Europäisches Amt für Betrugsbekämpfung 3.2.5
EUROPOL 3.2.3 ; 3.2.7
Evaluation 5.5.1
Evaluierungsbericht 5.1.2; 5.5.1
Event Data Recorder 12.3

Fast Identification 5.2.4.2
Fragebögen 13.1.3
Festplatten 4.8
Finanzkontrolle Schwarzarbeit (FKS) 8.3
Fingerabdruck-, Iris- und Gesichtserkennung 4.5
Flatrate-Tarife 10.5
flugmedizinische Untersuchung 12.6
Flugpassagierdaten 3.3; 3.3.2; 3.3.3
Folgenbeseitigungsanspruch 9.1

Forschungsdatenzentren 7.6
Fortentwicklungsgesetz 13.5.1
Foto-Fahndung 5.2.6
Föderalismusreform 7.3
Freitexte 5.2.2
Früherkennung von Krankheiten bei Kindern 19.8
Fundpapierdatenbank 19.1
Funketiketten 4.3
Funkzellenabfrage 6.1
Fußball-WM 2006 5.2.5

Gefahrenabwehr 5.2.1
Geldwäscherichtlinie 5.2.7
Geldwäscheverdachtsanzeige 5.2.7
Gemeinsame Kontrollinstanz (GK) 3.2.3; 3.2.4.2
Gemeinsames Terrorismusabwehrzentrum 5.1.4
Gemeinsame-Dateien-Gesetz 5.1.1
Genanalysen 6.3; 13.2
Gendiagnostikgesetz 13.2
genetischer Fingerabdruck 6.3
Genomanalyse im Strafverfahren 6.3
Gentests 13.2
Geomarketing 9.1
Georeferenzierung 7.5
Gesetzliche Krankenversicherung 13.1
Gesichtserkennung, Gesichtserkennungssystem 4.5; 5.2.6
Gesundheitsdaten 4.1
Gesundheitskarte 4.1
Gesundheitsreform 13.1.1.
GK Europol 3.2.3.2
Gleichstellungsbeauftragte 14.3
Grenzkontrolle 4.5.2
Großer Lauschangriff 6.2
Großraumbüros 13.5.5
Grundsatz der Verfügbarkeit 3.2.1
Gutachterregelung 13.3.1;13.3.2

Haager Programm 3.2.1
Handy-Ortung 6.4; 10.2
Hartz IV 13.5.1
häusliche Krankenpflege 13.1.8
HERKULES 16.1
Hersteller von Heil- und Hilfsmitteln 13.1.5
Hotlines 3.3.1

Identifikationsnummer für steuerliche Zwecke 8.1
Identitätsmanagement 4.4
IFOS Bund 19.11
Informationsaustausch 18.4
Informationsfreiheit 18.7
Informationsfreiheitsgesetz 2.8
Informationsverarbeitung beim MAD 5.6.1
INPOL 5.2.2
INPOL-Fall-System 5.2.2
Insolvenzbekanntmachungen 10.8.2
Integrationsgeschäftsdatei 7.1.2
Integrationskurse 7.1.2
integrierte Versorgung 13.1.7
Internationale Datenschutzkonferenz 3; 3.5; 10.10
Internet 5.1.3, 10.10.; 10.8; 10.8.1
Internetangebot der BA 13.5.5
Internetauftritt des BfDI 18.1
Internetdatenbanken 10.8.1
Interpol 3.2.6
INZOLL 5.4.2
IPR-Enforcement-Richtlinie 6.5
Irakkrieg 5.7.4
Iriserkennung 4.5; 4.5.2
IT-Gipfel 4.13
IT-Hosting 14.3
IT-Struktur beim BND 5.7.3
IVBB 4.9

Job-Card 4.6
Jugendamt 7.1.5
Jugendschutzgesetz 4.4.3
Jugendstrafvollzug 19.12

Kernbereich privater Lebensgestaltung 5.4.1
Kernbereichsschutz 5.7.1
Klageregister 19.3
Kleiderkasse der Bundeswehr 16.2

