Bayerischer Landtag
16. Wahlperiode

Drucksache 16/**6336**
01.12.2010

24. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

(gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes)

Berichtszeitraum 2009/2010

Drucksachen, Plenarprotokolle sowie die Tagesordnungen der Vollversammlung und der Ausschüsse sind im Internet unter www.bayern.landtag.de - Dokumente abrufbar. Die aktuelle Sitzungsübersicht steht unter www.bayern.landtag.de – Aktuelles/Sitzungen zur Verfügung.

Der Bayerische Landesbeauftragte für den Datenschutz

Nr. DSB/510 – 25 München, 01.12.2010

An die
Präsidentin
des Bayerischen Landtags
Frau Barbara Stamm
Maximilianeum

81627 München

24. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz

Sehr geehrte Frau Landtagspräsidentin,

in der Anlage übersende ich gem. Art. 30 Abs. 5 des Bayerischen Datenschutzgesetzes den 24. Bericht über die Tätigkeit des Landesbeauftragten für den Datenschutz.

Mit freundlichen Grüßen

Dr. Thomas Petri

Der Bayerische Landesbeauftragte für den Datenschutz informiert die Öffentlichkeit

24. Tätigkeitsbericht

Berichtzeitraum
2009/2010

24. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

gemäß Artikel 30 Absatz 5
des Bayerischen Datenschutzgesetzes

Berichtzeitraum: 2009/2010
Veröffentlichungsdatum: 01.02.2011

Inhaltsverzeichnis

1 Überblick ... 12

1.1 Das Internet lädt zu Verhaltensweisen ein, die der Rechtsstaat seit Jahrhunderten versucht zurückzudrängen ... 12

1.2 Reformen im Datenschutzrecht - Reformbedarf im Freistaat Bayern ... 13

1.2.1 Das Grundrecht auf Datenschutz ... 13

1.2.2 Uberlegungen zur Fortentwicklung der Europäischen Datenschutzrichtlinie 14

1.2.3 Stockholmer Programm ... 15

1.2.4 Vorratsspeicherung von Telekommunikations-Verkehrsdaten ... 16

1.2.5 Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsicht ... 16

1.2.6 Bundesdatenschutzgesetz - Novellen 2009 ... 18

1.2.7 Beschäftigtendatenschutz ... 20

1.3 Datenschutz und Informationsfreiheit ... 23

1.4 Öffentlichkeitsarbeit ... 23

1.5 Schlussbemerkung ... 24

2 IuK-Technik und Organisation ... 25

2.1. Grundsatzthemen ... 25

2.1.1 IT-Grundrecht ... 25

2.1.2 Die neue IuK-Organisation im Bayerischen Behördennetz ... 27

2.1.3 Übertragung kritischer Funktionalitäten an zentrale Einrichtungen - am Beispiel des Active Directory und der E-Mail-Server ... 28

2.1.4 Verschlüsselung im Bayerischen Behördennetz ... 30

2.1.5 Datenschutz in der Wolke - Cloud Computing ... 31

2.1.6 Benutzerstatistiken von Internetauftritten ... 32

2.1.7 Verpflichtung auf das Datengeheimnis und nach dem Verpflichtungsgesetz ... 35

2.2 Prüfungen, Kontrollen und Beratungen ... 36

2.2.1 Erkenntnisse ... 36

2.2.2 Sparen an der falschen Stelle ... 39

2.2.3 Freiberuflicher Datenschutzbeauftragter ... 40

2.2.4 Datenverlust im Krankenhaus ... 40

2.2.5 KV-Ident ... 42

2.2.6 TIZIAN ... 43

2.2.7 Mammographie-Screening ... 44

2.2.8 RFID-Benutzerausweise in der Münchner Stadtbibliothek ... 45

2.2.9 Kennzeichenbasierte Reisezeitmessung auf Autobahnen ... 46

2.2.10 Projekt elektronische Fallakte (eFA) im Städtischen Klinikum München ... 47

2.2.11 Elektronische Dokumentation und Abrechnung von Notarzteinsätzen (‘emDoc) ... 48

2.2.12 Fingerabdruckscanner als Zugangskontrollsysme ... 49
2.2.13 Auftragsdatenverarbeitung im Bereich Personalverwaltung ... 49
2.2.14 Einsatz eines elektronischen Türöffnungssystems ... 50
2.2.15 Übermittlung gaststättenrechtlicher Gestattungen per E-Mail an die örtliche Polizeidienststelle ... 51
2.2.16 Betrieb eines Internetcafes ... 51
2.2.17 Zusammenlegung der EDV-Administration einer Gemeinde und eines Kurbetriebs ... 52
2.3 Technische Einzelprobleme ... 53
2.3.1 Der Elektronische Personalausweis ... 53
2.3.2 Deutschland Online KFZ - Kfz-Zulassung über das Internet ... 56
2.3.3 Intelligente Stromzähler - Smart Meter ... 58
2.3.4 Fundsachen mit digitalen Inhalten ... 60
2.3.5 Beleg- und E-Mail-Archivierung ... 60
2.3.6 Unterarbeitsgruppe Krankenhausinformationssysteme ... 62

3 Polizei ... 65

3.1 Änderungen des Polizeiaufgabengesetzes ... 65
3.1.1 Verzicht auf eine "nur automatische Aufzeichnung" beim sog. Großen Lauschangrif ... 65
3.1.2 Regelung der Benachrichtigungspflicht bei der "polizeilichen Beobachtung" ... 67
3.1.3 Abschaffung der Befugnis zur heimlichen Wohnungsdurchsuchung ... 67
3.1.4 Kürzere Aufbewahrungsfrist für polizeiliche Bild- und Tonaufnahmen ... 67
3.2 Änderungen des Bayerischen Versammlungsgesetzes (BayVersG) ... 67
3.2.1 Bayerisches Versammlungsgesetz teilweise außer Kraft gesetzt - Die einstweilige Anordnung des Bundesverfassungsgerichts vom 17.02.2009 ... 68
3.2.2 Die Änderungen im Einzelnen ... 69
3.3 Ausgestaltung der "Vorratsdatenspeicherung" verfassungswidrig ... 71
3.4 Datenschutz und Versammlungsrecht ... 74
3.4.1 Polizeiliche Speicherung von Versammlungsanmeldern und -leitern ... 74
3.4.2 Videoüberwachung durch fest installierte Kameras ... 74
3.4.3 Datenschutzrechtliche Kontrolle von Übersichtsaufzeichnungen ... 74
3.5 Speicherungen in polizeilichen Dateien ... 75
3.5.1 Auskunftsablehnungen bei Speicherungen ... 75
3.5.2 Integrationsverfahren der Bayerischen Polizei - IGVP ... 76
3.5.3 Speicherungen im Kriminalaktennachweis ... 76

3.6 Pressearbeit der Polizei ... 77
3.7 Quellen-Telekommunikationsüberwachung ... 79
3.8 Videoüberwachung ... 80
3.8.1 Videoüberwachung öffentlicher Straßen und Plätze ... 80
3.8.2 Videoaufzeichnungen von Fußballfans ... 81
3.9 Erkennungsdienstliche Behandlungen ... 82
3.10 DNA-Maßnahmen ... 84
3.11 Akkreditierungsverfahren bei Großereignissen ... 85

4 Verfassungsschutz ... 86
4.1 Änderungen des Bayerischen Verfassungsschutzgesetzes (BayVSG) ... 86
4.2 Datenschutzrechtliche Prüfungen beim Verfassungsschutz ... 88
4.2.1 Protokolldatei für das Dokumentenmanagementsystem DOMEA ... 88
4.2.2 Speicherung von Kindern und Jugendlichen ... 88
4.2.3 Auskunftserteilungen durch das Landesamt für Verfassungsschutz und Bürgereingaben ... 89

5 Justiz ... 90
5.1 Gesetze und Rechtsverordnungen ... 90
5.2 Aus der Justiz allgemein ... 90
5.2.1 Videoüberwachung von Justizgebäuden ... 90
5.2.2 Bezeichnung des behördlichen Datenschutzbeauftragten im Geschäftsverteilungsplan und in sonstigen Verzeichnissen ... 91
5.2.3 Unbeabsichtigte Datenübermittlung bei der Benutzung von Sichtfensterumschlägen ... 92
5.2.4 Justiz und "Reality-TV" ... 92
5.3 Strafverfolgung ... 94
5.3.1 Einsatz von Hypnose bei der Aufklärung von Straftaten ... 94
5.3.2 Pressearbeit der Staatsanwaltschaften ... 95
5.3.3 Anordnung von Blutentnahmen bei Gefahr im Verzug ... 95
5.3.4 Kontenabfragen durch die Staatsanwaltschaft ... 97
5.4 Straf- und Maßregelvollzug ... 98
5.4.1 Brieföffnungen ... 98
5.4.2 Anwesenheit von Vollzugsbeamten bei der ärztlichen Untersuchung von Gefangenen in der Justizvollzugsanstalt ... 99
5.5 Ordnungswidrigkeitenverfahren ... 99
5.5.1 Videogestützte Geschwindigkeits - und Abstandsmessungen ... 99
5.5.2 Lichtbildabgleich in Bußgeldverfahren ... 100

6 Kommunales ... 101

6.1 Videoüberwachung öffentlicher Orte und Einrichtungen durch Kommunen ... 101

6.2 Videoüberwachung eines Wahllokals ... 102

6.3 Anfertigen von Fotografien der Gäste einer Erlebnistherme ... 103

6.4 Information der Presse über kommunale Angelegenheiten ... 105

6.5 Veröffentlichung von Karten und Luftbildern zum Solarpotential auf Gebäuden durch Kommunen im Internet ... 105

6.6 Bekanntgabe personenbezogener Daten der Einwender im Zusammenhang mit der Aufstellung eines Bebauungsplans ... 108

6.7 Nennung des Eingabeführers bei der Einholung einer Stellungnahme ... 109

6.8 Veröffentlichung personenbezogener Daten im amtlichen Mitteilungsblatt zur Benachrichtigung von Bürgern ... 111

6.9 Herausgabe eines Schreibens mit strafbarem Inhalt an den betroffenen Amtsträger ... 111

6.10 Auskunftserteilung über Behördeninformanten ... 112

6.11 Nachträgliche Bekanntgabe von in nichtöffentlicher Gemeinderatssitzung gefassten Beschlüssen ... 114

6.12 Anfertigen von Kopien von Unterstützungsunterschriften für Wahlkreisvorschläge ... 115

6.13 Melderegisterauskünfte in besonderen Fällen ... 117

6.14 Weitergabe von Melderegisterdaten Jugendlicher an die FreiwilligeFeuerwehr zur Nachwuchswerbung ... 117

6.15 Veröffentlichung von Gewerberegisterdaten im Sinne des § 14 Abs. 6 Satz 2 GewO auf der Homepage einer Gemeinde ... 118

7 Gesundheitswesen ... 120

7.1 Krebsregistrierung - Klinikregister datenschutzgerecht ausgestalten! ... 120

7.2 Schulgesundheitspflege - Pflicht zur Vorlage des Impfausweises und des gelben Kinderuntersuchungshefts? ... 121

7.3 Videoüberwachung in den Aufzügen eines Krankenhauses ... 122

7.4 Einsichtsrecht eines Angehörigen in Patientenakten eines Verstorbenen ... 124

7.5 Weitergabe von Behandlungsunterlagen an Rechtsanwälte ... 125

7.6 Veröffentlichung eines Notarzteinsatzprotokolls in Fernsehen und Internet ... 126

7.7 Verbundverfahren TIZIAN ... 128

8 Sozialwesen ... 129

8.1 Hausbesuche bei Eltern anlässlich der Geburt von Kindern ... 129

8.2 Vorlage eines ärztlichen Untersuchungsbogens durch Tagesbetreuungspersonen ... 130

8.3 Überprüfung von Laborabrechnungen durch ein "Kompetenzzentrum Labor" bei der Kassenärztlichen Vereinigung Bayerns ... 131
8.4 Elektronische Dokumentation und Abrechnung von Notarzteinsätzen ("emDoc") ... 133
8.5 Bereitstellung eines Internetdienstes "Arztsuche" ... 135
8.6 Erinnerung an Impfungstermin (Impf-Recall) ... 136
8.7 Datenübermittlung an Taxiunternehmen im Zusammenhang mit vertragsärztlichem Bereitschaftsdienst ... 137
8.8 Pflegeservice Bayern ... 138
8.9 Unzulässige Datenübermittlung durch einen Rentenversicherungsträger ... 139
8.10 Antrag auf Betreuungsleistungen ... 140
8.11 Jobcenter-Reform - Wechsel in der Zuständigkeit der Datenschutzkontrolle ... 141
8.12 Mangelnde Unterstützung des Landesbeauftragten für den Datenschutz ... 141
8.13 Weitergabe von Sozialdaten an eine Betriebskrankenkasse ... 142
8.14 Lebensmittelgutscheine ... 143
8.15 Vorlage von Kontoauszügen ... 144
8.16 Verräterischer Zusatz bei der Ablehnung von Auskünften an Dritte ... 145
8.17 Private Nutzung von Sozialdaten durch Mitarbeiter ... 146
8.18 Zusatzerklärung zum Leistungsantrag ... 146
8.19 Einzelne ARGE-Mitarbeiter: furcht- oder doch eher gedankenlos? ... 147
8.20 Beiblatt zum Sozialhilfeantrag ... 147
8.21 Verstoß gegen das Sozialgeheimnis ... 148

9 Steuer- und Finanzverwaltung ... 149

9.1 eGovernment in der Steuerverwaltung ... 149
9.1.1 Projekt RMS ... 149
9.1.2 Projekt ELSTEROnline ... 149
9.1.3 Projekt ELSTERLohn II ... 150
9.2 Nochmals: Auskunftsanspruch in der Abgabenordnung ... 151
9.3 Datenschutz bei Alterseinkünften ... 152
9.4 Bürgerentlastungsgesetz Krankenversicherung ... 153
9.5 Nochmals: Automatisierte Kontenabfrage im Besteuerungsverfahren ... 155
9.6 Adressierung von Steuerbescheiden ... 156
9.7 Prüfung des Servicezentrums des Finanzamts München ... 157
9.7.1 Tätigkeiten im Servicezentrum ... 158
9.7.2 Zugriffsrechte der Bediensteten auf Steuerdaten ... 158

9.7.3 Zugriffsrecht auf die zentrale Datenbank ZAUBER ... 158
9.7.4 Freie Suche nach Lohndaten - "Neugierabfragen" ... 159
9.7.5 Veranlagung von Steuerfällen ... 159
9.7.6 Diskretionsräume ... 160

10 Schulen und Hochschulen ... 161
10.1 Und nochmals: eGovernment-Projekt "Amtliche Schuldaten" ... 161
10.1.1 Schulverwaltung (Art. 85 a, 113 a BayEUG) ... 162
10.1.2 Schulstatistik (Art. 113 b BayEUG) ... 162
10.1.3 Zusammenfassung und Ausblick ... 162
10.2 Nochmals: Internetauftritt von Schulen ... 163
10.2.1 Grundsatz: schriftliche Einwilligung ... 163
10.2.2 Kein bloßes Widerspruchsrecht ... 163
10.2.3 Landeshauptstadt München: Einwilligungsformulare ... 164
10.2.4 Passwortgeschützter Bereich ... 164
10.3 Passwortgeschützte Lernplattformen wie "BayernMoodle" ... 165
10.3.1 Datenschutzrechtliche Problematik ... 166
10.3.2 Rechtsgrundlage: Einwilligung ... 166
10.3.3 Rundschreiben des Kultusministeriums ... 166
10.4 Weitergabe von Schülerdaten zu Werbezwecken ... 167
10.5 Meldungen von Erkrankungen an der Neuen Grippe durch Schulen ... 169
10.6 Datenschutz beim "Nationalen Bildungspanel" ... 170
10.6.1 Einwilligung ... 171
10.6.2 Umgang mit den erhobenen Daten ... 172
10.6.3 Fazit und Ausblick ... 173
10.7 Neuregelung der studentischen Evaluation der Lehre ... 173
10.8 Zugriff auf elektronische Notenkonten von Studierenden ... 175

11 Personalwesen ... 178
11.1 Neues Dienstrecht - Dienstunfallunterlagen und Beamtenversorgung ... 178
11.1.1 Dienstunfallunterlagen ... 178
11.1.2 Bayerisches Beamtenversorgungsgesetz ... 180
11.2 eGovernment-Großprojekte im Personalbereich - VIVA, BayZeit und BayRMS ... 183
11.2.1 Personal- und Stellenmanagementsystem VIVA ... 183
11.2.2 Zeitmanagementsystem BayZeit ... 185
11.2.3 Reisekostenmanagementsystem BayRMS ... 186
11.3 Drogentests bei der Einstellung neuer Mitarbeiter ... 187

11.4 Polizeiliche Daten zur Überprüfung von Bewerbern, Praktikanten und Fremdpersonal in der bayerischen Staatsverwaltung ... 189
11.5 Gesundheitsdaten von bayerischen Polizeibeamten ... 190
11.6 DNA-Reihentests im Finanzamt ... 191
11.7 Durchsicht der persönlichen Laufwerke aller Mitarbeiter ... 192

12 Spezielle datenschutzrechtliche Themen ... 194
12.1 Vorbereitung der Volkszählung 2011 ... 194
12.1.1 Bundesebene ... 194
12.1.2 Landesebene ... 196
12.1.3 Ausblick ... 196
12.2 Einheitlicher Ansprechpartner nach der EU-Dienstleistungsrichtlinie ... 196
12.3 Weitergabe von personenbezogenen Daten der Einwendungsführer an den Vorhabensträger in Planfeststellungsverfahren ... 198
12.4 Nochmals: Mitteilung Daten Reisegewerbetreibender an Industrie- und Handelskammern ... 199
12.5 Unzulässige Führung einer "Schwarzen Liste" als Entscheidungshilfe für die Verhängung von Fahrtenbuchauflagen ... 200
12.6 Regelmäßige Übermittlung personenbezogener Daten über die Entziehung von Fahrerlaubnissen an die Polizei ... 201
12.7 Weitergabe von Fahrzeug- und Halterdaten durch eine Kfz-Zulassungsstelle ... 201

13 Datenschutzkommission ... 204

Anlage 1: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.02.2009 Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes! ... 206
Anlage 2: Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz ... 207
Anlage 3: Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009 Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten! ... 208
Anlage 4: Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009 Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage ... 209
Anlage 5: Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009 Defizite beim Datenschutz jetzt beseitigen! ... 209
Anlage 6: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16.04.2009 Datenschutz beim vorgesehenen Bürgerportal unzureichend ... 210

Anlage 7: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur 212

Anlage 8: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben 213

Anlage 9: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Krankenhausinformationssysteme datenschutzgerecht gestalten! 213

Anlage 10: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 "Reality-TV" - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen 214

Anlage 11: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Datenschutzdefizite in Europa auch nach Stockholmer Programm 215

Anlage 12: Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Kein Ausverkauf von europäischen Finanzdaten an die USA! 216

Anlage 13: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung 217

Anlage 14: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Für eine umfassende wissenschaftliche Evaluierung imSicherheitsbereich 218

Anlage 15: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Körperscanner - viele offene Fragen 219

Anlage 16: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Keine Vorratsdatenspeicherung! 220

Anlage 17: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Ein modernes Datenschutzrecht für das 21. Jahrhundert 220

Anlage 18: Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010 Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle! 222

Anlage 19: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22.06.2010 Beschäftigtendatenschutz stärken statt abbauen 223

Anlage 20: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.06.2010 Erweiterung der Steuerdatenbank enthält große Risiken 224

Anlage 21: Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2010 Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz! 226

Anlage 22: Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010 Keine Volltextsuche in Dateien der Sicherheitsbehörden 227

Anlage 23: Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010 Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs 228

Anlage 24: Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010 Förderung des Datenschutzes durch Bundesstiftung 229

Abkürzungsverzeichnis **231**

Stichwortverzeichnis **235**

1 Überblick

1.1 Das Internet lädt zu Verhaltensweisen ein, die der Rechtsstaat seit Jahrhunderten versucht zurückzudrängen

Ein im Internet veröffentlichtes Video zeigt eine junge Frau, die vor laufender Kamera junge Hundewelpen in einem Fluss ertränkt. Ein Teil der Internetgemeinde macht innerhalb kürzester Zeit "die Schuldige" ausfindig. Die Folge: Eine junge Frau aus Oberbayern erhält telefonische Beschimpfungen bis hin zu Drohanrufen. Der Schönheitsfehler dabei: Als Täterin wird die Falsche identifiziert. Gleichwohl ist nicht nur ihr Ruf geschädigt, sie ist sogar auf Polizeischutz rund um die Uhr angewiesen. Dieses in der Presse jüngst berichtete Beispiel verdeutlicht: Wer Forderungen aufstellt, Straftäter in öffentlichen Medien wie dem Internet bekannt zu machen, muss sich redlicherweise stets auch die Fragen nach dem Missbrauch der verbreiteten Informationen und nach der Möglichkeit des Irrtums gefallen lassen. Das Internet als Pranger - mittelalterliche Methoden mithilfe modernster Technologie.

Ohne Zweifel bietet das Internet viele Informationen und viele Möglichkeiten der Kommunikation. Seine zahlreichen Verknüpfungsmöglichkeiten und die Vielzahl seiner Nutzer bieten viele Chancen, können aber auch dazu führen, dass für den Einzelnen erhebliche Risiken und Gefahren für seine Persönlichkeitsrechte entstehen.

Dieser Befund gilt auch für die öffentliche Hand. Glücklicherweise haben meine Prüfungen der bayerischen öffentlichen Stellen im Berichtszeitraum keine so dramatischen Erfahrungen wie den eingangs geschilderten Fall zutage gebracht. Allerdings nutzen auch öffentliche Stellen das Internet nicht mehr nur zur Gestaltung von eigenen Webseiten. Im Berichtszeitraum beispielsweise tauschten sich Mitarbeiter von JobCentern im Rahmen eines bekannten sozialen Netzwerkes über Empfänger von Sozialleistungen aus - mit zumindest personenbeziehbaren Daten (siehe hierzu Nr. 8.19). Um Kostendämpfung bemüht, ziehen immer mehr Kommunen das "Cloud Computing" ernsthaft in Betracht ohne zu berücksichtigen, dass eine solche Vergabe von Datenverarbeitung an Dienstleistungsanbieter im Internet datenschutzrechtlich problematisch ist (siehe hierzu Nr. 2.1.5). Bei einer Prüfung der Webseiten der bayerischen öffentlichen Verwaltungen musste ich feststellen, dass über zweihundert Stellen das Webanalysetool "Google Analytics" einsetzten. Mit dieser Software kann man das Nutzerverhalten von Webseitenbesuchern erforschen. Zugleich könnten die erfassten Daten an das Unternehmen Google übermittelt werden. Dies geschah teilweise ohne eine Unterrichtung der Betroffenen, geschweige denn mit ihrer Einwilligung (siehe hierzu Nr. 2.1.6). Schulen nutzen web2.0-Anwendungen als automatisierte Lernplattformen; hier hat das zuständige Ministerium auf meine Anregung hin datenschutzrechtlich angemessene Vorgaben entwickelt (siehe hierzu Nr. 10.3.3).

Die vorangegangenen Beispiele zeigen: Die öffentlichen Stellen haben das Internet und seine Möglichkeiten entdeckt. Sind sie sich aber auch in jedem Fall der Risiken für das Persönlichkeitsrecht bewusst? Es ist datenschutzrechtlich geboten, dass die Verwaltung nicht nur auf die vorhandene Schweigepflicht ihrer Be-

schäftigten setzt, sondern sich selbst und ihren Beschäftigten **Leitlinien für den Umgang mit dem Internet**, insbesondere mit dem "web2.0" gibt. Bei Bedarf stehe ich für Beratungen zur Verfügung.

1.2 Reformen im Datenschutzrecht - Reformbedarf im Freistaat Bayern

Das Bayerische Datenschutzgesetz ist ein gutes, klar strukturiertes Gesetz, das sich in vielfacher Hinsicht bewährt hat. Es ist allerdings nicht zu übersehen, dass es mittlerweile "in die Jahre" gekommen ist; die wesentlichen Teile des Gesetzes stammen aus dem Jahr 1993. Kann dieses Gesetz noch sachgerechte Antworten auf die Entwicklungen des Internet, insbesondere auf das web2.0 geben? Die Ankunft des "web3.0", des "Internet der Dinge" steht bereits konkret bevor. Es kündigt sich bereits mit Projekten wie der detailgenauen Stromerfassung in Privatwohnungen an ("smart metering", "smart grid", siehe hierzu Nr. 2.3.3). Das Bayerische Datenschutzgesetz muss internetfähig gemacht werden.

Bereits im Zusammenhang mit dem in der Vergangenheit beschriebenen Projekt TIZIAN habe ich auch auf die Entwicklung zu mehr **Verbunddateien** hingewiesen. Insoweit ist mittlerweile ein dringender Regelungsbedarf gegeben, nicht um die speichernden Stellen zu mehr Datenverbünden einzuladen, sondern um für sie sachgerechte Rahmenbedingungen zu schaffen und Grenzen zu setzen (siehe hierzu 23. Tätigkeitsbericht, Nr. 14.1). Mittlerweile liegen konkrete Überlegungen zu einer sachgerechten Regelung vor; sie sollten möglichst zeitnah in ein parlamentarisches Gesetzgebungsverfahren überführt werden.

Es würde den Rahmen dieser Übersicht sprengen, alle wesentlichen Reformen auf Europäischer Ebene, auf Bundes- und Landesebene darzustellen, die Auswirkungen auf das Datenschutzrecht in Bayern haben können. Insoweit sei auch auf die Einzeldarstellungen in den nachfolgenden Kapiteln verwiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat unter meiner Beteiligung ein Eckpunktepapier zur Modernisierung des Datenschutzrechts veröffentlicht. Die dort angestellten Überlegungen sind grundsätzlicher Natur und deshalb auch für den Freistaat Bayern von Bedeutung. Nach meiner Einschätzung ist angesichts der angedeuteten technischen Entwicklung vor Allem die Fortentwicklung des technischen und organisatorischen Datenschutzes geboten. Insoweit schlägt die Konferenz vor, die bisher im § 9 BDSG (in Bayern: Art. 7 BayDSG) beschriebenen Maßnahmen durch die Definition **technologieunabhängiger Schutzziele** zu ersetzen. Das Eckpunktepapier ist unter dem Titel "Ein modernes Datenschutzrecht für das 21. Jahrhundert" auf meinen Webseiten veröffentlicht.

1.2.1 Das Grundrecht auf Datenschutz

Im Berichtszeitraum sind zahlreiche Bemühungen zur Reform des Datenschutzrechts auf europäischer und nationaler Ebene im Gange gewesen, die Auswirkungen auf die Gesetzeslage in Bayern haben können.

Am 01.12.2009 ist der Vertrag von Lissabon in Kraft getreten, der mit erheblichen Veränderungen für die EU verbunden ist. Das Bundesverfassungsgericht hat ihn für verfassungsgemäß erklärt. Aus datenschutzrechtlicher Sicht ist hervorzuheben, dass mit der neuen Ordnung des Vertrags auch die Charta der

Grundrechte der Europäischen Union (ECGR) rechtsverbindlich geworden ist. Sie verbrieft in Art. 7 und in Art. 8 ein **Europäisches Grundrecht auf Datenschutz**:

Art. 7 ECGR
Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.

Art. 8 ECGR
(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.
(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

Der Vertrag von Lissabon sieht weiterhin vor, dass die EU der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) beitritt. Die Verbindlichkeit der Grundrechtecharta und der bevorstehende Beitritt zur EMRK bedeuten eine wichtige Stärkung des Grundrechtsschutzes in der Europäischen Union. Die grundrechtlichen Gewährleistungen aus Art. 7 und Art. 8 ECGR stehen allen Menschen zu, die sich im Gebiet der Europäischen Union aufhalten.

1.2.2 Überlegungen zur Fortentwicklung der Europäischen Datenschutzrichtlinie

Im Übrigen sind es unter anderem zwei EG-Richtlinien, die den Datenschutz auf nationaler Ebene prägen: Seit 1995 existiert bereits eine **allgemeine Datenschutzrichtlinie** (Richtlinie 95/46/EG). Sie verfolgte und verfolgt zwei Ziele: Einerseits soll die Richtlinie das Grundrecht auf Datenschutz auch im Europäischen Binnenmarkt zur Geltung bringen, andererseits soll zugleich der freie Verkehr von Daten gewährleistet werden. Diese Richtlinie wurde im Jahr 2002 durch besondere datenschutzrechtliche Vorschriften für die elektronische Kommunikation (Richtlinie 2002/58/EG) ergänzt. Diese Richtlinie ist durch verschiedene Richtlinien weiter entwickelt worden, unter anderem durch die nicht nur in Deutschland umstrittene Richtlinie zur Vorratsspeicherung von Telekommunikationsverkehrsdaten (Richtlinie 2006/24/EG).

Nach Einschätzung der Europäischen Kommission hat sich die allgemeine Datenschutzrichtlinie 95/46/EG bewährt, bedarf aber angesichts der neuen Herausforderungen einer Fortentwicklung. Die Europäische Kommission hat deshalb im Jahr 2009 eine öffentliche Anhörung zu den neuen Herausforderungen für den Datenschutz durchgeführt. Anfang November 2010 hat die Europäische Kommission ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“ vorgelegt (KOM (2010) 609 endg.), das erste Schlussfolgerungen aus der Anhörung zieht. Im Frühjahr 2011 sollen dann Antworten und neue Regelungsvorschläge auf diese Fragen folgen. Wer den Normfindungsprozess auf EU-Ebene kennt, weiß: Der Freistaat Bayern hat insoweit noch einige Jahre Zeit, bis neue Vorgaben der novellierten Datenschutzrichtlinie zu einem gesetzgeberischen Handeln zwingen. Ob es klug ist, solange zu warten, ist eine andere Frage.

1.2.3 Stockholmer Programm

Unter schwedischer Ratspräsidentschaft wurde das so genannte "Stockholmer Programm" verabschiedet, das die politischen Ziele für den Zeitraum 2010 - 2015 für einen "Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger" umfasst. Positiv zu bewerten ist zwar, dass das Programm den Schutz der Freiheitsrechte der Bürgerinnen und Bürger zur Priorität erhebt. Aus datenschutzrechtlicher Sicht ist jedoch zu befürchten, dass diese Zielsetzung lediglich einen Programmsatz ohne praktische Schutzwirkung für das Datenschutzrecht darstellt. Die konkreten Regelungen sehen neue zentrale EU-Datenbanken (etwa für Ein- und Ausreisen in die oder aus der EU) mit weitreichenden Eingriffen auch in die Persönlichkeitsrechte der EU-Bürgerinnen und -Bürger vor. Deshalb habe ich die Forderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder nachhaltig unterstützt, in Europa ein ausgewogenes Verhältnis zwischen Freiheit und Sicherheit insbesondere im Bereich der polizeilichen und justiziellen Zusammenarbeit herzustellen.

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009
Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem "Europa der Bürger". Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z.B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- *Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.*

- *Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.*
- *Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.*
- *Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.*
- *Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.*

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

Diese Forderungen sind auch vom Europäischen Parlament mit breiter Mehrheit unterstützt worden (vgl. Bundesrats-Drucksache 910/09).

1.2.4 Vorratsspeicherung von Telekommunikations-Verkehrsdaten

Nach den Bestimmungen der Richtlinie 2006/24/EG hat die Bundesrepublik Deutschland dafür Sorge zu tragen, dass ein Katalog von Telekommunikations-Verkehrsdaten für mindestens sechs Monate zu speichern ist. Die aufzubewahrenden Daten sollen den Sicherheitsbehörden zur Verfügung stehen. Mit Urteil vom 02.03.2010 hat das Bundesverfassungsgericht die Vorschriften zur Umsetzung dieser Richtlinie für nichtig erklärt (zu Einzelheiten siehe Nr. 3.3).

In ihrer 80. Konferenz haben die Datenschutzbeauftragten des Bundes und der Länder ihre bisher nahezu einhellige Ablehnung gegenüber der sechsmonatigen Vorratsdatenspeicherung bekräftigt, zugleich aber ihre Haltung etwas modifiziert. In tatsächlicher Hinsicht sehen die Datenschutzbeauftragten das so genannte Quick-Freeze-Verfahren als eine ernst zu nehmende Alternative zu einer sechsmonatigen Datenerfassung an. Hierunter verstehe ich die Möglichkeit von Sicherheitsbehörden, bei einem entsprechenden Sachverhalt unter den gesetzlichen Voraussetzungen die Anbieter von Telekommunikationsdienstleistungen zu einem "Einfrieren" vorhandener Daten zu verpflichten. Wer ein Quick-Freeze-Verfahren vorschlägt, muss allerdings auch dafür Sorge tragen, dass Daten zum "Einfrieren" für einen gewissen, kurzen Zeitraum zugreifbar vorhanden sind.

1.2.5 Entscheidung des Europäischen Gerichtshofs zur Unabhängigkeit der Datenschutzaufsicht

Unmittelbaren Handlungsbedarf löst ein Urteil des Europäischen Gerichtshofs vom 09.03.2010 (Rechtssache 518/07) aus, wonach die gegenwärtige Datenschutzaufsicht über die Privatwirtschaft gegen Art. 28 Abs. 1 der Datenschutzrichtlinie verstößt. Nach dieser Vorschrift sind in den Mitgliedstaaten eine oder mehrere öffentliche Stellen zu beauftragen, die Anwendung der innerstaatlichen

Vorschriften zur Umsetzung der Richtlinie zu überwachen. Diese Kontrollstellen haben die ihnen zugewiesenen Aufgaben in "völliger Unabhängigkeit" wahrzunehmen.

Art. 28 Abs. 1 Richtlinie 95/46/EG
Die Mitgliedstaaten sehen vor, dass eine oder mehrere öffentliche Stellen beauftragt werden, die Anwendung der von den Mitgliedstaaten zur Umsetzung dieser Richtlinie erlassenen einzelstaatlichen Vorschriften in ihrem Hoheitsgebiet zu überwachen.
Diese Stellen nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr.

Der Europäische Gerichtshof hat in seiner Entscheidung klargestellt, dass die Kontrollstellen **keinerlei äußerer Einflussnahme**, sei sie unmittelbar oder mittelbar, unterworfen sein dürfen (Rdnr. 30 der Entscheidung). Diese Anforderungen können regelmäßig nur erfüllt werden, wenn der Datenschutzkontrollinstanz eine institutionelle Unabhängigkeit eingeräumt wird. Damit steht die bis dahin übliche Rechts- und Fachaufsicht über die Datenschutzaufsicht durch die Innenministerien nicht im Einklang mit Europäischem Recht. Auch der bayerische Gesetzgeber muss deshalb die bisherige Form der Datenschutzaufsicht im Sinne der Vorgaben der Datenschutzrichtlinie verändern. Soll eine praxisgerechte Lösung gefunden werden, stehen dazu wohl zwei Wege im Raum. Erstens kann das bestehende Landesamt für Datenschutzaufsicht in eine unabhängige Behörde umgewandelt werden. Dann würde neben dem Bayerischen Landesbeauftragten für den Datenschutz eine weitere unabhängige Datenschutzbehörde entstehen. Angesichts der bereits bestehenden vielfältigen Aufgabenüberschneidungen kommt alternativ in Betracht, das Landesamt für Datenschutzaufsicht in den heute schon unabhängigen Bayerischen Landesbeauftragten für den Datenschutz - ggf. unter Beibehaltung beider Standorte - einzugliedern. Bis zum Redaktionsschluss dieses Tätigkeitsberichts stand die Entscheidung über die Zukunft der Datenschutzaufsicht in Bayern noch aus.

Die 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu den Folgerungen aus der Entscheidung des Europäischen Gerichtshofs eine Entschließung gefasst.

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 09.03.2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- *Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.*
- *Es darf keine Fach- und Rechtsaufsicht geben.*
- *Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.*
- *Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.*
- *Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.*
- *Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.*

1.2.6 Bundesdatenschutzgesetz - Novellen 2009

Im Jahr 2009 hat der Bundesgesetzgeber gleich dreimal das Bundesdatenschutzgesetz (BDSG) geändert. Aus Sicht des Datenschutzes im öffentlichen Bereich könnten insbesondere zwei Regelungen Auswirkungen auf den Freistaat Bayern haben.

Zunächst wurden die Grundsätze der **Datenvermeidung und Datensparsamkeit** in § 3 a verbindlicher gefasst.

§ 3 a Datenvermeidung und Datensparsamkeit
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

Die Prinzipien der Datenvermeidung und Datensparsamkeit sind mit dem Erforderlichkeitsprinzip verwandt. Als Grundnorm für das Konzept eines Datenschutzes durch Technik setzen die Grundsätze jedoch weit früher an, als es beispielsweise Art. 7 BayDSG tut. Nach dieser Vorschrift haben öffentliche Stellen die technischen und organisatorischen Maßnahmen zu treffen, die "erforderlich sind", die Ausführung des Datenschutzgesetzes zu gewährleisten. Anders als Art. 7 BayDSG knüpft § 3 a BDSG nicht erst bei dem Umgang mit personenbezogenen Daten an, sondern stellt bereits Anforderungen an die Auswahl und Ausgestaltung der technischen Verarbeitungssysteme. Die Einbeziehung des Datenschutzes in die Systeme und Verfahren würde spätere Datenschutzprobleme vermeiden helfen. Auch wenn man sich nicht die heutigen Modewörter "Privacy by Design" (Datenschutz durch Technikgestaltung) oder "Privacy by Default" (Datenschutz durch technische Voreinstellungen) zu Eigen macht, ist die

Festschreibung der Grundsätze der Datenvermeidung und Datensparsamkeit im Bayerischen Datenschutzgesetz in Ansehung der technischen Entwicklung zur allgegenwärtigen Datenverarbeitung längst überfällig.

In diesem Zusammenhang sei auch erwähnt, dass der Katalog der nach Art. 7 Abs. 2 BayDSG zu beachtenden technischen und organisatorischen Maßnahmen nach wie vor auf dem Stand des BDSG 1990 ist und verfassungsrechtlich begründete Grundsätze wie das **Trennungsprinzip** nach wie vor gesetzlich nicht ausdrücklich vorsieht (anders: Anlage Nr. 8 zu § 9 BDSG, Anlage Nr. 8 zu § 78 a SGB X).

Nr. 8 zu § 9 BDSG
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, …
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Gerade im Zusammenhang mit der gegenwärtigen Vernetzung von Datensystemen gewinnt das Trennungsprinzip zunehmend an Bedeutung (anschaulicher Anwendungsfall dazu: Nr. 2.2.1).

Unmittelbare Auswirkungen auf bayerische öffentliche Stellen als Auftragnehmer entfaltet weiterhin die **Neuregelung der Auftragsdatenverarbeitung** in § 11 BDSG. Auftragsdatenverarbeitung ist dadurch gekennzeichnet, dass der "Auftraggeber" eine andere Stelle mit der Durchführung bestimmter Datenverarbeitungsvorgänge beauftragt, die er ansonsten selbst ausführen müsste. Zugleich behält der Auftraggeber im Außenverhältnis die volle datenschutzrechtliche Verantwortlichkeit für den Umgang mit den personenbezogenen Daten. Nach der Novelle muss der Auftraggeber gemäß § 11 Abs. 2 eine ganze Reihe von Pflichten erfüllen, damit eine rechtskonforme Auftragsdatenverarbeitung vorliegt.