Kompetenzcheck 13.5.5
Konsultationsverfahren nach Artikel 17 Abs. 2 SDÜ 19.10
Kontenabruf 8.2
Kooperation 5.1.5
Kopierschutzregelung 10.8.2
Kraftfahrtbundesamt (KBA) 9.1; 12.5
Kraftfahrzeugversicherer 12.4
Krankenhausentlassungsberichte 13.3.3
Krankenversichertenkarte 13.1.6
Krankenversicherung 3.3.4; 13.1
kreditorisches Risiko 9.1
Kundendaten 10.6
Kundenprofile 9.1

lebens- oder verteidigungswichtige Einrichtung 5.8.2
LKW-Maut 12.1
Location Based Services 6.4; 10.2
Logdateien 4.9
Löschungsüberprüfungen 5.7.6
Luftfahrt-Bundesamt (LBA) 12.6
Luftsicherheitsgesetz 5.8.1

Malta 18.3
Massengentest 6.3
Mautdaten zur Verbrechensbekämpfung 12.1
Mediennutzungsgeheimnis 4.13
Meldepflicht 2.3
Melderechtsrahmengesetz 8.1
Merkmalsausprägung 4.5.1
Militärischer Abschirmdienst (MAD) 5.6; 19.9
Minderjähriger vor Vollendung des 16. Lebensjahres 5.7.6
Mitarbeiterdatenschutz 14; 14.4
Mittelstandsentlastungsgesetz 2.3
Modernisierung des Datenschutzrechts 2.1

Nachrichtendienste 3.2.7
Nachsendeantrag 11.1
nachweispflichtige Sendung 11.1
Nano-Technologie 4.12
Neuordnung des Beamtenrechts 14.2
Nutzungsverhalten 4.13

Observation 5.5.2
„offene“ Zusendung 17.2
öffentliche Ausschreibungen 13.1.9
öffentliche Petition 15.1
Öffentlichkeitsarbeit 18.2
Online-Anbindung 12.5
Online-Durchsuchung 5.1.3
Ortung 6.4; 10.2
Outsourcing 2.5; 16.1

Parlamentarisches Kontrollgremium 5.7.4
Patientenfahrten 13.1.9
Pay as You Drive 12.4
PERFIS 19.9
Personalakten 5.8.3.2; 14.3
Personalaktendaten 14.1; 14.3; Kasten zu Nr. 14.3
Personalaktengeheimnis 14.1; 14.2; 14.4
Personalausweis 4.5.3
Personalausweiskopien 13.5.5
Personaldaten, Personaldatenschutz 14.5; Kasten zu Nr. 14.3
Personalinformationssystem 14.3
Personalvertretung 14.3; 19.7
Personalverwaltungssystem 14.3
Personenstandsrecht 7.4
Petitionsausschuss 15.1; 15.2
Piktogramm 4.2.3
PNR 3.3.2; Kasten zu 3.3.2
Postablagestellen 11.1
Postgeheimnis 11.1
Postunternehmen 11
präventive Befugnisse 5.2.1
private „Hilfsmittelberater“ 13.1.5
Profilbildung 9.1
Profile 10.10
Protection Profiles 4.2.1
Protokolldaten 4.9
Prozesskostenhilfe 6.7

qualifizierte elektronische Signatur 4.4.1; 8.4
Qualitätssicherung 13.1.4

Rahmenbeschlussvorschlag über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit 3.2.1
Rasterfahndung 5.2.3
Ratingverfahren der Kreditinstitute 9.2
Ratspräsidentschaft 3.1
Rechnungsprüfungsdatei 13.3.4
Rechte am geistigen Eigentum 6.5; 10.9
Rechtsanwälte 9.7
Rechtsextremismus in der Bundeswehr 5.6.2
Rechtsfolgen 13.3.2
Rechtshilfe in Strafsachen 3.4
Reform des Datenschutzrechts 2.1
Rehabilitationsklinik 13.4.2
Rentenversicherung 13.4
Research-Systeme zur Aufdeckung von Geldwäsche 9.3
RFID 4.3
Risikostrukturausgleich 13.1.2
Rufnummernunterdrückung 10.3
Russland 3.1

Safe Habor 3.3.5
Schadprogramme 4.10
Scheinvaterschaften 7.1.5
Schengener Durchführungsübereinkommen (SDÜ) 3.2.4; 3.2.4.2
Schengener Informationssystem der zweiten Generation (SIS II) 3.2.4.1
Schutzprofil 4.2.1
Schweigepflichtentbindungserklärung 9.6; 13.1.3; 13.1.8
Scoreverfahren 9.1; 9.2
Scorewerte 9.1
Selbstauskunftsbögen 13.1.3
Selbstverpflichtung 13.3.1
sichere Grundeinstellungen 4.13
Sicherheitsarchitektur 5.1.4
Sicherheitsbehörden 3.2.7; 5.1; 5.1.1; 5.1.2; 5.1.3; 5.1.5;
Sicherheitsinfrastruktur 5.1
Sicherheitsüberprüfungen 5.8; 5.8.3; 5.8.3.1; 5.8.3.2; 5.8.4
Silikonfinger 4.5.1
Sozialleistungsmissbrauch 13
Spam 4.10
Staatsangehörigkeitsdatei 7.1.1
Stasi 7.2, 7.2.1
Stasi-Unterlagen-Gesetz (StUG) 7.2; 7.2.1
Statistisches Bundesamt (StBA) 7.5; 7.6
Steuerdatenabrufverordnung 19.5
Steuerdatenübermittlungsverordnung (StDÜV) 4.4.1; 8.4
Steuer-ID 8.1
Strafregister 3.4
Strukturreformgesetz 14.2
Suchmaschinen 10.10; 15.1
SWIFT 3.3; 9.4
Symposium 4.5.4
Symposium „Datenschutz bei der Telekommunikation und im Internet“ 10.11
Symposium „Datenschutz in der Telekommunikation und bei Telediensten“ 10.11

technikunterstützte Verfahren der Personalbewirtschaftung Kasten zu Nr. 14.3
Technologischer Datenschutz 4
Telekommunikationsdaten 10.1
Telekommunikationsgesetz 10.1
Telekommunikationsüberwachung 5.4.1; 6.1
Telemediengesetz 10.9
Terrorismusbekämpfungsgesetz 5.1.2
Ticketvergabeverfahren 5.2.5
Toll Collect 12.1
Transparenz 4.13
Trennungsgebot 5.1
Trusted Computing (TC) 4.11
Trusted Platform Module 4.11
Twinning-Projekt Malta 18.3

Überwachungsgesellschaft 3.5
Überweisungsdaten 9.4
Unfalldatenschreiber 12.3
Unfallversicherung 13.3
Unionsbürger 7.1.1
Uniwagnis 9.5

UPS 11.2
Urheberrecht 6.6
Urkundenüberprüfungsverfahren 17.1
USA 3.3; 3.3.2; Kasten zu 3.3.2; 9.4
USB-Sticks 4.8
US-Vertretungen 5.8.4

Verantwortungs- und Einstehensgemeinschaft 13.5.2
Verbindungsbüro 18.6
Vereinsrecht 7.1.6
Verfahrensvorschrift 13.3.2
Verfassung 3.1
Vergütungssystem 13.1.1
Verkehrstelematik 12
vermisste Personen/unbekannte Tote 3.2.6
Veröffentlichung von Mitarbeiterdaten 14.4
Verschlüsselung, -sverfahren 4.4.2
Versicherungswirtschaft 9.5
Vertrag von Prüm 3.2.2
Vertragsverletzungsverfahren 2.2
Vertraulichkeit von Petitionen 15.2
Verwaltungsermittlungen 14.5
Verwendung der Vertragsdaten für Kundenberatung 10.7
Videotechnik 4.2; 4.2.2
Videoüberwachung 4.2; 4.2.2
Videoüberwachungssystem 4.2.3
VISA-Informationssystem 3.2.7; 7.1.4
Visakodex 7.1.4
Visamissbrauch 7.1.4
vorbeugender personeller Sabotageschutz 5.8.2
Volkszählung 7.5
Vorgangsbearbeitungssystem 5.3.1
Vorratsdatenspeicherung 6.5; 10.1