§ 11 Abs. 2 BDSG
Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. *der Gegenstand und die Dauer des Auftrags,*
2. *der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,*
3. *die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,*
4. *die Berichtigung, Löschung und Sperrung von Daten,*
5. *die nach Abs. 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,*
6. *die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,*
7. *die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,*

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

Von einigen bayerischen Behörden, die Daten im Auftrag von Bundesbehörden verarbeiten, bin ich mittlerweile darüber informiert worden, dass die Aufträge entsprechend der neuen gesetzlichen Vorgaben abgeändert worden sind. Der Gesetzesbegründung zufolge soll die Abänderung des § 11 Abs. 2 BDSG die bisherige Rechtslage klarstellen und damit die Verantwortlichkeit der Auftraggeber für die Rechtmäßigkeit der delegierten Datenverarbeitung verdeutlichen (vgl. Bundestags-Drucksache 16/12011, S. 40 f.). Es wäre deshalb zu überlegen, ob der bayerische Gesetzgeber entsprechende Klarstellungen in Art. 6 BayDSG ebenfalls vornimmt.

Trotz der zahlreichen Änderungen im Bundesdatenschutzgesetz besteht der Reformbedarf auf Bundesebene fort. Der Bundesminister des Inneren soll dazu beabsichtigen, zeitnah ein Eckpunktepapier zu einer Neukonzeption des Bundesdatenschutzrechts vorzulegen.

1.2.7 Beschäftigtendatenschutz

Im Spätsommer 2010 hat die Bundesregierung einen Gesetzentwurf zum Beschäftigtendatenschutz in den Bundestag eingebracht (Bundesrats-Drucksache 535/10), der voraussichtlich ebenfalls Auswirkungen auf die Beschäftigten bayerischer öffentlicher Stellen haben wird. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat seit Jahren immer wieder auf die Notwendigkeit der Regelung des Beschäftigtendatenschutzes hingewiesen, ohne dass je eine Bundesregierung einen Gesetzesentwurf in den Bundestag eingebracht hat. Unbestritten ist ein solches Regelungsprojekt angesichts der vielfältigen widerstreitenden Interessen ein schwieriges Unterfangen. Dass die Bundesregierung nun diesen überfälligen Schritt gegangen ist, ist deshalb - bei aller Kritik an Details - im Grundsatz verdienstvoll.

Wer sich intensiver mit den Fragen des Beschäftigtendatenschutzes befassen will, interessiert sich sicherlich dafür, dass die Bundestagsfraktion der SPD einen Ressortentwurf des Bundesministeriums für Arbeit und Soziales aus der 16. Legislaturperiode für ein Beschäftigtendatenschutzgesetz inhaltlich übernommen und zu Beginn der 17. Legislaturperiode in den Bundestag eingebracht hat (vgl. Bundestags-Drucksache 17/69). Auch die Fraktion Bündnis 90/Die Grünen hat einen eigenen Gesetzesentwurf zur Diskussion gestellt, ohne ihn allerdings im Berichtszeitraum in den Bundestag einzubringen (im Internet abrufbar unter http://beschaeftigten-datenschutz.de). Diese beiden Entwürfe unterscheiden sich im Grundansatz vom Entwurf der Bundesregierung insoweit, als sie den Be-

schäftigtendatenschutz nicht im BDSG, sondern in einem eigenständigen Gesetz regeln wollen.

Beide Reformansätze - Ergänzung des BDSG durch ein Kapitel über den Beschäftigtendatenschutz und eine bereichsspezifische Vollregelung - haben nachvollziehbare Argumente auf ihrer Seite. Für den Grundansatz der Bundesregierung spricht unter anderem, dass die Regelung des Beschäftigtendatenschutzes in einem Kapitel des BDSG zahlreiche Redundanzen und Verweisungen vermeidet. Für den Lösungsansatz der beiden genannten Oppositionsfraktionen lässt sich argumentieren, dass der Beschäftigtendatenschutz durchaus Besonderheiten aufweist, die eine bereichsspezifische Vollregelung nahelegt.

Letztlich wird es darauf ankommen, die berechtigten Verarbeitungsinteressen von Arbeitgebern mit den schutzwürdigen Rechtsgütern der Beschäftigten in ein angemessenes Verhältnis zu einander zu setzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat den politischen Willensbildungsprozess zum Beschäftigtendatenschutz intensiv begleitet. Unter anderem hat sie hierzu zwei Entschließungen verabschiedet.

Mit der Konferenz bin ich der Meinung, dass der Regierungsentwurf noch in einigen Punkten grundlegend zu verbessern ist.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22.06.2010
Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz "Qualität vor übereilten Regelungen" gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- *Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.*
- *Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur "Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten" würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln - etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.*
- *Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn - wie im Entwurf vorgesehen - Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv - und nicht erst auf Nachfrage - darüber aufzuklären, woher die verwendeten Daten stammen.*
- *Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.*
- *Die im Gesetzentwurf an mehreren Stellen vorgesehene "Einwilligung" der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-) Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.*

Im Sinne der jüngsten Entschließung zum Beschäftigtendatenschutz habe ich den Staatsminister des Innern gebeten, auf entsprechende Verbesserungen im

Rahmen der Beteiligung des Bundesrats hinzuwirken. Soweit anhand von Ausschussdrucksachen ersichtlich, hat der Freistaat im Rahmen seiner Stellungnahme überwiegend meine Empfehlungen aufgegriffen.

1.3 Datenschutz und Informationsfreiheit

Im Berichtszeitraum haben die Oppositionsfraktionen im Bayerischen Landtag im Ergebnis erfolglos jeweils einen Gesetzesentwurf zur Regelung des Zugangs zu Informationen im Freistaat Bayern (Informationsfreiheitsgesetz) in das Parlament eingebracht. Im Sinne der Transparenz öffentlicher Datenverarbeitung habe ich das Scheitern dieser Gesetzesinitiativen mit Bedauern zur Kenntnis genommen. Klarstellend möchte ich darauf hinweisen, dass ich eine inhaltliche Wechselbeziehung zwischen dem Recht auf Informationszugang und dem Datenschutz als gegeben ansehe (siehe hierzu 23. Tätigkeitsbericht, Nr. 2.7). Dementsprechend erhebe ich auch keine Bedenken gegen ein Informationsfreiheitsgesetz, wenn es Vorschriften enthält, die einen angemessenen Schutz personenbezogener Daten gewährleisten.

Im Berichtszeitraum haben sich mehrere Kommunen an mich gewandt, um die Übereinstimmung ihrer Informationsfreiheitssatzungen mit dem Datenschutzrecht überprüfen zu lassen. In solchen Fällen weise ich stets darauf hin, dass eine Informationsfreiheitssatzung den Vorrang des Gesetzes beachten muss. Konkret bedeutet dies: Die Vorgaben des Art. 19 BayDSG (teilweise in Verbindung mit Art. 17 Abs. 1 Nr. 2, Absätze 2 bis 4 BayDSG) für die Datenübermittlung an nichtöffentliche Stellen müssen auch in Informationsfreiheitssatzungen eingehalten werden.

1.4 Öffentlichkeitsarbeit

Die Bedeutung des Selbstdatenschutzes und der Datenschutzkompetenz habe ich bereits im vergangenen Tätigkeitsbericht hervorgehoben (siehe hierzu 23. Tätigkeitsbericht, Nr. 2.3). Allerdings müssen die Bürgerinnen und Bürger auch in die Lage versetzt werden, ihre Datenschutzrechte tatsächlich auch wahrnehmen zu können. Im Rahmen meiner Öffentlichkeitsarbeit habe ich deshalb besonderen Wert auf die Darstellung gelegt, welche konkreten Möglichkeiten die Bürgerinnen und Bürger haben, ihr Persönlichkeitsrecht zu schützen.

Mit meiner Broschüre zum Thema "Datenschutz im Krankenhaus" möchte ich Patientinnen und Patienten für typische datenschutzrechtliche Problemfelder eines Krankenhausaufenthalts sensibilisieren.

Mit Hilfe einer aus Sicht eines fiktiven Patienten erzählten Geschichte wird der Leser durch die verschiedenen Stationen eines Krankenhausaufenthalts geführt. In den Abschnitten "Bei der Aufnahme", "Auf der Station", "Auskünfte über mich", "Forschung mit meinen Daten" und "Nach dem Aufenthalt" werden jeweils wichtige datenschutzrechtliche Fragestellungen in einer für den fachlichen Laien verständlichen Art und Weise angesprochen. Auf detaillierte juristische Ausführungen zu den jeweiligen Rechtsvorschriften sowie auf komplexe technisch-organisatorische Darlegungen habe ich bewusst verzichtet.

Der Erfolg gibt diesem Konzept recht: Über 7.000 Exemplare dieser Broschüre sind bereits verteilt worden, darüber hinaus wird sie auch von meiner Webseite abgerufen.

Im Berichtszeitraum wurde von meiner Geschäftsstelle auch eine neue Orientierungshilfe zur "Auftragsdatenverarbeitung" erstellt und auf meiner Homepage veröffentlicht. Diese Orientierungshilfe

- zeigt die Vor- und Nachteile einer Auftragsdatenverarbeitung auf,
- erläutert die zu beachtenden Rechtsvorschriften und Formen der Auftragsdatenverarbeitung,
- weist auf die bestehenden Rechte und Pflichten von Auftraggeber und Auftragnehmer hin,
- gibt Hinweise bezüglich der Auswahl des Auftragnehmers und der Vertragsgestaltung,
- schildert die erforderliche Verfahrensweise bezüglich der Überprüfung der Einhaltung der Vertragsregelungen und
- grenzt die Auftragsdatenverarbeitung zur Funktionsübertragung ab.

Am 16.10.2010 nahm der Bayerische Landesbeauftragte für den Datenschutz zum ersten Mal am Tag der offenen Tür des Bayerischen Landtags teil. Dieses Ereignis nahm ich zum Anlass, die grundlegend überarbeitete Webseite meiner Dienststelle vorzustellen (www.datenschutz-bayern.de).

1.5 Schlussbemerkung

Die nachfolgenden Kapitel geben einen Überblick über meine Beteiligung an weiteren wesentlichen, hier nicht erwähnten Gesetzgebungsverfahren und meine Praxis der Datenschutzkontrolle der bayerischen öffentlichen Stellen im Berichtszeitraum 2009/2010.

2 IuK-Technilk und Organisation

2.1 Grundsatzthemen

2.1.1 IT-Grundrecht

Von grundlegender Bedeutung sowohl für den öffentlichen wie auch für den nicht-öffentlichen Bereich war im Berichtszeitraum das Urteil des Bundesverfassungsgerichts zur sog. Online-Durchsuchung (Urteil vom 27.02.2008, 1 BvR 370/07), mit dem Teile des Verfassungsschutzgesetzes Nordrhein-Westfalen für nichtig erklärt wurden. Hervorzuheben ist dabei die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst.

Dabei wurden die verfassungsrechtlichen Grundlagen des Datenschutzes an die technische Entwicklung angepasst und ein sog. "IT-Grundrecht" bzw. "Computer-Grundrecht" vom Bundesverfassungsgericht entwickelt. Dieses Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ergänzt das bislang schon aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) abgeleitete Recht auf informationelle Selbstbestimmung beim Einsatz informationstechnischer Systeme. Knapp 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt und ihn an die Herausforderungen des elektronischen Zeitalters angepasst. Mit dem IT-Grundrecht wird anerkannt, dass sich auf Personalcomputern und anderen IT-Systemen mit Wissen des Nutzers, aber vor allem auch unbemerkt, eine Vielzahl von persönlichen Informationen und Datenspuren befinden, die besonders zu schützen sind.

Die Datenschutzbeauftragten des Bundes und der Länder haben daher in ihrer Entschließung vom 03./04.04.2008 den Gesetzgeber u.a. dazu aufgefordert, sich aktiv für die Vertraulichkeit und Integrität von IT-Systemen durch Verbesserung der Regelungen zum Schutz der Betroffenen vor einer elektronischen Ausforschung einzusetzen.

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.04.2008
Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

1. *Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nichtig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. 25 Jahre nach dem Volkszählungsurteil hat das Bundesverfassungsgericht damit den Datenschutz verfassungsrechtlich weiter gestärkt*

und ihn an die Herausforderungen des elektronischen Zeitalters angepasst.

2. *Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer "elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government- und E-Commerce-Verfahren herzustellen.*
3. *Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.*
4. *Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.*
5. *Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.*
6. *Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.*
7. *Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:*
   - *Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.*
   - *Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.*
   - *Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.*

- *Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.*
- *Für die Durchführung von "Quellen-Telekommunikationsüberwachungen", die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.*

8. *Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z.B. bei der Überwachung der Telekommunikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.*

Die Entscheidung des Bundesverfassungsgerichts verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer "elektronischen Ausforschung" schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden.

Auch die öffentliche Verwaltung ist aufgefordert, bereits jetzt verfügbare und von mir seit langem geforderte Maßnahmen zu ergreifen. Konkret bedeutet dies z.B., dass

- dem Nutzer endlich standardmäßig die Möglichkeit zur vertraulichen, d.h. verschlüsselten, Kommunikation per E-Mail zumindest angeboten wird,
- Formulareingaben standardmäßig verschlüsselt über das Web übertragen und
- auf aktive Komponenten für den Aufruf von Web-Seiten verzichtet werden, weil dafür der Nutzer u.U. seine sonstigen Sicherheitseinstellungen aufheben oder zumindest aufweichen muss.

Will der Nutzer angebotene Schutzmaßnahmen nicht anwenden, so ist dies seine eigene Entscheidung. Er sollte dann aber von der öffentlichen Stelle wenigstens über die möglichen Risiken unterrichtet werden.

Mit einer derartigen Umsetzung der verfassungsrechtlichen Vorgaben würde ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government-Verfahren herzustellen.

2.1.2 Die neue IuK-Organisation im Bayerischen Behördennetz

Am 19.05.2009 wurde Staatssekretär im Bayerischen Staatsministerium der Finanzen Franz Josef Pschierer zum Beauftragten für Informations- und Kommunikationstechnik der Bayerischen Staatsregierung (CIO Bayern) bestellt.

Der CIO Bayern verfügt über umfassende Befugnisse zur ressortübergreifenden strategischen Steuerung und Koordinierung des IT-Einsatzes in der Staatsverwaltung. Dabei wird er unterstützt durch seine neu gegründete Stabsstelle mit ih-

ren drei Referaten sowie durch den Rat der Ressort-CIOs. Dem Rat der Ressort-CIOs arbeitet die sog. Vorkonferenz der IT-Referenten der Ressorts zu. Beiden Gremien stehe ich als beratendes Mitglied zur Verfügung.

Sowohl mit der CIO-Stabsstelle als auch dem CIO selbst stehe ich überdies in unmittelbarem Kontakt und Informationsaustausch.

Die früher im Staatsministerium des Innern eingerichtete Zentrale IuK-Leitstelle (ZIL) sowie der IuK-Fachausschuss wurden durch die neu gegründete Stabsstelle des CIO ersetzt.

Im Hinblick auf diese neue IuK-Organisationsstruktur bin ich zuversichtlich, dass die durch die Vorgängerstrukturen bereits eingeschlagenen Wege weiter und mit noch mehr Nachdruck als bisher verfolgt werden. Damit betroffen sind auch meine langjährigen Forderungen nach flächendeckenden Maßnahmen zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität innerhalb des Behördennetzes und auch bei der Kommunikation des Bürgers mit der staatlichen Verwaltung.

2.1.3 Übertragung kritischer Funktionalitäten an zentrale Einrichtungen - am Beispiel des Active Directory und der E-Mail-Server

Vermutlich schon solange es IT im größeren Umfang in Unternehmen und Behörden gibt, gibt es immer wieder sich umkehrende Trends, entweder hin zu zentralisierten IT-Ressourcen (Rechenzentren) oder hin zu dezentralisierten Standorten in den einzelnen Bereichen (verteilte Betriebsstätten). Vor allem aus wirtschaftlichen Gründen verspricht gegenwärtig die Reduzierung der Standorte niedrigere Gesamtkosten.

Der Freistaat Bayern ist seit dem Beschluss des Ministerrats vom 29.7.2003, die bisherigen Rechen- und IT-Betriebszentren der Staatsverwaltung organisatorisch in zwei Rechenzentren zusammenzufassen, auf dem Weg der Zentralisierung, der aber noch nicht abgeschlossen ist. Sowohl die Heterogenität der vorhandenen IT-Anwendungen als auch die Heterogenität der Aufgaben der Staatsverwaltung verhindern zum Teil ein schnelles Zusammenwachsen der vorhandenen IT. Dies resultiert auch aus der verfassungsrechtlich zu beachtenden Ressortunabhängigkeit, die jedem Staatsminister zusichert, seinen Geschäftsbereich selbständig und unter eigener Verantwortung gegenüber dem Landtag gemäß den vom Ministerpräsidenten bestimmten Richtlinien der Politik zu führen.

Art. 51 Abs. 1 Verfassung des Freistaates Bayern
Gemäß den vom Ministerpräsidenten bestimmten Richtlinien der Politik führt jeder Staatsminister seinen Geschäftsbereich selbständig und unter eigener Verantwortung gegenüber dem Landtag.

In der Verwaltung des Freistaates Bayern wird überwiegend als Verzeichnisdienst ein Active Directory (AD) verwendet. Allerdings gab es bei der Einführung und der Erweiterung des AD unterschiedliche Ziele und Vorgehensweisen der einzelnen, zum Teil unabhängigen Teilnehmer, so dass es zu einigen Problemen kam, die nun gelöst werden müssen. Bis vor kurzem wurde das AD hauptsächlich dezentral von den einzelnen Teilnehmern, d.h. Behörden, administriert und gepflegt. Bedingt durch die Produkteigenschaften können, wie mir immer wieder versichert wurde, bestimmte Fehler und Nachlässigkeiten einzelner Teilnehmer

aber das ganze System in einen potentiell unsicheren Zustand bringen oder sogar zu einem völligen Ausfall führen. Auch ließe sich für Administratoren mit geringeren Rechten nicht generell verhindern, dass diese sich unerlaubt höhere Rechte verschaffen.

Um beide Probleme schnell zu lösen, wurde beschlossen, den Betrieb des AD komplett in die Hände der Rechenzentren zu legen. Unter der Voraussetzung, dass diese keine Fehler machen, lässt sich so verhindern, dass die Verfügbarkeit des Systems reduziert wird. Und unter der Voraussetzung, dass die Administratoren in den Rechenzentren ihre Rechte nicht missbrauchen, kann man auch verhindern, dass unerlaubte Zugriffe stattfinden.

Zentrale IT bringt aber nicht nur Vorteile, sondern hat auch Nachteile. Die Nutzer (und auch der Behördenleiter) können nicht mehr direkt mit den IT-Verantwortlichen und den Administratoren in Kontakt treten, die Reaktionszeiten auf neue oder geänderte Anforderungen können deutlich länger werden. Ebenso führt auch erfahrungsgemäß eine "Entfernung" von den eigenen Daten zu einer Reduzierung des diesbezüglichen Datenschutzbewusstseins. Es entsteht das Gefühl, die eigenen Daten und Anwendungen wären im Rechenzentrum schon sicher aufgehoben und von Problemen wird viel weniger durchdringen. Aber auch im Rechenzentrum lässt aufgrund der zu bewältigenden Datenmassen unter Umständen die Sensibilität für einzelne verarbeitete Daten nach.

Selbst wenn sich das Ausfallrisiko für einzelne, vorher autonom administrierte Teilbereiche durch eine unter Umständen professionellere Administration reduzieren kann, steigt das Ausfallrisiko für das Gesamtsystem etwa durch einen Software- bzw. Administrationsfehler an zentraler Stelle. Tritt ein solcher Schadensfall im zentralen System ein, dann ist davon unter Umständen die gesamte IT des Freistaates Bayern betroffen.

Für einen Angreifer, der versucht, sich Zugriff auf Daten und Systeme zu verschaffen, ist ein Rechenzentrum ein attraktives Ziel, da er bei einem erfolgreichen Angriff unter Umständen vollen Zugriff auf Daten der gesamten Staatsverwaltung erlangt. Dezentrale Datenbestände bieten unter Umständen mehrere Angriffspunkte, aber ein erfolgreicher Angriff bleibt auf eine deutlich kleinere Teilmenge öffentlicher Stellen beschränkt. Deshalb habe ich auch gefordert, nicht einfach alle Dienste, hier im speziellen das Active Directory, zu zentralisieren und dann zu hoffen, dass sich damit alle Probleme lösen. Geboten ist vielmehr ein Gesamtkonzept, das sicherstellt, dass ein zuverlässiger Betrieb (Datensicherheit) der Systeme und Anwendungen ohne Reduzierung des Datenschutzniveaus möglich ist. Dies ist aber bis heute leider noch nicht geschehen.

Auch wenn mit der Zentralisierung des AD noch nicht begonnen wurde, so ist bereits heute klar, dass in nicht allzu ferner Zukunft auch eine Zentralisierung aller Exchange-Server notwendig werden wird. Denn zumindest in den folgenden Produktversionen wird es nicht mehr möglich sein, die Administration des AD von der der Exchange-Server getrennt zu halten.

Dies wird dazu führen, dass alle Benutzerkonten, alle Postfächer, Kalender etc. von einer zentralen Stelle aus zugreifbar sein werden. Auf den zentralen Rechnern sind die E-Mails in der Regel unverschlüsselt gespeichert, so dass auf dort gespeicherte personenbezogene Daten auch Personen außerhalb der originär hierzu berechtigten Stelle zugreifen können. Auch wird es immer wieder nötig sein, Mitarbeitern externer Firmen im Wartungsfall umfassende Rechte einzu-

räumen. Es ist zu berücksichtigen, dass auch Dokumente, die besonderen Berufs- und Amtsgeheimnissen unterliegen oder sonstige sensitive oder politisch brisante Informationen enthalten, dadurch potentiell gefährdet wären.

Dass die Gefahr einer Veröffentlichung von geschützten Daten nicht rein theoretischer Natur ist, zeigen Webseiten wie Wikileaks, die sich zum Ziel gesetzt haben, Informationen ohne Autorisierung oder amtliche Genehmigung aufzudecken - trotz intensivster Bemühungen um deren Geheimhaltung. Deshalb muss alles unternommen werden, nicht nur den funktionalen Schadensfall an Systemen und Anwendungen zu vermeiden, sondern auch den Umfang der Daten, die im Schadensfall kompromittiert werden würden, so weit wie möglich zu reduzieren.

Die einzige Möglichkeit, die Administration und den IT-Betrieb außerhalb des eigenen Bereichs zu geben, besteht aus datenschutzrechtlicher Sicht in der sogenannten Datenverarbeitung im Auftrag gemäß Art. 6 BayDSG. Danach entscheidet der potenzielle Auftraggeber unter Berücksichtigung evtl. bestehender bereichsspezifischer Vorschriften über deren generelle Zulässigkeit. Im Falle einer Auftragsdatenverarbeitung bleibt er aber unverändert für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen (Art. 6 Abs. 3 Satz 2 BayDSG). Für einige Behörden oder ggf. ganze Behördenzweige wird eine solche Auftragsvergabe danach aufgrund bereichsspezifischer Vorschriften schwierig bis unmöglich sein.

Deshalb muss jede Behörde genau prüfen, ob und unter welchen Umständen sie Dienstleistungen, Daten und Verfahren in ein Rechenzentrum verlagern kann. Da jede Behörde verantwortlich bleibt, muss sie über eventuell notwendige Maßnahmen wie Verschlüsselung, die Ausnahme von Diensten von der Zentralisierung, die Kontrolle der Auftragsdatenverarbeitung und die genaue vertragliche Ausgestaltung selbst entscheiden.

Die zwischen den Rechenzentren und den entsprechenden Dienststellen getroffenen Vereinbarungen zur Datenverarbeitung im Auftrag so wie deren technische Umsetzung werde ich zum gegebenen Zeitpunkt überprüfen.

2.1.4 Verschlüsselung im Bayerischen Behördennetz

Immer wieder begegnet mir das Wort vom "sicheren" Bayerischen Behördennetz. In dieser Pauschalität kann das aber nicht einfach so angenommen werden, denn es muss im Gegenzug sofort gefragt werden: Sicher gegen welche Bedrohung? Gegen Angriffe von außen, wenn ja gegen welche Angriffsszenarien, gegen Verfügbarkeitseinschränkungen, gegen Angriffe von innen, wenn ja gegen welche Arten, gegen Vertraulichkeits-, Integritäts- und/oder Authentizitätsverlust bzgl. der darüber übertragenen Daten, …?

Gegen alle diese Bedrohungsformen sind Maßnahmen getroffen und es sollen weitere ergriffen werden (siehe Nr. 2.1.3). Aber insbesondere hinsichtlich der Vertraulichkeits-, Integritäts- und Authentizitätsaspekte besteht noch immer dringender Handlungsbedarf. Seit meinem 19. Tätigkeitsbericht habe ich immer wieder diese Themenbereiche aufgegriffen und die zügige flächendeckende Einführung geeigneter Verfahren zu Signatur und Verschlüsselung sowie der zugehörigen Infrastruktur angemahnt. Bisher sind wir leider immer noch weit davon entfernt.

Zum Ende 2010 findet nun für das Bayerische Behördennetz (BayKOM 2010) nach erfolgter Ausschreibung ein Wechsel des Providers statt. Teil der Ausschreibung war, dass das bereitgestellte Datennetz einen Grundschutz hinsichtlich der Vertraulichkeit der Kommunikation gewährleisten soll, d.h. zwischen den Endpunkten der angemieteten Leitungen (Edge-Router) soll nach den Maßgaben und unter Kontrolle der staatlichen Verwaltung eine sog. Leitungsverschlüsselung stattfinden. Ich begrüße diesen Ansatz ausdrücklich und gehe davon aus, dass dieser nun auch konsequent angegangen und mit Betriebsaufnahme bereits vollständig umgesetzt ist und dass nicht widrige Umstände erneut zu einer Hintanstellung dieser Sicherheitsmaßnahmen führen.

Gleichzeitig weise ich in aller gebotenen Deutlichkeit darauf hin, dass es sich bei dieser Leitungsverschlüsselung wirklich nur um einen Grundschutz handelt und auch damit keineswegs von BayKOM 2010 als dem sicheren Behördennetz gesprochen werden kann. Damit allein ist nämlich noch nicht einmal eine durchgängige Vertraulichkeit der übertragenen Information sichergestellt. Ohne weitere Maßnahmen, z.B. Verschlüsselung von E-Mails durch den Absender, werden die übertragenen Daten auf Teilstrecken des Behördennetzes ungeschützt übertragen und insbesondere auf den entsprechenden Servern vor unbefugter Kenntnisnahme ungeschützt gespeichert. Außerdem wird den Ansprüchen auf Integrität und Authentizität der übertragenen Daten ohne zusätzliche Maßnahmen zu der von BayKOM 2010 bereitgestellten Leitungsverschlüsselung in keiner Weise Rechnung getragen. Dafür sind andere technische und organisatorische Maßnahmen erforderlich.

Im Übrigen ist die Kommunikation mit Einrichtungen und Personen außerhalb des Bayerischen Behördennetzes durch die netzseitig bereitgestellte Maßnahme, die sich nur innerhalb des Bayerischen Behördennetzes auswirkt, ebenso wenig geschützt.

2.1.5 Datenschutz in der Wolke - Cloud Computing

Unter dem Begriff "Cloud Computing" verbirgt sich eine Vielzahl unterschiedlicher Technologien, die aber in der Regel bedeuten, dass Verfahren und Daten auf externe, virtuelle Systeme ausgelagert werden.

Bei "Software as a Service" werden die Anwendungen nicht mehr lokal ausgeführt, sondern laufen komplett auf der Infrastruktur des Anbieters. Der Kunde hat hier in aller Regel keine Möglichkeit, die Anwendung zu kontrollieren. Unter "Platform as a Service" versteht man, dass der Anbieter die Kontrolle über das Betriebssystem hat und der Kunde eigene Anwendungen installieren kann. Und schließlich gibt es noch "Infrastructure as a Service". Hier mietet der Kunde nach Bedarf Ressourcen wie Arbeitsspeicher, Datenspeicher und Rechenzeit.

Sofern personenbezogene Daten gespeichert oder verarbeitet werden, kann es sich aus Sicht des Datenschutzes um Fälle der Auftragsdatenverarbeitung handeln. Der Auftraggeber bleibt in solchen Fällen für die Einhaltung des Datenschutzes verantwortlich.

Im Vergleich zur "normalen" Auftragsdatenverarbeitung ist bei Cloud Computing die Überprüfung der Zuverlässigkeit des Anbieters noch wichtiger. Da etwaig vorhandene Sicherheitskonzepte auf Grund der Virtualität weitgehend abstrakt

gehalten sind, muss der Kunde darauf vertrauen, dass alle Detailprobleme sicher und korrekt gelöst werden. Ein reines "Vertrauen müssen" ist aus Sicht der IT-Sicherheit jedoch eine schlechte Lösung.

Nach Art. 6 BayDSG sind Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihnen getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse konkret festzulegen sind. Der Auftraggeber hat sich soweit erforderlich von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen. Bereichsspezifische Vorschriften, wie z.B. § 80 SGB X, stellen weitere Anforderungen.

Bei den meisten am Markt befindlichen Anbietern für Cloud Dienste ist es für den öffentlichen Auftraggeber praktisch ausgeschlossen, diese gesetzlichen Anforderungen zu erfüllen. Die hohe Flexibilität und Skalierbarkeit, die ein Ziel von Cloud Computing sind, bedingen, dass eben nicht genau festgelegt ist, wo und wie genau die Daten verarbeitet werden. Beispielsweise können Daten im Arbeitsspeicher, auf Festplatten oder im Extremfall auch auf Bändern gespeichert werden. Der Kunde kann also nicht den Speicherort oder die Speicherart bestimmen, sondern nur, dass er eine gewisse Speicherkapazität mit bestimmten Eigenschaften benötigt.

Viele Cloud Anbieter legen ihr internes Betriebsmodell aus Wettbewerbsgründen nicht offen. Um die Skalierbarkeit auch in Zukunft gewährleisten zu können, gibt es meist keine Aussagen, wo sich die Rechenzentren befinden bzw. wo die Daten der Kunden (im Moment) verarbeitet und gespeichert werden. Sich "von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen beim Auftragnehmer zu überzeugen", etwa mit einem eigenem Audit vor Ort, ist damit in der Regel unmöglich.

Es ist deshalb für öffentliche Stellen notwendig, bei der Inanspruchnahme von Cloud Diensten äußerste Zurückhaltung walten zu lassen.

2.1.6 Benutzerstatistiken von Internetauftritten

Verständlicherweise möchten viele Betreiber von Internetauftritten ("Homepages") in Erfahrung bringen, wie ihr Internetangebot genutzt wird. Dazu bietet sich an, die Zugriffe auf die einzelnen Seiten selbst zu protokollieren und auszuwerten oder sich einer der vielen zum Teil kostenlosen Dienste zu bedienen.

In früheren Tätigkeitsberichten sowie in meiner Orientierungshilfe "Gestaltung des Internetauftritts" habe ich bereits darauf hingewiesen, dass die Protokollierung von IP-Adressen zu diesem Zweck grundsätzlich nicht zulässig ist, da die Bestimmungen der §§ 13 und 15 Telemediengesetz (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist hier jedoch kein Pseudonym im Sinne des Telemediengesetzes.

§ 13 Abs. 1 TMG
Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten

sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist. Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

§ 15 TMG
(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind insbesondere

1. *Merkmale zur Identifikation des Nutzers,*
2. *Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und*
3. *Angaben über die vom Nutzer in Anspruch genommenen Telemedien.*

…
(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Neben einer eigenen Auswertung der Protokolldateien kann man alternativ auch eine Vielzahl von externen Analysediensten benutzen, so dass man so auf eine eigene Protokollierung verzichten kann. Die Speicherung der unter Umständen personenbezogenen Nutzerstatistiken erfolgt dann beim Dienstleister. Verantwortlich für die Speicherung und Auswertung bleibt aber nach wie vor der Betreiber der Webseite, auch wenn die Speicherung nicht unmittelbar bei ihm stattfindet. Die rechtliche Unzulässigkeit im Bezug auf das Telemediengesetz bleibt davon unberührt.

Der Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich vom 26./27.11.2009 "Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten" kommt zu demselben Ergebnis.

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 26./27.11.2009
Datenschutzkonforme Ausgestaltung von Analyseverfahren zur Reichweitenmessung bei Internet-Angeboten

Viele Web-Seitenbetreiber analysieren zu Zwecken der Werbung und Marktforschung oder bedarfsgerechten Gestaltung ihres Angebotes das Surf-Verhalten der Nutzerinnen und Nutzer. Zur Erstellung derartiger Nutzungsprofile verwenden sie vielfach Software bzw. Dienste, die von Dritten kostenlos oder gegen Entgelt angeboten werden.

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen darauf hin, dass bei Erstellung von Nutzungsprofilen durch Web-Seitenbetreiber die Bestimmungen des Telemediengesetzes (TMG) zu beachten sind. Demnach dürfen Nutzungsprofile nur bei Verwendung von Pseudonymen erstellt werden. Die IP-Adresse ist kein Pseudonym im Sinne des Telemediengesetzes.

Im Einzelnen sind folgende Vorgaben aus dem TMG zu beachten:

- *Den Betroffenen ist eine Möglichkeit zum Widerspruch gegen die Erstellung von Nutzungsprofilen einzuräumen. Derartige Widersprüche sind wirksam umzusetzen.*
- *Die pseudonymisierten Nutzungsdaten dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Sie müssen gelöscht werden, wenn ihre Speicherung für die Erstellung der Nutzungsanalyse nicht mehr erforderlich ist oder der Nutzer dies verlangt.*
- *Auf die Erstellung von pseudonymen Nutzungsprofilen und die Möglichkeit zum Widerspruch müssen die Anbieter in deutlicher Form im Rahmen der Datenschutzerklärung auf ihrer Internetseite hinweisen.*
- *Personenbezogene Daten eines Nutzers dürfen ohne Einwilligung nur erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Jede darüber hinausgehende Nutzung bedarf der Einwilligung der Betroffenen.*
- *Die Analyse des Nutzungsverhaltens unter Verwendung vollständiger IPAdressen (einschließlich einer Geolokalisierung) ist aufgrund der Personenbeziehbarkeit dieser Daten daher nur mit bewusster, eindeutiger Einwilligung zulässig. Liegt eine solche Einwilligung nicht vor, ist die IP-Adresse vor jeglicher Auswertung so zu kürzen, dass eine Personenbeziehbarkeit ausgeschlossen ist.*

Werden pseudonyme Nutzungsprofile durch einen Auftragnehmer erstellt, sind darüber hinaus die Vorgaben des Bundesdatenschutzgesetzes zur Auftragsdatenverarbeitung durch die Anbieter einzuhalten.

Auch der wohl am häufigsten genutzte Dienst "Google Analytics" verstößt ohne die ausdrückliche Einwilligung der betroffenen Nutzer gegen das Telemediengesetz. Eine andere Sicht kann sich nur dann ergeben, wenn eine von Google angebotene Anonymisierung mittels IP-Maske (anonymizeIP) verwendet wird. Sie verkürzt die IP4-Adresse und erschwert damit die Zuordnung der Analysedaten zu einem bestimmten Nutzer. Doch auch in diesem Fall müssten zahlreiche Voraussetzungen erfüllt sein, damit die Auswertung den Anforderungen des Telemediengesetzes genügt.

Im Laufe des Jahres 2010 unterzog ich die Internetauftritte von allen Ministerien, Fachbehörden, Landratsämtern, Städten und Gemeinden in Bayern einer technischen Untersuchung hinsichtlich der dortigen Verwendung von Google Analytics. Im Schnitt nutzten knapp 10 Prozent davon den Dienst, nur zwei Behörden setzten dabei die Anonymisierung mittels IP-Maske ein.

Ich habe daraufhin die bayerischen Behörden aufgefordert, auf den Einsatz von Google Analytics gänzlich zu verzichten oder zumindest einen Zusatzcode zu verwenden, der die Identität von Webnutzern verschleiert.

2.1.7 Verpflichtung auf das Datengeheimnis und nach dem Verpflichtungsgesetz

Immer wieder erkundigen sich Dienststellenleiter und Datenschutzbeauftragte von bayerischen Behörden und Kommunen bei meiner Geschäftsstelle danach, ob ihre Bediensteten sowohl auf das Datengeheimnis als auch nach dem Verpflichtungsgesetz zu verpflichten sind. Dazu ist Folgendes festzustellen:

Gemäß Art. 5 BayDSG ist es den bei öffentlichen Stellen beschäftigten Personen untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

Die Tätigkeit öffentlicher Stellen besteht zu einem erheblichen Teil aus dem Umgang mit personenbezogenen Daten. Die Regelung des Art. 5 BayDSG hat die Funktion, den bei solchen Stellen tätigen Personen bewusst zu machen, dass dem Schutz vor unzulässigen Beeinträchtigungen des Persönlichkeitsrechts bei der Tätigkeit öffentlicher Stellen ein besonderer Stellenwert zukommt.

Eine bis zur Neufassung des BayDSG vom 23.07.1993 ausdrücklich geforderte Belehrung der Beschäftigten im Sinne einer förmlichen Verpflichtung auf das Datengeheimnis sieht das BayDSG seither nicht mehr vor. In der Gesetzesbegründung zu Art. 5 BayDSG heißt es hierzu: "Die (...) vorgesehene förmliche Verpflichtung auf das Datengeheimnis entfällt künftig nach dem Vorbild von § 5 BDSG. Im öffentlichen Bereich sind förmliche Verpflichtungen auf das Datengeheimnis entbehrlich. Die Mitarbeiter haben aufgrund dienst- oder arbeitsrechtlicher Vorschriften Verschwiegenheit über die ihnen bei ihrer Tätigkeit bekannt gewordenen Angelegenheiten zu wahren. Sie sind entweder als Amtsträger vereidigt oder über ihre Schweigepflicht belehrt oder nach dem Verpflichtungsgesetz auf die gewissenhafte Erfüllung ihrer Obliegenheiten verpflichtet worden".

Eine Verpflichtung nach dem Verpflichtungsgesetz kommt gemäß § 1 Abs. 1 Nr. 1 des Gesetzes über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz) hinaus nur für Personen infrage, die bei einer Behörde oder bei einer sonstigen Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt, beschäftigt oder für sie tätig sind, ohne Amtsträger (§ 11 Abs. 1 Nr. 2 des Strafgesetzbuches) zu sein. In diesem Fall ist auch eine Belehrung über das Datengeheimnis dringend zu empfehlen.

Mit Hilfe des Verpflichtungsgesetzes soll bei Personen, die nicht Amtsträger sind, eine den Amtsträgern annähernd vergleichbare strafrechtliche Verantwortlichkeit bei Korruption, Geheimnisverrat und Verwahrungsbruch herbeigeführt werden.