Warn- und Hinweissystem 9.5
Werbung 10.6
Werbung und Marktforschung 10.7
Whistleblowing 3.3.1
Wirtschaftlichkeitsgebot 13.3.4

Zentrales Vorsorgeregister 19.2
Zigarettenautomaten 4.4.3
Zinsinformationsverordnung 19.4
Zollfahndung 5.4
Zollfahndungsdienstgesetz 5.4.1
Zollinformationssystem 3.2.5
Zollkriminalamt 5.4.1
Zugriffsberechtigungs- und Protokollierungskonzept 13.5.3
Zustellbesonderheiten 11.1
Zuverlässigkeitsüberprüfung 5.2.5; 5.8.1

**Abkürzungsverzeichnis/Begriffe**

| | |
|---|---|
| AA | Auswärtiges Amt |
| a.a.O | am angegebenen Orte |
| ABl. | Amtsblatt der Europäischen Gemeinschaften |
| ABMG | Autobahnmautgesetz |
| Abs. | Absatz |
| AEAO | Anwendungserlass zur Abgabenordnung |
| AFIS | Automatisches Fingerabdruck-Identifizierungssystem |
| AG | Aktiengesellschaft, aber auch: Arbeitsgruppe, Amtsgericht |
| AGB | Allgemeine Geschäftsbedingungen |
| AIS | Arbeitgeber-Informations-Service |
| ALG II | Arbeitslosengeld II |
| Alt. | Alternative |
| AO | Abgabenordnung |
| ARGE | Arbeitsgemeinschaften nach dem Sozialgesetzbuch II |
| ATDG | Antiterrordateigesetz |
| ATLAS | Internes Informatikverfahren der deutschen Zollverwaltung |
| AufenthG | Aufenthaltsgesetz |
| AufenthV | Aufenthaltsverordnung |
| AuslG | Ausländergesetz |
| AVV | Allgemeine Verwaltungsvorschrift |
| AWG | Außenwirtschaftsgesetz |
| Az. | Aktenzeichen |
| AZR | Ausländerzentralregister |
| AZRG | Gesetz über das Ausländerzentralregister |
| | |
| BA | Bundesagentur für Arbeit |
| BaFin | Bundesanstalt für Finanzdienstleistungen |
| BAföG | Bundesausbildungsförderungsgesetz |
| BAG | Bundesamt für Güterverkehr |
| BAköV | Bundesakademie für öffentliche Verwaltung |
| BAMF | Bundesamt für Migration und Flüchtlinge |
| BAN | Bundespolizeiaktennachweis |
| BArchG | Bundesarchivgesetz |
| BAZ | Bundesamt für den Zivildienst |
| BBG | Bundesbeamtengesetz |
| bDSB | behördlicher Datenschutzbeauftragter |
| BDSG | Bundesdatenschutzgesetz |
| BfA | Bundesversicherungsanstalt für Angestellte |
| BFD | Bundesbeauftragter für den Datenschutz |

| | |
|---|---|
| BfDI | Bundesbeauftragter für den Datenschutz und die Informationsfreiheit |
| BfD/BA | Beauftragter für den Datenschutz der Bundesanstalt für Arbeit |
| BfF | Bundesamt für Finanzen |
| BfV | Bundesamt für Verfassungsschutz |
| BGBl. | Bundesgesetzblatt |
| BIZ | Berufsinformationszentrum der BA |
| BKA | Bundeskriminalamt |
| BKAG | Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten |
| Bluetooth | Standard für die drahtlose Übermittlung von Sprache und Daten im Nahbereich |
| BMAS | Bundesministerium für Arbeit und Soziales |
| BMF | Bundesministerium der Finanzen |
| BMFSFJ | Bundesministerium für Familie, Senioren, Frauen und Jugend |
| BMG | Bundesministerium für Gesundheit |
| BMI | Bundesministerium des Innern |
| BMJ | Bundesministerium der Justiz |
| BMVBW | Bundesministerium für Verkehr, Bau- und Wohnungswesen |
| BMVg | Bundesministerium der Verteidigung |
| BMWi | Bundesministerium für Wirtschaft und Technologie |
| BND | Bundesnachrichtendienst |
| BNDG | Gesetz über den Bundesnachrichtendienst |
| BPol | Bundespolizei |
| BPolG | Bundespolizeigesetz |
| BR | Bundesrat |
| BR-Drs. | Bundesrats-Drucksache |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BStU | Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR |
| BT | Bundestag |
| BtBG | Betreuungsbehördengesetz |
| BVA | Bundesverwaltungsamt, aber auch: Bundesversicherungsamt |
| BVerfG | Bundesverfassungsgericht |
| BVerfGE | Entscheidungen des Bundesverfassungsgerichts |
| BVerfSchG | Bundesverfassungsschutzgesetz |
| BVerwG | Bundesverwaltungsgericht |
| BVV | Bundesvermögensverwaltung |
| BZR | Bundeszentralregister |
| BZRG | Bundeszentralregistergesetz |
| BZSt | Bundeszentralamt für Steuern |
| bzw. | beziehungsweise |
| | |
| ca. | circa |
| CC | Common Criteria |

| | |
|---|---|
| CD / CD-ROM | Compact Disc - Read Only Memory |
| Colibri | Computerunterstütztes Leistungsberechnungs- und Informationssystem (BA) |
| DALEB | Datenabgleich Leistungsempfänger-Beschäftigten-Datei |
| DB | Deutsche Bahn |
| d. h. | das heißt |
| DDR | Deutsche Demokratische Republik |
| DMP | Disease-Management-Programme |
| DANN | Desoxyribonoclein acid (acid=Säure) |
| Dok. | Dokument |
| DPMA | Deutsches Patent- und Markenamt |
| DRM | Digital Rights Management (Digitales Rechte Management) |
| Drs. | Drucksache |
| Düsseldorfer Kreis | Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich |
| DV/dv | Datenverarbeitung |
| e.V. | eingetragener Verein |
| E-Commerce | Elektronic Commerce/Elektronischer Handel |
| ED | Erkennungsdienst |
| EDPS | Europäischer Datenschutzbeauftragter |
| EDV | Elektronische Datenverarbeitung |
| EG | Europäische Gemeinschaft(en) |
| EG-ZIS | Europäisches Zollinformationssystem |
| EGGVG | Einführungsgesetz zum Gerichtsverfassungsgesetz |
| EIS | Europäisches Informationssystem |
| EHUG | Gesetz über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister |
| EJG | Eurojust-Gesetz |
| ELENA | Elektronischer Einkommensnachweis (JobCardverfahren) |
| ELSTER | Elektronische Steuererklärung |
| E-Mail | Electronic Mail |
| EMF | Elektromagnetische Felder |
| EP | Europäisches Parlament |
| EPC | Electronic Product Code — Der EPC besteht aus vier Datenblöcken zur Identifizierung der Version, des Herstellers, der Produktkategorie und des individuellen Gegenstands |
| EPCglobal | EPCglobal Inc. ist ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC). Die Aufgabe des Nonprofit-Unternehmens liegt in der kommerziellen Vermarktung sowie der Administration des EPC |
| EPOS | Elektronisches Personal-, Organisations- und Stellenmanagement-System |
| EStG | Einkommensteuergesetz |
| ETB | Elektronisches Tagebuch |