Neben diesen Personen der eigenen öffentlichen Stelle ist insbesondere im Rahmen einer Auftragsdatenverarbeitung darauf zu achten, dass der Auftragnehmer für die auftragsgemäße Verarbeitung personenbezogener Daten nur Personal einsetzt, das auf das Datengeheimnis nach § 5 BDSG und nach dem Verpflichtungsgesetz verpflichtet wurde.

2.2 Prüfungen, Kontrollen und Beratungen

2.2.1 Erkenntnisse

Im Berichtszeitraum 2009/2010 wurde von mir eine ganze Reihe öffentlicher Stellen unter technisch-organisatorischen Datenschutzaspekten geprüft und beraten. Teilweise wurden diese Prüfungen und Beratungen von meinem Technikreferat gemeinsam mit dem zuständigen Rechtsreferat durchgeführt. Besonders hervorzuheben sind folgende Stellen:

- ARGE Nürnberg mit vier Standorten und Zentrale
- Finanzamt München - Servicezentrum
- Kassenärztliche Vereinigung Bayerns (KVB)
- Klinikum Bayreuth
- Klinikum Memmingen
- Klinikum Nürnberg
- Landeshauptstadt München - Ausländeramt im Kreisverwaltungsreferat
- Landeshauptstadt München - Stadtbibliothek
- Landratsamt Bamberg - Veterinäramt
- Landratsamt Landshut - Zulassungstelle
- Landratsamt Roth
- Landratsamt Schweinfurt - Veterinäramt
- Psychiatrische Klinik des Universitätsklinikum Würzburg
- Psychiatrische Klinik des Universitätsklinikum Erlangen
- Regierung der Oberpfalz - EU-Dienstleistungsrichtlinie
- Stadt Ansbach - Passamt
- Stadt Fürstenfeldbruck - Passamt
- Stadt Schweinfurt
- Stadt Bayreuth - Passamt
- Stadtwerke Bayreuth

Generell ist festzustellen, dass alle Stellen bemüht sind, dem Datenschutz grundsätzlich Rechnung zu tragen und die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen und umzusetzen. Gleichwohl zeigen sich nach wie vor vielerorts noch Schwachstellen hinsichtlich der zeitlich und inhaltlich angemessenen Beteiligung und Einbindung des jeweiligen behördlichen Datenschutzbeauftragten. Auch eine große Zahl von Internetauftritten genügt nach wie vor nicht immer vollständig den Anforderungen des Telemediengesetzes, z.B. derart, dass keine Möglichkeit zur Verschlüsselung von E-Mails angeboten wird oder dass die Datenschutzerklärung nicht von jeder Seite aus leicht auffindbar und unmittelbar erreichbar ist. Da ist noch einiges Verbesserungspotential gegeben.

Leider musste ich in diesem Berichtszeitraum im technisch-organisatorischen Bereich auch drei Beanstandungen nach Art. 31. Abs. 1 BayDSG aussprechen.

Die **erste Beanstandung** betraf **Staatliche Schulämter einer Stadt und des betreffenden Landkreises**. Diese übermittelten mittels unverschlüsseltem Dateianhang an eine E-Mail personenbezogene Daten aller Lehrkräfte aus dem Schulamtsbezirk an alle Schulleiter der Volksschulen in der Stadt und an den Personalratsvorsitzenden der Stadt. Bei dem Dateianhang der versandten E-Mail handelte es sich um eine Excel-Mappe bestehend aus drei Tabellenblät-

tern. Beabsichtigt war lediglich der Versand eines dieser drei Tabellenblätter mit personenbezogenen Daten aller zu beurteilenden Lehrkräfte in der Ansparphase der Altersteilzeit im Blockmodell in der Stadt - ohne jeweiliges vorläufiges Beurteilungsprädikat. Das Löschen der beiden überschüssigen Tabellenblätter wurde wegen hohen Zeitdrucks vergessen. In der irrigen Annahme, dass die Excel-Datei nur aus dem einen Tabellenblatt ohne Beurteilungsprädikatseintragungen bestünde, wurde auch keine Verschlüsselung der Datei vorgenommen. Sofort nach Bekanntwerden der Datenübermittlung haben die Staatlichen Schulämter in der Stadt und im Landkreis versucht, die E-Mail automatisch zurückzurufen. Darüber hinaus wurden die Empfänger der E-Mail mittels Telefax auf ihre Dienstpflicht zum Stillschweigen hingewiesen und zum Vernichten der übersandten Listen, d.h. des Dateianhangs der E-Mail, aufgefordert. Schließlich haben die Staatlichen Schulämter in der Stadt und im Landkreis amtsintern sowie in Besprechungen mit der zuständigen Regierung organisatorische Maßnahmen festgelegt, die die Wiederholung eines solchen Vorfalls verhindern sollen, wie z.B. Anweisungen zum Umgang beim Datenversand, Hinweise zur Optimierung des Büroablaufs und regelmäßig zu wiederholende Belehrungen der Mitarbeiter.

Die Übermittlung der drei Listen aller Lehrkräfte in der Stadt und im Landkreis mit den jeweiligen Beurteilungsmerkmalen an alle Schulleiter der Volksschulen in der Stadt und an den Personalratsvorsitzenden der Stadt war nicht erforderlich, denn für jeden Schulleiter einer Volksschule hätte eine Liste mit den betreffenden Lehrkräften seiner Schule zur Aufgabenerfüllung ausgereicht. Es liegt somit ein schwerwiegender Verstoß gegen Datenschutzbestimmungen vor. Auch die unverschlüsselte Übertragung der personenbezogenen Daten mittels E-Mail über das Internet stellt einen schwerwiegenden Verstoß gegen Datenschutzbestimmungen dar. Ebenso stellt die unterlassene abschließende Kontrolle der E-Mail in Anbetracht der Schutzwürdigkeit der übermittelten Daten einen Verstoß gegen Datenschutzbestimmungen dar.

Die **zweite Beanstandung** betraf eine **Stadt**, die die Briefumschläge von schriftlich eingegangenen Briefwahlanträgen, auch soweit sie mit der Absenderadresse versehen waren, seit mehreren Jahren - wohl zuletzt für die Europawahl 2009 - einem Dritten überlassen hatte. Zweck der Überlassung war das dortige Ablösen der Briefmarken von den Umschlägen, deren anschließende Veräußerung an Briefmarkensammler sowie der Verwendung des erzielten Verkaufserlöses für wohltätige Zwecke. Im Februar 2010 wurden mehrere 10.000 derartige Original-Briefumschläge von einer norddeutschen Firma potentiellen Interessenten per E-Mail zum Kauf angeboten. In dem Verkaufsangebot wurde ausdrücklich darauf hingewiesen, dass es sich bei den Adressen um Daten von Briefwählern aus einer bestimmten bayerischen Region handele.

(Brief-)Wahlscheinanträge zählen zu den Wahlunterlagen im Sinne der §§ 89, 90 Bundeswahlordnung (BWO) bzw. §§ 82, 83 Europa-Wahlordnung (EuWO). Die für die Übersendung benutzten Briefumschläge sind als "Teil des Antrags" anzusehen und ebenso zu behandeln. Demnach sind die von den Antragstellern für die Übersendung der (Brief-)Wahlscheinanträge benutzten Umschläge zu den "übrigen Wahlunterlagen" zu zählen. Wahlunterlagen sind nach § 89 Abs. 1 BWO bzw. § 82 Abs. 1 EuWO so zu verwahren, dass sie gegen Einsichtnahme durch Unbefugte geschützt sind. Die Weitergabe der Umschläge zu den eingegangenen Briefwahlanträgen mit den Adressen der Absender an Dritte stellt damit einen Verstoß gegen datenschutzrechtliche Bestimmungen dar. Die Vernichtung von übrigen Wahlunterlagen richtet sich nach § 90 Abs. 3 BWO bzw. § 83 Abs. 1 Satz 1 EuWO, d.h. diese können 60 Tage vor der Wahl vernichtet werden. Auch

einer sofortigen datenschutzgerechten Vernichtung steht jedoch nichts entgegen, da diese Umschläge für Wahlzwecke nicht benötigt werden und kein Bedarf für eine weitere Aufbewahrung besteht. Spätestens nach Ablauf von sechs Monaten nach der Wahl sind die Unterlagen gemäß § 90 Abs. 2 BWO bzw. § 83 Abs. 3 EuWO zu vernichten. Die Umschläge zu den Briefwahlanträgen hätten gemäß obigen Bestimmungen und unter Berücksichtigung des Erforderlichkeitsprinzips vernichtet werden können und müssen. Die Übermittlung von personenbezogenen Daten - hier konkret die Eigenschaft Briefwähler i.V.m. mit der Wohnadresse - an Dritte bedarf in jedem Einzelfall einer Rechtsgrundlage oder der Einwilligung des Betroffenen. Im vorliegenden Fall findet sich hierfür weder eine Rechtsgrundlage in der BWO noch in der EuWO noch haben die Betroffenen ihre Einwilligung zur Weitergabe ihrer Adressdaten in Verbindung mit der Eigenschaft Briefwähler erteilt. Die unberechtigte Weitergabe der Information, dass die Adressen auf den Briefumschlägen Briefwählern zuzuordnen sind, stellt somit einen erheblichen Verstoß gegen datenschutzrechtliche Bestimmungen dar.

Wenn auch im Grunde keine böse, sondern eine lobenswerte Absicht hinter der Abgabe der Briefmarken stand, so ist jedoch die praktizierte Art nicht mit den Datenschutzvorschriften vereinbar.

Der **dritte Fall** betraf ein **Internetportal**, in dem regional bezogen nach Ärzten z.B. bestimmter Fachrichtungen gesucht werden kann. Bei einem Arzt für Psychotherapie wurden für einen Zeitraum von ca. 14 Tagen neben seinen Kontaktdaten und Sprechzeiten auch Namen seiner Patienten mit zugehörigem zugelassenem Behandlungsumfang angezeigt. Diese Daten stammten aus einer anderen spezifischen Ärztedatenbank und wurden einfach in das Internetportal kopiert. Obwohl die Arztdaten im Internetportal erst nach schriftlicher Einwilligung durch diesen zum Abruf freigeschaltet wurden, unterblieb die Überprüfung der freizuschaltenden Daten bzw. wurde nicht sorgsam genug durchgeführt. Hätte die speichernde Stelle das einschlägige Gebot der Datentrennung beachtet, wäre es nicht zur Veröffentlichung sensibelster Daten gekommen. Die Offenbarung der Patientennamen sowie die mangelhaften technisch-organisatorischen Maßnahmen zur Vermeidung eines solchen Ereignisses stellen einen schwerwiegenden Verstoß gegen Datenschutzvorschriften dar.

Nr. 8 der Anlage zu § 78 a SGB X
Werden Sozialdaten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden Sozialdaten oder Kategorien von Sozialdaten geeignet sind,
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Sozialdaten getrennt verarbeitet werden können.

Erfreulich ist, dass die Nachfragen öffentlicher Stellen nach Beratung sowohl postalisch als auch per E-Mail und telefonisch auch in diesem Berichtszeitraum sehr ausgeprägt waren. Gerne komme ich diesen Wünschen nach, ist doch eine Beratung vorab allemal besser als eine Kontrolle hinterher, die dann ggf. einen größeren eigentlich vermeidbaren Änderungsaufwand nach sich zieht. Ich bitte allerdings um Verständnis, dass ich in Anbetracht meiner begrenzten Personalressourcen und der Vielzahl der Anfragen und Eingaben auf einer Vorabbewertung des behördlichen Datenschutzbeauftragten beharren muss und dass auch manche Beratungsleistungen nicht immer in der gewünschten kurzen Zeitspanne erbracht werden können.

Auf wesentliche Projekte und Anfragen gehe ich in den folgenden Abschnitten im Einzelnen ein.

2.2.2 Sparen an der falschen Stelle

Aufgrund der auch im öffentlichen Dienst immer knapper werdenden Haushaltsmittel sind die Behörden dazu angehalten, Einsparungen vorzunehmen. Dass dieses Vorhaben allerdings auch eine unerwünschte Auswirkung haben kann, zeigt folgendes Beispiel:

Als Ergebnis einer europaweiten Ausschreibung wurden die Briefdienstleistungen für die Dienststellen des Freistaates Bayern im Stadtgebiet von Nürnberg an eine Arbeitsgemeinschaft (ARGE) privater Postdienstleister vergeben.

Damit war diese Arbeitsgemeinschaft ab 01.10.2009 für die Briefdienstleistungen für alle Dienststellen des Freistaates Bayern im Stadtgebiet von Nürnberg zuständig, somit auch für die Sendungen des Landesamtes für Finanzen und des Landesamtes für Steuern, die im Rechenzentrum Nord des Landesamtes für Steuern (RZ-Nord) gedruckt und in den Versand gegeben werden.

Bereits Ende des Jahres 2009 wurden jedoch erste Probleme in der Qualität der Zustellung der Briefsendungen der beiden Landesämter festgestellt. So wandten sich verschiedene Petenten an meine Dienststelle und beschwerten sich darüber, dass der Datenschutz bei der Zustellung von Schreiben der beiden Landesämter nicht gewährleistet sei. Zum Teil kamen Schreiben dieser Ämter bei den Empfängern nicht an, wurden statt in den Briefkasten lediglich in die Zeitungsrolle gesteckt, waren unverschlossen oder aufgerissen.

Aufgrund dieser Vorfälle, die auch zu Beginn des Jahres 2010 nicht aufhörten, wandte ich mich mehrmals an die beiden Landesämter und forderte sie auf, entsprechende Abhilfemaßnahmen zu ergreifen.

Als Reaktion auf die aufgezeigten Mängel bei der Zustellung - viele Beschwerdeführer wandten sich auch direkt an die beiden Landesämter - wurden bei der Arbeitsgemeinschaft zunächst Bemühungen um eine nachhaltige Verbesserung der Leistungen angemahnt.

Die daraufhin von der ARGE ergriffenen Maßnahmen zeigten zunächst auch Erfolg. Doch im März 2010 traten wieder verstärkt Mängel in der Leistungserbringung auf und der ARGE wurde zur Beseitigung der Mängel eine Frist bis zum 31.05.2010 gesetzt.

Trotz vielfältiger Bemühungen erreichte die ARGE jedoch keine nachhaltige Verbesserung der Situation. Aus diesem Grunde und um einen mittlerweile bereits erkennbaren Imageschaden der beiden Landesämter, des Rechenzentrums Nord und insgesamt des Freistaates Bayern entgegenzuwirken, wurde der Vertrag mit der ARGE zum 31.05.2010 gekündigt und diese lediglich noch übergangsweise mit der Postzustellung beauftragt. Zum 01.10.2010 sollte der Briefpostversand durch einen neuen Dienstleister erfolgen.

Ich hoffe, dass ab diesem Zeitpunkt der Datenschutz beim Briefpostversand der beiden Landesämter und des Rechenzentrums Nord wieder gewährleistet ist.

2.2.3 Freiberuflicher Datenschutzbeauftragter

Gemäß Art. 25 Abs. 2 BayDSG haben öffentliche Stellen in Bayern, die personenbezogene Daten mit Hilfe von automatisierten Verfahren verarbeiten oder nutzen, einen ihrer Beschäftigten zum behördlichen Datenschutzbeauftragten zu bestellen. Dies stellt immer wieder insbesondere kleinere Behörden und Kommunen vor das Problem, einen geeigneten Mitarbeiter zu finden, der dieses Amt bekleiden soll. Schließlich muss der behördliche Datenschutzbeauftragte über die für seine Tätigkeit erforderliche Sach- und Fachkunde verfügen.

Einen Externen, z.B. einen Freiberufler oder einen Mitarbeiter eines privatwirtschaftlichen Unternehmens, zum behördlichen Datenschutzbeauftragten zu bestellen, scheidet aus, da nur ein Beschäftigter einer öffentlichen Stelle zu deren Datenschutzbeauftragten bestellt werden kann. Ein Freiberufler oder ein Mitarbeiter eines privatwirtschaftlichen Unternehmens ist nicht Beschäftigter einer öffentlichen Stelle und steht in keinem Arbeitsverhältnis zu dieser, sondern hat in der Regel nur einen Dienstleistungsvertrag mit einem Kunden abgeschlossen.

Die Behörden und Gemeinden sind also in jedem Fall grundsätzlich verpflichtet, einen ihrer eigenen Mitarbeiter zum Datenschutzbeauftragten zu bestellen - ergänzend wird auf die Ausführungen bezüglich eines gemeinsamen sowie externen Datenschutzbeauftragten in meinen früheren Tätigkeitsberichten verwiesen (siehe hierzu 21. Tätigkeitsbericht, Nr. 22.1.6, und 23. Tätigkeitsbericht, Nr. 25.6.1). Unbenommen bleibt aber, mit einem Externen einen Beratungsvertrag bezüglich der Gewährleistung des Datenschutzes abzuschließen.

2.2.4 Datenverlust im Krankenhaus

In Krankenhäusern gibt es immer wieder Fälle, bei denen Daten verloren gehen oder Unbefugten zur Kenntnis gelangen. Insbesondere elektronisch verarbeitete Daten sind sehr einfach zu vervielfältigen und zu übermitteln. Zudem sind in Krankenhäusern sehr viele Geräte zur elektronischen Datenverarbeitung vorhanden, so dass die Datenflusskontrolle sehr schwierig ist. Unter anderem erwiesen sich bei Überprüfungen besonders häufig technische und organisatorische Maßnahmen zur Kontrolle der Speicherorte und Schnittstellen als verbesserungsbedürftig:

Inventarisierung

PCs und andere Geräte, auf denen personenbezogene Daten gespeichert werden können, müssen inventarisiert werden. Nur so ist überhaupt feststellbar, ob Geräte abhanden gekommen sind. Zudem muss auch die Beschaffung zentral geregelt werden um sicherzustellen, dass alle Geräte auch wirklich inventarisiert werden und kein "Wildwuchs" an selbst beschafften Geräten entsteht.

Änderung der Rechnerkonfiguration

Eine eigenmächtige Änderung der Rechnerkonfiguration (z.B. Ausbau der Festplatte) muss verboten und soweit möglich technisch verhindert werden. Der Umbau von Rechnern darf nur durch festgelegte Personen erfolgen, die die ausgeführten Aktionen im Inventarverzeichnis entsprechend dokumentieren. Alternativ kann auch eine Software zur Verwaltung der Hardware-Konfiguration eingesetzt werden.

Reduzierung der Speicherorte

Nach Möglichkeit sollte Speicherplatz insbesondere auch für Forschungsdatenbanken zentralisiert im Rechenzentrum des Krankenhauses vorgehalten werden. Die entsprechenden Datenbanken und Server können dann einheitlich gewartet werden. Auf den Arbeitsplatzrechnern sollte die Speicherung personenbezogener medizinischer Daten verboten werden, da sonst nicht mehr kontrolliert werden kann, welche Daten wo abgelegt sind und wer darauf Zugriff erhalten kann.

Richtlinien für örtlich begrenzte Systeme

Neben den zentral bereitgestellten Verfahren wie Krankenhausinformationssysteme, Laborsysteme, Radiologieinformationssysteme etc. gibt es eine Vielzahl örtlich begrenzter Systeme sowohl für die Behandlung der Patienten als auch für die Forschung. Es müssen daher Richtlinien für den Betrieb örtlich begrenzter Systeme festgelegt werden, die u.a. die Einrichtung und Wartung, die Modalitäten für den Datenzugriff und die Sicherheitsmaßnahmen festlegen. Darin sollte auch eine Erforderlichkeitsprüfung bei der Einrichtung neuer Systeme enthalten sein, die vor der Beschaffung neuer Rechner durchgeführt wird, und es sollte auch die Vorgehensweise für die datenschutzrechtliche Freigabe gemäß Art. 26 BayDSG geregelt sein.

Schnittstellen, Laufwerke

USB-Sticks und CDs/DVDs sind eine einfache Möglichkeit, Daten in großen Mengen aus den Systemen des Krankenhauses abzuziehen. Die USB-Schnittstellen und Laufwerke dürfen daher nicht frei nutzbar sein. Sie müssen entweder gesperrt oder per Software kontrolliert werden. Im letzteren Fall muss konfigurierbar und prüfbar sein, wer welche Daten auf ein externes Medium gespeichert hat.

Mobile Geräte

Die Speicherung personenbezogener medizinischer Daten auf mobilen Geräten muss entweder verboten oder es muss eine verschlüsselte Speicherung sichergestellt werden. Sie sollte nur in den wirklich erforderlichen Fällen zulässig sein. Auf privaten Geräten dürfen keinesfalls personenbezogene medizinische Daten gespeichert werden.

E-Mail-Nutzung von außerhalb des Krankenhauses

Der Zugriff auf dienstliche E-Mails von außerhalb, z.B. von zu Hause, muss möglichst restriktiv gehandhabt werden. Er sollte nur im Einzelfall nach einer strengen Prüfung der Erforderlichkeit erlaubt werden. Zudem empfiehlt sich eine Protokollierung und stichprobenartige Kontrolle derartiger Zugriffe. Die Speicherung von E-Mails mit personenbezogenen Daten auf privaten Rechnern muss technisch verhindert werden.

Entsorgung

Die Entsorgung ebenso wie die Beschaffung von Rechnern darf nur nach einem geregelten Verfahren erfolgen. Zu entsorgende Rechner und insbesondere Festplatten sollten zentral gesammelt und entsorgt werden. Eine ungeregelte

Entsorgung durch die Mitarbeiter vor Ort kann dazu führen, dass die Geräte einfach weggeworfen werden. Gerade bei Speichermedien wie Festplatten muss jedoch dafür gesorgt werden, dass die Daten entweder zuvor datenschutzgerecht gelöscht werden oder der Datenträger vorab physisch zerstört wird. Erst dann darf eine Weitergabe an einen externen Dienstleister o.ä. stattfinden.

Berechtigungskonzept / Protokollierung

Über ein Berechtigungskonzept muss sichergestellt werden, dass nur die erforderlichen Datenzugriffe stattfinden können. Zudem sollte eine Protokollierung auch der lesenden Zugriffe sowie eine Auswertung der Protokolldaten erfolgen, um den Missbrauch von Zugriffsrechten aufdecken zu können.

2.2.5 KV-Ident

Laut einem Vorstandsbeschluss der Kassenärztlichen Bundesvereinigung (KBV) wird die Online-Abrechnung für die Mitglieder der Kassenärztlichen Vereinigung Bayerns (KVB) ab 01.01.2011 Pflicht. Dies bedeutet, dass ab dem 1. Quartal 2011 keine Abrechnungsdaten mehr auf Papier, Diskette, CD etc. eingereicht werden dürfen, sondern über eine Online-Anbindung an die KVB übermittelt werden müssen.

Eine Möglichkeit hierzu ist das KV-Safenet (siehe hierzu 21. Tätigkeitsbericht, Nr. 22.2.3.1), das eine sichere Anbindung von Arztpraxen an die KVB über ein Hardware-VPN bietet. Allerdings fand KV-Safenet nicht die gewünschte starke Verbreitung - zum einen weil für Ärzte, die nur selten auf Online-Dienste der KVB zugreifen, relativ hohe Kosten entstehen, zum anderen weil viele Ärzte in den Aufbau einer eigenen IT-Infrastruktur in den Praxen investiert haben, so dass erforderliche technische Änderungen daran abgelehnt werden.

Deshalb wurde von der KVB als Alternative KV-Ident entwickelt, das eine sichere Identifikation und Authentifizierung der Benutzer am Online-Portal der KVB bieten soll. Im Gegensatz zum KV-Safenet handelt es sich hierbei nicht um eine "Komplettlösung", die alle Aspekte einer sicheren Anbindung abdeckt, sondern um eine browserbasierte Lösung, für deren sicheren Einsatz zusätzliche Maßnahmen auf den IT-Systemen des Arztes erforderlich sind. KV-Ident ist gedacht für Wenignutzer des Online-Angebots und für Nutzer, die die Absicherung der Rechner gemäß der Vorgaben der Kassenärztlichen Bundesvereinigung zu Datenschutz und Datenverarbeitung selbst sicherstellen können. Sie eignet sich also nicht für Arztpraxen, in denen kein eigenes Know-How zur IT-Sicherheit vorhanden ist.

Zweck von KV-Ident ist es, die Benutzer am Online-Portal der KVB eindeutig zu identifizieren und sodann eine verschlüsselte Übertragung der Daten anzubieten. Der Zugriff erfolgt über den Web-Browser und die darin integrierten Verschlüsselungsmechanismen (SSL), zusätzliche Software wird nicht benötigt. Die Benutzeridentifikation und Authentifizierung erfolgt zweistufig, indem sich der Arzt zunächst mit Benutzerkennung und Passwort bei der KVB einloggt und dann noch eine PIN von einer "Grid-Karte" (Tabelle aus mehreren Spalten und Zeilen ähnlich einem Koordinatensystem, gefüllt mit Buchstaben und Ziffern) abgefragt wird. Erst dann sind die Übermittlung und der Zugriff auf medizinische Daten möglich.

Die Zugangsdaten müssen vom Arzt schriftlich beantragt werden und werden ihm in zwei getrennten Briefen zugestellt: Zunächst erhält er per Post die Benutzerkennung und ein Erstpasswort, das er beim ersten Login ändern muss, anschließend wird die Gridkarte per PostIdent-Verfahren zugestellt, um die Identität des Arztes zu bestätigen. Alle drei Jahre erhält der Arzt automatisch eine neue Grid-Karte.

In den Teilnahmebedingungen sind die Pflichten der teilnehmenden Ärzte geregelt, insbesondere zum Umgang mit den Zugangsdaten und zur Pflicht der Absicherung der eigenen Computer.

Aus Sicht des technisch-organisatorischen Datenschutzes ist die Lösung des KV-Safenet als Hardware-VPN nach wie vor vorzugswürdig. Ich habe KV-Ident jedoch unter der Voraussetzung akzeptiert, dass die Ärzte über die Unterschiede zwischen beiden Verfahren aufgeklärt werden und die Pflicht zur Absicherung der eigenen IT-Systeme deutlich gemacht wird. Es müssen Maßnahmen gemäß dem aktuellen Stand der Technik ergriffen werden, wie z.B. Firewall, Schutz gegen Schadsoftware, regelmäßige Software-Updates, bewusste Nutzung des Internet, Passwortschutz und Bildschirmsperren an den Arbeitsplätzen, um die Praxissysteme gegen Angriffe aus dem Internet zu schützen. Ist der Rechner des Arztes angreifbar, so können die Daten bereits dort, vor der Übertragung an die KVB abgegriffen werden, wodurch die weiteren Sicherheitsmaßnahmen hinfällig werden.

2.2.6 TIZIAN

Auf meine Anregung hin wurde mittlerweile unabhängig von der rechtlichen Diskussion ein Datenschutzkonzept für das Verfahren TIZIAN erstellt, das auch die nach Art. 26 Abs. 3 BayDSG erforderliche Beschreibung der technisch-organisatorischen Maßnahmen beinhaltet.

Das Datenschutzkonzept orientiert sich am Vorgehen der IT-Grundschutzkataloge des BSI und betrachtet die gängigen Sicherheitsaspekte. Zudem gibt es gesonderte Konzepte zu einigen aus Datenschutzsicht interessanten Fragestellungen wie ein Berechtigungskonzept, ein Protokollierungskonzept und ein Löschkonzept, die jedoch teilweise noch nicht fertig gestellt sind. Einige der Regelungen, die nun in diesen Konzepten getroffen werden sollen, waren früher im Gesetzesentwurf für TIZIAN enthalten. Ich bedaure, dass diese konkreten Regelungen zu technisch-organisatorischen Fragen entgegen meiner Forderungen in späteren Gesetzentwürfen nicht mehr enthalten sind.

Zu den einzelnen Konzepten lässt sich grundsätzlich Folgendes feststellen:

Das **Berechtigungskonzept** sieht für gewisse Nutzergruppen die Möglichkeit vor, bayernweit in die Daten der Lebensmittelüberwachungsbehörden Einsicht zu nehmen. Im bisherigen Betrieb wurden diese bayernweiten Zugriffe nicht freigeschaltet, da noch einige Funktionen zur Protokollierung und Protokollauswertung nicht implementiert und mit dem Hauptpersonalrat abgestimmt waren. Aus Datenschutzsicht muss für bayernweite Zugriffe immer die Erforderlichkeit für die jeweilige Benutzergruppe geprüft werden.

Im **Löschkonzept** müssen möglichst konkrete Formulierungen für die Löschfristen und die Vorgehensweisen zur Löschung von personenbezogenen Daten

enthalten sein. Dabei muss sichergestellt werden, dass die Daten nach Fristablauf physikalisch gelöscht und nicht nur ausgelagert oder gesperrt werden.

Im **Protokollierungskonzept** muss geregelt werden, welche Zugriffe protokolliert werden, wie lange die Aufbewahrungsfristen für Protokolldaten sind und wie und zu welchen Zwecken die Auswertung erfolgen darf. Eine Protokollierung der schreibenden Zugriffe ist vor allem für die Integrität der Daten und die Nachvollziehbarkeit von Änderungen erforderlich. Eine Protokollierung der lesenden Zugriffe wird insbesondere für die Kontrolle der Datenzugriffe benötigt. Nur so ist feststellbar, ob missbräuchliche Zugriffe stattgefunden haben. Gleichzeitig muss jedoch auch festgelegt werden, wie und durch wen die Protokolle ausgewertet werden. Neben einer anlassbezogenen Auswertung sollte auch eine Auswertung in Stichproben erfolgen. Auswertungen dürfen jedoch nur zur Datenschutzkontrolle vorgenommen werden, nicht jedoch zur Verhaltens- und Leistungskontrolle der Mitarbeiter.

Ich werde in diesem Projekt die Entwicklung der technisch-organisatorischen Maßnahmen sowie deren Umsetzung weiterhin begleiten und kritisch beobachten.

2.2.7 Mammographie-Screening

Übersicht

Im Berichtszeitraum habe ich die Zentrale Stelle des Mammographie-Screenings einer rechtlichen und technisch-organisatorischen Prüfung unterzogen, bei der vor allem der Umgang mit den Meldedaten und den Einladungsdaten in der Praxis geprüft werden sollte. Die grundlegenden Abläufe zum Mammographie-Screening und zum Einladungswesen wurden bereits in den Tätigkeitsberichten der vorigen Jahre beschrieben (siehe hierzu 23. Tätigkeitsbericht, Nr. 15.2).

Die Zentrale Stelle des Mammographie-Screenings befindet sich in den Räumen der Kassenärztlichen Vereinigung Bayerns (KVB), ist jedoch technisch, organisatorisch und personell von dieser getrennt. Das gesamte Mammographie-Screening, also auch die Zentrale Stelle, arbeitet mit der von der KVB entwickelten Software MammaSoft. Die Server werden von der IT-Abteilung der KVB als Auftragnehmer im Rechenzentrum der KVB betrieben, es arbeiten jedoch nur die Zentrale Stelle und die Screening-Einheiten damit. Andere Abteilungen der KVB haben keinen Zugriff.

Erzeugung der Einladungslisten

Die Zentrale Stelle erhält quartalsweise die Meldedaten der anspruchsberechtigten Frauen von der Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB) verschlüsselt angeliefert. Dieser Auszug aus den Meldedaten wird in MammaSoft importiert. Da im Einladungswesen dauerhaft keine personenbezogenen Meldedaten gespeichert werden dürfen, werden nach dem Einlesen der Meldedaten aus diesen Pseudonyme erzeugt, der Abgleich mit den Pseudonymen der bereits vorhandenen Einladungsdaten durchgeführt und die Terminplanung für die Screening-Einheiten festgelegt. Dazu kennt die Zentrale Stelle die Kapazitäten und verfügbaren Zeiten aller Screening-Einheiten.

Aus den Terminen werden Terminlisten und Einladungslisten erzeugt, die an einen externen Druckdienstleister weitergegeben werden, mit dem ein Vertrag zur Auftragsdatenverarbeitung abgeschlossen wurde. Zudem werden die Terminlisten und Einladungslisten für die Screening-Einheiten freigeschaltet. Bei meiner Prüfung musste ich feststellen, dass diese Listen auch nach Erledigung der Termine sowohl für die Zentrale Stelle als auch für die Screening-Einheiten noch abrufbar waren. Ich habe die Zentrale Stelle aufgefordert, dies zu ändern, was auch zugesagt wurde.

Ein Zugriff auf medizinische Daten ist für die Zentrale Stelle nicht zulässig und technisch auch nicht möglich.

Call Center

Für Rückfragen von Klientinnen, Terminverschiebungen u.ä. werden das Vermittlungs- und Beratungszentrum der KVB sowie die Gedikom GmbH (Tochterunternehmen der KVB) genutzt. Dazu haben diese Stellen einen eingeschränkten Zugriff auf MammaSoft entsprechend ihren Aufgaben. Für das Mammographie-Screening wurde eine eigene Telefonnummer eingerichtet, so dass die Anrufe von speziell für das Einladungswesen geschulten Mitarbeitern entgegengenommen werden.

KVB als Dienstleister für das Mammographie-Screening in anderen Bundesländern

Die KVB betreibt als technischer Dienstleister für einige andere Bundesländer das Mammographie-Screening. Es liegen daher auch Einladungsdaten und medizinische Daten anderer Bundesländer auf den Servern der KVB. Diese sind aber von den Daten des bayerischen Screenings sowie untereinander getrennt, so dass ein übergreifender Zugriff auf die Daten anderer Bundesländer nicht möglich ist.

Krebsregisterabgleich

Der Abgleich mit den Daten der Krebsregister, der bereits seit längerem in den Krebsfrüherkennungsrichtlinien vorgesehen ist, findet derzeit noch nicht statt, da die entsprechenden landesrechtlichen Regelungen erst im Entstehen sind (siehe hierzu Nr. 7.1).

2.2.8 RFID-Benutzerausweise in der Münchner Stadtbibliothek

Wie schon im 22. Tätigkeitsbericht, Nr. 23.4.5, angekündigt, hat die Münchner Stadtbibliothek auch die Benutzerausweise auf RFID-Technologie umgestellt. Dabei werden die Ausweise mit Chips mit Antenne versehen, die von Lesegeräten der Stadtbibliothek kontaktlos erfasst werden können. Dafür wurde jedem Benutzer eine neue Benutzernummer zugewiesen. Im Gegensatz zu den alten, barcode-basierten Ausweisen wird hierbei keine sprechende Nummer mehr verwendet.

Auf dem RFID-Chip des Benutzerausweises ist neben der 12-stelligen Benutzernummer noch ein Länderkennzeichen für den Standort der Bibliothek sowie das

Siegel der Stadtbibliothek gespeichert. Personenbezogene Angaben wie Name oder Adresse sind nicht enthalten. Ich habe daher keine Einwände gegen die Umstellung des Benutzerausweises.

2.2.9 Kennzeichenbasierte Reisezeitmessung auf Autobahnen

Sowohl eine Autobahndirektion als auch eine Universität haben bei mir wegen einer Reisezeitmessung auf Basis von Kennzeichenerfassung, einer modernen Form der Verkehrszählung sowie der Verkehrsüberwachung und Verkehrssteuerung, angefragt. Diese wird sowohl zeitlich befristet für einzelne Straßenabschnitte wie z.B. Ortszufahrten verwendet, als auch zunehmend auf bayerischen Autobahnen zur dynamischen Verkehrssteuerung. Dabei sollen durch Kameras an der Autobahn die Kennzeichen der vorbeifahrenden Fahrzeuge erfasst und damit ermittelt werden, wie lange die Fahrt von einem Messpunkt zum nächsten gedauert hat. Hierzu schicken die Kameras ihre Messwerte üblicherweise an eine zentrale Datenbank, über die die Auswertung erfolgt.

Da es sich bei Kfz-Kennzeichen um ein personenbezogenes oder zumindest personenbeziehbares Datum handelt, kann ein derartiges Vorgehen nur dann zulässig sein, wenn insbesondere eine Reidentifizierung, d.h. Rückführung der gespeicherten Daten auf das Kfz-Kennzeichen und damit den Halter, faktisch unmöglich ist. Zudem darf keine Vollerfassung des Verkehrs stattfinden, d.h. die Erfassung darf sich auch nicht auf alle Fahrspuren auf allen Autobahnen Bayerns erstrecken. Es muss sichergestellt sein, dass sich ein Großteil der Verkehrsteilnehmer unerfasst auf den Autobahnen bewegen kann, um weitere Begehrlichkeiten auf die so erhobenen Daten zu vermeiden. Desweiteren ist die Bildung von langfristigen Bewegungsprofilen zu einzelnen Fahrzeugen zu verhindern, d.h. die einzelnen Fahrzeuge dürfen nicht über mehrere Tage hinweg erkennbar und mit ihren Messwerten verknüpfbar sein.

Dies bedeutet im Einzelnen für die technische Realisierung:

Da die Reidentifizierung des Fahrzeug-Halters verhindert werden muss, dürfen keine Kfz-Kennzeichen in der Datenbank zur Auswertung der Reisezeit gespeichert werden. Die Kennzeichen müssen bereits in der Messstation, also sofort nach ihrer Aufnahme, so transformiert werden, dass daraus das Kennzeichen nicht mehr erkennbar ist und auch nicht wiederhergestellt werden kann, z.B. mittels Einweg-Hash-Funktionen. Das aufgenommene Kennzeichen muss sodann sofort gelöscht werden, so dass es auch direkt in der Messstation nicht mehr ausgelesen werden kann.

Um die Möglichkeit für eine Profilbildung über einzelne Fahrzeuge auszuschließen, muss verhindert werden, dass Messwerte tagesübergreifend einem Fahrzeug zugeordnet werden können. Dies kann z.B. dadurch erreicht werden, dass die Hashwerte nicht dauerhaft in der Datenbank gespeichert werden, sondern nach Zusammenführung der Messwerte und spätestens nach einem Tag gelöscht werden. Dann sind nur noch die ermittelten Reisezeiten in der Datenbank vorhanden.

Eine andere Möglichkeit Profilbildung zu verhindern ist die Erzeugung von täglich anderen Hashwerten aus dem gleichen Kfz-Kennzeichen, z.B. durch ein Hashverfahren mit wechselnden Schlüsseln in der Kamera. So sind die Messwerte ebenfalls für maximal einen Tag einem Fahrzeug zuordenbar. Auch mehrstufige

Verfahren, bei denen der Hashwert durch eine laufende Nummer ersetzt wird, sind denkbar, wenn sichergestellt ist, dass einem bestimmten Kfz-Kennzeichen damit täglich eine andere Nummer zugeordnet werden würde.

Im Hinblick auf eine bayernweite oder sogar deutschlandweite Ausdehnung der Bereiche mit Reisezeitmessung müssen Maßnahmen ergriffen werden, um eine großflächige Erfassung von Bewegungsprofilen auch an einem Tag zu verhindern. Hierzu könnten beispielsweise verschiedene Regionen unterschiedliche Hashwerte erzeugen und in verschiedenen Datenbanken ausgewertet werden, zwischen denen dann keine Verknüpfung möglich ist.

Zudem müssen für die Messstationen, die Datenbank und die Datenübermittlung die üblichen technischen und organisatorischen Sicherheitsmaßnahmen nach Art. 7 BayDSG angewendet werden.

Die aufgeführten Grundvoraussetzungen gelten auch für die Reisezeitmessung auf Basis anderer Merkmale als dem Kfz-Kennzeichen, allerdings können sich hierbei noch weitere Anforderungen ergeben.

2.2.10 Projekt elektronische Fallakte (eFA) im Städtischen Klinikum München

Basierend auf der eFA-Spezifikation und den bereits im letzten Tätigkeitsbericht dargelegten Anforderungen (siehe hierzu 23. Tätigkeitsbericht, Nr. 25.5.3) wurde für das Darmkrebsprojekt des Städtischen Klinikums München eine eFA nunmehr implementiert. Das Projekt befindet sich mittlerweile im Echtbetrieb. Projektbeteiligte sind auch eine Gruppe von niedergelassenen Ärzten und einige Patienten.

Das Städtische Klinikum München tritt hierbei für die niedergelassenen Ärzte als Provider auf, bei dem alle Daten gespeichert werden, um die 24-stündige Verfügbarkeit der eingestellten Daten zu gewährleisten. Alle Daten der Fallakte werden somit im Krankenhaus gespeichert, allerdings nicht im normalen KIS, sondern in einem eigenen Systembereich. Der Zugriff auf die Daten ist nur über das eFA-Portal und die eFA-Sicherheitsmechanismen möglich.

Für die Einrichtung einer Fallakte muss der behandelnde Arzt zunächst ein Aufklärungsgespräch mit dem Patienten führen. Stimmt der Patient zu, wird eine Fallakte für eine bestimmte Diagnose eingerichtet. Für jede angelegte Fallakte wird automatisch ein Gültigkeitsdatum eingerichtet, so dass eine unbefristete Speicherung von Daten von vornherein verhindert wird. Läuft die Gültigkeitsfrist ab, wird der Arzt systemseitig angefragt, ob die Akte weiter benötigt wird. Die Frist kann dann mit Zustimmung des Patienten verlängert werden.

Bei der Anlage der Fallakte werden zudem die Benutzerberechtigungen festgelegt. Hierzu wird eine Liste von potenziell geeigneten Mitbehandlern angezeigt, aus denen der Arzt zusammen mit dem Patienten die gewünschten Personen / Einrichtungen auswählen kann. Daraus werden automatisch die entsprechenden Zugriffsberechtigungen erzeugt. Zudem wird die Einwilligungserklärung für den Patienten generiert, die automatisch die Liste der ausgewählten Mitbehandler enthält. Nach der Unterschrift des Patienten können medizinische Dokumente in der Akte abgelegt werden und die Mitbehandler erhalten automatisch eine Benachrichtigung, wenn neue Dokumente bzw. eine neue Akte vorliegen.

Damit der Patient den Kreis der Berechtigten spontan erweitern kann (z.B. für eine Zweitmeinung), steht ein Offline-Token zur Verfügung. Mit Übergabe an einen Arzt, der grundsätzlich am eFA-System teilnimmt, kann dieser auf die Fallakte zugreifen. Für die eigentliche Behandlung sollte der Offline-Token jedoch nicht benutzt werden, da der Patient sonst leicht die Übersicht über die berechtigten Personen verliert. Neu hinzugekommene Behandler müssen vielmehr mit Zustimmung des Patienten über die Berechtigungsverwaltung der eFA eingerichtet werden.

Ich begrüße, dass meine Anregungen und Anforderungen aufgegriffen und umgesetzt wurden. Insbesondere mit Blick auf die praktische Nutz- und Handhabbarkeit der Datenschutzmaßnahmen werde ich dieses Projekt auch weiterhin begleiten.

2.2.11 Elektronische Dokumentation und Abrechnung von Notarzteinsätzen ("emDoc")

Seit dem 01.01.2010 erfolgt die Notarzteinsatz-Dokumentation in Bayern (emDoc) online über ein Web-Portal der KVB. Im Rahmen der Diskussion zwischen Notärzten und der Kassenärztlichen Vereinigung Bayerns zu diesem Verfahren habe ich eine rechtliche (siehe hierzu Nr. 8.4) und eine technisch-organisatorische Bewertung vorgenommen.

Der Zugriff auf emDoc durch die Ärzte erfolgt über KV-Safenet oder KV-Ident (siehe hierzu Nr. 2.2.5). Über dieses Portal werden arzt- und patientenbezogen die Dokumentationsbögen zum jeweiligen Einsatz ausgefüllt. Der Arzt kann nach Abschluss der Dokumentation seine eigenen Fälle zu Zwecken der Qualitätssicherung auswerten. Hierzu erhält er anonymisierte Vergleichsdaten von Einsätzen anderer Ärzte.

Die Zugriffe für die anderen am Verfahren beteiligten Stellen werden über ein Berechtigungskonzept realisiert. Übergreifende Zugriffe durch den ÄLRD (ärztlichen Leiter Rettungsdienst) oder auch durch den Fachadministrator bei der KVB erfolgen in der Regel ohne Personenbezug. Der Zugriff auf die Dokumentation mit Arzt- und / oder Patientenbezug darf nur in geregelten Ausnahmefällen, z.B. bei Patientenbeschwerden, mit einer dokumentierten Begründung erfolgen.

Die Daten des Verfahrens sind auf Servern im Rechenzentrum der KVB gespeichert, wobei die Datenbank von anderen Verfahren der KVB getrennt ist. Der technische Betrieb wird von der IT-Abteilung der KVB übernommen. Um sowohl für emDoc als auch für andere Verfahren die Schutzziele der IT-Sicherheit und des technisch-organisatorischen Datenschutzes zu gewährleisten, hat die KVB einen Sicherheitsprozess etabliert, der sowohl die Zuständigkeiten für die IT-Sicherheit und den Datenschutz als auch Vorgehensweisen und Maßnahmen definiert. Sicherheitsuntersuchungen und -konzepte werden auf Basis des BSI-Grundschutzes vorgenommen. Zudem werden jährlich interne und externe Audits der verschiedenen Verfahren durchgeführt, um eine laufende Aktualisierung der implementierten Sicherheitsmaßnahmen zu erreichen.

Für emDoc wurden zwei Sicherheitsaudits durch eine externe Firma durchgeführt. Die KVB hat mitgeteilt, dass alle in diesen Audits festgestellten Mängel behoben worden seien. Unter der Voraussetzung, dass die Sicherheit der emDoc-

Anwendung auch weiterhin regelmäßig geprüft und entsprechende Aktualisierungen vorgenommen werden, bestehen derzeit keine Bedenken gegen die technische Realisierung von emDoc.

Weitere Voraussetzung für die Sicherheit ist neben den Sicherheitsmaßnahmen auf Seiten der KVB jedoch insbesondere bei der Nutzung von KV-Ident, dass der Zugriff auf emDoc immer in einer geschützten Einsatzumgebung wie z.B. einer Arztpraxis oder einem Krankenhaus erfolgt, wo ein hinreichender IT-Sicherheitsstandard gegeben ist und auch nur ein kontrollierter Zugriff auf das Internet stattfindet. Die Nutzung von PCs im Internet-Café oder von heimischen Privat-PCs, die von verschiedenen Personen zu privaten Zwecken genutzt werden, ist nicht akzeptabel, da hier das Risiko von Schadsoftware etc. besteht.

2.2.12 Fingerabdruckscanner als Zugangskontrollsysteme

Durch einen Presseartikel wurde mir bekannt, dass in einer bayerischen Grundschule ein Fingerabdruckscanner zur Zugangskontrolle eingesetzt werden sollte. Ziel des Systems war, außerhalb der normalen Unterrichtszeiten einen Zugang zum verschlossenen Schulgebäude etwa für Musikschüler zu ermöglichen.

Grundsätzlich kann ein solches System die Sicherheit erhöhen, allerdings wird es in der Regel nur innerhalb eines Gesamtsicherheitskonzeptes für gefährdete Bereiche eingebunden. Die erfassten biometrischen Daten sind dann mit technischen Maßnahmen so zu sichern, dass ein unbefugter Zugriff darauf wirksam unterbunden wird. Die Erstellung eines IT-Sicherheits- und Berechtigungskonzepts ist dafür eine notwendige Maßnahme.

Vor dem Einsatz solcher Systeme ist sehr genau abzuwägen, ob der potentielle Sicherheitsgewinn die Erfassung von biometrischen, personenbezogenen Daten rechtfertigt. Im vorliegenden Fall war dies wohl nicht zutreffend, zumal es sich überwiegend um die biometrischen Daten von Kindern und Jugendlichen handelte und eine Grundschule im Allgemeinen nicht als besonders gefährdeter Bereich betrachtet werden kann. Hinzu kam, dass die Grundschule angeblich auch über nicht gesicherte Zugänge betreten werden konnte.

Auf Grund der Proteste vieler Eltern und der Öffentlichkeit sowie meiner Nachfrage wurde das System nach kurzer Zeit wieder entfernt. Es wurde zugesichert, dass alle bis zu diesem Zeitpunkt erfassten Daten wieder gelöscht wurden.

2.2.13 Auftragsdatenverarbeitung im Bereich Personalverwaltung

Ein Outsourcing im Bereich der Personalverwaltung kann unter bestimmten Voraussetzungen als Auftragsdatenverarbeitung zu werten sein. Allerdings können insoweit jedenfalls nicht ganze Teilbereiche der Personaldatenverarbeitung ausgegliedert werden. Werden die Voraussetzungen beachtet, ist eine solche Auftragsdatenverarbeitung nicht generell ausgeschlossen, selbst wenn hiervon Personalaktendaten (§ 50 Satz 2 Beamtenstatusgesetz) betroffen sind. Wünschenswert ist dies allerdings auch im Hinblick auf die besondere Schutzwürdigkeit von Personalaktendaten nicht. Daher empfehle ich vor jedem Vertragsabschluss gründlich zu prüfen, ob eine derartige Auftragsdatenverarbeitung im Einzelfall wirklich erforderlich und angemessen ist.

Wird an dem Outsourcing festgehalten, bleibt der Auftraggeber für die Einhaltung der Vorschriften des Bayerischen Datenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Somit sind auch die Vorschriften des Art. 6 BayDSG zu beachten. Die im zweiten Abschnitt des Bayerischen Datenschutzgesetzes genannten Rechte, zum Beispiel das Auskunftsrecht des Betroffenen, sind dem Auftraggeber gegenüber geltend zu machen (Art. 6 Abs. 1 BayDSG). Nach Art. 6 Abs. 2 BayDSG ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei Datenerhebung, -verarbeitung oder -nutzung, die technischen und organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind.

Darüber hinaus muss auch bei einer Auftragsdatenverarbeitung gewährleistet sein, dass die personaldatenschutzrechtlichen Vorgaben der Art. 102 ff. Bayerisches Beamtengesetz (BayBG) eingehalten sind. Dies betrifft vor allem die Regelung über den Zugang zu Personalaktendaten in Art. 103 BayBG. Danach dürfen Zugang zu Personalaktendaten nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist.

Es ist deshalb insbesondere sicherzustellen, dass eine Kenntnisnahme und ein Zugriff auf die Personaldaten durch die Mitarbeiter des Auftragnehmers im Hinblick auf die schutzwürdigen Belange der Betroffenen durch Verschlüsselung ausgeschlossen sind. Selbstverständlich muss auch jede Datenübertragung personenbezogener Daten zum bzw. vom Auftragnehmer verschlüsselt erfolgen.

Die von meiner Geschäftsstelle bezüglich einer Auftragsdatenverarbeitung im Bereich der Personalverwaltung beratenen Stellen haben aufgrund dieser Rahmenbedingungen zum Großteil von einem entsprechenden Outsourcing-Vorhaben wieder Abstand genommen.

2.2.14 Einsatz eines elektronischen Türöffnungssystems

Werden bei einen elektronischen Türöffnungssystem personifizierte Tags (dabei handelt es sich um Meta- oder Zusatzinformationen, die einer Datei angefügt werden) verwendet, handelt es sich um eine automatisierte Verarbeitung personenbezogener Daten im Sinne des Bayerisches Datenschutzgesetzes (BayDSG), bei der zumindest personenbeziehbare Daten erhoben und verarbeitet werden. Damit kann festgestellt werden, wer hat wann welchen Türöffnungsmechanismus betätigt. Ob diese Daten dann auch tatsächlich entsprechend genutzt werden (z.B. zur Erstellung von Persönlichkeitsprofilen) oder nur genutzt werden können, ist für die weitere Betrachtung ohne Belang.

Da diese Daten im Regelfall - auch bei einer relativ kurzen Speicherdauer - nicht in so genannten Zwischen- oder Hilfsdateien im Sinne des Art. 4 Abs. 3 BayDSG gespeichert werden, ist das Bayerische Datenschutzgesetz voll anwendbar. Somit ist für dieses Verfahren auch eine datenschutzrechtliche Freigabe gemäß Art. 26 Abs. 1 Satz 1 BayDSG durch die die Daten erhebende Stelle erforderlich.

Für die Überwachung der Einhaltung des Datenschutzes beim Einsatz des elektronischen Türöffnungssystems ist der Datenschutzbeauftragte der dieses System einsetzenden öffentlichen Stelle zuständig.

2.2.15 Übermittlung gaststättenrechtlicher Gestattungen per E-Mail an die örtliche Polizeidienststelle

Bezüglich der häufig von der örtlichen Polizeidienststelle gewünschten Übertragung aller gaststättenrechtlicher Gestattungen sowie aller Veranstaltungsanzeigen durch die Kommune per E-Mail ist aus datenschutzrechtlicher Sicht Folgendes anzumerken:

- Vor dem Hintergrund des zunehmenden Alkoholmissbrauchs hat das Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie mit Rundschreiben vom 16.05.2007 die Bezirksregierungen darauf hingewiesen, dass die Polizei bereits beim Gestattungsantrag zu beteiligen bzw. zu informieren ist.
- Eine rechtliche Beteiligungspflicht wurde in die Gewerbeverordnung aufgenommen (§ 1 Abs. 3 Satz 3 GewV).
- Gemäß § 1 Abs. 7 der Gaststättenverordnung stehen die Überwachungsbefugnisse nach § 22 des Gaststättengesetzes im Zusammenhang mit der Sperrzeit auch den Polizeiinspektionen zu.

Somit ist eine Weitergabe entsprechender Genehmigungen und Anzeigen - auch wenn sie personenbezogene Daten beinhalten - an die örtliche Polizeiinspektion im Grundsatz möglich. Allerdings müssen auch in diesem Falle entsprechende technische und organisatorische Maßnahmen getroffen werden, die erforderlich sind, um die Datensicherheit gemäß Art. 7 BayDSG zu gewährleisten. Dies bedeutet, dass bei einer elektronischen Datenübermittlung über das Internet, also auch per E-Mail, insbesondere die Vertraulichkeit der Daten gewährleistet sein muss, die nur durch eine Verschlüsselung der Daten erreichbar ist. Werden die zu übermittelnden Dokumente als E-Mail-Anhang versandt, so genügt es, wenn nur diese verschlüsselt werden - sofern im E-Mail-Text selbst keine personenbezogenen Daten enthalten sind.

2.2.16 Betrieb eines Internetcafes

Einige Gemeinden und andere öffentliche Stellen (z.B. Jugendzentren) möchten ihren Bürgern (insbesondere Jugendlichen) die Möglichkeit geben, von zentraler Stelle aus im Internet zu surfen. Zu diesem Zweck planen sie, sogenannte Internet-Cafes einrichten. Da sie sich aber darüber unschlüssig sind, welche datenschutzrechtlichen Anforderungen an ein derartiges Internet-Cafe bestehen, wenden sie sich häufig zwecks diesbezüglicher Beratung an mich und meine Dienststelle. Zu derartigen Vorhaben ist Folgendes zu sagen:

Betreibt eine öffentliche Stelle ein Internetcafé, hat es die dabei geltenden datenschutzrechtlichen, jugendschutzrechtlichen und strafrechtlichen Vorschriften zu beachten. Dabei ist es unerheblich, ob die Nutzung des bereitgestellten Internetzuganges unentgeltlich oder gegen eine Gebühr erfolgt.

Der Betreiber des Internetcafes wird als so genannter Access-Provider zum Diensteanbieter im Sinne des § 2 Nr. 1 Telemediengesetz (TMG), da er den Zugang zur Nutzung von Telemedien vermittelt. Für die fremden Inhalte (auf den von den Nutzern aufgesuchten Web-Seiten), zu denen der Zugang vermittelt wird, ist ein Access-Provider sowohl gemäß Telemediengesetz als auch gemäß Telekommunikationsgesetz (TKG) in der Regel nicht verantwortlich.

Diensteanbieter sind in der Regel auch nicht verpflichtet, die von ihnen übermittelten oder auf den PCs der Nutzer gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen. Dies bedeutet, dass der Betreiber als diejenige Stelle, die das Abrufen von Internetangeboten ermöglicht, in der Regel nicht für die Tätigkeiten haftet, die der Nutzer ausführt (z.B. Aufsuchen von Seiten mit pornografischen oder extremistischen Inhalten, Herunterladen von Dateien mit pornografischen oder sonstigen jugendgefährdenden Inhalten), außer der Betreiber hat Kenntnis von den entsprechenden Vorgängen und unternimmt nichts dagegen. In diesem Falle haftet der Betreiber für diese Tätigkeiten mit.

Ein Diensteanbieter darf eventuell gespeicherte Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus nur verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Somit müssen personenbezogene Daten, die während der Internetnutzung im Rahmen von systemseitigen Protokollierungen entstehen, spätestens nach Ende der jeweiligen Sitzung gelöscht werden - soweit es sich nicht um Abrechnungsdaten handelt.

Protokollierungen bezüglich der Einhaltung der jugendschutz- und strafrechtlichen Bedingungen sind nur mit Einwilligung der Betroffenen zulässig. Daher sollte in diesem Fall von jedem Internet-Nutzer eine schriftliche Einwilligungserklärung eingeholt werden, die die entsprechenden Nutzungskontrollen erlaubt. In dieser Einwilligungserklärung sind die Formen der Kontrollen ausdrücklich festzulegen. Bei Minderjährigen ist diese Einwilligungserklärung von den Erziehungsberechtigten zu unterschreiben.

Als Fazit ergibt sich, dass der Betrieb eines Internetcafés durch öffentliche Stellen zwar möglich, aber mit zahlreichen Einschränkungen verbunden ist. So ist vor allem zu beachten, dass bei der Nutzung des Internets durch Minderjährige eine visuelle Überwachungspflicht besteht.

2.2.17 Zusammenlegung der EDV-Administration einer Gemeinde und eines Kurbetriebs

In den beiden letzten Jahren haben sich mehrere bayerische Marktgemeinden mit der Frage an mich gewandt, ob gegen eine Zusammenlegung der EDV-Verwaltung ihrer Kommune mit dem örtlichen Kurbetrieb datenschutzrechtliche Bedenken bestehen würden. Ich habe ihnen dazu folgende Auskunft gegeben:

Gegen eine gemeinsame Administration der IT-Anwendungen und -Geräte einer Kommune und ihrer Kurbetriebe ist aus datenschutzrechtlicher Sicht grundsätzlich nichts einzuwenden. Allerdings muss gewährleistet sein, dass alle (wesentlichen) Aktivitäten nicht nur der IT-Benutzer, sondern auch der Systemverwaltung protokolliert werden. Diese Aufzeichnung liegt auch im Interesse einer "ehrlichen" Systemverwaltung, da sie aufgrund der Aufzeichnungen gegebenenfalls nachweisen kann, dass sie nicht verbotenerweise auf Daten zugegriffen, diese gelöscht oder verändert hat, was ihr aufgrund ihrer umfangreichen Zugriffsmöglichkeiten jederzeit möglich wäre. Dazu muss es auch möglich sein, alle Protokollierungen gegen Manipulation (wie Unterdrückung von Nachrichten) und nachträgliche Änderungen (z.B. Löschung von Einträgen) zu schützen.

Diese Protokolle müssen zwar über einen längeren Zeitraum (etwa ein halbes Jahr) aufbewahrt werden, um Verfehlungen gezielt nachgehen zu können. Diese

Protokolle brauchen jedoch nicht online verfügbar zu sein - es genügt, diese auf maschinenlesbaren Datenträgern (z.B. Festplatte, Magnetband, DVD, CD, Streamer Tape) aufzubewahren. Nach Ablauf der vorgegebenen Aufbewahrungsdauer sind alle Protokolldaten - sofern sie nicht zu anderen Zwecken noch benötigt werden - datenschutzgerecht zu entsorgen.

Die regelmäßige Auswertung der Protokolle stellt eine zusätzliche Arbeitsbelastung für die damit beauftragten Personen dar, ist aber unvermeidbar. Sinn dieser Auswertung ist, Zugriffsverletzungen (Fehlverhalten, Eindring- und Missbrauchsversuche) aufzudecken und Sanktionen ergreifen zu können.

Bei der Auswertung dieser Protokolle muss das Vier-Augen-Prinzip gewährleistet sein, d.h. ein Zugriff auf die Protokolldaten und deren Auswertung darf erst nach gemeinsamer Anmeldung eines Systemverwalters und des behördlichen Datenschutzbeauftragten bzw. eines Mitglieds der Personalvertretung möglich sein. Auch diese Maßnahme soll kein generelles Misstrauen gegenüber der IT-Abteilung bezeugen, sondern in erster Linie dazu dienen, dass sich die Personalvertretung - soweit sie es möchte - davon überzeugen kann, dass die Protokolldaten ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebes und nicht für Zwecke der Verhaltens- und Leistungskontrolle verwendet werden. Deshalb müssen die aufgezeichneten Protokolldaten und ihre Auswertung auch für Außenstehende und nicht nur für DV-Fachleute hinreichend aussagekräftig sein.

Falls durch die Zusammenlegung der beiden DV-Abteilungen von Kommune und Kurbetrieb irgendwelche Begehrlichkeiten bezüglich einer erweiterten Zugriffsmöglichkeit der Sachbearbeiter (z.B. Zugriff auf die jeweils anderen Datenbestände) geweckt werden sollten, weise ich die Auskunft suchenden Stellen immer darauf hin, dass auch nach einer erfolgten Zusammenlegung der Grundsatz gilt, dass jeder IT-Berechtigte nur auf die Daten zugreifen darf, die er zur Erfüllung seiner Aufgaben benötigt. Dies schließt im Regelfall eine Zugriffserweiterung aufgrund der Zusammenlegung der IT-Administration aus. Im Übrigen sind im Rahmen der Zugriffsrechtevergabe auch weiterhin einschlägige bereichsspezifische Vorschriften zu beachten. So unterliegen z.B. die besonderen Meldescheine für Beherbungsstätten (Art. 23 und 24 MeldeG) den Nutzungsbeschränkungen nach Art. 26 MeldeG. Der jeweilige behördliche Datenschutzbeauftragte muss natürlich bei der revisionsfähigen Benutzerrechtevergabe beteiligt werden.

2.3 Technische Einzelprobleme

2.3.1 Der Elektronische Personalausweis

Der neue Personalausweis (nPA), der seit dem 01.11.2010 ausgegeben wird, unterscheidet sich sowohl in den äußeren Abmessungen als auch den möglichen Anwendungsgebieten deutlich vom bisherigen Personalausweis. Da dies auch erhebliche Auswirkungen auf die EDV-Verfahren in den ausgebenden Stellen hat, habe ich im Rahmen des Feldtests zur Einführung des nPA mehrere Passämter geprüft.

Der nPA weicht vom alten ID-2 Format (entspricht DIN-A7) ab und hat nun die Größe einer Kredit- bzw. EC-Karte (ID-1 nach ISO/IEC 7810). Im Gegensatz zu

den im Zahlungsverkehr üblichen Karten enthält er keinen Magnetstreifen und keinen kontaktbehafteten Chip, sondern einen kontaktlosen Chip mit Antenne - einen sogenannten RFID (Radio-Frequency Identification) Chip, wie er auch bereits im elektronischen Reisepass verwendet wird.

Zusätzlich zur optischen Identifizierung durch Abgleich von Foto und Unterschrift kann der Nachweis der Identität nun auch vollständig elektronisch erfolgen, so dass neue Anwendungsgebiete etwa im elektronischen Warenverkehr z.B. über das Internet möglich werden. Außerdem kann optional eine qualifizierte elektronische Signatur nach dem Signaturgesetz geladen und verwendet werden.

Gespeicherte Daten

Sichtbar auf dem nPA aufgebracht sind neben der Seriennummer und Zugangsnummer das Lichtbild und die Unterschrift des Ausweisinhabers, Name, Vornamen und ggf. Geburtsname, Doktorgrad, Tag und Ort der Geburt, Größe, Augenfarbe, gegenwärtige Anschrift und die Staatsangehörigkeit. Gegenüber dem vorher ausgegebenen Ausweis ist der Ordens-/Künstlername wieder hinzugekommen, nachdem er 2007 entfernt worden war.

Der Umfang der Daten der aufgedruckten maschinenlesbaren Zeile hat sich gegenüber dem alten Ausweisformat nicht geändert. Neben Seriennummer und Prüfziffern enthält diese Name und Vorname, Tag der Geburt sowie Gültigkeitsdauer des Personalausweises.

Der RFID-Chip kann zusätzlich zu den vorgenannten Daten, genau wie der elektronische Reisepass auch, zwei Fingerabdrücke speichern. Diese Speicherung ist aber freiwillig, so dass bei der Beantragung eines neuen Personalausweises der Bürger selbst entscheiden kann, ob seine Fingerabdrücke aufgenommen werden oder nicht. Aus Sicht des Datenschutzes ist diese Wahlfreiheit begrüßenswert.

Im Gegensatz zum Reisepass besteht die Möglichkeit, Daten auf dem Chip zu aktualisieren, so dass etwa bei einem Umzug zusätzlich zum Überkleben der rückseitig aufgedruckten Anschrift auch die digital gespeicherte Anschrift aktualisiert werden kann.

Elektronischer Identitätsnachweis (eID)

Zusätzlich zu diesen klassischen Funktionen eines Personalausweises kann der Chip auch als elektronischer Identitätsnachweis (eID) verwendet werden. Der Ausweisinhaber kann sich beispielsweise mit Hilfe des nPA und eines geeigneten Lesegerätes im Internet gegenüber einer autorisierten Anwendung ausweisen. Ebenso wie die Speicherung der Fingerabdrücke ist die Aktivierung und Verwendung der eID freiwillig. Sie kann auch nachträglich aktiviert oder deaktiviert werden.

Zugriffsschutz

Der nPA soll nicht unbemerkt ausgelesen werden können (etwa im Vorbeigehen). Jeder Abruf von Daten benötigt neben einem Berechtigungszertifikat auch eine PIN, die bei jedem Auslesen eingegeben werden muss. Der Zugriffsschutz unterscheidet zwischen hoheitlichen Funktionen sowie eID- und Signaturfunktionen.

Bei einer hoheitlichen Funktion, also etwa wenn der nPA bei einer Personenkontrolle geprüft wird, muss das Lesegerät mit einem gültigen, hoheitlichen elektronischen Zertifikat ausgestattet sein, um auf die gespeicherten Ausweisdaten zugreifen zu können. Zusätzlich muss die auf dem Ausweis aufgedruckte Zugriffsnummer eingegeben oder automatisch eingelesen werden. Erst danach kann auf die biometrischen und identifizierenden Daten des nPA zugegriffen werden. Ein Zugriff auf die eID- und Signaturfunktionen ist jedoch auch mit einem hoheitlichen Zertifikat nicht möglich. Die aufgedruckte Zugriffsnummer soll verhindern, dass der nPA "im Vorbeigehen" automatisch ausgelesen wird, da in diesem Fall die Zugriffsnummer nicht bekannt wäre und ein Verbindungsaufbau somit unmöglich ist.

Jede Anwendung, die den nPA zur elektronischen Identifizierung (eID-Funktion) verwenden möchte, benötigt ein Zertifikat des Bundesverwaltungsamts. Über dieses wird für jede Anwendung festgelegt, welche Daten sie vom nPA auslesen darf und kann. Der Chip verhindert ein unberechtigtes Auslesen, so dass beispielsweise bei einer reinen Altersverifikation das Auslesen der Anschrift unmöglich ist.

Um die eID nutzen zu können, benötigt der Inhaber eine PIN, die er bei oder vor der Ausgabe des nPA erhält. Bei jeder Identitätsfeststellung muss diese PIN vom Inhaber eingegeben werden. Die eID ist eine komplexe Funktion, die eine Vielzahl von Möglichkeiten bietet, bestimmte Daten einer Anwendung zur Verfügung zu stellen. Es ist auch möglich, Pseudonyme zu bilden, so dass zwei unterschiedliche Anwendungen, bei denen sich der nPA identifiziert hat, nicht erkennen können, dass es sich um die gleiche Person handelt. Ein Zugriff auf das Foto, die Unterschrift oder die Fingerabdrücke ist über die Zertifikate für die eID generell nicht möglich.

Sicherheit des Gesamtsystems

Auch wenn aus Sicht des Datenschutzes die Verwendung von RFID-Chips grundsätzlich bedenklich ist, so wurde für den nPA eine Vielzahl von Sicherheitsmaßnahmen entwickelt, die für den Chip eine ausreichende Sicherheit gewährleisten können sollten. Auch wenn der nPA an sich nicht in meinen originären Aufgabenbereich fällt, so habe ich die Entwicklung im Rahmen des Arbeitskreises Technische und organisatorische Datenschutzfragen der Datenschutzbeauftragten des Bundes und der Länder der Datenschutzkonferenz und in Treffen mit dem Bundesministerium des Inneren mit begleitet.

Die Sicherheit des Ausweises allein reicht allerdings nicht aus, um den Datenschutz zu gewährleisten. Aus meiner Sicht sind auch die Systeme, die auf den Ausweis elektronisch zugreifen und die Daten weiterverarbeiten, kritisch zu sehen.

Bei der Verwendung der eID Funktion ist dies in der Regel der PC des Nutzers mit angeschlossenem Lesegerät, der den bekannten Angriffsszenarien wie Viren und Spyware ausgesetzt ist. Ein sicherer PC ist Grundvoraussetzung für einen sicheren Einsatz der eID Funktion über das Internet.

Darüber hinaus muss sichergestellt werden, dass personenbezogene Daten, die mit eID-Zertifikaten ausgelesen wurden, auch nur zweckgebunden genutzt und nicht etwa unberechtigt an Dritte weitergeben werden. Die Kontrolle darüber ob-

liegt dem Bundesverwaltungsamt als ausgebender Stelle für die Berechtigungszertifikate und den jeweils zuständigen Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich.

Bei der Beantragung, Änderung und Sperrung der Ausweise müssen alle gesetzlichen Vorgaben beachtet werden. Deshalb habe ich den in einigen Städten und Gemeinden vorab durchgeführten Feldversuch mit mehreren Prüfungen begleitet. Das Hauptaugenmerk lag hier auf den in den Behörden eingesetzten Software- und Hardwarekomponenten. Speziell bei der Verarbeitung und Speicherung der biometrischen Daten ist sicherzustellen, dass diese nur innerhalb der erlaubten Fristen außerhalb des Ausweises gespeichert werden. Spätestens nach der Aushändigung des Ausweises sind die Fingerabdrücke zu löschen.

Bei der Prüfung der bisher verwendeten Software für den elektronischen Reisepass hatten wir bereits festgestellt, dass bei einigen Softwareprodukten die Fingerabdrücke etwa auf Sicherungsbändern länger als erlaubt gespeichert blieben (siehe hierzu 23. Tätigkeitsbericht, Nr. 25.4.8). Deshalb habe ich bei den Prüfungen der Feldtestinstallationen die Softwarehersteller darauf hingewiesen, dass mit der Einführung des nPA die biometrischen Fingerabdruckdaten von der regulär stattfindenden sonstigen Datensicherung ausgenommen werden müssen. Dies wurde zugesichert und ich werde in nächster Zeit stichprobenartig Nachprüfungen vornehmen.

Besonders wichtig ist aus meiner Sicht auch, dass das Personal in den ausgebenden Stellen die Antragssteller auf die neuen Funktionen des nPA und die Möglichkeit, Fingerabdrücke nicht abzugeben und die eID ausschalten zu lassen, ausführlich und verständlich hinweist. Den Antragsstellern muss klar mitgeteilt werden, dass die eID-Funktion nicht für die hoheitliche Verwendung des Ausweises als Identifizierungsmerkmal benötigt wird und dass sie keinerlei Nachteile zu befürchten haben, wenn sie der Speicherung der Fingerabdrücke nicht zustimmen. Auch dies werde ich in Zukunft in meine Prüfungen mit einbeziehen.

Aus meiner Sicht bedenklich sind die bei den Ausweisbehörden eingesetzten Lese- und Schreibgeräte - zumindest bei den von mir geprüften Behörden. Zum einen war bei einer Änderung der PIN durch den Antragsteller nicht sichergestellt, dass Dritte die Eingabe nicht beobachten können, da kein Sichtschutz der Eingabe wie etwa bei EC-Automaten vorhanden ist. Alle Daten, die auf dem nPA Chip gespeichert sind, können nur am Sachbearbeiterbildschirm angezeigt werden. Ein Standalone-Leserät, das wie beim elektronischen Reisepass sicherstellt, dass die im Chip gespeicherten Daten angezeigt werden können, ist für den nPA nicht vorgesehen. Auch haben Ausweisinhaber und ausstellende Behörde keine Möglichkeit, die Korrektheit der gespeicherten Fingerabdrücke zu prüfen. Sollten durch ein Versehen oder einen Softwarefehler falsche Fingerabdruckdaten auf den Chip gelangen, so wird dies unter Umständen erst Jahre später - etwa bei einer polizeilichen Kontrolle - auffallen. Bei diesen Lese- und Schreibgeräten besteht meiner Meinung nach erheblicher Nachbesserungsbedarf.

2.3.2 Deutschland Online KFZ - Kfz-Zulassung über das Internet

Deutschland Online ist die nationale E-Government-Strategie von Bund, Ländern und Kommunen für eine moderne öffentliche Verwaltung. Ein Projektbereich dieser Initiative ist der Bereich Kfz-Wesen, da dies einer der häufigsten Fälle ist,

bei denen die Bürger mit Behörden im direkten Kontakt stehen. Zukünftig sollen die mit einer Fahrzeugregistrierung verbundenen Abläufe (z.B. An-, Um-, Abmeldung) möglichst durchgängig elektronisch abgewickelt werden können.

Viele Landratsämter und Städte in Bayern bieten bereits heute die Möglichkeit, Wunschkennzeichen über das Internet zu reservieren. Bei einigen Zulassungsstellen können zudem bereits vorab alle zur An-, Um- oder Abmeldung benötigten Angaben über das Internet erfasst und an die Zulassungsstelle geschickt werden. Zudem kann ein Termin vereinbart werden, an dem dann die restlichen erforderlichen Schritte durchgeführt werden. Eine vollständig elektronische Beantragung ist allerdings erst möglich, wenn der Bürger ein elektronisches Ausweisdokument besitzt, mit dem er sich im Internet eindeutig ausweisen und rechtskräftig elektronisch unterschreiben kann. Dies soll zukünftig durch den elektronischen Personalausweis (siehe hierzu Nr. 2.3.1) ermöglicht werden. Für eine vollständig elektronische Abwicklung der Vorgänge müssen zudem alle benötigten Dokumente in rechtsgültiger elektronischer Form vorliegen. Die Nummernschilder können dem Bürger durch einen Hol- und Bringdienst übergeben werden, so dass der Behördengang für ihn völlig entfällt. Elektronische Nummernschilder o.ä., so dass auch dieser Medienbruch entfällt, werden allerdings wohl erst in ferner Zukunft realisierbar sein.

Wenn auf den Webseiten von Gemeinden und Landratsämtern nicht nur Informationen, sondern auch E-Government-Anwendungen angeboten werden, dann steigt auch der technische Aufwand, der betrieben werden muss, um die Webseite und Abläufe gegen unbefugte Kenntnisnahme, Manipulation, Datenverlust etc. zu schützen. Für eine vollständige Online-Zulassung werden umfangreiche und sensible Daten zum Fahrzeug und zum Bürger benötigt, wie z.B. Name, Adresse, Fahrzeugtyp, Bankverbindung, Angaben zur Versicherung.

Da die Dienste für den Bürger über das Internet erreichbar sein sollen, müssen IT-Systeme, die bisher ohne Verbindung zum Internet betrieben wurden, an das Internet angebunden werden. Hierzu müssen Schutzmaßnahmen nach dem Stand der Technik ergriffen werden, wie Firewall, Intrusion Detection / Prevention Systems, Virenscanner etc, um gegen die Bandbreite der aktuell verfügbaren Angriffe geschützt zu sein. Zudem muss sich der Server, bei dem der Bürger seine Daten eingeben soll, durch ein Zertifikat ausweisen. Der Bürger muss sicher sein, dass er seine Daten auch wirklich beim Server der Behörde eingibt.

Des Weiteren ist zwingend eine verschlüsselte Verbindung erforderlich, da ansonsten die sensiblen Daten des Bürgers ungeschützt über das Internet übertragen werden. Diese Verbindung sollte so ausgestaltet werden, dass der Benutzer selbst überprüfen kann, ob tatsächlich eine verschlüsselte Verbindung besteht, z.B. über die Funktionen aktueller Browser.

Damit auch die Behörde sicher sein kann, dass sie mit dem richtigen Bürger kommuniziert, muss ein sicheres Verfahren zur Identifikation und Authentifikation des Benutzers vorhanden sein. Dies wird in Zukunft wahrscheinlich vor allem der elektronische Personalausweis sein.

Zudem muss der Bürger sich darüber im Klaren sein, dass wie beispielsweise beim Online-Banking auch, seine Daten nur geschützt sind, wenn er selbst seinen PC gegen Angriffe wie Trojaner, Keylogger etc. schützt. Sind die eingegebenen Daten bereits am lokalen PC abgreifbar, bieten die Schutzmaßnahmen der Be-

hörde keine Sicherheit. Deswegen sollte die Nutzung des elektronischen Angebots nicht verpflichtend werden, sondern immer als Alternative auch der Weg zur Zulassungsstelle möglich sein.

2.3.3 Intelligente Stromzähler - Smart Meter

Auch wenn das Thema Smart Meter vorwiegend in den Zuständigkeitsbereich der Aufsichtsbehörden für den nicht-öffentlichen Bereich fällt, hat sich der Arbeitskreis Technische und organisatorische Datenschutzfragen der Datenschutzbeauftragten des Bundes und der Länder in Zusammenarbeit mit dem Düsseldorfer Kreis als Zusammenschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich mit diesem Thema beschäftigt. Das Thema fällt nur dann in meinen Zuständigkeitsbereich, wenn kommunale Versorgungswerke als Bestandteile der einheitlichen Behörde „Gemeindeverwaltung“ Smart Meter einsetzen.