| | |
|---|---|
| etc. | ecetera |
| eTIN | Lohnsteuerliches Ordnungsmerkmal |
| EU | Europäische Union |
| EuGH | Europäischer Gerichtshof |
| Eurodac | Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern |
| Europol | Europäisches Polizeiamt |
| EVN | Einzelverbindungsnachweis |
| EWG | Europäische Wirtschaftsgemeinschaft |
| EWR | Europäischer Wirtschaftsraum |
| | |
| f. | folgend |
| FDZ | Forschungsdatenzentrum |
| ff. | folgende |
| FH Bund | Fachhochschule des Bundes für öffentliche Verwaltung |
| FIDE | automatisiertes Aktennachweissystem im Zollbereich |
| FIFA | Fédération Internationale de Football Association |
| FIU | Financial Intelligence Unit |
| FKS | Finanzkontrolle Schwarzarbeit |
| FVG | Finanzverwaltungsgesetz |
| | |
| G.10 | Artikel 10 Gesetz |
| GBA | Generalbundesanwalt beim Bundesgerichtshof |
| gem. | gemäß |
| GFG | Gemeinsame Finanzermittlungsgruppe |
| GG | Grundgesetz |
| ggf. | gegebenenfalls |
| GGO | Gemeinsame Geschäftsordnung der Bundesministerien |
| GJVollz-E | Gesetzentwurf zur Regelung des Jugendstrafvollzugs |
| GK | Gemeinsame Kontrollinstanz von Europol |
| GKI | Gemeinsame Kontrollinstanz von Schengen |
| GKV | Gesetzliche Krankenversicherung |
| GKV-WSG | Gesetz zur Stärkung des Wettbewerbs in der Gesetzlichen Krankenversicherung |
| GmbH | Gesellschaft mit beschränkter Haftung |
| GMBl | Gemeinsames Ministerialblatt |
| GMG | Gesetz zur Modernisierung der gesetzlichen Krankenversicherung |
| GTAZ | Gemeinsames Terrorismusabwehrzentrum |
| GwG | Geldwäschegesetz |

| | |
|---|---|
| Hartz-Kommission | Kommission „Moderne Dienstleistungen am Arbeitsmarkt“ |
| Hartz IV | Viertes Gesetz für moderne Dienstleistungen am Arbeitsmarkt |
| HKP | häusliche Krankenpflege |
| HPC | Health Professional Card |
| HTML | Hypertext Markup Language-Standardisierte Seitenbeschreibungssprache für Seiten im Internet/ Intranet |
| HVBG | Hauptverband der gewerblichen Berufsgenossenschaften |
| | |
| i.d.F. | in der Fassung |
| i.S.d. | im Sinne des (der) |
| i.S.v. | im Sinne von |
| i.V.m. | in Verbindung mit |
| ICAO | International Civil Aviation Organization |
| ICHEIC | International Commission on Holocaust Era Insurance Claims |
| IFG | Informationsfreiheitsgesetz |
| IFOS-Bund | Interaktives Fortbildungssystem für die Bundesverwaltung |
| IHK | Industrie- und Handelskammer |
| IKPO | Internationale Kriminalpolizeiliche Organisation |
| ILO | International Labour Organization |
| IMK | Ständige Konferenz der Innenminister und -senatoren der Länder |
| IMSI | International Mobile Subscriber Identity |
| InGe | Integrationsdatei |
| INPOL | Informationssystem der Polizei |
| InsO | Insolvenzordnung |
| INZOLL | Informationssystem der Zollverwaltung |
| IP | Internet Protocol |
| IPR | Internationales Privatrecht |
| IPSec | Internet Protocol Security |
| ISDN | Integrated Services Digital Network |
| ISO | International Organization for Standardization |
| IT | Informationstechnik |
| IVBB | Informationsverbund Berlin-Bonn |
| | |
| JI-Rat | Rat der Innen- und Justizminister der Europäischen Union |
| | |
| KapMuG | Gesetz über Musterverfahren in kapitalmarktrechtlichen Streitigkeiten |
| KBA | Kraftfahrt-Bundesamt |
| KFU | Krebsfrüherkennungsrichtlinien |
| Kfz | Kraftfahrzeug |
| KlagRegV | Klageregisterverordnung |
| KOM | Europäische Kommission |