Seit Januar 2010 sind Energieversorgungsunternehmen nach dem Energiewirtschaftsgesetz (EnWG) verpflichtet, ihren Kunden Messeinrichtungen anzubieten, die den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegeln. Für Neubauten ist der Einbau derartiger "Intelligenter Stromzähler" oder "Smart Meter" verpflichtend.

Gegenüber den bisherigen Stromzählern soll bei der neuen Generation zusätzlich zum aktuellen und zum Gesamtverbrauch seit Herstellung des Zählers auch etwa der Verbrauch der letzten 24 Stunden, der letzten Woche und des letzten Monats angezeigt werden. Es ist aber auch denkbar, den Verbrauch in sehr kurzen Zeitabständen (im Minutenbereich) zu messen und diesen dann unmittelbar elektronisch an das Versorgungsunternehmen zu übermitteln.

Grundsätzlich sind derartige Verbrauchswerte von privat genutzten Immobilien personenbezogene Daten, da sie unter Umständen Rückschlüsse über die Lebensgewohnheiten der dort wohnenden Personen ermöglichen - etwa ob die Bewohner im Urlaub sind oder wann sie morgens das Haus verlassen. Ein Rückschluss darauf, welches Gerät jeweils eingeschaltet ist, ist dabei jedoch nicht möglich.

Aus technisch-organisatorischer Sicht des Datenschutzes ist es wichtig, dass kein unbefugter Dritter auf diese Verbrauchswerte zugreifen kann, etwa in dem er die Daten fremder Zähler in einem Gemeinschaftszählerraum eines Mietshauses ausliest. Hierfür sind vom Betreiber der Zähler geeignete Maßnahmen zu treffen, um die Verbrauchsdaten gegen unbefugtes Auslesen ausreichend zu schützen.

Auch bei intelligenten Stromzählern ist das Prinzip der Datenvermeidung und Datensparsamkeit zu beachten. Der Kunde muss weiterhin die Hoheit über seine Daten haben und die Verarbeitung dieser muss für ihn so transparent wie möglich sein. Ablesezeitpunkte, Ableseintervalle und Übertragungswege müssen daher mit ihm vertraglich vereinbart werden.

Sollen weitere als die abrechnungsrelevanten Daten an den Energieversorger übermittelt werden, so erfordert dies das Einverständnis der Betroffenen.

Soll zusätzlich oder anstatt der optischen Ablesung eine elektronische Auslesung und Übertragung der Daten erfolgen, so ist diese gegebenenfalls mit kryptographischen Verfahren abzusichern.

Wünschenswert aus Sicht des Datenschutzes wäre, dass keine nicht abrechnungsrelevanten Daten erfasst werden, solange dies der Kunde nicht explizit wünscht. Wünscht der Kunde es aber, so sollten die Daten soweit wie möglich in der Hand des Kunden bleiben, in dem sie etwa direkt auf eine lokale Anzeigeeinrichtung (PC etc.) übertragen und nicht zentral beim Energieversorger gespeichert werden.

Vor diesem Hintergrund hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Sitzung am 03./04.11.2010 nachfolgende Entschließung gefasst:

Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010
Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z.B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der

durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

2.3.4 Fundsachen mit digitalen Inhalten

In kommunalen Fundbüros werden vermehrt Fundsachen abgegeben, die digitale Speichermedien enthalten, wie beispielsweise Laptops, Mobiltelefone und Kameras. Holt der Eigentümer die Fundsachen nicht innerhalb von sechs Monaten ab und beansprucht der Finder nicht das Eigentum, so darf das Fundbüro die Fundsache versteigern. Aus datenschutzrechtlicher Sicht kann sich ein solches Versteigern aber nicht auf die auf den Fundsachen digital gespeicherten Inhalte beziehen.

Daher sind vor einer Versteigerung dieser Gegenstände an den Ersteiger die Daten durch das Fundbüro sicher zu löschen. Ich weise darauf hin, dass die Betätigung einfacher "Löschfunktionen" etwa einer Speicherkarte oder Festplatte unter Umständen sehr leicht wieder rückgängig gemacht werden kann. Sie ist ggf. nicht als Löschung im Sinne des Art. 4 Abs. 6 Nr. 5 BayDSG anzusehen. Geräte oder Datenträger, bei denen der Verdacht besteht, dass sie personenbezogene Daten erhalten, und bei denen eine Löschung nicht oder nicht mit angemessenem Aufwand erfolgen kann, sind datenschutzgerecht zu entsorgen.

2.3.5 Beleg- und E-Mail-Archivierung

Viele Behörden stellt die stetig wachsende Flut von aufzubewahrenden Dokumenten vor große Probleme, belegen diese Dateien doch immer mehr Speicherplatz, was wiederum entsprechende Kosten für eine Hardware-Erweiterung

verursacht. Dieses Speicherproblem wird in der Zukunft eher noch relevanter werden, da es auch im eigenen Interesse immer notwendiger wird, beispielsweise auch E-Mails langfristig aufzubewahren. Dies dient auch der Vorsorge für Rechtsstreitigkeiten, da häufig nur mit Hilfe gespeicherter elektronischer Dokumente ein bestimmter Sachverhalt nachvollzogen werden kann.

Grundsätzlich ist zu unterscheiden zwischen einer Langzeitaufbewahrung, um spezifischen gesetzlichen Forderungen wie z.B. den Grundsätzen ordnungsgemäßer Buchführung (GOBS), dem Gesetz zur Kontrolle und Transparenz im Geschäftsverkehr (KonTraG) sowie dem Handelsgesetzbuch (HGB) Rechnung zu tragen, und einer Archivierung im Sinne des Bayerischen Archivgesetzes (BayArchivG) vom 22.12.1989.

Für die Archivierung im Sinne des BayArchivG sind im Bereich der staatlichen Verwaltung zentrale Bemühungen in Zusammenarbeit mit dem Bayerischen Staatsarchiv im Gange. An dieser Stelle soll daher nur auf die Langzeitaufbewahrung eingegangen werden.

Es ist wichtig und sinnvoll, wichtige Unterlagen und Dokumente zentral und zugriffssicher im Rahmen der Zulässigkeit und Erforderlichkeit längerfristig aufbewahren zu können. Dabei kommt den elektronischen Dokumenten zunehmend größere Bedeutung zu, wobei bei diesen insbesondere auch gewährleistet sein muss, dass deren Integrität, Vertraulichkeit und Authentizität über den gesamten Zeitraum der Aufbewahrung erhalten bleibt.

Konkrete Produktbewertungen bzw. Produktempfehlungen kann ich aus rechtlichen Gründen nicht abgeben. Allerdings seien hier datenschutzrelevante Kriterien für die Auswahl eines Produktes genannt:

Bei der Langzeitaufbewahrung von Dokumenten mit personenbezogenen Daten sind die Grundsätze der Verhältnismäßigkeit, der Zweckmäßigkeit und der Datensparsamkeit zu beachten. Somit dürfen nur die Daten archiviert werden, die unbedingt benötigt werden und solange es der dienstliche Zweck erfordert. Die anderen personenbezogenen Unterlagen, deren Kenntnis zur Aufgabenerfüllung nicht mehr benötigt werden, sind datenschutzgerecht zu löschen bzw. zu vernichten. Dabei sind auch eventuelle Löschungspflichten zu beachten. So ist bei der Produktauswahl darauf achten, dass das gewählte System diese Möglichkeiten anbietet.

Während der gesamten Aufbewahrungsdauer muss auch die Vertraulichkeit der Dokumente gewährleistet sein. Dazu sind unter Umständen entsprechende Verschlüsselungsroutinen einzusetzen (z.B. zum Schutz von Personalunterlagen gegen eine unbefugte Kenntnisnahme).

Außerdem sollte mit Hilfe einer revisionsfähigen Zugriffsrechtevergabe gewährleistet werden, dass nur dazu Berechtigte auf die Dokumente zugreifen können. Dies erhöht gleichzeitig den Veränderungsschutz.

Zur Gewährleistung der Integrität und Authentizität der Dokumente bietet sich der Einsatz der elektronischen Signatur an. Durch die elektronische Signatur kann zwar keine Datenveränderung verhindert werden, andererseits kann aber an Hand der Überprüfung der Signatur festgestellt werden, ob die Daten verändert wurden.

Erfolgt eine Aufbewahrung auch zum Zwecke der Beweissicherung, sollte eine qualifizierte elektronische Signatur (nach Signaturgesetz - SigG) zum Einsatz kommen, da derart signierte Dokumente eine höhere Beweiskraft besitzen und die Verkehrsfähigkeit dieser Dokumente gewährleistet ist.

Mit einem Langzeitspeichersystem müssen zudem die Rechte der Betroffenen - insbesondere bezüglich ihres Auskunftsanspruchs - sichergestellt werden können.

Umfasst die Langzeitaufbewahrung auch E-Mails und gestattet eine Behörde den Mitarbeitern die private E-Mail-Nutzung oder duldet sie, ist sie ihren Bediensteten gegenüber Telemedien- bzw. Teledienste-Anbieter und zur Wahrung des Fernmeldegeheimnisses gemäß § 88 TKG verpflichtet. Bei einer gestatteten Privatnutzung ist für die revisionsfähige E-Mail-Langzeitaufbewahrung neben einer entsprechenden Vereinbarung mit der Beschäftigtenvertretung auch das schriftliche Einverständnis aller betroffenen Mitarbeiter einzuholen.

Verweigert ein Bediensteter sein Einverständnis, wird ihm im Regelfall die Privatnutzung des dienstlichen E-Mail-Accounts untersagt. Dann gelten alle E-Mails als Teil der dienstlichen Korrespondenz und sie dürfen regelmäßig langzeitaufbewahrt werden.

Gelegentlich stellt eine Behörde auch jedem Mitarbeiter sowohl einen dienstlichen als auch einen privaten Account zur Verfügung. Langzeitaufbewahrt werden dann nur die (dienstlichen) E-Mails, die sich im dienstlichen Account befinden.

2.3.6 Unterarbeitsgruppe Krankenhausinformationssysteme

Die Datenverarbeitung in Krankenhäusern entwickelt sich zunehmend hin zu einer elektronischen Datenverarbeitung. Zusätzlich ändern sich auch die Organisationsstrukturen und Prozessabläufe in Richtung einer flexibleren und interdisziplinären Behandlung, bei der eine Vielzahl von Behandlern aus unterschiedlichen Bereichen auf die Daten eines Patienten zugreifen muss. Die neuen Strukturen und Anforderungen sind in heutigen Krankenhausinformationssystemen (KIS) nur unzureichend umgesetzt und führen in der Praxis bei Datenschutzprüfungen immer wieder zu Diskrepanzen zwischen dem, was rechtlich erforderlich wäre und dem, was technisch mit vertretbarem Aufwand möglich ist.

So habe ich z.B. immer wieder festgestellt, dass Zugriffsrechte aus dem Blickwinkel des Erforderlichkeitsprinzips und der ärztlichen Schweigepflicht technisch bedingt zu umfassend und unflexibel vergeben werden. Im Extremfall führt dies dazu, dass alle Ärzte eines Krankenhauses Zugriff auf alle Patientendaten haben. Es ist zwar nur ein kleiner Teil der Ärzte wirklich Behandler, aber um flexibel Vertretungen, Notfälle, Konsile oder auch interdisziplinäre Behandlungspfade abzubilden, erhalten schlichtweg alle Ärzte Zugriff.

Eine Protokollierung und Auswertung lesender Zugriffe, um Missbräuche überhaupt aufdecken zu können, findet in vielen Fällen nicht statt oder wird durch das KIS erst gar nicht angeboten. Auch fehlen häufig entsprechende Tools, die eine effiziente Auswertung von Protokolldaten ermöglichen.

Des Weiteren ist es häufig der Fall, dass die Patientendaten auch Jahre nach der Entlassung des Patienten für die ehemaligen Behandler online noch abrufbar

sind, obwohl dies längst nicht mehr erforderlich ist. Eine Sperrung von Daten nach der Entlassung des Patienten ist nicht in allen Häusern umgesetzt. Häufig gibt es zudem kein Konzept, wie die Patientendaten oder zumindest einzelne Behandlungsfälle nach Ablauf der Aufbewahrungsfristen gelöscht werden. Viele KIS sehen diese Möglichkeit nicht oder nur unzureichend vor.

Zudem stehen in vielen Fällen auch bei einer Wiederaufnahme eines Patienten die Daten aus früheren Krankenhausaufenthalten ohne weiteres zur Verfügung. Eine Information des Patienten hierüber sowie die Möglichkeit, auf Wunsch des Patienten den Zugriff auf Vorbehandlungsdaten, z.B. bei Erkrankungen, die dem Ansehen schaden, einzuschränken, ist häufig nicht vorgesehen.

Vor diesem Hintergrund wurde im Jahr 2009 von den Arbeitskreisen Technische und organisatorische Datenschutzfragen sowie Gesundheit und Soziales der Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Unterarbeitsgruppe zum Thema Krankenhausinformationssysteme (UAG KIS) unter der Federführung Berlins eingerichtet, in der ich Mitglied bin. Darüber hinaus sind Vertreter des Düsseldorfer Kreises sowie der Kirchen beteiligt. Neben den Treffen in Berlin habe ich auch die behördlichen Datenschutzbeauftragten großer bayerischer Krankenhäuser zu einem Meinungsaustausch eingeladen, um die Anforderungen zu diskutieren. Ziel der Arbeitsgruppe ist, in Form einer Orientierungshilfe bundesweit einheitliche Anforderungen an KIS zu formulieren.

Die in Arbeit befindliche Orientierungshilfe besteht aus zwei Teilen: Im ersten Teil sollen die rechtlichen Anforderungen definiert werden. Da heute nicht alle diese Forderungen in den KIS abgebildet oder nur mit großem Aufwand umsetzbar sind, sollen im zweiten Teil der Orientierungshilfe die daraus abgeleiteten technischen Anforderungen formuliert und mit Experten und Herstellern diskutiert werden, um deren Realisierung zu erreichen.

Diese derzeit noch in Arbeit befindlichen Vorgaben werden nach ihrer Veröffentlichung unter Berücksichtigung landesrechtlicher Besonderheiten den Rahmen meiner Prüfungen und Beratungen in Bayern bilden. Sie werden die Aussagen zu KIS in früheren Tätigkeitsberichten (siehe hierzu 18. Tätigkeitsbericht 1998, Nr. 3.3.2) oder der Orientierungshilfe "Technisch-organisatorische Forderungen an ein benutzer- und datenschutzfreundliches Patientenverwaltungssystem bzw. Krankenhausinformationssystem (KIS)", konkretisieren bzw. an die Gegebenheiten moderner Krankenhausorganisationen anpassen.

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009
Krankenhausinformationssysteme datenschutzgerecht gestalten!

- *Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen allerdings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.*

- *Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.*
- *Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.*
- *Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.*
- *Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.*

3 Polizei

Im Polizeibereich habe ich auf die datenschutzkonforme Ausgestaltung von Gesetzen und Errichtungsanordnungen zu Dateien hingewirkt. Schwerpunkte waren dabei die Streichung der Möglichkeit zur "nur automatischen Aufzeichnung" bei der polizeilichen Wohnraumüberwachung und die Streichung der Befugnis zur heimlichen Wohnungsdurchsuchung im Polizeiaufgabengesetz (PAG).

Darüber hinaus habe ich insbesondere die Kontrolle von Speicherungen in Dateien überprüft, wie z.B. in der polizeilichen Vorgangsverwaltungsdatei "IGVP" und im Kriminalaktennachweis (KAN). Die datenschutzrechtliche Beurteilung von Datenerhebungsmaßnahmen wie z.B. Videoaufzeichnungen von Versammlungsteilnehmern und Fußballfans, erkennungsdienstlichen Behandlungen und Speichelprobenentnahmen zum Zwecke der DNA-Analyse und die Überprüfung von Auskunftserteilungen zu Speicherungen waren ebenfalls Schwerpunkte im Berichtszeitraum. Darüber hinaus habe ich auch wieder Datenübermittlungen der Polizei an die Presse überprüft. Neben der Kontrolle von Datenerhebung, -nutzung und -verarbeitung durch die Polizei aufgrund von Bürgereingaben, Pressemitteilungen und sonstigen Meldungen habe ich erneut anlassunabhängige Prüfungen beim Landeskriminalamt und bei drei Präsidien vorgenommen.

Meine datenschutzrechtliche Beratung von Polizeidienststellen umfasste auch Vorträge bei Aus- und Fortbildungsveranstaltungen der Polizei.

Die nachfolgenden Darstellungen enthalten eine Auswahl meiner Feststellungen im Polizeibereich.

3.1 Änderungen des Polizeiaufgabengesetzes

In meinem letzten Tätigkeitsbericht berichtete ich über umfangreiche Änderungen des Polizeiaufgabengesetzes (PAG). Diese enthielten - wie die Befugnisse zur "Online-Durchsuchung" und zur "heimlichen Wohnungsdurchsuchung" - neue, zum Teil tiefgreifende Eingriffsbefugnisse, die das Recht auf informationelle Selbstbestimmung erheblich einschränkten.

Zum 01.08.2009 wurden einige der am 01.08.2008 in Kraft getretenen Regelungen polizeilichrechtlicher Befugnisse wieder entschärft (siehe hierzu Nr. 3.1.1 bis 3.1.4).

Die damit eingetretenen Änderungen enthalten nicht unwesentliche datenschutzrechtliche Verbesserungen gegenüber der bisherigen Gesetzeslage.

3.1.1 Verzicht auf eine "nur automatische Aufzeichnung" beim sog. Großen Lauschangriff

Die bisherige Gesetzeslage gestattete es der Polizei, in Privatwohnungen geführte Gespräche im Rahmen einer Wohnraumüberwachung ("Großer Lauschangriff") nur automatisch aufzuzeichnen. Gleiches galt für die Aufzeichnung von Gesprächen mit sog. Berufsgeheimnisträgern (z.B. Geistliche, Ärzte, Rechtsanwälte), wenn diese selbst Zielperson der Maßnahme waren und die Gespräche in

den zur Berufsausübung bestimmten Räumlichkeiten stattfanden. Bereits in seinem Urteil vom 03.03.2004 zum "Großen Lauschangriff" hat das Bundesverfassungsgericht ausdrücklich darauf hingewiesen, dass "es der Schutz des Art. 1 Abs. 1 GG erforderlich machen [kann], bei dem Abhören einer Privatwohnung auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, um jederzeit die Ermittlungsmaßnahme unterbrechen zu können." Führt ein Polizeibeamter die akustische Wohnraumüberwachung durch, kann er erkennen, wenn sich Gespräche mit höchstpersönlichem Inhalt anbahnen. Gemäß dem Menschenwürdeschutz sind dann Überwachungsmaßnahmen zu unterbrechen. Eine nur automatisierte Aufzeichnung führt dagegen dazu, dass solche menschenwürderelevanten Gespräche erfasst werden. Vor dem Hintergrund dieser Hinweise des Gerichts habe ich deshalb die grundsätzliche Möglichkeit einer nur automatischen Datenerhebung aus Wohnungen für sehr problematisch angesehen. Mit der Streichung dieser Befugnis hat der Gesetzgeber eine langjährige datenschutzrechtliche Forderung von mir erfüllt (siehe hierzu 21. Tätigkeitsbericht, Nr. 7.12.2).

Leider hat der Gesetzgeber die Gesetzesänderung nicht auch dazu genutzt, die im Gesetz vorgesehene Unterscheidung zwischen "weniger" und "mehr" geschützten Berufsgeheimnisträgern aufzugeben. Berufsgeheimnisträger können im Strafprozess unter Berufung auf ihre Schweigepflicht die Aussage verweigern. Das Polizeiaufgabengesetz verbietet der Polizei hingegen nur, in Privatwohnungen geführte Gespräche abzuhören, über die Geistliche, Verteidiger, Rechtsanwälte, Ärzte, Berater für Fragen der Betäubungsmittelabhängigkeit, psychologische Psychotherapeuten oder Kinder- und Jugendlichenpsychotherapeuten die Aussage verweigern können. Das gilt auch, wenn das Gespräch einen unmittelbaren Bezug zu einer dringenden Gefahr für z.B. Leib, Leben oder Freiheit einer Person aufweisen sollte. Nur wenn solche Berufsgeheimnisträger ebenfalls Zielpersonen der Maßnahme sind, dürfen die Gespräche erfasst werden.

Im Gegensatz dazu dürfen jedoch Gespräche mit anderen Berufsgeheimnisträgern (z.B. Notaren, Zahnärzten, Apothekern, Hebammen und Schwangerenkonfliktberatern) bereits dann abgehört werden, wenn sie einen unmittelbaren Bezug zu einer dringenden Gefahr für z.B. Leib, Leben oder Freiheit einer Person aufweisen. Bei diesen Berufsgruppen ist nicht erforderlich, dass der Berufsgeheimnisträger selbst auch Zielperson der Maßnahme ist.

Aus datenschutzrechtlicher Sicht erkenne ich nach wie vor keinen sachlichen Grund für die konkret getroffene Differenzierung zwischen "mehr" und "weniger" geschützten Berufsgeheimnisträgern. Der Abhörschutz dient dazu, die Vertrauensbeziehung zwischen dem Berufsgeheimnisträger und dem betroffenen Gesprächspartner zu schützen. In diesem Sinne führt beispielsweise eine werdende Mutter bei einer Schwangerschaftskonfliktberatung mindestens mit einer vergleichbar hohen Wahrscheinlichkeit höchstpersönliche Gespräche wie z.B. mit einem Arzt oder einem Berufspsychologen. Ich habe im Gesetzgebungsverfahren deshalb gefordert, auf die Unterscheidung zwischen "privilegierten" und "anderen" Berufsgeheimnisträgern zu verzichten oder zumindest eine nachvollziehbare Differenzierung vorzusehen.

3.1.2 Regelung der Benachrichtigungspflicht bei der "polizeilichen Beobachtung"

Mit der ausdrücklichen Regelung einer grundsätzlichen Benachrichtigungspflicht bei der "polizeilichen Beobachtung" wurde eine langjährige datenschutzrechtliche Forderung von mir erfüllt (siehe hierzu 23. Tätigkeitsbericht, Nr. 4.1.4). Nach der ständigen Rechtsprechung des Bundesverfassungsgerichts steht den Bürgerinnen und Bürgern bei für sie nicht erkennbaren Grundrechtseingriffen grundsätzlich ein Anspruch auf spätere Kenntnis der staatlichen Maßnahme zu. Ohne eine solche Kenntnis können die Betroffenen weder die Unrechtmäßigkeit der Informationsgewinnung noch etwaige Rechte auf Löschung der gespeicherten Daten geltend machen.

3.1.3 Abschaffung der Befugnis zur heimlichen Wohnungsdurchsuchung

Ebenfalls wieder gestrichen wurde die zum 01.08.2008 in Kraft getretene Befugnis für die Polizei, zur Durchführung einer Wohnraumüberwachung, einer Telekommunikationsüberwachung oder einer Online-Durchsuchung die Wohnung des Betroffenen heimlich zu betreten und zu durchsuchen (zur Streichung der entsprechenden Befugnis des Landesamts für Verfassungsschutz siehe hierzu Nr. 4.1). Auch hier hat der Gesetzgeber mit der Änderung meinen erheblichen verfassungsrechtlichen Bedenken Rechnung getragen, die ich im Gesetzgebungsverfahren vorgetragen hatte.

3.1.4 Kürzere Aufbewahrungsfrist für polizeiliche Bild- und Tonaufnahmen

Seit 01.08.2009 darf die Polizei zur Gefahrenabwehr gefertigte personenbezogene Bild- und Tonaufnahmen oder -aufzeichnungen (z.B. von stationären polizeilichen Überwachungskameras) und daraus gefertigte Unterlagen grundsätzlich nur noch drei Wochen statt bisher zwei Monate aufbewahren. Auch diese Gesetzesänderung stellt eine erhebliche datenschutzrechtliche Verbesserung der Rechte der Betroffenen dar. Nicht erfasst von dieser Neuregelung ist allerdings die Speicherung von Bild- und Tonaufnahmen oder -aufzeichnungen von Versammlungsteilnehmern; diese ist im Bayerischen Versammlungsgesetz speziell geregelt (siehe hierzu Nr. 3.2.2).

Werden die Aufzeichnungen der Polizei jedoch zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder von Straftaten benötigt, dürfen sie länger gespeichert werden.

3.2 Änderungen des Bayerischen Versammlungsgesetzes (BayVersG)

Bereits in meinem letzten Tätigkeitsbericht (siehe hierzu 23. Tätigkeitsbericht, Nr. 4.2) hatte ich über die wesentlichen datenschutzrechtlich relevanten Regelungen des neuen Bayerischen Versammlungsgesetzes berichtet. Meine Kritik hatte dabei vor allem die neu geschaffene Befugnis zur Anfertigung polizeilicher "Übersichtsaufzeichnungen" und ihre zeitlich unbefristete Speicherung und Nutzung zum Gegenstand. Mehrere Landesverbände von Gewerkschaften und Parteien sowie andere nichtstaatliche Organisationen haben gegen annähernd das gesamte Bayerische Versammlungsgesetz Verfassungsbeschwerde eingelegt. In seiner Eilanordnung vom 17.02.2009 hat das Bundesverfassungsgericht vor al-

lem die sehr weitgehenden polizeilichen Befugnisse zu Anfertigung und Speicherung sog. Übersichtsaufnahmen und -aufzeichnungen beschränkt und zum Teil sogar außer Kraft gesetzt (siehe hierzu Nr. 3.2.1). Eine abschließende Entscheidung des Bundesverfassungsgerichts steht noch aus. Vor dem Hintergrund der vom Gericht gemachten Hinweise hat der Landtag am 14.04.2010 umfangreiche Gesetzesänderungen beschlossen; die Änderungen sind am 01.06.2010 in Kraft getreten (siehe hierzu Nr. 3.2.2).

3.2.1 Bayerisches Versammlungsgesetz teilweise außer Kraft gesetzt - Die einstweilige Anordnung des Bundesverfassungsgerichts vom 17.02.2009

Das Bundesverfassungsgericht hat mit deutlichen Worten insbesondere die - inzwischen geänderte (siehe hierzu Nr. 3.2.2) - Befugnis der Polizei zur Anfertigung von sog. Übersichtsaufzeichnungen kritisiert. Sie ermächtige zu einer anlasslosen Aufzeichnung des gesamten Versammlungsgeschehens einschließlich der Ablichtung der einzelnen Versammlungsteilnehmer, die hierzu zurechenbar keinen Anlass gesetzt haben. Folglich musste bei jeder Versammlung jeder Teilnehmer damit rechnen, dass seine Teilnahme unabhängig von der Größe und dem Gefahrenpotential der Versammlung aufgezeichnet wird. Jedenfalls im Hinblick auf den Stand der heutigen Technik sieht das Bundesverfassungsgericht keinen prinzipiellen Unterschied mehr zwischen Übersichtsaufzeichnungen und personenbezogenen Aufzeichnungen. Auch in Übersichtsaufzeichnungen werden die gefilmten Einzelpersonen in der Regel individualisierbar - und damit personenbezogen - erfasst.

Dem Bundesverfassungsgericht zufolge führt eine solche - nach der ursprünglichen Gesetzesfassung sogar zeitlich unbegrenzt mögliche - anlasslose Datenbevorratung, die allein an die Wahrnehmung der Versammlungsfreiheit und damit an das Gebrauchmachen von einem elementaren Grundrecht anknüpft, "zu durchgreifenden Nachteilen". Durch diesen "Datenvorratsspeicher" könne auch nachträglich eine zunächst unauffällige Teilnahme an einer Versammlung aufgegriffen, neu interpretiert und zum Anknüpfungspunkt weiterer Maßnahmen gemacht werden, ohne dass dieses gesetzlich klar und sachhaltig begrenzt würde.

Vor diesem Hintergrund sind bis zur endgültigen Entscheidung des Bundesverfassungsgerichts Übersichtsaufzeichnungen einstweilen nur zulässig, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass von der Versammlung erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen und auch die anschließende Nutzung und Speicherung anlassbezogen begrenzt bleibt. Übersichtsaufzeichnungen sind innerhalb von zwei Monaten zu löschen oder irreversibel zu anonymisieren, soweit die Daten nicht in Bezug auf einzelne Personen zur Verfolgung von Straftaten im Zusammenhang mit der aufgezeichneten Versammlung oder zur Abwehr künftiger versammlungsspezifischer Gefahren benötigt werden.

Darüber hinaus hat das Bundesverfassungsgericht auch die Befugnis zur Anfertigung von Übersichtsaufnahmen beschränkt. Übersichtsaufnahmen werden live in die Einsatzzentrale übertragen und - anders als Übersichtsaufzeichnungen - nicht aufgezeichnet. Die Übersichtsaufnahmen zur Lenkung und Leitung des Polizeieinsatzes sind nach der gerichtlichen Anordnung nur zulässig, wenn sie wegen der Größe oder Unübersichtlichkeit der Versammlung im Einzelfall erforderlich sind.

Die vom Bundesverfassungsgericht bestätigten Einschränkungen hatte ich bereits bei der Schaffung des Bayerischen Versammlungsgesetzes 2008 gegenüber dem Innenministerium gefordert. Das Bundesverfassungsgericht hat mit seiner Eilentscheidung wesentliche datenschutz- und verfassungsrechtliche Mängel des Bayerischen Versammlungsgesetzes beseitigt. Die verfassungsrechtlichen Anforderungen im Einzelfall - insbesondere zur grundsätzlichen Zulässigkeit von Übersichtsaufzeichnungen - sind allerdings erst in der noch ausstehenden endgültigen Entscheidung des Gerichts zu erwarten.

3.2.2 Die Änderungen im Einzelnen

Die am 01.06.2010 in Kraft getretenen Änderungen des Bayerischen Versammlungsgesetzes enthalten wesentliche datenschutzrechtliche Verbesserungen, auch wenn meine grundsätzlichen Bedenken gegenüber Übersichtsaufnahmen und -aufzeichnungen nicht ausgeräumt werden:

Über die ausdrücklich gemachten Vorgaben des Bundesverfassungsgerichts hinaus wurde die Befugnis der Polizei gestrichen, "personenbezogene Daten" von Versammlungsteilnehmern erheben zu dürfen. Ebenfalls gestrichen wurde die Befugnis, heimlich Foto- und Videografien einzelner Versammlungsteilnehmer und heimliche Übersichtsaufnahmen auf versammlungsrechtlicher Grundlage anzufertigen. Nach wie vor darf die Polizei aber unter bestimmen Voraussetzungen Foto- und Videoaufnahmen und -aufzeichnungen einzelner Versammlungsteilnehmer und der Versammlung anfertigen. Sie hat allerdings nunmehr die Gründe dafür zu dokumentieren. Damit kann die Rechtmäßigkeit der polizeilichen Maßnahmen effektiver überprüft werden.

Darüber hinaus sind insbesondere folgende Gesetzesänderungen hervorzuheben:

- Übersichtsaufnahmen

  Übersichtsaufnahmen von Versammlungen unter freiem Himmel darf die Polizei nur offen und nur noch dann vornehmen, wenn dies im Einzelfall wegen der Größe oder Unübersichtlichkeit der Versammlung erforderlich ist (z.B. um zu erkennen, ob und wo Gefahren drohen und deshalb weitere Einsatzkräfte erforderlich sind).

- Übersichtsaufzeichnungen

  Werden die live in die Einsatzzentrale übertragenen Übersichtsaufnahmen auch aufgezeichnet, spricht das Bayerische Versammlungsgesetz von sog. Übersichtsaufzeichnungen. Diese sind nur noch zulässig, soweit Tatsachen die Annahme rechtfertigen, dass von Versammlungen, Versammlungsteilen oder ihrem Umfeld erhebliche Gefahren für die öffentliche Sicherheit oder Ordnung ausgehen (z.B. drohende Pflastersteinwürfe, sich anbahnende Schlägerei zwischen Demonstranten und Gegendemonstranten). Auch insoweit hat die Polizei die Gründe dafür zu dokumentieren.

- Speicherungsdauer von Aufzeichnungen

  Bild-, Ton- und Übersichtsaufzeichnungen sind unverzüglich auszuwerten und - anders als bisher - grundsätzlich spätestens nach zwei Monaten zu

löschen. Die zulässige Speicherfrist kann im Einzelfall deutlich kürzer ausfallen, sie ist insbesondere eine Frage der Erforderlichkeit. Die Aufzeichnungen dürfen nur länger gespeichert werden, soweit sie für die Strafverfolgung oder im Einzelfall zur Abwehr erheblicher Gefahren erforderlich sind. Soweit die Identifizierung von Personen zur Gefahrenabwehr auf diesen Aufzeichnungen nicht erforderlich ist, muss sie technisch unumkehrbar ausgeschlossen werden (z.B. durch Verpixelung). Zur Gefahrenabwehr verwendete Aufzeichnungen müssen spätestens nach sechs Monaten gelöscht werden, wenn sie nicht inzwischen zur Strafverfolgung benötigt werden.

Die bislang vorgesehene unbefristete Speicherung von Übersichtsaufzeichnungen zur polizeilichen Aus- und Fortbildung hat der Gesetzgeber zum 01.06.2010 gestrichen. Sollen Übersichtsaufzeichnungen für diesen Zweck verwendet werden, muss die Polizei eine eigene Fassung herstellen, die eine Identifizierung der abgebildeten Personen irreversibel ausschließt.

- Datenschutzrechtliche Änderungen für den Veranstalter

  Die zuständige Behörde darf vom Veranstalter seine persönlichen Daten und die Daten des Versammlungsleiters und der Ordner nur noch in geringerem Umfang als bisher anfordern (Familiennamen, Vornamen, Geburtsnamen und Anschrift). Die Pflicht zur Angabe des Geburtsdatums, des Geburtsortes und der telefonischen Erreichbarkeit ist entfallen.

  Bei Anforderung der Daten muss die Behörde folgende Voraussetzungen beachten:

  Bei Versammlungen in geschlossenen Räumen darf die Behörde die genannten Daten über Versammlungsleiter und Ordner nur verlangen, wenn sie die Friedlichkeit der Versammlung mutmaßlich gefährden. Bei Versammlungen unter freiem Himmel müssen zwar die persönlichen Daten des Veranstalters und des Leiters der Behörde in der Anzeige mitgeteilt werden. Die Behörde darf die Daten von Ordnern aber nur anfordern, wenn diese die Friedlichkeit der Versammlung mutmaßlich gefährden.

Mit diesen Änderungen wurden durchaus auch wesentliche datenschutzrechtliche Anregungen von mir aufgegriffen. Die abschließende Klärung der verfassungsrechtlichen Anforderungen im Einzelfall - insbesondere zur grundsätzlichen Zulässigkeit von Übersichtsaufzeichnungen - ist allerdings erst in der noch ausstehenden endgültigen Entscheidung des Bundesverfassungsgerichts zu erwarten. Ich kann nicht ausschließen, dass das Gesetz dann erneut nachgebessert werden muss. Vor dem Hintergrund, dass das Gericht in seiner Eilanordnung die problematischen Teile des Bayerischen Versammlungsgesetzes bereits selbst außer Kraft gesetzt hatte, wäre es deshalb wohl sinnvoller gewesen, die endgültige Entscheidung des Gerichts vor einer gesetzlichen Neuregelung abzuwarten.

Aus datenschutzrechtlicher Sicht ist es derzeit beispielsweise nach wie vor unbefriedigend, dass Versammlungsteilnehmer nicht erkennen können, ob eine polizeiliche Kamera außer Betrieb ist oder ob sie einzeln oder im Rahmen von Übersichtsaufnahmen gefilmt werden. Wer damit rechnet, dass die Teilnahme an einer Versammlung behördlich registriert wird und dass ihm dadurch persönliche Risiken entstehen können, wird möglicherweise auf die Ausübung seines Grund-

rechts verzichten (Bundesverfassungsgericht, Volkszählungsurteil vom 15.12.1983). Betroffene können auch nach jetziger Gesetzeslage kaum in Erfahrung bringen, ob und ggf. wie sie gefilmt wurden. Allerdings können sie theoretisch von ihrem allgemeinen datenschutzrechtlichen Auskunftsanspruch Gebrauch machen. Damit können sie allerdings nur erfahren, ob die Polizei ihre Teilnahme an einer Versammlung in Akten und in polizeilichen Dateien gespeichert hat. Aus datenschutzrechtlicher Sicht wäre eine vollständige Streichung der Befugnis zu Übersichtsaufnahmen und -aufzeichnungen wünschenswert gewesen.

Die Einhaltung der zum Schutz der Versammlungsteilnehmer geschaffenen Einschränkungen werde ich in der Praxis sorgfältig überprüfen.

3.3 Ausgestaltung der "Vorratsdatenspeicherung" verfassungswidrig

Das Bundesverfassungsgericht hat in seinem Urteil vom 02.03.2010 die gesetzlichen Regelungen zur Speicherung von Telekommunikationsverkehrsdaten auf Vorrat ("Vorratsdatenspeicherung") durch die Anbieter von öffentlich zugänglichen Telekommunikations-, E-Mail- und Internetzugangsdiensten für nichtig erklärt. Es hat die Diensteanbieter darüber hinaus verpflichtet, die bisher gespeicherten Vorratsdaten unverzüglich zu löschen; die Daten dürfen auch nicht an die ersuchenden Stellen (z.B. Polizei, Verfassungsschutz) übermittelt werden. Telekommunikationsverkehrsdaten, die die Diensteanbieter für die Dauer von sechs Monaten auf Vorrat speichern mussten, sind z.B.: Rufnummern des anrufenden und des angerufenen Anschlusses, Beginn und Ende der Verbindung nach Datum und Uhrzeit, IP-Adresse, beim Beginn von Mobilfunkgesprächen genutzte Funkzellen. Die Speicherpflicht galt nicht für die Inhalte von Telefongesprächen, E-Mails und die aufgerufenen Internetseiten. Darüber hinaus für nichtig erklärt hat das Bundesverfassungsgericht auch die gesetzliche Befugnis der Strafverfolgungsbehörden, auf die vorsorglich gespeicherten Daten für die Strafverfolgung zuzugreifen. Es bewertet die Speicherung von Telekommunikationsverkehrsdaten auf Vorrat als "einen besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt".

Das Gericht stellt in seinem Urteil allerdings auch fest, dass eine sechsmonatige, vorsorglich anlasslose Speicherung von Telekommunikationsverkehrsdaten durch private Diensteanbieter nicht generell gegen das Fernmeldegeheimnis des Grundgesetzes (Art. 10 GG) verstößt. Sie unterliege jedoch besonders strengen Anforderungen im Hinblick auf Begründung und Ausgestaltung - insbesondere auch bezüglich der vorgesehenen Verwendungszwecke. Strikt verboten sei lediglich die Speicherung von personenbezogenen Daten auf Vorrat zu unbestimmten und noch nicht bestimmbaren Zwecken. Das Gericht betont aber, dass eine vorsorglich anlasslose Speicherung eine Ausnahme bleiben muss und die Freiheitswahrnehmung der Bürger nicht total erfasst und registriert werden darf.