| | |
|---|---|
| KuZ | Kundenzentrum der Zukunft (BA) |
| KWEÄ | Kreiswehrersatzämter |
| KWG | Kreditwesengesetz |
| LAN | Local Area Network |
| LfD | Landesbeauftragter für den Datenschutz |
| lit. | litera (=Buchstabe) |
| LKA/LKÄ | Landeskriminalamt/Landeskriminalämter |
| LuftSiG | Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz) |
| m.E. | meines Erachtens |
| MAD | Militärischer Abschirmdienst |
| MADG | Gesetz über den MAD |
| MAK | Mindestanforderungen an das Kreditgeschäft der Kreditinstitute |
| MDK | Medizinischer Dienst der Krankenversicherung |
| MRRG | Melderechtsrahmengesetz |
| MZG | Mikrozensusgesetz |
| NADIS | Nachrichtendienstliches Informationssystem |
| NJW | Neue Juristische Wochenschrift |
| Nr. | Nummer |
| NTS | Nato-Truppenstatut |
| o. a. | oben aufgeführt |
| o. g. | oben genannt |
| OECD | Organisation für wirtschaftliche Zusammenarbeit und Entwicklung |
| OFD | Oberfinanzdirektion |
| OK | Organisierte Kriminalität, aber auch: Organisationskomitee |
| OLAF | Europäisches Amt für Betrugsbekämpfung |
| PassG | Passgesetz |
| PAVOS | Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS) |
| PC | Personalcomputer |
| PEPSY | Personalverwaltungssystem des Auswärtigen Amtes |
| PERFIS | Personalführungs- und Informationssystem der Bundeswehr |
| PersauswG | Personalausweisgesetz |
| PKGr | Parlamentarisches Kontrollgremium |
| PNR | Passenger Name Record |
| Protection Profile | Schutzprofil |
| Ratsdok. | Ratskokument (EU) |
| RatSWD | Rat für Sozial- und Wirtschaftsdaten |

| | |
|---|---|
| Rdn. | Randnummer |
| Reha | Rehabilitation |
| RFID | Radio Frequency Identification – Transpondertechnik für die berührungslose Erkennung von Objekten |
| RFID-Chip | Radio Frequency Identification-Chip (Funkchip) |
| RSAV | Risikostrukturausgleichsverordnung |
| RVOrgG | Organisationsreform in der gesetzlichen Rentenversicherung |
| | |
| S. | Seite |
| s. | siehe |
| s. o. | siehe oben |
| s. u. | siehe unten |
| SCHUFA | Schutzgemeinschaft für allgemeine Kreditsicherung |
| SchwarzArbG | Schwarzarbeiterbekämpfungsgesetz |
| SDÜ | Schengener Durchführungsübereinkommen |
| SGB | Sozialgesetzbuch |
| SGB I | Sozialgesetzbuch Erstes Buch (Allgemeiner Teil) |
| SGB II | Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende) |
| SGB III | Sozialgesetzbuch Drittes Buch (Arbeitsförderung) |
| SGB IV | Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung) |
| SGB V | Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung) |
| SGB VI | Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung) |
| SGB VII | Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung) |
| SGB VIII | Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe) |
| SGB IX | Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen) |
| SGB X | Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz) |
| SGB XI | Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung) |
| SGB XII | Sozialgesetzbuch Zwölftes Buch (Sozialhilfe) |
| SigG | Signaturgesetz |
| SIS | Schengener Informationssystem |
| SMS | Short Message Service |
| SOG | Gesetz über öffentliche Sicherheit und Ordnung |
| sog. | so genannt |
| STADA | Staatsangehörigkeitsdatei |
| Stasi | Staatssicherheitsdienst der ehemaligen DDR |
| StDAV | Steuerdaten-Abruf-Verordnung |
| StDÜV | Steuerdatenübermittlungsverordnung |
| Steuer-ID | Identifikationsnummer für steuerliche Zwecke (steuerliches Identifikationsmerkmal/-nummer) |
| StGB | Strafgesetzbuch |
| StPO | Strafprozessordnung |
| StUG | Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz) |