Die gesetzlichen Regelungen, die die Vorratsdatenspeicherung und den Zugriff von Strafverfolgungsbehörden auf Vorratsdaten ausgestalten sollten, wurden deshalb für verfassungswidrig erklärt, weil sie den verfassungsrechtlichen Anforderungen an Datensicherheit, Verwendungszwecke, Transparenz und Rechtschutz nicht genügen: Die Ausgestaltung der Vorratsdatenspeicherung entspricht nicht dem Verhältnismäßigkeitsgrundsatz.

Ein Abruf der Vorratsdaten zu **Strafverfolgungszwecken** kann nur zulässig sein, wenn mindestens ein durch bestimmte Tatsachen begründeter Verdacht einer auch im Einzelfall schwerwiegenden Straftat besteht. Die nichtige Regelung hatte dagegen den Zugriff auf Vorratsdaten zur Verfolgung jedweder - und damit auch wenig gewichtiger - Straftaten gestattet, die mittels Telekommunikation begangen wurden.

Im Hinblick auf den Verhältnismäßigkeitsgrundsatz kann ein Abruf der Vorratsdaten zur **Gefahrenabwehr** - z.B. durch die **Polizei** - nur zulässig sein, wenn bestimmte Tatsachen eine konkrete Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes hinreichend belegen oder der Abruf zur Abwehr einer gemeinen Gefahr dienen soll. Dies gelte auch für die Verwendung der Daten durch die **Nachrichtendienste**.

Darüber hinaus fordert das Gericht - zumindest für einen engen Kreis von auf besondere Vertraulichkeit angewiesenen Telekommunikationsverbindungen - ein **grundsätzliches Übermittlungsverbot**. Dazu sollen etwa Verbindungen zu Anschlüssen von Personen, Behörden und Organisationen in sozialen oder kirchlichen Bereichen zählen, die den grundsätzlich anonym bleibenden Anrufern Beratung in seelischen oder sozialen Notlagen anbieten und dabei selbst Verschwiegenheitsverpflichtungen unterliegen.

Im Hinblick auf die "diffuse Bedrohlichkeit", die von einer Vorratsdatenspeicherung ausgehen kann, kann eine **heimliche Verwendung der Daten** verfassungsrechtlich nur dann zulässig sein, wenn sonst - wie grundsätzlich im Bereich der **polizeilichen Gefahrenabwehr** und der **Nachrichtendienste** - der Zweck der Untersuchung vereitelt wird. Im Bereich der **Strafverfolgung** kommt dagegen auch eine offene Erhebung und Nutzung der Daten in Betracht. Eine heimliche Verwendung der Daten kann hier nur zulässig sein, wenn sie im Einzelfall erforderlich und richterlich angeordnet ist. Bei einer heimlichen Datenverwendung muss der Gesetzgeber die Behörde zu einer zumindest nachträglichen Benachrichtigung verpflichten. Um dem Betroffenen einen möglichst effektiven Rechtschutz gewährleisten zu können, muss jede - sowohl heimliche als auch offene - Abfrage oder Übermittlung von Vorratsdaten grundsätzlich **unter Richtervorbehalt gestellt** werden.

Das Bundesverfassungsgericht hat auch verfassungsrechtliche Vorgaben für die Nutzung von Vorratsdaten festgestellt, um den **Inhaber** bestimmter, bereits bekannter **IP-Adressen** identifizieren zu können. Damit kann eine Strafverfolgungsbehörde ermitteln, welcher Person ein bestimmter Anschluss zu einer bestimmten Zeit zugeordnet war, von dem aus z.B. im Internet eine Straftat begangen wurde. Die Behörde darf vom Diensteanbieter eine solche Auskunft über den Inhaber einer IP-Adresse nicht ins Blaue hinein einholen. Das Gericht fordert vielmehr einen **hinreichender Anfangsverdacht** oder eine **konkrete Gefahr** auf einzelfallbezogener Tatsachenbasis. Ein Richtervorbehalt sei nicht erforderlich; die Betroffenen müssten von der Einholung der Auskunft aber **benachrichtigt** werden. Der Gesetzgeber dürfe Auskünfte über den Inhaber einer IP-Adresse für die **Verfolgung aller Straftaten**, für die Gefahrenabwehr und die Aufgabenwahrnehmung der Nachrichtendienste vorsehen.

Im Gegensatz dazu dürfen solche Auskünfte im Hinblick auf das erhebliche Gewicht des Eingriffs jedoch nicht allgemein und uneingeschränkt zur Verfolgung

oder Verhinderung jedweder **Ordnungswidrigkeit** zugelassen werden. Es muss sich vielmehr um - auch im Einzelfall - besondere gewichtige Ordnungswidrigkeiten handeln, die der Gesetzgeber ausdrücklich benennen muss.

Die Landesbeauftragten für den Datenschutz hatten gegenüber dem Bundesverfassungsgericht eine gemeinsame Stellungnahme zu der Verfassungsbeschwerde abgegeben. Wesentliche Argumente hieraus finden sich in den Entscheidungsgründen wieder.

Die Datenschutzbeauftragten des Bundes und der Länder haben vor dem Hintergrund des Urteils die Bundesregierung aufgefordert, sich für eine Abschaffung der Europäischen Richtlinie zur Vorratsdatenspeicherung einzusetzen:

Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 02.03.2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen "besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Die Sicherheitsbehörden tragen zwar immer wieder die Notwendigkeit einer Vorratsspeicherung von Telekommunikationsverkehrsdaten vor. Abgesehen von einigen wenigen Einzelfällen bleiben sie aber den konkreten Nachweis schuldig, dass die Sicherheitslage ohne Vorratsspeicherung nachhaltig verschlechtert wird. Vor diesem Hintergrund ist es nicht einzusehen, warum eine flächendeckende Erfassung der Telekommunikation in Deutschland geboten sein soll.

3.4 Datenschutz und Versammlungsrecht

3.4.1 Polizeiliche Speicherung von Versammlungsanmeldern und -leitern

Im Zusammenhang mit den Demonstrationen unter dem Motto "Bildungsstreik 2009" habe ich bei verschiedenen Polizeipräsidien Datenspeicherungen überprüft. Hierbei musste ich mehrfach feststellen, dass - auch bei störungsfreiem Verlauf - die personenbezogenen Daten von Versammlungsanmeldern oder Versammlungsleitern im Vorgangsverwaltungs- und Dokumentationsverfahren (Integrationsverfahren - IGVP) der Polizei erfasst worden sind. Die gespeicherten Personendaten sollten somit lediglich aufgrund der Ausübung eines verfassungsrechtlich geschützten Grundrechts für mehrere Jahre in einer polizeilichen Datei gespeichert werden, auf die jede Polizeidienststelle zugreifen kann. Ich habe die betreffenden Polizeipräsidien umgehend zur Löschung dieser Daten aufgefordert und darauf hingewiesen, zukünftig die diesbezüglichen Speicherungsverbote einzuhalten. Alle betroffenen Polizeipräsidien sind der Aufforderung gefolgt und haben diese Daten gelöscht.

3.4.2 Videoüberwachung durch fest installierte Kameras

Schon in meinem 21. Tätigkeitsbericht, Nr. 7.13.1, habe ich darauf hingewiesen, im Falle von Versammlungen oder Aufzügen die Kameras der fest installierten Videoüberwachungsanlagen für öffentliche Straßen und Plätze abzuschwenken oder auszuschalten. Nach der Entscheidung des Bundesverfassungsgerichts (siehe hierzu Nr. 3.2.1) sind gerade solche anlasslosen Aufzeichnungen von Versammlungsteilnehmern unzulässig. Auch bei meinen Prüfungen polizeilicher Videoüberwachungskonzepte habe ich jeweils darauf hingewirkt, entsprechende Regelungen aufzunehmen. Die betroffenen Polizeipräsidien sind diesen Anregungen gefolgt. Ob die Regelung in der Praxis tatsächlich auch Anwendung findet, habe ich durch die Einsichtnahme in Aufzeichnungen von Überwachungsanlagen während des Zeitraums einer Versammlung geprüft. Im Gegensatz zu einer früheren Prüfung waren dieses Mal alle Kameras abgeschwenkt. Versammlungsteilnehmer wurden nicht aufgezeichnet.

3.4.3 Datenschutzrechtliche Kontrolle von Übersichtsaufzeichnungen

Gerade die anlasslose Aufzeichnung von Versammlungsteilnehmern durch Einsatzkräfte der Polizei bot in der Vergangenheit immer wieder Anlass zu datenschutzrechtlicher Kritik. Nach der Eilanordnung des Bundesverfassungsgerichts (siehe hierzu Nr. 3.2.1) stellte daher die Kontrolle polizeilicher Aufzeichnungen bei Versammlungen einen Schwerpunkt meiner Tätigkeit im Berichtszeitraum dar. Ich habe zu diesem Zweck mehrmals von verschiedenen Polizeipräsidien die Bildaufzeichnungen von Versammlungen zur Kontrolle angefordert und überprüft.

Leider wurde ich bei der Erfüllung meines Kontrollauftrages durch ein Polizeipräsidium erneut nur sehr zögerlich unterstützt. Erst nachdem ich den Verstoß des Polizeipräsidiums gegen die gesetzliche Verpflichtung, den Landesbeauftragten für den Datenschutz in der Erfüllung seiner Aufgaben zu unterstützen, beanstandet habe, wurden mir die angeforderten Aufzeichnungen zur Verfügung gestellt.

Dies geschah aber erst mehr als acht Monate nach der Versammlung. Ein solch langer Zeitraum ist für die Durchführung einer zeitnahen datenschutzrechtlichen Kontrolle nicht akzeptabel. Darüber hinaus könnten durch die verspätete Übersendung gegebenenfalls erforderliche Anschlussermittlungen, z.B. durch die auf ein Jahr begrenzte Auswertemöglichkeit der Protokolldatei, verhindert werden. Wie schließlich die Einsichtnahme in die Aufzeichnungen ergab, befanden sich darunter auch Sequenzen mit Aufnahmen von Versammlungsteilnehmern, die laut Polizei keine Relevanz für Strafverfahren gehabt hätten und zu löschen waren.

Schon rund ein halbes Jahr zuvor hatte ich die Behördenleitung des gleichen Polizeipräsidiums auf die lange Bearbeitungszeit für die Übersendung von Aufzeichnungen hingewiesen. Auch in diesem Fall hatte es sechs Monate gedauert, bis ich die Aufzeichnungen einsehen konnte. Unter den übersandten Aufzeichnungen waren einige Sequenzen, die Versammlungsteilnehmer in Großaufnahme zeigten und für die, auch nach Auffassung der Polizei, keine rechtfertigenden Voraussetzungen erkennbar waren. Ich habe das Polizeipräsidium daher aufgefordert, die Aufzeichnungen zu löschen und die betreffenden Einsatzkräfte nochmals über die einschlägigen gesetzlichen Bestimmungen zu belehren. Darüber hinaus wurden mit der Polizei weitere Schulungen für Videobeamte und entsprechende rechtliche Hinweise in den polizeilichen Einsatzbefehlen vereinbart. Meine Feststellungen im Berichtszeitraum lassen auch für die Zukunft verstärkt Kontrollen in diesem Bereich erforderlich erscheinen.

3.5 Speicherungen in polizeilichen Dateien

3.5.1 Auskunftsablehnungen bei Speicherungen

Art. 48 Polizeiaufgabengesetz legt den grundsätzlichen gesetzlichen Anspruch des Betroffenen gegenüber der Polizei auf Auskunft über die zu seiner Person gespeicherten Daten fest. Darüber hinaus regelt Art. 48 auch, unter welchen Voraussetzungen die Polizei von einer Auskunftserteilung absehen kann. In solchen Fällen sieht das Polizeiaufgabengesetz vor, dass sich der Betroffene an mich wenden kann und die Polizei im Regelfall mir gegenüber die Auskunft erteilt. Im Zuge solcher Verfahren wurde ich immer wieder mit Auskunftsablehnungen konfrontiert, deren Gründe für mich aus datenschutzrechtlicher Sicht nicht nachvollziehbar erschienen. Insbesondere war dies der Fall bei Speicherungen, die polizeiliche Maßnahmen dokumentieren, die der Bürger ohnehin selbst miterlebte und deren polizeiliche Registrierung er daher vermuten konnte. Durch meine Interventionen konnte ich die Polizei in der Vergangenheit immer wieder davon überzeugen, im Einzelfall doch die Auskunft an die Betroffenen zu erteilen. Die vorgetragenen Gründe für Auskunftsverweigerungen werde ich auch weiterhin mit strengem Maßstab prüfen.

Ablehnungen von Auskunftsersuchen aus der Verbunddatei Gewalttäter Sport habe ich zum Anlass genommen, die diesbezügliche Auskunftspraxis in anderen Bundesländern abzufragen. Das Bayerische Landeskriminalamt hatte mir zuvor mitgeteilt, Auskünfte aus dieser Datei aus grundsätzlichen Erwägungen nicht zu erteilen. Hierdurch könnte vorgeblich die polizeitaktische Bedeutung solcher Speicherungen gefährdet werden. Eine ähnlich restriktive Handhabung bei Auskunftserteilungen war in keinem anderen Bundesland in Erfahrung zu bringen.

Laut Rückmeldung erteilen die zuständigen Dienststellen in 14 Bundesländern grundsätzlich die Auskunft, ob der Antragsteller in ihrem Zuständigkeitsbereich in der Datei Gewalttäter Sport erfasst worden ist. Ich habe dem Bayerischen Landeskriminalamt das Ergebnis meiner Anfrage mitgeteilt und darum gebeten, die diesbezügliche Auskunftspraxis nochmals zu überdenken. Inzwischen wurde mir seitens der Polizei mitgeteilt, dass nunmehr auch bezüglich der Speicherungen in der Datei Gewalttäter Sport jeweils im Einzelfall über die Auskunftserteilung entschieden wird.

3.5.2 Integrationsverfahren der Bayerischen Polizei - IGVP

In meinen zurückliegenden Tätigkeitsberichten sah ich mich regelmäßig veranlasst, über die datenschutzrechtlichen Verschlechterungen, die mit der zunehmenden Erweiterung des Integrationsverfahrens - IGVP einhergingen, zu berichten. Das System wird nunmehr von allen bayerischen Polizeipräsidien gemeinsam zur Erfassung und Verarbeitung der erhobenen Personen und Falldaten, zur Vorgangsverwaltung und Dokumentation polizeilicher Maßnahmen aber auch im Rahmen der Informationsgewinnung für die polizeiliche Aufgabenerfüllung genutzt. Eben diese zweckübergreifende Verwendung des Systems bedingt nicht nur eine enorme Fülle dort gespeicherter Daten, sondern auch vielfältige Auswertungsmöglichkeiten. Beispiele für meine Kritik in der Vergangenheit waren die langen Aussonderungsprüffristen, die erheblichen Erweiterungen der landesweiten Zugriffsberechtigungen oder zuletzt die Realisierung der Freitextrecherche über sämtliche Datenfelder. Leider hat das Bayerische Staatsministerium des Innern in den vergangenen Jahren meine Vorschläge für datenschutzrechtliche Verbesserungen des Systems nicht aufgegriffen (siehe hierzu 22. Tätigkeitsbericht, Nr. 4.2 und 21. Tätigkeitsbericht, Nr. 7.2).

Zweifellos stellt die Möglichkeit, personenbezogene Daten nunmehr nicht nur in den hierfür vorgesehenen Datenfeldern, sondern auch in den gespeicherten Texten (z.B. Sachverhaltsschilderungen) zu recherchieren eine erhebliche Veränderung dar, der auch aus datenschutzrechtlicher Sicht Rechnung getragen werden muss. Dabei geht es mir nicht darum, den verantwortungsbewussten Umgang der Polizeibeamten mit einer solchen verbesserten Recherchemöglichkeit in Frage zu stellen, sondern um die Beachtung gesetzlicher Vorgaben. Art. 37 Abs. 3 Polizeiaufgabengesetz fordert die Festlegung von Prüfungsterminen für die suchfähige Speicherung personenbezogener Daten. Werden diese Personendaten durch die Einführung der Freitextrecherche in IGVP suchbar, besteht Regelungsbedarf. Ich habe das Bayerische Staatsministerium des Innern daher gebeten, darzulegen, wie in solchen Fällen die Prüfungs- und Löschungsfristen eingehalten werden können oder welche Möglichkeiten es zur Vermeidung der Speicherung von Personendaten außerhalb der vorgesehenen Datenfelder sieht. Eine Einigung konnte noch nicht erreicht werden.

3.5.3 Speicherungen im Kriminalaktennachweis

Auch wenn die bayernweite Nutzung von IGVP mitsamt dessen zunehmenden Auswertungsmöglichkeiten die datenschutzrechtliche Brisanz dieses Systems in der Vergangenheit wesentlich erhöhte, bleiben die Überprüfungen von Speicherungen im Kriminalaktennachweis (KAN) nach wie vor ein Schwerpunkt meiner Tätigkeit im Polizeibereich. Dabei sind es besonders oft Bürgereingaben, die hier Anlass zu datenschutzrechtlicher Kritik geben. Ein Beispiel:

Eine Frau hatte sich an mich gewandt, da sie im Rahmen einer beruflich veranlassten Sicherheitsüberprüfung mit ihren polizeilichen Speicherungen konfrontiert wurde. Laut diesen sei sie Betäubungsmittelkonsumentin und in zwei Fällen aufgrund von Verstößen gegen das Betäubungsmittelgesetz im Kriminalaktennachweis gespeichert. Ein Blick in die staatsanwaltschaftliche Ermittlungsakte erbrachte dazu Näheres. Im Rahmen ihrer beruflichen Tätigkeit hatte die Frau - neben anderen Beschäftigten - Zugriff auf Medikamente, die unter das Betäubungsmittelgesetz fallen. Als solche Medikamente abhanden kamen und sie zu den möglichen Tatzeiten Dienst hatte, kam sie in den Kreis der Verdächtigen. Eine - wenn auch später widerlegte - Aussage einer Kollegin ließ dann sogar vorübergehend den Tatverdacht weiter ansteigen. Zu ihrer Entlastung willigte sie in die toxikologische Untersuchung einer Haarprobe ein und ihre Wohnung wurde durchsucht. Der Tatverdacht konnte durch keine der beiden Maßnahmen erhärtet werden. Schließlich stellte sich auch die belastende Aussage der Kollegin nachweislich als falsch heraus. Das zuständige Amtsgericht sprach die Frau daraufhin von der Anklage frei und kam zu dem Schluss, ein bislang unbekannter Dritter sei für die Taten verantwortlich. Trotz des gerichtlichen Freispruchs und keinerlei sonstiger Hinweise auf einen Drogenkonsum wurden die personenbezogenen Daten der Betroffenen, einschließlich der erkennungsdienstlichen Unterlagen und dem Hinweis "Betäubungsmittelkonsument" weiterhin im Kriminalaktennachweis gespeichert. Erst auf meine Nachfrage hin erfolgte umgehend die Löschung der Daten.

3.6 Pressearbeit der Polizei

Im Berichtszeitraum habe ich festgestellt, dass die Polizei im Rahmen ihrer Öffentlichkeitsarbeit personenbezogene Daten an die Medien übermittelt hat (siehe hierzu auch 21. Tätigkeitsbericht, Nr. 7.16). Solche Datenübermittlungen liegen nicht erst dann vor, wenn die Polizei Daten herausgibt, sondern schon dann, wenn sie auf Anfrage der Presse bekannte Informationen bestätigt. Dadurch erhalten diese Informationen eine amtliche Autorisierung, die ihren Wahrheitsgehalt und damit ihre Qualität steigert. Die Frage, ob es sich um die Weitergabe personenbezogener Daten handelt, hängt dabei davon ab, ob das soziale Umfeld (Nachbarn, Kollegen, Bekannte, Geschäftspartner, etc.) den Betroffenen aufgrund der bekanntgegebenen Daten identifizieren kann. Maßgeblich hierfür sind wiederum Menge und Qualität dieser Daten.

Die Übermittlung personenbezogener Daten durch die Polizei an die Presse ist nur aufgrund einer Rechtsgrundlage möglich. Als solche kann nur Art. 41 PAG in Betracht kommen, der insoweit jedoch keine genaueren Vorgaben enthält. Hinweise können aber bundesgesetzliche Regelungen wie z.B. §§ 169 ff. Gerichtsverfassungsgesetz (GVG) geben, auch wenn sie nicht unmittelbar auf Verlautbarungen der Polizei anwendbar sind. Kriterien zur Zulässigkeit von Presseauskünften sind des Weiteren dem Urteil des Bundesverfassungsgerichts vom 10.06.2009 (Az. 1 BvR 1107/09) zu entnehmen. Dabei ist zu berücksichtigen, dass Adressat dieser Entscheidung nicht eine öffentliche Stelle, sondern die Presse ist, die durch das Medienprivileg besonders begünstigt ist.

Aus all dem ergibt sich, dass in bestimmten Fällen eine personenbezogene Pressearbeit von vorneherein grundsätzlich unzulässig ist. In den Fällen, in denen etwa das GVG einen Ausschluss der Öffentlichkeit von der Verhandlung vorsieht, ist diese Vorgabe auch im Rahmen der polizeilichen Pressearbeit regelmäßig zu

beachten. In diesem Sinne unterliegen z.B. Minderjährige und geistig Erkrankte, aber auch Zeugen und insbesondere Opfer einem gesteigerten Schutz (vgl. §§ 171 a, 172 Nr. 1 a GVG, § 48 JGG).

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 10.06.2009 hinsichtlich der Zulässigkeit der Berichterstattung nach Fällen der schweren Gewaltkriminalität und Fällen sonstiger Kriminalität unterschieden.

Demnach ist in den Fällen der nicht schweren Gewaltkriminalität regelmäßig die Veröffentlichung von Namen, Abbildungen oder sonstiger identifizierender Merkmale des Tatverdächtigen unzulässig.

Meines Erachtens kann eine personenidentifizierende Pressearbeit der Polizei somit regelmäßig nur bei Verbrechen, und hierbei insbesondere bei Fällen der Gewaltkriminalität, in Betracht kommen.

In Fällen sonstiger Kriminalität ist eine personenidentifizierende Pressearbeit datenschutzrechtlich allenfalls dann vertretbar, wenn besondere Kriterien hinzukommen, die ein überwiegendes Interesse der Öffentlichkeit an der Berichterstattung begründen. Solche Kriterien können sich u.U. aus Besonderheiten bezüglich der Person des Täters oder des Tathergangs ergeben. Gleichwohl ist aber, gerade am Anfang eines Ermittlungsverfahrens, die Unschuldsvermutung zu berücksichtigten und eine nicht personenbezogene Berichterstattung regelmäßig erforderlich. Zu berücksichtigen ist überdies, dass eine Identifizierung des Täters oft auch einen Personenbezug der betroffenen Opfer zur Folge haben kann.

Bei meiner datenschutzrechtlichen Prüfung bin ich in einigen Fällen zu dem Ergebnis gekommen, dass bei der polizeilichen Pressearbeit die oben angeführten Grundsätze nicht ausreichend berücksichtigt wurden:

So hatte z.B. ein Polizeipräsidium bei der Berichterstattung über einen Verkehrsunfall über den genauen Unfallzeitpunkt und -ort hinaus personenbezogene Daten des Unfallverursachers an die Presse weitergegeben (Alter, Beruf, Alkoholisierung, genaue Modellbezeichnung des gefahrenen Fortbewegungsmittels). Auf Anfragen der Presse hat das Polizeipräsidium die Alkoholbeeinflussung und den Namen des Ortsteils, aus dem der Betroffene stammt, bestätigt.

In einem weiteren Fall hatte sich die betroffene Person bei mir über die individualisierende Berichterstattung der Polizei beschwert und mitgeteilt, dass bereits zwei Journalisten vor ihrer Tür gestanden hätten. Bei meiner datenschutzrechtlichen Prüfung habe ich ein überwiegendes legitimes Interesse der Öffentlichkeit gerade an der vorgenommenen personenbezogenen Information (Alter, Geschlecht, Beruf, Familienstand, Staatsangehörigkeit, Wohnort mit Ortsteil, Geschlecht und Alter des Kindes) nicht erkennen können. Neugierde und Sensationslust begründen jedenfalls kein solches Informationsinteresse. Ich habe deshalb die Übermittlung der personenbezogenen Daten an die Presse in diesem Fall förmlich beanstandet.

Für den Betroffenen kann eine derartige personenbezogene Berichterstattung zu bleibenden Nachteilen führen, weil die Frage, ob er später verurteilt oder freigesprochen wird, in der öffentlichen Wahrnehmung nur noch von untergeordneter Bedeutung ist.

Aufgrund weiterer, datenschutzrechtlich problematischer Fälle, habe ich deshalb die Thematik gemeinsam mit dem Präsidenten eines Polizeipräsidiums in einem Gespräch ausführlich erörtert. Im Sinne der dargestellten Maßstäbe werde ich auf eine landesweit einheitliche Handhabung der polizeilichen Berichterstattung hinwirken.

3.7 Quellen-Telekommunikationsüberwachung

Die Benutzung eines Computers hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung, nicht nur für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte und Tagebuchaufzeichnungen, sondern zunehmend auch für das Führen von Telefongesprächen über das Internet ("Voice over IP" - VoIP). Eine etwaige Überwachung und Aufzeichnung der über das Internet geführten Telefongespräche durch Polizei und Strafverfolgungsbehörden geschieht im Wege der sog. Quellen-Telekommunikationsüberwachung ("Quellen-TKÜ"). Die überwachende Behörde bringt dazu auf dem Computer des Betroffenen (Zielrechner) eine Software an, die die Daten aus dem laufenden Kommunikationsvorgang (Internettelefonie, aber auch E-Mail-Verkehr) vor ihrer Verschlüsselung erfasst und in Kopie an die Behörde weiterleitet. Die Technik der Vorgehensweise zur Vorbereitung der Maßnahme bei der sog. Quellen-TKÜ entspricht der der sog. Online-Durchsuchung.

Das Bundesverfassungsgericht hat bereits in seinem Urteil zur "Online-Durchsuchung" vom 27.02.2008 (siehe hierzu 23. Tätigkeitsbericht, Nr. 4.1.2) darauf hingewiesen, dass mit der Infiltration des Zielrechners zum Zweck der "Quellen-TKÜ" die entscheidende Hürde genommen sei, um das System insgesamt auszuspähen. Die dadurch bedingte Gefährdung gehe weit über die hinaus, die mit einer bloßen Überwachung der laufenden Telekommunikation verbunden ist. Insbesondere könnten auch die auf dem Personalcomputer abgelegten Daten zur Kenntnis genommen werden, die keinen Bezug zu einer telekommunikativen Nutzung des Systems aufweisen. Im Hinblick auf diese Gefährdung genüge das Fernmeldegeheimnis (Art. 10 Abs. 1 GG) nur dann als alleiniger grundrechtlicher Maßstab für die Beurteilung einer "Ermächtigung" zu einer "Quellen-Telekommunikationsüberwachung", wenn sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt. Dazu stellt das Gericht fest: "Dies muss durch technische Vorkehrungen und rechtliche Vorgaben sichergestellt sein".

Ich bin der Auffassung, dass eine "Quellen-TKÜ" auf die polizeirechtliche Ermächtigung zur - herkömmlichen - Telekommunikationsüberwachung (vgl. Art. 34 a PAG) nicht gestützt werden kann, weil Art. 34 a PAG die vom Bundesverfassungsgericht geforderten rechtlichen Vorgaben nicht enthält. Eine spezielle Befugnis für die "Quellen-TKÜ" enthält das Polizeiaufgabengesetz nicht. Das Staatsministerium des Innern sieht dagegen Art. 34 a PAG als bereichsspezifische Rechtsgrundlage auch für diese neue Art der Telekommunikationsüberwachung an. Es könne durch entsprechende Vorgaben in der gerichtlichen Anordnung der Überwachung rechtlich sichergestellt werden, dass die Überwachung auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt ist. Zugriffe auf Festplatten seien technisch ausgeschlossen. Die Notwendigkeit solcher Vorgaben ergebe sich, so das Staatsministerium des Innern, bereits unmittelbar und hinreichend bestimmt aus Art. 34 a PAG, der nur die Erhebung von Daten aus einer laufenden Telekommunikation erlaube und nicht etwa auch den Zugriff auf gespeicherte Daten.

Die Auffassung des Staatsministeriums teile ich nicht. Das Bundesverfassungsgericht hat seine Ausführungen zu technischen Vorkehrungen und rechtlichen Vorgaben ausdrücklich auf die Beurteilung einer "Ermächtigung" - und damit einer Befugnisnorm - bezogen. Eine Anordnung des Gerichts oder - bei Gefahr im Verzug - der Polizei kann eine gesetzliche Regelung nicht ersetzen, wenn es um Eingriffe in grundlegende Bereiche geht. Dies folgt aus dem Grundsatz des Vorbehalts des Gesetzes. Gemäß der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre muss der Gesetzgeber in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung alle wesentlichen Entscheidungen selbst treffen (vgl. BVerfGE 61, 260, 275; E 88, 103, 116). Ich halte vor diesem Hintergrund eine präventive "Quellen-TKÜ" ohne entsprechende gesetzliche Grundlage, die den verfassungsrechtlichen Anforderungen genügt, für unzulässig.

Der Bundesgesetzgeber sowie die Länder Thüringen und Hessen haben bei vergleichbarer Rechtslage das Erfordernis einer speziellen "Ermächtigung" anerkannt und im Bundeskriminalamtgesetz (§ 20 l Abs. 2 BKAG) bzw. in den entsprechenden Landespolizeigesetzen eine entsprechende Befugnisnorm geschaffen. Die Ermächtigung schreibt technische Schutzvorkehrungen zugunsten des betroffenen Bürgers vor, um den Eingriff in das infiltrierte System auf das unbedingt erforderliche Mindestmaß zu begrenzen und die Datensicherheit zu gewährleisten. Derartige Schutzvorkehrungen fehlen im bayerischen Polizeirecht.

§ 20 l Abs. 2 BKAG
Die Überwachung und Aufzeichnung der Telekommunikation darf ohne Wissen des Betroffenen in der Weise erfolgen, dass mit technischen Mitteln in vom Betroffenen genutzte informationstechnische Systeme eingegriffen wird, wenn

1. *durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird, und*
2. *der Eingriff in das informationstechnische System notwendig ist, um die Überwachung und Aufzeichnung der Telekommunikation insbesondere auch in unverschlüsselter Form zu ermöglichen.*

§ 20 k Abs. 2 und 3 gilt entsprechend. § 20 k bleibt im Übrigen unberührt.

3.8 Videoüberwachung

3.8.1 Videoüberwachung öffentlicher Straßen und Plätze

In meinen vorangegangenen Tätigkeitsberichten habe ich regelmäßig über die Zunahme der polizeilichen Videoüberwachung auf öffentlichen Straßen und Plätzen in Bayern berichtet. Auch in diesem Berichtszeitraum hat die Polizei in verschiedenen Städten weitere Überwachungskameras installiert. Ich kam daher erneut meiner Ankündigung nach, jede geplante polizeiliche Videoüberwachung daraufhin zu überprüfen, ob die gesetzlichen Vorschriften erfüllt sind (siehe hierzu 21. Tätigkeitsbericht, Nr. 7.13.1). Grund für diese Ankündigung war die Nichtbeachtung meiner Bedenken und Anregungen in der Vollzugsbekanntmachung zum Polizeiaufgabengesetz für die Videoüberwachung öffentlicher Straßen und Plätze. Es ist deshalb notwendig gewesen, die datenschutzrechtlichen Erfordernisse für die praktische Umsetzung der Videoüberwachung im Einzelfall jeweils im Dialog mit den betreffenden Polizeipräsidien zu verdeutlichen. Die Polizeiprä-

sidien sind in ihren Planungen größtenteils meinen Anregungen gefolgt - sowohl hinsichtlich der Darlegung der besonderen Kriminalitätsbelastung der überwachten Örtlichkeiten, der Zugriffsregelungen, der Protokollierungen, als auch der zusätzlichen Anbringung von Hinweisschildern. Mit der Verkürzung der gesetzlichen Höchstspeicherungsfrist in Art. 32 Abs. 4 Polizeiaufgabengesetz (siehe hierzu Nr. 3.1.4) auf drei Wochen, haben sich nunmehr auch meine immer wieder gegenüber der Polizei vorgetragenen Forderungen einer kürzeren Speicherungsdauer weitgehend erübrigt.

Aus datenschutzrechtlicher Sicht positiv zu bewerten war die Rücknahme der polizeilichen Videoüberwachung am Münchner Orleansplatz. Man kann daraus auch das Bestreben der Polizei ableiten, nur tatsächliche Kriminalitätsschwerpunkte zu überwachen. Da mit dem Rückgang der Kriminalitätszahlen die gesetzlich geforderten Voraussetzungen entfielen, war der Rückbau der Anlage - trotz der Proteste mancher Anwohner - geboten. Ich begrüße diese Entscheidung ausdrücklich.

Hingegen stellt die Verhinderung der Einsichtnahme in Privaträume umliegender Gebäude durch polizeiliche Videoüberwachungsanlagen weiterhin ein Problem dar, bei dem ich bislang mit dem Bayerischen Staatsministerium des Innern noch keinen Konsens erzielen konnte. Das Verwaltungsgericht Hamburg (Az. 4 K 2800/06) und das Oberverwaltungsgericht Hamburg (Az. 4 Bs 244/06) haben einer Wohnungsinhaberin einen Anspruch auf Schwarzschaltung der polizeilichen Überwachungskamera zuerkannt, sobald diese ihre Wohnung erfasst. Zur Begründung führten die Gerichte aus, dass für eine solche Art der Wohnungsüberwachung keine Rechtsgrundlage existiere, die den Anforderungen des Grundgesetzes genüge. Ich hatte vor diesem Hintergrund das Staatsministerium des Innern um Prüfung gebeten, mit welchen Maßnahmen (z.B. mechanische Schwenksperre oder Schwarzschaltung) in Bayern eine Einsichtnahme in die grundrechtlich geschützten Bereiche ausgeschlossen werden kann. Zunächst sah das Staatsministerium des Innern wegen der bestehenden dienstlichen Weisungen und des polizeilichen Überwachungskonzeptes keinen Bedarf für zusätzliche Schutzmechanismen. Auf mein Drängen hin wurde nun doch ein Polizeipräsidium beauftragt, die Möglichkeiten und Auswirkungen einer technischen Begrenzung im Rahmen eines Pilotversuchs zu testen. Das Ergebnis des Pilotversuchs und die Entscheidung des Staatsministeriums des Innern liegen mir dazu bislang noch nicht vor.

3.8.2 Videoaufzeichnungen von Fußballfans

Art. 32 Abs. 1 Polizeiaufgabengesetz erlaubt es der Polizei im Zusammenhang mit öffentlichen Veranstaltungen personenbezogene Daten durch den Einsatz technischer Mittel zur Anfertigung von Bildaufnahmen zu erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dabei Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden. Die Vollzugsbekanntmachung zum Polizeiaufgabengesetz (Ziffer 32.2) nennt dafür als Beispiel Fankurven der Sportstadien oder deren Zugänge. Der Polizei soll damit die rechtliche Möglichkeit eingeräumt werden, einen Geschehensablauf aufzuzeichnen, der sich nach den polizeilichen Erkenntnissen zu einer Störung der öffentlichen Sicherheit und Ordnung entwickeln könnte. Kommt es dann im Verlauf einer Veranstaltung zu Ausschreitungen, dienen die Aufzeichnungen als Beweismaterial zur Dokumentation der Situation und ermöglichen der Polizei, anhand

der Aufnahmen Störer ausfindig zu machen. Hat die Polizei die Störer festgestellt, kann deren Identität (ggf. auch mit Hilfe vorhandener erkennungsdienstlicher Unterlagen) ermittelt werden.

Durch eine Petition erlangte ich Kenntnis von einem Sachverhalt, bei dem Polizeibeamte vor einem Fußballspiel einen Fanbus kontrollierten, da sie darin als gewaltbereit bekannte Fans vermutetet hatten. Die Prognose sei dabei auf Erkenntnisse aus vorausgegangenen Ausschreitungen dieser Fangruppe gestützt worden. Laut Schilderung des Petenten begnügten sich die Beamten aber nicht damit, die Anreise der Gruppe oder den Verlauf der Kontrolle auf Video festzuhalten, sondern erhoben von jeder einzelnen Person die Personalien, versahen die Personen mit einer Nummer und fotografierten sie einzeln ab. Ich habe mich daher an das zuständige Polizeipräsidium gewandt und um Stellungnahme zu den Gründen und zu der Rechtsgrundlage für diese Maßnahmen gebeten. Wie mir das Polizeipräsidium antwortete, sehe es auch die oben geschilderten Aufzeichnungen durch die Befugnis des Art. 32 Abs. 1 PAG gedeckt. In der Vergangenheit habe sich gezeigt, dass potentielle Störer durch präventive Feststellungen ihrer Personalien und Fertigung von Lichtbildern vielfach deshalb keine Ordnungsstörungen oder Straftaten begingen, weil sie damit aus ihrer Anonymität herausgerissen worden seien und sich das Entdeckungsrisiko bei Straftaten erhöhe. Auch wenn die Wirkung solcher Maßnahmen auf Fußballfans aus polizeilicher Sicht nachvollziehbar erscheint und die Lichtbilder nach Mitteilung der Polizei wieder gelöscht werden, kann ich dieser Rechtsauffassung nicht zustimmen. Im vorliegenden Fall hatte die Polizei nicht Aufzeichnungen einer gefahrenträchtigen Situation angefertigt, sondern gezielt einzelne Personen aufgezeichnet und gleichzeitig, auf einer Liste zuordenbar, deren Personalien festgehalten. Bei dieser Sachlage werte ich die Aufzeichnungen nicht als Datenerhebung nach Art. 32 Abs. 1 PAG, sondern als erkennungsdienstliche Behandlung. Ich habe dem Polizeipräsidium diese Einschätzung mitgeteilt und gebeten, dies bei künftigen Kontrollen zu beachten.

3.9 Erkennungsdienstliche Behandlungen

Nachfolgender Sachverhalt, auf den ich durch eine Petition aufmerksam gemacht wurde, bot mir Anlass, die bestehenden Regelungen für erkennungsdienstliche Maßnahmen näher zu hinterfragen. Als in einem Pausenhof einer Schule ein Schüler von mehreren Mitschülern geschubst und geschlagen wurde, geriet zunächst auch der Petent in Tatverdacht. Die tatsächlichen Täter konnten jedoch ermittelt werden und das Gericht sprach den Jugendlichen frei. Die Sache schien für ihn damit erledigt. Was er zunächst nicht beachtete, im Zuge des Ermittlungsverfahrens wurde er erkennungsdienstlich behandelt und die Daten wurden gespeichert. Sein Bild war neben dem der anderen Verdächtigen, dem Geschädigten zur Identifizierung vorgelegt worden. Die Abwicklung solcher erkennungsdienstlichen Behandlungen wird landesweit im sogenannten Täterbildverfahren (TBV) vorgenommen. Die Bilddaten werden dabei auf einem Zentralserver gespeichert.

Als es nun parallel zu dem oben geschilderten Fall in einer anderen Stadt, in einer anderen Schule ebenfalls zu einer Körperverletzung zwischen Schülern kam, sollten auch hier dem Opfer Bilder zur Identifizierung des Täters vorgelegt werden. Die Richtlinien für Strafverfahren sehen für solche Fälle eine Wahllichtbildvorlage vor (vgl. Nr. 18 RiStBV). Dabei werden zugleich, neben dem Bild des Verdächtigen, auch noch Bilder Nichtverdächtiger - die aber dem Verdächtigen

ähneln - zur Auswahl herangezogen. Bei der Zusammenstellung unterstützt das o.g. TBV den Polizeibeamten. Im vorliegenden Fall wurde vom System aus den gespeicherten Datensätzen u.a. das Bild des 15-jährigen Schülers als Vergleichsbild angeboten und dann auch eingearbeitet. Wie sich herausstellte, sah er dem Täter in diesem Fall so sehr ähnlich, dass der Geschädigte ihn und nicht den tatsächlichen Täter zu erkennen glaubte. Für solche Fälle erlaubt das TBV dann, dem zunächst anonymen Vergleichsbild wieder die Personendaten zuzuordnen. So geschehen und unser Petent sah sich plötzlich mit einem zweiten Tatvorwurf - in einer anderen Stadt, in einer anderen Schule - konfrontiert. Hierbei half es ihm nicht, dass er auch in diesem Fall seine Unschuld beteuerte. Obwohl keinerlei Verbindungen zwischen ihm und der Tat bzw. der handelnden Tätergruppe hergestellt werden konnte, musste sich der 15-jährige innerhalb kurzer Zeit ein zweites Mal vor einem anderen Gericht für eine Straftat, die er nicht begangen hatte, als Angeklagter rechtfertigen. Ich habe mich mit dieser Eingabe sofort an das zuständige Polizeipräsidium gewandt. Die Löschung des Schülers aus dem Kriminalaktennachweis, einschließlich der Vernichtung der erkennungsdienstlichen Unterlagen wurde mir inzwischen bestätigt. Darüber hinaus habe ich diesen Fall zum Anlass genommen, dass Verfahren Erkennungsdienst Digital (ED-DI), welches die Bayerische Polizei derzeit zur Ablösung von TBV einführt, hinsichtlich der detaillierten Ausführungsregelungen genau auf den Prüfstand zu stellen.

Nicht die gespeicherten Bilddaten, sondern die gespeicherten Fingerabdrücke wurden in einem anderen Fall einem unschuldigen jungen Mann, der sich ebenfalls mittels einer Petition an mich wandte, zum Verhängnis.

Nachdem ein zuvor gestohlenes Fahrzeug wieder aufgefunden wurde, erfolgte darin routinemäßig die Spurensuche durch die Kriminalpolizei. Dabei wurden im Fahrzeug Fingerspuren auf einer Plastiktüte festgestellt und mittels des Automatisierten Fingerabdruck-Identifizierungssystems (AFIS) mit dem polizeilichen Datenbestand abgeglichen. Darin befanden sich wegen eines zurückliegenden Tatverdachts auch die Fingerabdrücke des o.g. jungen Mannes und AFIS stellte folglich eine Übereinstimmung fest.

Neun Monate nach der Tat wurde der Petent daher von der Polizei zur Beschuldigtenvernehmung vorgeladen. Wie seine Fingerabdrücke auf eine Plastiktüte in einem gestohlenen Auto kamen, konnte er sich nicht vorstellen. Gleichwohl musste er aber das laufende Ermittlungsverfahren wegen schweren Diebstahls seinem Arbeitgeber erklären. Da sich der junge Mann noch in der Probezeit in einem Betrieb des Sicherheitsgewerbes befand, kündigte ihm sein Arbeitgeber rund zwei Wochen, nachdem er von der Polizei als Beschuldigter vernommen worden war. Durch die weitere Ermittlungsarbeit der Polizei ließ sich schließlich dann doch eine Verbindung zwischen der aufgefundenen Plastiktüte und dem Petenten herstellen. Er war früher als Sicherheitskraft in einem Drogeriemarkt tätig und der Autobesitzer erinnerte sich, am Abend des Diebstahls wegen eines Sicherheitsetiketts am Ausgang genau dieses Marktes kontrolliert worden zu sein. Die alten Dienstpläne konnten schließlich belegen, dass an dem Abend der junge Mann dort die Kontrollen durchführte und seine Fingerabdrücke auf der Plastiktüte wohl von dieser Kontrolle stammten. Obwohl sich der einzige Grund für den Tatverdacht damit aufgelöst hatte, wollte die Polizei an der Speicherung der Daten des jungen Mannes weiter festhalten. Zudem waren im Laufe der Ermittlungen auch noch dessen DNA-Daten gespeichert worden. Erst als ich das zuständige Polizeipräsidium aufgefordert habe, mir die Gründe für eine weitere Speicherung darzulegen, wurden die Speicherungen zu diesem Fall, die erkennungsdienstlichen Unterlagen und die DNA-Daten gelöscht.

Vorübergehender Verlust des Arbeitsplatzes oder als 15jähriger unschuldig angeklagt vor Gericht. Diese beiden drastischen Fälle aus meinem Prüfungsalltag sollen zeigen, welche tief einschneidenden Auswirkungen Datenspeicherungen - hier erkennungsdienstlicher Unterlagen - haben können. In beiden Fällen hatten die Betroffenen nichts zu ihrem Tatverdacht beigetragen.

Vor diesem Hintergrund werde ich auch weiterhin die Gründe für die Speicherung erkennungsdienstlicher Daten genau überprüfen. Insbesondere werde ich im Rahmen meiner Prüfungen darauf achten, ob dabei die vom Bundesverwaltungsgericht bereits im Jahr 1982 (Urteil vom 19.10.1982, Az. 1 C 114/79) umrissenen Anhaltspunkte für rechtmäßige ED-Erfassungen beachtet wurden.

3.10 DNA-Maßnahmen

Der Erhebung und Speicherung von DNA-Daten habe ich bereits in meinem vorangegangenen Tätigkeitsbericht eine große Bedeutung zugemessen. Dabei bin ich insbesondere auf die Voraussetzungen für DNA-Maßnahmen eingegangen, die wegen der wiederholten Begehung nicht-erheblicher Straftaten angeordnet wurden (siehe hierzu 23. Tätigkeitsbericht, Nr. 4.11.1). Auch im Berichtszeitraum wurde ich durch Bürgereingaben immer wieder mit polizeilichen Anordnungen konfrontiert, die hinsichtlich der Erheblichkeit der Anlasstat oder ihrer Prognoseentscheidungen nicht den gestellten Anforderungen entsprachen. Ein Beispiel dafür zeigt die Entnahme einer DNA-Probe nach einem vermeintlichen Fahrraddiebstahl.

Ein Mann hatte sich in der Nacht an einem Bahnhof im angetrunkenen Zustand ein unversperrtes Fahrrad genommen, um damit nach Hause zu fahren. Er wurde dabei beobachtet und angezeigt. Als er vereinbarungsgemäß drei Tage nach der Tat zur Beschuldigtenvernehmung bei der Polizei erschien, entnahmen ihm die Beamten auch eine DNA-Probe. Auf Rückfrage erklärt das zuständige Polizeipräsidium mir gegenüber, die DNA-Maßnahme sei zur Identifizierung in künftigen Strafverfahren gerechtfertigt, erforderlich und auch verhältnismäßig. Der Betroffene habe neben dem versuchten Diebstahl des Fahrrades (das Verfahren wurde von der Staatsanwaltschaft nach § 153 a StPO eingestellt) in der Vergangenheit noch weitere Straftaten begangen, die einer Straftat erheblicher Bedeutung gleichstünden. Dazu führte die Polizei ein mehr als sechs Jahre zurückliegendes Ermittlungsverfahren gegen den Betroffenen wegen des Verdachts einer gemeinschaftlich begangenen Körperverletzung an. In diesem Verfahren hatte die Staatsanwaltschaft bei der Verfahrenseinstellung jedoch gerade betont, dass durch die Tat der Rechtsfriede über den Lebenskreis der Verletzten hinaus nicht gestört worden sei und die Strafverfolgung kein gegenwärtiges Anliegen der Allgemeinheit sei. Des Weiteren führte die Polizei noch ein sieben Jahre zurückliegendes Verfahren wegen gemeinschädlicher Sachbeschädigung an. Damals habe der Betroffene zusammen mit anderen betrunken ein Verkehrsschild beschädigt.

Ich entgegnete dem Polizeipräsidium, dass ich bei der vorliegenden Sachlage weder in der Anlasstat eine Straftat von erheblicher Bedeutung, noch in der Summe der früheren Verfahren eine Gleichbedeutung mit einer erheblichen Straftat von erkennen könne. Zudem entspräche auch die Prognose, ob gegen den Betroffenen künftig Verfahren wegen Straftaten von erheblicher Bedeutung

zu führen sind, nicht den Vorgaben des Bundesverfassungsgerichts (vgl. BVerfG, Beschluss vom 14.12.2000, 2 BvR 1741/99). Die Polizei teilte mir daraufhin die Löschung der DNA-Daten mit.

3.11 Akkreditierungsverfahren bei Großereignissen

Meine im 23. Tätigkeitsbericht, Nr. 4.14.1, geäußerte Befürchtung, dass Zuverlässigkeitsüberprüfungen bei einzelnen Großveranstaltungen auf der Grundlage "informierter Einwilligungen" inzwischen offenbar als Regelverfahren durchgeführt werden, hat sich inzwischen bestätigt. Das Bayerische Landeskriminalamt und das Landesamt für Verfassungsschutz waren beteiligt an Zuverlässigkeitsüberprüfungen im Zusammenhang mit der Leichtathletik-Weltmeisterschaft 2009 und der FIFA U 20-Frauen-Weltmeisterschaft 2010 in Deutschland. Darüber hinaus werden diese Behörden bei Zuverlässigkeitsüberprüfungen anlässlich der FIFA Frauen-Weltmeisterschaft 2011 in Deutschland sowie der Alpinen Ski-Weltmeisterschaft 2011 in Garmisch-Partenkirchen beteiligt sein.

Eine bereichsspezifische gesetzliche Grundlage für Zuverlässigkeitsüberprüfungen bei Großveranstaltungen auf der Grundlage "informierter Einwilligungen" bestand und besteht weiterhin nicht. Ich bedaure, dass das Staatsministerium des Innern meiner Rechtsauffassung, die ich anlässlich der Akkreditierungsverfahren im Rahmen der Leichtathletik-Weltmeisterschaft 2009 erneut mitgeteilt habe, nicht beigetreten ist. Ich bin weiterhin der Ansicht, dass Zuverlässigkeitsüberprüfungen bei Großveranstaltungen aufgrund ihrer Bedeutung und ihres Umfangs zu erheblichen Eingriffen in das Grundrecht auf informationelle Selbstbestimmung einer Vielzahl Betroffener führen. An der Freiwilligkeit einer Einwilligung in solche Eingriffe habe ich erhebliche Zweifel, weil Betroffene oft unzumutbare Nachteile befürchten müssen, wenn sie ihre Einwilligung verweigern. Auch im Hinblick auf den Grundsatz des Vorbehalts des Gesetzes halte ich eine Einwilligung für problematisch. Gemäß der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre darf der Gesetzgeber die wesentlichen Entscheidungen über die Voraussetzungen, Umstände und Folgen von Eingriffen nicht an die Verwaltung delegieren, sondern muss sie selbst treffen.

Das Landeskriminalamt und das Landesamt für Verfassungsschutz haben die anlässlich der Zuverlässigkeitsüberprüfungen im Rahmen des Akkreditierungsverfahrens zur Leichtathletik-Weltmeisterschaft 2009 erhobenen personenbezogenen Daten nach dem offiziellen Ende der Weltmeisterschaft gelöscht. Bürgereingaben oder Beschwerden im Zusammenhang mit den Zuverlässigkeitsüberprüfungen sind im meiner Geschäftsstelle bisher nicht eingegangen. Dieser Umstand ändert jedoch nichts an meinen grundsätzlichen Bedenken gegenüber der beschriebenen Vorgehensweise.

4 Verfassungsschutz

Im Bereich der Bayerischen Gesetzgebung habe ich auf eine datenschutzkonforme Ausgestaltung des Bayerischen Verfassungsschutzgesetzes hingewirkt. Von besonderer Bedeutung waren dabei der Verzicht auf die "nur automatische Aufzeichnung" bei der Wohnraumüberwachung und der Verzicht auf die Befugnis zur heimlichen Wohnungsdurchsuchung. Aus datenschutzrechtlicher Sicht ist auch hervorzuheben, dass das Bundesverfassungsgericht in seinem Urteil vom 02.03.2010 zur "Vorratsdatenspeicherung" den Anbietern öffentlich zugänglicher Telekommunikationsdienste untersagt hat, die mit behördlichen Auskunftsersuchen - z.B. durch das Landesamt für Verfassungsschutz - erhobenen "Vorratsdaten" an die ersuchenden Stellen zu übermitteln.

Auch in diesem Berichtszeitraum habe ich beim Landesamt für Verfassungsschutz wieder Datenerhebungen, -speicherungen und -übermittlungen sowie Auskunftserteilungen bzw. -ablehnungen überprüft. Schwerpunkte waren diesmal die Zugriffe auf personenbezogene Daten der Protokollierungsdatei des Vorgangsverwaltungssystem DOMEA und die Speicherung personenbezogener Daten von Kindern und Jugendlichen. Die Prüfungen erfolgten anlassunabhängig oder aufgrund von Bürgereingaben.

4.1 Änderungen des Bayerischen Verfassungsschutzgesetzes (BayVSG)

Die 2008 geänderten oder neu geschaffenen Befugnisse des Landesamts für Verfassungsschutz (siehe hierzu 23. Tätigkeitsbericht, Nr. 5.1) wurden im Berichtszeitraum in zwei Fällen datenschutzrechtlich entschärft oder sogar ganz gestrichen; diese Änderungen sind am 01.08.2009 in Kraft getreten. Allerdings bleiben auch hier datenschutzrechtliche Bedenken bestehen:

- Verzicht auf eine "nur automatische Aufzeichnung" beim sog. Großen Lauschangriff

  Wie im Polizeiaufgabengesetz (siehe hierzu Nr. 3.1.1) wurde auch im BayVSG die bislang enthaltene Befugnis gestrichen, im Rahmen einer Wohnraumüberwachung ("Großer Lauschangriff") in Privatwohnungen und Räumen von sog. Berufsgeheimnisträgern (z.B. Geistliche, Ärzte, Rechtsanwälte) geführte Gespräche "nur automatisch" aufzeichnen zu dürfen. Dem Bundesverfassungsgericht zufolge (vgl. Urteil zum "Großen Lauschangriff" vom 03.03.2004) kann es wegen der Unterbrechungspflicht bei Kernbereichsgesprächen notwendig sein, bei dem Abhören einer Privatwohnung auf eine nur automatische Aufzeichnung der abgehörten Gespräche zu verzichten, um jederzeit die Ermittlungsmaßnahme unterbrechen zu können. Ich begrüße, dass meine datenschutzrechtliche Forderung (siehe hierzu 23. Tätigkeitsbericht, Nr. 5.1.1.) nun in die Gesetzgebung Eingang gefunden hat.

  Nicht berücksichtigt wurde allerdings meine im Gesetzgebungsverfahren vorgebrachte Forderung, die im Gesetz vorgesehene Unterscheidung zwischen "weniger" und "mehr" geschützten Berufsgeheimnisträgern aufzugeben (siehe Nr. 3.1.1). Aus datenschutzrechtlicher Sicht erkenne ich

auch beim Verfassungsschutz keinen sachlichen Grund für eine Differenzierung zwischen "mehr" und "weniger" geschützten Berufsgeheimnisträgern.

- Verzicht auf die Befugnis zur heimlichen Wohnungsdurchsuchung

  Der Gesetzgeber hat die zum 01.08.2008 in Kraft getretene Befugnis für das LfV wieder gestrichen, zur Durchführung einer Wohnraumüberwachung, einer Beschränkung der Telekommunikation und einer Online-Durchsuchung die Wohnung des Betroffenen heimlich zu betreten und zu durchsuchen (zur Streichung der entsprechenden polizeilichen Befugnis siehe hierzu Nr. 3.2.2). Auch hier sind meiner datenschutzrechtlichen Forderung und meinen massiven verfassungsrechtlichen Bedenken (siehe hierzu 23. Tätigkeitsbericht, Nr. 5.1.5) teilweise Rechnung getragen worden.

  Trotz dieser Verbesserungen bedaure ich, dass die Gesetzesänderung nicht auch dazu benutzt wurde, auf die Befugnis zur "Online-Durchsuchung" für das Landesamt für Verfassungsschutz zu verzichten und die Regelung zum "verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Worts außerhalb von Wohnungen" wie folgt anzupassen:

- "Online-Durchsuchung"

  Das Bundesverfassungsgericht hat in seinem Urteil vom 27.02.2008 die "Online-Durchsuchung" nur für zulässig erklärt bei tatsächlichen Anhaltspunkten für eine konkrete Gefahr für ein überragend wichtiges Rechtsgut. Die Abwehr konkreter Gefahren ist aber typischerweise Aufgabe der Polizei und der Sicherheitsbehörden (vgl. Art. 6 Landesstraf- und Verordnungsgesetz). Das Landesamt für Verfassungsschutz hat hingegen als "Frühwarnsystem" der Staatsregierung die Aufgabe, im Vorfeld konkreter Gefahren Entwicklungen und Bestrebungen zu beobachten. Hinzu kommt, dass auch für die Polizei eine Befugnis für Online-Durchsuchungen besteht. Auch wenn bislang von der Befugnis zur Online-Durchsuchung im Polizeibereich kein Gebrauch gemacht wurde, ist es bei der stetigen Verbesserung der technischen Möglichkeiten mittelfristig zu befürchten, dass eine solche parallele Zuständigkeit von Verfassungsschutz und Polizei ohne ausreichende Abgrenzung zu überlappenden und damit zusätzlichen Rechtseingriffen führt.

- "Verdeckter Einsatz technischer Mittel"

  In der Befugnis zum "verdeckten Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht-öffentlich gesprochenen Wortes außerhalb von Wohnungen" fehlt ein zweistufiges Schutzkonzept für den Kernbereich privater Lebensgestaltung. Die Norm enthält keine Regelungen, die - so weitgehend wie möglich - sicherstellen, dass Daten mit Kernbereichsbezug gar nicht erst erhoben werden. Die Vorschrift befasst sich vielmehr nur mit der Verwendung der Daten. Im Anwendungsbereich dieser Maßnahme sind vielfältige Gesprächskonstellationen denkbar, die mit einer gewissen Wahrscheinlichkeit höchstpersönlichen Bezug haben. Beispielsweise entspricht es der allgemeinen Lebenserfahrung, dass Personen des persönlichen Vertrauens in Personenkraftfahrzeugen oft intime Gespräche

führen. Vergleichbares gilt etwa für höchst vertrauliche Gespräche bei Aufenthalten in der Natur (Parkgelände, Gärten usw.), bei denen die Gesprächspartner nicht mit einer Kenntnisnahme ihrer Gesprächsinhalte durch Dritte rechnen. Ein ausdrückliches Erhebungsverbot für Daten, die einem Berufsgeheimnis - z.B. aus der Tätigkeit als Geistlicher oder Strafverteidiger - zuzuordnen sind, fehlt ebenfalls.

Aus verfassungsrechtlicher Sicht bestehen weiterhin erhebliche Bedenken, weil die gesetzliche Regelung eine Pflicht des Landesamts für Verfassungsschutz zur grundsätzlichen Benachrichtigung nicht vorsieht. Das Bundesverfassungsgericht indes hat in mehreren Entscheidungen die Bedeutung der Pflicht zur grundsätzlichen Benachrichtigung von heimlichen Eingriffen hervorgehoben.

4.2 Datenschutzrechtliche Prüfungen beim Verfassungsschutz

Schwerpunkte meiner Prüfungen im Bereich des Verfassungsschutzes waren diesmal insbesondere die Zugriffe auf Daten der Protokolldatei von DOMEA und die Speicherung von Kindern und Jugendlichen. Daneben wurden Datenerhebungen, -speicherungen und -übermittlungen sowie Auskunftserteilungen bzw. -ablehnungen durch das Landesamt für Verfassungsschutz überprüft.

4.2.1 Protokolldatei für das Dokumentenmanagementsystem DOMEA

Nach meinen Feststellungen ließen sich aus Protokollierungsdaten von DOMEA (siehe hierzu 21. Tätigkeitsbericht, Nr. 8.5) teilweise konkrete Rückschlüsse auf die gespeicherten Personendaten ableiten. In der Protokolldatei bleiben diese Daten dann mehrere Jahre über die Löschungsfrist der Ursprungsspeicherung hinaus recherchierbar. Auch wenn ich bei meiner Kontrolle vor Ort keinerlei Hinweise auf eine missbräuchliche Nutzung der Protokollierungsdaten erkennen konnte, erfordert dieses Thema noch nähere Abstimmungen mit dem Landesamt für Verfassungsschutz. Weitere Gespräche sind daher vereinbart, um für das Nachfolgesystem von DOMEA eine datenschutzkonforme Lösung zu finden.

4.2.2 Speicherung von Kindern und Jugendlichen

Wie bereits in der Vergangenheit habe ich ein besonderes Augenmerk auf die Speicherung von Kindern und Jugendlichen gelegt. Über das Verhalten von Kindern darf der Verfassungsschutz nach Maßgabe des Verfassungsschutzgesetzes keine personenbezogenen Daten in Fachdateien speichern. Solche Speicherungen konnte ich bei meiner Prüfung auch nicht feststellen. Bei insgesamt siebzehn Speicherungen von Jugendlichen vermochte ich hingegen anhand der eingesehenen Unterlagen keine ausreichenden Belege erkennen, die bei vernünftiger Betrachtung auf Bestrebungen der Jugendlichen gegen die freiheitlich demokratische Grundordnung hingewiesen hätten. Vielmehr erschienen in einigen Fällen eher jugendliches Fehlverhalten oder Provokationen - ohne extremistischen Hintergrund - naheliegender. Das Landesamt für Verfassungsschutz ist in allen genannten Fällen meiner Aufforderung zur Löschung der Personendaten gefolgt. Darüber hinaus wurde mir zugesichert, zukünftig vor der Speicherung von Minderjährigen verstärkt die Zielrichtung und das Motiv der Anlasssachverhalte in die Bewertungen einzubeziehen.

4.2.3 Auskunftserteilungen durch das Landesamt für Verfassungsschutz und Bürgereingaben

Bezüglich des Landesamts für Verfassungsschutz habe ich auch die Behandlung von Auskunftsersuchen überprüft. Sowohl bei Bürgereingaben, als auch bei meinen Prüfungen vor Ort konnte ich dabei feststellen, dass das Landesamt für Verfassungsschutz die datenschutzrechtlichen Bestimmungen bei der Bearbeitung von Auskunftsersuchen grundsätzlich beachtet.

5 Justiz

Im Berichtszeitraum habe ich anlassunabhängig bei einer Staatsanwaltschaft, einer Justizvollzugsanstalt, zwei Amtsgerichten, einem Landgericht und einem Oberlandesgericht vor Ort eine datenschutzrechtliche Prüfung durchgeführt. Neben den anlassunabhängigen Prüfungen habe ich anlassbezogen aufgrund von Bürgereingaben auch Prüfungen konkreter Einzelfälle vorgenommen. Bei Gesetzentwürfen, Verordnungsentwürfen und Bekanntmachungsentwürfen habe ich auf die Umsetzung datenschutzrechtlicher Anforderungen unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts hingewirkt.

Die nachfolgenden Darstellungen sind eine Auswahl meiner Feststellungen im Justizbereich.

5.1 Gesetze und Rechtsverordnungen

Im Berichtszeitraum habe ich zu verschiedenen Gesetzentwürfen (Untersuchungshaftvollzugsgesetz, Dolmetschergesetz, Bayerisches Maßregelvollzugsgesetz), Verordnungsentwürfen (ALB-Abrufverordnung, Aufbewahrungs-VO, Internetversteigerungs-VO), Bekanntmachungen (Ausführungsbekanntmachung zum Dolmetschergesetz) und Konzepten (Aufbewahrung von Notariatsunterlagen) Stellungnahmen gegenüber den zuständigen Staatsministerien abgegeben.

Beim Dolmetschergesetz habe ich erreicht, dass dem betroffenen Dolmetscher oder Übersetzer für die Veröffentlichung "weitergehender Daten" im Internet - gemeint sind Daten, die über Stammdaten wie Namen, Vornamen, Berufsbezeichnung, Anschrift und Sprache, für die der Dolmetscher bestellt ist, hinausgehen - ein Widerspruchsrecht eingeräumt wird.

Bezüglich des Entwurfs eines Bayerischen Maßregelvollzugsgesetzes habe ich bereits im 23. Tätigkeitsbericht, Nr. 6.1.7, dringend eine normenklare und verhältnismäßige Rechtsgrundlage für die Gestaltung des Maßregelvollzugs gefordert. Eine solche existiert bis heute nicht. In das derzeit laufenden Gesetzgebungsverfahren habe ich einige datenschutzrechtliche Verbesserungen einbringen können. Das zuständige Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen hat etwa meine Bedenken hinsichtlich der Erforderlichkeit der getrennten Aufbewahrung von und des getrennten Zugriffs auf "besondere Daten" (etwa Krankenunterlagen) aufgegriffen.

5.2 Aus der Justiz allgemein

5.2.1 Videoüberwachung von Justizgebäuden

Im Berichtszeitraum habe ich die Videoüberwachung mehrerer Gebäude aus den verschiedenen Bereichen der Justiz geprüft. Die Prüfungen betrafen Dienstgebäude eines Oberlandesgerichts und einer Generalstaatsanwaltschaft, eines Landgerichts und einer Staatsanwaltschaft, zweier Amtsgerichte und einer Jus-

tizvollzugsanstalt. Anlass für diesen Prüfungsschwerpunkt ist der verstärkte Einsatz von Videoüberwachungsanlagen bei Justizgebäuden aufgrund mehrerer Vorfälle in Gerichtsgebäuden, etwa in Landshut und Dresden.

In allen Fällen konnte grundsätzlich davon ausgegangen werden, dass die Videoüberwachung aufgrund der besonderen Sensibilität von Justizgebäuden zur Ausübung des Hausrechts erforderlich ist. Allerdings war in mehreren Fällen die Videoüberwachung nicht auf den Bereich der unmittelbaren Nähe i.S.d. Art. 21 a Abs. 1 BayDSG beschränkt. So bestand teilweise die Möglichkeit, mit Hilfe einer Zoomfunktion bei Schwenkkameras auch weiter entfernte Objekte soweit heranzuzoomen, dass Personen, Gebäudeeinzelheiten oder etwa Fahrzeuge erkennbar waren. In den bereits abgeschlossenen Verfahren konnte hier durch technische Maßnahmen eine Reduzierung des Sichtbereichs erreicht werden. In einem Fall dauert der Schriftwechsel noch an.

Weiterhin reichten in den meisten Fällen die Hinweise auf die Videoüberwachung und die erhebende Stelle nicht aus. Dabei ist die Kennzeichnung - etwa durch Schilder in Form von sog. Piktogrammen - so anzubringen, dass ein von der Maßnahme Betroffener auf die Videoüberwachung hingewiesen wird, bevor er den Erfassungsbereich betritt. In allen abgeschlossenen Verfahren konnte dies erreicht werden, in den übrigen Verfahren dauert der Schriftwechsel hierzu noch an.

In zwei Fällen, in denen neben einer Videobeobachtung auch eine Videoaufzeichnung stattfindet, lag weder eine datenschutzrechtliche Freigabe noch eine Mitteilung an den behördlichen Datenschutzbeauftragten vor. Insbesondere die fehlende datenschutzrechtliche Freigabe erachte ich als sehr problematisch, da diese unerlässliche Voraussetzung für den Einsatz einer Videoaufzeichnung ist. Erst die datenschutzrechtliche Freigabe und die Mitteilung an den behördlichen Datenschutzbeauftragten ermöglichen einen auf einer Abwägung der betroffenen Rechtsgüter basierenden Einsatz der Videoaufzeichnung. So konnte im Rahmen der Prüfungen zwar die grundsätzliche Bedeutung der Einrichtungen erläutert werden, es fehlte jedoch regelmäßig am Bewusstsein für den konkreten Einsatzzweck. So ist in beiden Fällen auch zu kritisieren, dass keine Regelungen zur Speicherung der Videoaufzeichnungen vorlagen, obwohl gesetzlich eine maximale Speicherungsfrist von drei Wochen vorgesehen ist.

Da in Zukunft wohl noch mit einem verstärkten Einsatz von Videoüberwachungsanlagen zu rechnen ist, bleibt zu wünschen, dass ein stärkeres Bewusstsein für die rechtlichen Grenzen der Videoüberwachung entsteht. Dabei sollte insbesondere die Erforderlichkeit einer Videoüberwachung kritisch hinterfragt werden, da diese in vielen Fällen - etwa bei Angriffen auf Justizmitarbeiter durch Prozessbeteiligte - häufig die in sie gesetzten Erwartungen nicht wird erfüllen können.

5.2.2 Bezeichnung des behördlichen Datenschutzbeauftragten im Geschäftsverteilungsplan und in sonstigen Verzeichnissen

Von mehreren Petenten wurde mir geschildert, dass ihre Frage nach dem behördlichen Datenschutzbeauftragten nicht oder nicht unmittelbar beantwortet werden konnte. Im Rahmen der Überprüfung habe ich teilweise festgestellt, dass die behördlichen Datenschutzbeauftragten nicht oder zumindest nicht richtig in den Geschäftsverteilungsplänen bezeichnet waren.

Zur Wahrnehmung des datenschutzrechtlichen Interesses des Bürgers halte ich es für unerlässlich, dass der behördliche Datenschutzbeauftragte in der jeweiligen Geschäftsverteilung und den daraus abgeleiteten Verzeichnissen, wie etwa dem Telefonverzeichnis, klar und richtig benannt wird. Dazu gehört auch, dass im Geschäftsverteilungsplan dessen unmittelbare Unterstellung unter die Gerichts- bzw. Behördenleitung und die Weisungsfreiheit in dieser Eigenschaft hervorgehoben wird. Dies gilt insbesondere auch bei Gerichten und Behörden, die keinen eigenen, sondern einen gemeinsamen Datenschutzbeauftragten haben. Ferner ist sicherzustellen, dass dem anfragenden Bürger - auch bei telefonischer Anfrage - der zuständige behördliche Datenschutzbeauftragte unmittelbar benannt werden kann.

Für den Bereich der Gerichte und Justizbehörden hat das Staatsministerium der Justiz und Verbraucherschutz meine Bitte aufgegriffen und sämtliche Gerichte und Behörden des Geschäftsbereichs auf die Einhaltung der gesetzlichen Vorgaben hingewiesen. Die Einhaltung dieser Vorgaben werde ich stichprobenweise überprüfen.

5.2.3 Unbeabsichtigte Datenübermittlung bei der Benutzung von Sichtfensterumschlägen

Im Rahmen mehrerer Eingaben bin ich darauf aufmerksam gemacht worden, dass bei der Benutzung von Sichtfensterumschlägen häufig Daten außerhalb des Adressfeldes sichtbar sind. Bei Anschreiben von Justiz- oder Ordnungswidrigkeitenbehörden waren so auch personenbezogene Daten, wie der Geburtstag und Geburtsort des Adressaten oder Angaben zu Prozessparteien und gerichtliche Aktenzeichen sichtbar. Dieses Problem besteht in den Fällen, in denen solche Daten in der Nähe des Adressfeldes gedruckt und durch Verrutschen des Schriftstücks sichtbar werden.

Aus datenschutzrechtlicher Sicht liegt in diesen Fällen - ob bewusst oder unbewusst - eine unzulässige Datenübermittlung an unbeteiligte Dritte vor. Bei der Gestaltung von Musteranschreiben bzw. beim Falten von Schreiben ist unbedingt darauf zu achten, dass personenbezogene Daten auch bei Verrutschen eines Schriftstücks nicht im Sichtfenster erkennbar werden. Die betroffenen Behörden haben mir dies zugesagt. Vom Bayerischen Staatsministerium der Justiz und Verbraucherschutz wurde mir zusätzlich mitgeteilt, dass die Problematik durch die Einführung eines neuen EDV-Verfahrens in Zukunft erledigt sein werde.

5.2.4 Justiz und "Reality-TV"

In den letzten Jahren haben sogenannte "Reality-TV"-Produktionen über Einsätze von verschiedenen Behörden u.a. der Justiz und der Polizei erheblich zugenommen. Da solche Unterhaltungsformate ihren Reiz aus der "Echtheit" der gezeigten Fälle und Personen beziehen, sind diese nur mit Unterstützung staatlicher Stellen möglich. Indem staatliche Stellen Pressevertretern die Möglichkeit einräumen, Amtsträger bei der Arbeit zu begleiten und Filmaufnahmen anzufertigen, findet aus datenschutzrechtlicher Sicht eine Datenübermittlung an Dritte statt. Vor dem Hintergrund, dass bei manchen Fernsehformaten eher die Befriedigung der Sensationslust als die sachliche Information über die Behördenarbeit im Vordergrund stehen dürfte, ist in besonderem Maße das Persönlichkeitsrecht der Betroffenen zu berücksichtigen. Da eine Rechtsgrundlage für eine solche

Datenübermittlung nicht vorhanden ist, sind derartige Berichte nur zulässig, wenn das Einverständnis des Betroffenen vorliegt. Voraussetzung für ein solches Einverständnis ist jedoch, dass der Betroffene umfassend über die Hintergründe und die Tragweite seiner Einwilligung aufgeklärt wird (sog. "informierte Einwilligung"). Dazu ist es insbesondere erforderlich, den Betroffenen rechtzeitig über Umfang und Dauer und Verwendungszweck der Aufnahmen aufzuklären.

Eine solche umfassende Information des Betroffenen konnte ich in den von mir kontrollierten Fällen nicht feststellen. In einem besonders krassen Fall hat das Landgericht München I einen privaten Fernsehsender dazu verurteilt, einem von einer Reality-Reportage Betroffenen Schadensersatz zu bezahlen. Der Betroffene wurde in einer Fernsehsendung teilweise nur mit einer Unterhose bekleidet bei einer Wohnungsöffnung durch eine Gerichtsvollzieherin gezeigt. Dabei wurde auch der Name des Betroffenen wiedergegeben. Den Schadensersatzanspruch begründete das Landgericht damit, dass u.a. aufgrund der Überrumpelungssituation keine wirksame Einverständniserklärung des Betroffenen vorgelegen habe.

Die 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 08./09.10.2009 hat meine Bedenken aufgegriffen und in einer Entschließung Justiz und Polizei aufgefordert, von der Mitwirkung an "Reality"-Reportagen Abstand zu nehmen.

Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009
"Reality-TV" - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen - wobei auch schon einmal eine Wohnung zwangsgeöffnet wird - oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu er-

möglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality"-Reportagen Abstand zu nehmen.

5.3 Strafverfolgung

5.3.1 Einsatz von Hypnose bei der Aufklärung von Straftaten

Im Berichtszeitraum sind mir zwei Fälle bekannt geworden, in denen auf Veranlassung der Strafverfolgungsbehörden Hypnosesitzungen mit Zeugen durchgeführt worden sind. In beiden Fällen wurde der Versuch unternommen, durch Hypnose festzustellen, ob sich ein Zeuge an ein Kfz-Kennzeichen erinnern könne.

Die Strafprozessordnung (StPO) zählt die Anwendung von Hypnose bei der Vernehmung von Zeugen oder Beschuldigten zu den verbotenen Vernehmungsmethoden. Diese dürfen auch bei Vorliegen einer Einwilligung des Betroffenen nicht angewandt werden. Das Staatsministerium der Justiz und für Verbraucherschutz vertritt allerdings die Auffassung, dass dieses Verbot einer Hypnosesitzung außerhalb einer Vernehmungssituation nicht entgegenstehe. So dürfe sich ein Zeuge, der an der Aufklärung einer Straftat mitwirken wolle, von sich aus oder auf Initiative der Ermittlungsbehörden außerhalb einer Vernehmungssituation einer Hypnose zur Auffrischung seines Gedächtnisses unterziehen und danach den Ermittlungsbehörden neue Erkenntnisse mitteilen. Der Einsatz von Hypnosetechniken auf Initiative der Ermittlungsbehörden komme jedoch nur als ultima ratio bei schwerwiegenden Straftaten in Betracht. Der Zeuge müsse über das Ergebnis der Hypnose nach deren Ende selbst verfügen können. Er müsse über die Weitergabe an die Strafverfolgungsbehörden nach Kenntnis vom Ergebnis selbst entscheiden, um die Ausübung etwaiger Zeugnis- bzw. Aussageverweigerungsrechte zu ermöglichen. Dies schließe eine Teilnahme der Strafverfolgungsbehörden an der Hypnosesitzung - auch über Videoübertragung - aus.

Ich teile diesen Standpunkt nicht und halte Initiativen der Ermittlungsbehörden in Richtung einer Hypnosesitzung auch außerhalb von förmlichen Vernehmungssituationen für verfassungs- und datenschutzwidrig. In § 136 a StPO sind die Vernehmungsmethoden aufgezählt, die in den Strafverfolgungsbehörden ausdrücklich verboten sind. Mit der Aufnahme der Hypnose als verbotene Vernehmungsmethode hat der Gesetzgeber eine grundsätzliche Entscheidung gegen ihre Anwendung getroffen. Deshalb dürfen die Strafverfolgungsbehörden diese Methoden weder selbst anwenden, noch durch andere anwenden lassen. Dies gilt ohne Rücksicht auf die Einwilligung des Zeugen. Der Einsatz von Hypnosetechniken außerhalb einer Vernehmung auf Initiative der Ermittlungsbehörde ist dieser selbst als eigene Maßnahme zuzurechnen, da sie diese Maßnahme initiiert, maß-

geblich beeinflusst, ihre Ergebnisse nutzen möchte und möglicherweise - so war es in den beiden mir bekannten Fällen - auch die anfallenden Kosten übernimmt. Selbst wenn man diese Maßnahmen nicht der Ermittlungsbehörde zurechnen wollte, so hat sich die Ermittlungsbehörde aufgrund der gesetzlichen Negativbewertung des Einsatzes von Hypnose im Ermittlungsverfahren jeder darauf abzielenden Initiative zu enthalten. Eine solche Initiative halte ich für den Versuch einer (unzulässigen) Umgehung eines gesetzlichen Verbotes. Dies gilt auch, wenn der Einsatz von Hypnosetechniken auf Initiative der Ermittlungsbehörde als ultima ratio bei schwerwiegenden Straftaten in Betracht kommen soll. Über die Zulässigkeit und die Voraussetzungen von Ermittlungsmaßnahmen entscheidet im Hinblick auf den Grundsatz der Gesetzmäßigkeit der Verwaltung der Gesetzgeber und nicht die Ermittlungsbehörde. Es ist mir insofern auch nicht begreiflich, unter welchem rechtlichen Gesichtspunkt eine an sich unzulässige Ermittlungsmethode bei Anwendung als ultima ratio bei schwerwiegenden Straftaten anders zu bewerten sein soll.