| | |
|---|---|
| StVBG | Steuerverkürzungsbekämpfungsgesetz |
| StVergAbG | Steuervergünstigungsabbaugesetz |
| StVollzG | Strafvollzugsgesetz |
| SÜFV | Sicherheitsüberprüfungsfeststellungsverordnung |
| SÜG | Sicherheitsüberprüfungsgesetz |
| | |
| TAB | Büro für Technikfolgenabschätzung beim Deutschen Bundestag |
| TB | Tätigkeitsbericht |
| TBEG | Terrorismusbekämpfungsgesetz |
| TBG | Terrorismusbekämpfungsgesetz |
| TC | Trusted Computing |
| TK | Telekommunikation |
| TKG | Telekommunikationsgesetz |
| TOP | Tagesordnungspunkt |
| TPM | Trusted Platform Module |
| | |
| u. a. | unter anderem |
| u. ä. | und ähnliches |
| u. U. | unter Umständen |
| UIG | Umweltinformationsgesetz |
| UMTS | Universal Mobile Telecommunications System |
| US | United States |
| USB | Universal Serial Bus — eine Schnittstelle am PC |
| UStG | Umsatzsteuergesetz |
| usw. | und so weiter |
| | |
| VBM | vorläufiges Bearbeitungsmerkmal |
| VdAK | Verband der Angestellten-Krankenkassen |
| VDR | Verband Deutscher Rentenversicherungsträger |
| VG | Verwaltungsgericht |
| vgl. | vergleiche |
| VS | Verschlusssache |
| VIS | Visa-Informationssystem |
| vpS | Vorbeugender personeller Sabotageschutz |
| | |
| WiMax | Wordwide Interoperability for Microwave Access<br>Standard gemäß IEEE 802.16a für lokale Funknetze |
| WM | Weltmeisterschaft |
| WP | Working Paper |
| WPK | Wirtschaftsprüferkammer |
| WPO | Wirtschaftsprüferordnung |

| | |
|---|---|
| WPV | Versorgungswerk der Wirtschaftsprüfer |
| www | World wide web |
| | |
| z. B. | zum Beispiel |
| z. T. | zum Teil |
| ZAUBER | Abrufverfahren |
| ZDG | Zivildienstgesetz |
| ZFdG | Zollfahndungsdienstgesetz |
| ZIS | Zollinformationssystem |
| ZIV | Zinsinformationsverordnung |
| ZKA | Zollkriminalamt |
| ZORA | Zentralstelle für Risikoanalyse (Zoll) |
| ZPO | Zivilprozessordnung |
| ZSS | Zentrale Speicherstelle |
| ZStV | Zentrales Staatsanwaltschaftliches Verfahrensregister |

| Tätigkeitsbericht | Berichtszeitraum | Bundestagsdrucksachennummer |
|---|---|---|
| 1. | 1978 | 8/2460 |
| 2. | 1979 | 8/3570 |
| 3. | 1980 | 9/93 |
| 4. | 1981 | 9/1243 |
| 5. | 1982 | 9/2386 |
| 6. | 1983 | 10/877 |
| 7. | 1984 | 10/2777 |
| 8. | 1985 | 10/4690 |
| 9. | 1986 | 10/6816 |
| 10. | 1987 | 11/1693 |
| 11. | 1988 | 11/3932 |
| 12. | 1989 | 11/6458 |
| 13. | 1990 | 12/553 |
| 14. | 1991–1992 | 12/4805 |
| 15. | 1993–1994 | 13/1150 |
| 16. | 1995–1996 | 13/7500 |
| 17. | 1997–1998 | 14/850 |
| 18. | 1999–2000 | 14/5555 |
| 19. | 2001–2002 | 15/888 |
| 20. | 2003–2004 | 15/5252 |