Ich habe das Staatsministerium der Justiz und für Verbraucherschutz aufgefordert, dafür Sorge zu tragen, dass auf den Einsatz von Hypnosetechniken gerichtete Initiativen der Ermittlungsbehören unterbleiben. Seitens des Staatsministeriums wurde mir mitgeteilt, dass an der dortigen Auffassung festgehalten werde.

5.3.2 Pressearbeit der Staatsanwaltschaften

Die unter Nr. 3.6 ("Pressearbeit der Polizei") dargestellten datenschutzrechtlichen Grundsätze gelten auch für die Presse- und Öffentlichkeitsarbeit von Staatsanwaltschaften. Dabei ist insbesondere bei den Staatsanwaltschaften eine Entwicklung zu mehr Pressearbeit festzustellen. Während früher Presseanfragen von Staatsanwaltschaften häufig mit dem Hinweis auf das noch laufende Ermittlungsverfahren beantwortet wurden, ist in den letzten Jahren eine verstärkte Öffentlichkeitsarbeit wahrzunehmen. Diese beschränkt sich nicht darauf, Presseanfragen zu beantworten, sondern es wird aktiv mit Pressemitteilungen der Kontakt zu den Medien gesucht. Häufig wird dabei nicht nur über den Stand der Ermittlungen informiert, sondern auch über sonstige Erkenntnisse und Vorstrafen des Beschuldigten berichtet.

Insbesondere im Bereich von Sexualstraftaten, bei denen in besonderem Maße die Gefahr einer öffentlichen Vorverurteilung besteht, kann eine personenbezogene Berichterstattung zu unwiderruflichen Nachteilen sowohl für Beschuldigte als auch für Opfer führen. Für beschuldigte Personen gebietet es die Unschuldsvermutung, bei der Pressearbeit solche Vorverurteilungen und damit einhergehende irreversible Folgen von vornherein zu vermeiden. Zugleich begründet die Pressearbeit für die betroffenen Opfer die Gefahr, dass ihre Persönlichkeitsrechte durch die Staatsanwaltschaft noch einmal verletzt werden. Ich werde die staatsanwaltschaftliche Presse- und Öffentlichkeitsarbeit beobachten und ggf. auf die Einhaltung der unter Nr. 3.6 dargestellten Maßstäbe hinwirken.

5.3.3 Anordnung von Blutentnahmen bei Gefahr im Verzug

Bereits in meinem 23. Tätigkeitsbericht, Nr. 6.3.5, wies ich auf den Beschluss des Bundesverfassungsgericht vom 12.02.2007 (Az. 2 BvR 273/06) hin, in dem das Bundesverfassungsgericht festgestellt hat, dass die Anordnung einer Blutentnahme nach § 81 a Strafprozessordnung grundsätzlich dem Richter vorbehalten

ist. Weiterhin hatte ich mitgeteilt, dass sich das Staatsministerium der Justiz auf den Standpunkt gestellt hat, dass bei Blutprobenentnahmen wegen Alkoholgenusses im Hinblick auf den schnellen Abbau des Alkohols immer Gefahr im Verzug bestehe, da eine richterliche Entscheidung nur mit Verzögerung und daher nicht rechtzeitig erreicht werden könne. Es drohe insoweit ein Beweismittelverlust. Typischerweise handele es sich bei den den Blutprobenentnahmen zugrundeliegenden Sachverhalten um Vergehen im Zusammenhang mit Trunkenheit im Straßenverkehr bzw. um entsprechende Ordnungswidrigkeiten. Ich hatte darauf hingewiesen, dass diese Verfahrensweise m.E. den Anforderungen des Bundesverfassungsgerichts nicht gerecht werde.

Im Berichtzeitraum sind dazu mehrere (ober-)gerichtliche Entscheidungen ergangen, die meine Bedenken bestätigen und die genannte Rechtsprechung des Bundesverfassungsgerichts konsequent fortführen.

Das Bundesverfassungsgericht hat zuletzt mit Beschluss vom 11.06.2010 (2 BvR 1046/08) klargestellt, dass die oben dargestellten Grundsätze auch für den Bereich der Blutentnahme im Zusammenhang mit dem Verdacht von Straftaten oder Ordnungswidrigkeiten im Straßenverkehr gelten. Das Bundesverfassungsgericht hat dazu ausgeführt, dass die Ermittlungsbehörden die Annahme einer Gefahr im Verzug - sofern der drohende Verlust des Beweismittels nicht offensichtlich sei - mit auf den Einzelfall bezogenen Tatsachen zu begründen und in den Ermittlungsakten zu dokumentieren hätten, da die Annahme einer Gefahr im Verzug die Ausnahme der gesetzlichen Regel sei. Insbesondere die im zugrundeliegenden Verfahren vertretene Auffassung, dass richterliche Eilentscheidungen generell nur nach Vorlage schriftlicher Unterlagen getroffen werden könnten und entsprechend Zeit benötigen, somit also zwangsläufig mit der Gefährdung des Untersuchungszwecks einhergingen, lässt das Bundesverfassungsgerichts nicht gelten. Eine solche Auffassung würde nämlich dazu führen, dass die Entscheidung des Ermittlungsrichters zur Blutentnahme bei Verdacht auf Trunkenheit im Verkehr in der überwiegenden Zahl der Fälle nicht mehr eingeholt werden würde. Der Richtervorbehalt bei der Blutentnahme wäre damit im Regelfall bedeutungslos.

Das Oberlandesgericht Bamberg hat in einem Beschluss vom 19.03.2009 (Az. 2 Ss 15/09) darauf hingewiesen, dass die Strafverfolgungsbehörden regelmäßig versuchen müssen, eine Anordnung des zuständigen Richters zu erreichen, bevor sie selbst die ihnen vom Gesetzgeber nur ersatzweise zuerkannte Kompetenz zur eigenen Anordnung einer Blutentnahme in Anspruch nehmen. Nur in Ausnahmefällen, so das Oberlandesgericht, wenn schon die zeitliche Verzögerung wegen eines solchen Versuchs den Erfolg der Maßnahme gefährden würde, dürften die Strafverfolgungsbehörden selbst die Anordnung treffen, ohne sich zuvor um eine richterliche Entscheidung bemüht zu haben. Insbesondere könne bei Straftaten im Zusammenhang mit Alkohol und Drogen die typischer Weise bestehende abstrakte - und damit gerade nicht einzelfallbezogene - Gefahr, dass durch den körpereigenen Abbau der Stoffe der Nachweis der Tatbegehung erschwert oder gar verhindert werde, für sich allein noch nicht für die Annahme einer Gefährdung des Untersuchungserfolges ausreichen. Andernfalls würden die konkreten Umstände des Einzelfalls, etwa im Hinblick auf die jeweilige Tages- oder Nachzeit, die jeweiligen Besonderheiten am Ort der Kontrolle oder die Nähe zu rechtlich relevanten Grenzwerten, völlig außer Betracht gelassen werden. Im Übrigen bestehe die verfassungsrechtliche Verpflichtung der Gerichte, die Erreichbarkeit eines Ermittlungsrichters auch durch die Einrichtung eines All- oder Notdienstes am Abend und an den Wochenenden zu gewährleisten.

Die Annahme einer Gefährdung des Untersuchungserfolges müsse vielmehr auf Tatsachen gestützt werden, die auf den Einzelfall bezogen und in den Ermittlungsakten zu dokumentieren sind, sofern die Dringlichkeit nicht evident sei.

Zunehmend wird von der obergerichtlichen Rechtsprechung bei Nichtbeachtung der genannten Grundsätze auch ein Beweisverwertungsverbot angenommen. So hat das Oberlandesgericht Hamm mit Beschluss vom 12.03.2009 (Az. 3 Ss 31/09) eine Beweisverwertungsverbot bei einer polizeilichen Anordnung angenommen, da ein objektiv willkürliches Verhalten bzw. ein grober Verstoß des handelnden Polizeibeamten vorgelegen habe.

Das Staatsministerium des Innern und das Staatsministerium der Justiz und für Verbraucherschutz haben auf die geschilderte Problematik reagiert, indem die Vorgaben für die Praxis überarbeitet und ein neues Formblatt erstellt wurden. Gleichwohl reichen diese Maßnahmen für die Umsetzung der ober- und verfassungsgerichtlichen Rechtsprechung m.E. nicht aus. Dies habe ich den beiden Staatsministerien auch mitgeteilt.

5.3.4 Kontenabfragen durch die Staatsanwaltschaft

Bereits im 23. Tätigkeitsbericht, Nr. 6.3.4, habe ich auf die verfassungsrechtlichen Schranken hingewiesen, die das Bundesverfassungsgericht in seiner Entscheidung vom 13.06.2007 (Az. 1 BvR 1550/03) für die Kontenabfragen nach § 24 c Abs. 3 Nr. 3 KWG gesetzt hat. Ich hatte in diesem Zusammenhang berichtet, dass eine Prüfung gezeigt hat, dass bei bestimmten Deliktsarten, wie z.B. Betrug und Unterschlagung regelmäßig bereits direkt nach Anzeigeerstattung eine Kontenabfrage erfolgt ist. Diese wurde in der Regel zu einem Zeitpunkt veranlasst, zu dem noch keine Beschuldigtenvernehmung oder weitere Ermittlungen stattgefunden hatten. Eine solche routinemäßige Kontenabfrage ohne ausreichende Anhaltspunkte für die Erforderlichkeit entspricht nicht den gesetzlichen Voraussetzungen.

Auch im Berichtszeitraum habe ich mehrere Eingaben erhalten, die Kontenabfragen (gegenüber der Bundesanstalt für Finanzdienstleistungsaufsicht) und Kontenauskünfte (gegenüber den kontoführenden Banken) zum Gegenstand hatten.

In einem Fall wurde die Kontenabfrage zeitgleich mit der Beschuldigtenvernehmung angeordnet. Seitens der Staatsanwaltschaft wurde mir mitgeteilt, dass das Ergebnis der Beschuldigtenvernehmung nicht abgewartet worden sei, da aus einer Vielzahl anderer Verfahren gegen den Beschuldigten bekannt gewesen sei, dass sich dieser noch nie zur Sache geäußert habe und insofern zu erwarten gewesen sei, dass sich der Beschuldigte auch in diesem Verfahren nicht zur Sache äußern werde. Ich halte diese Ansicht für problematisch. Meines Erachtens kommt eine solche Argumentation nur in seltenen Einzelfällen in Betracht, wenn aufgrund stetig wiederholender Erfahrungen mit dem Betroffenen feststeht, dass die Beschuldigtenvernehmung keine neuen Erkenntnisse erbringen wird und insofern die Kontenabfrage zur Vorbereitung einer späteren Kontenauskunft notwenig ist.

In einem anderen Fall wurde mir bekannt, dass seitens der Staatsanwaltschaft von einer Bank Kontounterlagen eines Rechtsanwaltskontos angefordert und zur Akte genommen worden sind. Der Rechtsanwalt, bei dem es sich um den Anzei-

geerstatter handelte, hat diesen Maßnahmen nicht zugestimmt. Die Unterlagen enthielten Angaben über andere Mandatsverhältnisse des Rechtsanwaltes bzw. ließen hierauf Schlüsse zu. Die Anforderung von Anwaltskontounterlagen kommt nur in besonderen Situationen in Betracht, da es sich hierbei um besonders sensible Unterlagen handelt. Da im vorliegenden Verfahren noch andere Möglichkeiten zur Sachverhaltsermittlungen zur Verfügung standen, habe ich den Leitenden Oberstaatsanwalt aufgefordert, dafür Sorge zu tragen, dass in Zukunft bei der Erhebung von Kontounterlagen eines Rechtsanwalts sensibler vorgegangen wird.

5.4 Straf- und Maßregelvollzug

5.4.1 Brieföffnungen

Im Rahmen mehrerer Eingaben bin ich auf das Problem gestoßen, dass Briefe von Abgeordneten und von mir an Gefangene in bayerischen Justizvollzugsanstalten im Rahmen der Briefkontrolle geöffnet und den Gefangenen so übergeben wurden. In den jeweiligen Stellungnahmen wurde seitens der Justizvollzugsanstalten regelmäßig vorgetragen, dass die Umschläge nur aus Versehen und aufgrund der Menge der täglich zu überprüfenden Schreiben geöffnet worden seien, eine inhaltliche Kontrolle jedoch nicht stattgefunden habe.

Gem. Art. 32 Abs. 2 des Bayerischen Strafvollzugsgesetzes werden Schreiben von Abgeordneten des Bundestags und der Landtage sowie der Datenschutzbeauftragten des Bundes und der Länder nicht überwacht, sofern die Identität des Absenders zweifelsfrei feststeht. Diese rechtlichen Vorgaben sind unbedingt einzuhalten, da hierdurch wesentliche Grundrechte von Gefangenen geschützt werden. Insbesondere aus der Sicht der Gefangenen gibt es kaum einen Unterschied, ob eine Brieföffnung absichtlich oder irrtümlich erfolgte. Der Einwand, dass eine inhaltliche Überprüfung nicht stattgefunden habe, lässt sich insofern nicht überprüfen. Seitens der Justizvollzugsanstalten sind insofern unbedingt Maßnahmen zu ergreifen, die eine - auch nur irrtümliche - Öffnung geschützter Post ausschließt.

Art. 32 Abs. 2 BayStVollzG
Nicht überwacht werden ferner Schreiben der Gefangenen an Volksvertretungen des Bundes und der Länder sowie an deren Mitglieder, soweit die Schreiben an die Anschriften dieser Volksvertretungen gerichtet sind und den Absender zutreffend angeben. Entsprechendes gilt für Schreiben an das Europäische Parlament und dessen Mitglieder, den Europäischen Gerichtshof für Menschenrechte, den Europäischen Ausschuss zur Verhütung von Folter und unmenschlicher oder erniedrigender Behandlung oder Strafe und die Datenschutzbeauftragten des Bundes und der Länder. Schreiben der in den Sätzen 1 und 2 genannten Stellen, die an Gefangene gerichtet sind, werden nicht überwacht, sofern die Identität des Absenders zweifelsfrei feststeht.

Seitens des Staatsministeriums der Justiz und für Verbraucherschutz wurde mir mitgeteilt, dass man die Problematik im Rahmen einer Dienstbesprechung mit den Leiterinnen und Leitern der Justizvollzugsanstalten ausführlich erörtert habe, die Sache weiter im Auge behalten werde und dafür Sorge trage, dass der Beachtung der gesetzlichen Vorgaben die notwendige Aufmerksamkeit gewidmet werde.

5.4.2 Anwesenheit von Vollzugsbeamten bei der ärztlichen Untersuchung von Gefangenen in der Justizvollzugsanstalt

Im Rahmen einer Eingabe bin ich darauf aufmerksam gemacht worden, dass in einer bayerischen Justizvollzugsanstalt bei der Sprechstunde des Anstaltsarztes für weibliche Gefangene regelmäßig eine weibliche Bedienstete des allgemeinen Vollzugsdienstes anwesend war. Da die Justizvollzugsanstalt über keine weiblichen Sanitätsbediensteten verfügt, sah man die Anwesendheit einer weiblichen Vollzugsbeamtin als erforderlich an, um den Anstaltsarzt vor ungerechtfertigten Beschwerden und Anschuldigungen - insbesondere in Bezug auf sexuelle Übergriffe - zu schützen.

Ich habe gegen diese Vorgehensweise gegenüber der betroffenen Justizvollzugsanstalt und dem Staatsministerium der Justiz und für Verbraucherschutz datenschutzrechtliche Bedenken erhoben. Das besondere Vertrauensverhältnis zwischen Patient und Arzt, das auch durch die ärztliche Schweigepflicht geschützt wird, gilt auch im Strafvollzug. Eine Durchbrechung dieses Grundsatzes ist nur aufgrund enger gesetzlicher Ausnahmeregelungen möglich. Die regelmäßige Anwesenheit einer Bediensteten des allgemeinen Vollzugsdienstes bei Arztbesuchen ist aber gerade gesetzlich nicht vorgesehen.

Die betroffene Justizvollzugsanstalt hat mir daraufhin mitgeteilt, dass sie die bisherige Vorgehensweise abändern werde. Zukünftig werde eine Vertragsärztin die Versorgung der weiblichen Gefangenen übernehmen; der Anwesenheit einer Bediensteten des allgemeinen Vollzugsdienstes bei Arztbesuchen bedürfe es dann nicht mehr. Das Staatsministerium der Justiz und für Verbraucherschutz hat in einer - von mir angeregten - Umfrage unter den Leitern der bayerischen Justizvollzugsanstalten festgestellt, dass es sich bei der betroffenen Justizvollzugsanstalt um einen Einzelfall handle. Eine regelmäßige Anwesenheit von Bediensteten des allgemeinen Vollzugsdienstes zusätzlich zum medizinischen/pflegerischen Personal erfolge in den bayerischen Justizvollzugsanstalten nicht.

5.5 Ordnungswidrigkeitenverfahren

5.5.1 Videogestützte Geschwindigkeits - und Abstandsmessungen

Das Bundesverfassungsgericht hat mit Beschluss vom 11.08.2009 (Az. 2 BvR 941/08) festgestellt, dass eine videogestützte Verkehrskontrolle, bei der der gesamte Verkehr ohne konkreten Tatverdacht überwacht wird, unzulässig ist. Es liege insofern ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung vor, der einer gesetzlichen Grundlage bedürfe. Ein verwaltungsinterner Erlass genüge insofern nicht.

Vom Staatsministerium des Innern wurde mir dazu mitgeteilt, dass in Bayern ausschließlich Systeme zur Anwendung kämen, bei denen im Vorfeld lediglich Übersichtsaufnahmen angefertigt würden, die keine Erkennbarkeit von Kennzeichen oder Personen ermöglichen. Erst wenn aufgrund dieser Übersichtsaufnahmen ein konkreter Tatverdacht für die Begehung einer Verkehrsordnungswidrigkeit vorliege, werde eine weitere Kamera ausgelöst, die - zur Feststellung der Ordnungswidrigkeit - auch personenbezogene Daten erhebe. Es finde insofern lediglich eine verdachtsabhängige Aufzeichnung statt. Rechtsgrundlage für die An-

fertigung dieser Aufnahmen sei § 100 h Strafprozessordnung, der für das Ordnungswidrigkeitenverfahren gem. § 46 Ordnungswidrigkeitengesetz anwendbar sei. Danach dürfen auch ohne Wissen der Betroffenen außerhalb von Wohnungen Bildaufnahmen hergestellt werden, wenn die Erforschung des Sachverhalts auf andere Weise weniger Erfolg versprechend oder erschwert wäre.

Das Bundesverfassungsgericht hat mit Beschluss vom 05.07.2010 (2 BvR 759/10) bestätigt, dass § 100 h Abs. 1 Satz 1 Nr. 1 StPO als Rechtsgrundlage für die Anfertigung von Bildaufnahmen zum Beweis von Verkehrsverstoßen herangezogen werden könne. Die Erhebung personenbezogener Daten dürfe sich jedoch nur auf Fahrzeugführer richten, die selbst Anlass zur Anfertigung von Bildaufnahmen gegeben hätten, bei denen also der Verdacht eines bußgeldbewehrten Verkehrsverstosses bestehe.

Ich habe keine Anhaltspunkte dafür, dass in Bayern Systeme eingesetzt werden, die den Vorgaben des Bundesverfassungsgerichts nicht entsprechen.

5.5.2 Lichtbildabgleich in Bußgeldverfahren

Bereits in meinem 22. Tätigkeitsbericht, Nr. 6.5.1, habe ich darauf hingewiesen, dass mir eine Überprüfung der Voraussetzungen eines Lichtbildabgleichs im Ordnungswidrigkeitenverfahren nur möglich ist, wenn das Vorliegen der Voraussetzungen umfassend in den Akten dokumentiert ist. Ein allgemeiner Hinweis, wie z.B. "der Betroffene konnte nicht erreicht werden", genügt dieser Dokumentationspflicht nicht. Vielmehr muss sich aus der Dokumentation ergeben, dass ein "ernsthafter Kontaktversuch" unternommen worden ist. Dazu gehört m.E. neben der Angabe des Datums eines möglichen Kontaktversuches auch die Angabe der Uhrzeit, um - vor dem Hintergrund einer möglichen Berufstätigkeit des Betroffenen - bewerten zu können, ob der Kontaktversuch erfolgversprechend schien.

Ich habe insofern das Staatsministerium des Innern aufgefordert, darauf hinzuwirken, dass zukünftig auch die Uhrzeit eines möglichen Kontaktversuches dokumentiert wird. Das Staatsministerium hat meine Anregung aufgegriffen und mit Schreiben vom 04.06.2010 die nachgeordneten Behörden aufgefordert, neben dem Datum zukünftig auch die Uhrzeit zu dokumentieren.

Im Berichtszeitraum war ich mit mehreren Eingaben aus diesem Bereich befasst. Ich habe dabei in mehreren Fällen festgestellt, dass die Voraussetzungen für einen Lichtbildabgleich nicht vorlagen. So wurde in einem Fall etwa ein unterlassener Kontaktversuch damit begründet, dass die Dienststelle und der Wohnsitz des Betroffenen zu weit voneinander entfernt gewesen seien. Dieses Argument kann m.E. nicht berücksichtigt werden, da entweder ein telefonischer oder postalischer Kontaktversuch möglich gewesen wären.

Neben der Überprüfung von Einzelverfahren habe ich auch durch entsprechende Vortragstätigkeit auf die Einhaltung der datenschutzrechtlichen Bestimmung hingewirkt.

6 Kommunales

6.1 Videoüberwachung öffentlicher Orte und Einrichtungen durch Kommunen

Auch in diesem Berichtszeitraum habe ich immer wieder Anfragen von Gemeinden zur Zulässigkeit einer Videoüberwachung kommunaler Einrichtungen und öffentlicher Orte erhalten. In der Regel begründeten die Gemeinden die beabsichtigte Videoüberwachung damit, dass sie Straftaten, insbesondere Sachbeschädigungen von öffentlichem Eigentum, verhindern solle. So wollte z.B. eine Gemeinde einen Straßenabschnitt vor einem Freibad videoüberwachen, der Jugendlichen als Treffpunkt dient. Zur Begründung verwies die Gemeinde auf zerbrochene Flaschen und Müllablagerungen in diesem Bereich. Verunreinigungen und Sachbeschädigungen waren auch der Anlass für eine andere Kommune, eine Videoüberwachung des Eingangsbereichs einer öffentlichen Toilette ins Auge zu fassen. Ich habe dazu auf Folgendes hingewiesen:

Die Videoüberwachung ist in Art. 21 a BayDSG geregelt. Danach ist eine Videoüberwachung der in Absatz 1 dieser Vorschrift genannten Orte und Anlagen zu den dort genannten Zwecken zulässig, wenn dies im Rahmen der Erfüllung öffentlicher Aufgaben oder in Ausübung des Hausrechts erforderlich ist. Dabei dürfen keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen der Betroffenen beeinträchtigt werden.

In der Gesetzesbegründung wird ausdrücklich darauf hingewiesen, dass mit der Einführung des Art. 21 a BayDSG keine Ausweitung der Videoüberwachung durch bayerische öffentliche Stellen beabsichtigt ist und eine flächendeckende Videoüberwachung auch weiterhin unzulässig bleibt. Die Maßnahmen dürfen stets nur zum Schutz der genannten Rechtsgüter erfolgen. Es ist dabei in jedem Einzelfall zu prüfen, ob es überhaupt erforderlich ist, personenbezogene Daten zu erheben und ggf. zu speichern und ob es erforderlich ist, dies mittels Videotechnik zu tun. Erforderlich bedeutet, dass die Kenntnis der Daten zur Erreichung des Zwecks objektiv geeignet ist und im Verhältnis zu dem angestrebten Zweck auch angemessen erscheint.

Eine Videoüberwachung ist unzulässig, wenn weniger einschneidende Maßnahmen zum gleichen Ziel führen. Zu prüfen sind Anlass, der räumliche Überwachungsbereich, der Zeitraum der Überwachung und die Frage, welche Art der Videoüberwachung (Videobeobachtung, Videoaufzeichnung) zur Erreichung des Zwecks erforderlich ist. Soweit Mitarbeiter betroffen sind, sind die Beteiligungsrechte der Personalvertretung zu beachten.

Zur Frage, was unter "Erforderlichkeit" zu verstehen ist, hat das Bundesverfassungsgericht in einem Beschluss vom 23.02.2007 (1 BvR 2368/06) festgestellt, dass eine Videoüberwachung öffentlicher Orte und Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials einen erheblichen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellt, wenn überwiegend Personen erfasst werden, die in keiner Beziehung zu einem konkreten Fehlverhalten stehen und den Eingriff durch ihr Verhalten nicht veranlasst haben. Eine

Videoüberwachung öffentlicher Einrichtungen und Orte kann danach unter Beachtung der o.g. Grundsätze nur dann in Betracht kommen, wenn es sich um nachhaltige und schwerwiegende Beeinträchtigungen handelt.

Die Gemeinden hätten danach mit konkreten Angaben belegen müssen, dass der überwachte Bereich deutlich gefährlicher als der Rest des Gemeindegebietes oder vergleichbarer anderer Gemeinden ist.

Diese Voraussetzung lag in den oben beispielhaft genannten Fällen offenkundig nicht vor. Von einer Videoüberwachung wären hier überwiegend Personen betroffen gewesen, die sich völlig korrekt verhalten und keinerlei Anlass für eine Videoüberwachung geben. Zur Videoüberwachung öffentlicher Toilettenanlagen habe ich mich im Übrigen bereits in meinem 22. Tätigkeitsbericht, Nr. 8.8, geäußert.

Eine Arbeitsgruppe kommunaler Datenschutzbeauftragter größerer bayerischer Städte sowie eines Vertreters des Bayerischen Staatsministeriums des Innern hat ein Prüfungsschema zur Videoüberwachung und ein Muster einer allgemeinen Beschreibung der eingesetzten Videoaufzeichnungsanlage und der technisch-organisatorischen Maßnahmen nach Art. 21 a Abs. 6 i.V.m. Art. 7 und 8 BayDSG entwickelt. Die beiden Dokumente, an deren Ausarbeitung ich beteiligt war, habe ich auf meiner Homepage (www.datenschutz-bayern.de) veröffentlicht.

Zur weiteren Information verweise ich auf meine Beiträge Nr. 9.1 und 9.2 im 23. Tätigkeitsbericht.

6.2 Videoüberwachung eines Wahllokals

In einer Gemeinde war im Rahmen der Bezirks- und Landtagswahl 2008 ein Wahllokal in einer Bankfiliale eingerichtet worden. Auch am Wahltag waren die dort (in Banken üblicherweise) installierten Videokameras während der Abstimmungszeit in Betrieb. Ein Abschalten oder Verdecken der Kameras schied aus Sicherheitsgründen aus. Ein Bürger, der sich mit einer Eingabe an den Bayerischen Landtag gewandt hatte, sah darin eine Verletzung des Grundsatzes der geheimen Wahl. Bei der anschließenden Überprüfung wurde festgestellt, dass eine der Kameras von hinten in eine der Wahlkabinen gerichtet war und es nicht ausgeschlossen schien, dass bei einer entsprechenden Sitzposition oder durch die Handbewegung des Wählers beim Ankreuzen insbesondere des großen Stimmzettels eine direkte Beobachtung der Stimmabgabe oder zumindest ein Rückschluss darauf durch die Kamera möglich gewesen wäre. Nach Angaben der Bank sei das Bildmaterial der jeweils letzten 15 Minuten fortlaufend zwischengespeichert worden, eine Einsichtnahme oder Auswertung habe jedoch nicht stattgefunden.

Soweit auf Grund allgemein wahrnehmbarer Überwachungseinrichtungen eine unbeobachtete und unbefangene Stimmabgabe nicht uneingeschränkt sichergestellt werden kann, ist es jedenfalls nicht auszuschließen, dass sich Wähler bereits durch die Wahrnehmung solcher Überwachungsmöglichkeiten in ihrer freien Wahlentscheidung beeinflusst sehen können.

Gleichzeitig war mit der Videoüberwachung des Wahllokals eine unzulässige Erhebung und Speicherung personenbezogener Daten der von der Kamera erfassten und auf den Bildern identifizierbaren Personen verbunden. Soweit das

Gebrauchmachen vom Wahlrecht oder gar die Wahlentscheidung mittels Videoüberwachung festgehalten werden, liegt darin eine zusätzliche Beeinträchtigung schutzwürdiger Interessen der betroffenen Wähler. Die politische Meinung stellt zudem ein besonders sensibles personenbezogenes Datum im Sinne der EG-Datenschutzrichtlinie dar. Ein Bürger, der zur Wahl geht, muss keinesfalls damit rechnen, dass ein Wahllokal videoüberwacht wird. Eine solche Maßnahme stellt einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Personen dar.

Das Bayerische Staatsministerium des Inneren hat in der Folge auch in der Wahlanweisung für die Bundestagswahl 2009 darauf hingewiesen, dass Räume mit Videoüberwachung als Wahlräume nicht in Betracht kommen. Diese Klarstellung begrüße ich.

6.3 Anfertigen von Fotografien der Gäste einer Erlebnistherme

Gäste einer Erlebnistherme haben sich bei mir darüber beschwert, sie seien beim Betreten des Bades fotografiert worden. Ich bin der Eingabe nachgegangen und habe im Rahmen der Prüfung festgestellt:

Badegäste konnten die Therme nur mit einer Münze, einem sog. Chip-Coin benutzen. Dieser war mit einer Nummer versehen und ermöglichte dem Badegast den Zutritt zum Bad.

Bei Betreten des Bades am Drehkreuz sowie beim Zugang zur Sauna wurde mit Hilfe einer Videokamera ein Foto von jedem Badegast im Sinne einer Momentaufnahme erstellt. Dem jeweiligen Foto wurde die entsprechende Chip-Coin-Nummer zugeordnet.

Beim Verlassen der Therme musste das Drehkreuz mit einem entwerteten Chip-Coin bestückt werden. Der Badegast entwertete seinen Chip-Coin, indem er die in Anspruch genommenen Leistungen am Automaten oder an der Kasse bezahlte. Das Foto des Badegastes wurde im Anschluss daran im System automatisch gelöscht, wenn eine bestimmte Anzahl von Drehkreuzbewegungen erreicht wurde; die Speicherdauer lag je nach Besuchsandrang bei ca. zwei bis drei Tagen.

Verließ ein Badegast die Therme, ohne das Drehkreuz mit einem entwerteten Chip-Coin zu bestücken, wurde dieser Vorfall am Ende des Tages bei der Abrechnung festgestellt. Mit Hilfe des Software-Systems konnten dann die Fotos derjenigen Personen ausgedruckt werden, deren Chip-Coin nicht entwertet wurde.

Nach Auskunft der Therme diente das Anfertigen der Fotos dazu, bei Nichtbezahlung oder anderer Streitigkeiten den Coin einer Person zuordnen zu können. Beispielsweise wurde das Foto nach Aussage der Therme der Polizei vorgelegt, wenn dort ein Strafantrag gestellt wurde, weil sich ein Badegast unerlaubt aus dem Bad entfernt und seine Leistungen nicht beglichen hat.

Die Therme teilte außerdem mit, die Badegäste würden in der Haus- und Badeordnung, die im Eingangsbereich sowie an der Kasse ausgehängt sei, über das Chip-Coin-System informiert.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Das Anfertigen von Fotografien der Badegäste war eine Erhebung personenbezogener Daten. Die Speicherung der Fotografien und die Verwendung der Fotografien der Personen, die ihren Chip-Coin nicht entwertet hatten, war eine Verarbeitung und Nutzung personenbezogener Daten. Nach Art. 15 Abs. 1 BayDSG ist die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Wie es sich aus dem Folgenden ergibt, erfolgte die Anfertigung, Speicherung und Nutzung der Fotografien weder auf einer Rechtsgrundlage noch lag eine wirksame Einwilligung der Betroffenen vor.

Da die Gäste beim Betreten des Bades und dem Zugang zur Sauna mit Hilfe einer Videokamera fotografiert wurden, war als Rechtsgrundlage für die Datenerhebung und -speicherung zunächst Art. 21 a BayDSG, der die Videoüberwachung regelt, in Betracht zu ziehen. Ich habe allerdings bereits Zweifel, ob das Anfertigen eines Fotos (Momentaufnahme) als ein Fall der Videobeobachtung und der Videoaufzeichnung (Erfassen und Festhalten eines Geschehnisses in einem Bewegungsablauf) angesehen werden kann. Aber auch wenn man diese Frage bejaht, war Art. 21 a BayDSG nicht anwendbar, weil mit dem Chip-Coin-System (nur) das Vermögen der Therme, nicht aber in Art. 21 a Abs. 1 Nr. 1 und 2 BayDSG genannte Rechtsgüter geschützt werden sollten. Die Videoüberwachung nach Art. 21 a BayDSG dient dem Schutz der in dieser Vorschrift bezeichnenden Rechtsgüter, ist jedoch keine zulässige Maßnahme im allgemeinen Verwaltungsvollzug bzw. Betriebsablauf.

Darüber hinaus wurden durch die Maßnahme überwiegende schutzwürdige Interessen der Badegäste, die sich vertragstreu verhalten und ihre in Anspruch genommenen Leistungen bezahlen, beeinträchtigt (Art. 21 a Abs. 1 Satz 2 BayDSG).

Im Hinblick auf die Entscheidung des Bundesverfassungsgerichts vom 23.02.2007 - 1 BvR 2368/06 - (städtische Videoüberwachung eines Kunstwerks in Regensburg) konnte das Fotografieren der Badegäste auch nicht auf Art. 16 Abs. 1 und Art. 17 Abs. 1 BayDSG gestützt werden. Von den Personen, die die Therme nutzen, bezahlt nur eine verschwindend geringe Minderheit die in Anspruch genommenen Leistungen nicht. Es wurden daher ganz überwiegend Personen fotografiert, die keinen Anlass für diese Maßnahme gegeben haben. Angesichts des erheblichen Gewichts der Grundrechtsbeeinträchtigung dieser Personen konnte die Aufnahme und das Speichern von Bildern nicht auf die allgemeinen Vorschriften über die Datenerhebung und -speicherung des Bayerischen Datenschutzgesetzes gestützt werden.

Die Datenerhebung und -speicherung erfolgte auch nicht mit Einwilligung der Betroffenen (Art. 15 Abs. 1 Nr. 2 BayDSG). Zwar wurde nach Mitteilung der Therme in der Haus- und Badeordnung, die im Eingangsbereich sowie an der Kasse aushängt, über das Chip-Coin-System informiert. Der bloße Aushang einer Haus- und Badeordnung erfüllt jedoch nicht die Voraussetzung eines Hinweises nach Art. 15 Abs. 2 BayDSG. Die Gäste rechnen auch regelmäßig weder mit derart außergewöhnlichen Kontrollverfahren, noch dass darüber lediglich in einer allgemeinen Hausordnung informiert wird.

Darüber hinaus käme eine (konkludente) Einwilligung durch den Erwerb des Chip-Coins und die Nutzung der Therme als Ausnahme vom grundsätzlichen Er-

fordernis der Schriftform auch deswegen nicht in Betracht, weil es an der Freiwilligkeit der Einwilligung fehlen würde. Die Teilnahme an dem Chip-Coin-System war zwingend. Die Personen, die die Therme benutzen wollten, hatten keine Alternative.

Im Ergebnis war daher weder eine Rechtsgrundlage für die mit der Anfertigung der Fotografien verbundenen Eingriffe in das Persönlichkeitsrecht der betroffenen Badegäste vorhanden noch lag eine wirksame Einwilligung der Betroffenen in das Verfahren vor. Ich habe deshalb die Therme aufgefordert, das Anfertigen von Fotografien der Badegäste zu unterlassen und noch gespeicherte Fotografien unverzüglich zu löschen.

6.4 Information der Presse über kommunale Angelegenheiten

Bürger, die sich gegen ein Verfahren nach dem Flurbereinigungsgesetz ausgesprochen hatten, fanden sich plötzlich in der örtlichen Presseberichterstattung wieder. Die Gemeinde hatte eine entsprechende Unterschriftenliste weitergegeben. Ich habe diesen Vorfall zum Anlass genommen, erneut darauf hinzuweisen, dass die Gemeinden bei der Unterrichtung der Presse über kommunale Angelegenheiten den Datenschutz nicht außer Acht lassen dürfen.

Die Kommunen haben in jedem Fall zu prüfen, welche Informationen sie im Hinblick auf schutzwürdige Belange von Betroffenen und unter Rücksichtnahme auf das Wohl der Allgemeinheit der Presse geben dürfen. Sollen personenbezogene Daten übermittelt werden, hat die Gemeinde das aus Art. 1 Abs. 1 und Art. 2 Abs. 1 Grundgesetz abgeleitete Recht der Betroffenen auf informationelle Selbstbestimmung zu beachten. Die Weitergabe personenbezogener Daten an die Presse ist eine Datenübermittlung an nicht-öffentliche Stellen, die ohne Einwilligung der Betroffenen nach Art. 19 Abs. 1 Nr. 2 Bayerisches Datenschutzgesetz nur zulässig ist, wenn die Presse ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht, bzw. ein solches Interesse offenkundig ist, und dadurch schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Will eine Gemeinde danach z.B. die Presse durch Übermittlung von Sitzungsvorlagen über Tagesordnungspunkte unterrichten, die in öffentlicher Gemeinderatssitzung behandelt werden, dann muss sie diese Sitzungsvorlagen durch Kürzen, Schwärzen etc. so abändern, dass sie nur noch Informationen enthalten, die ohne Bedenken der Öffentlichkeit zugänglich gemacht werden dürfen.

Im vorliegenden Fall wäre es danach zulässig gewesen, wenn die Gemeinde die Presse über die Tatsache, dass sich Bürger gegen ein Flurbereinigungsverfahren in der Kommune gewandt hatten, informiert hätte. Auch die Anzahl der geleisteten Unterschriften hätte mitgeteilt werden dürfen. Die Weiterleitung der Unterschriftenlisten selbst war jedoch ein grober Datenschutzverstoß, den ich beanstandet habe.

6.5 Veröffentlichung von Karten und Luftbildern zum Solarpotential auf Gebäuden durch Kommunen im Internet

Eine Kommune hatte in der örtlichen Presse mitgeteilt, sie beabsichtige, Luftbilder der Anwesen ihrer Bürger im Internet zu veröffentlichen. Gebe der Bürger seine Adresse ein, dann könne er ein Luftbild seines Anwesens sehen und erhal-

te Informationen zur solartechnischen Nutzung seines Gebäudes geliefert. Auf Beschwerden von Bürgern hin habe ich den Vorgang überprüft und dabei folgenden Sachverhalt festgestellt:

Aus den Internetseiten der Gemeinde konnte zur Ermittlung der Eignung von Gebäuden zur Solarstromerzeugung ein Straßenname gewählt werden. Anschließend wurden alle vorhandenen Hausnummern zur Auswahl angeboten. Für eine gewählte Hausnummer erhielt man dann die "Eignungsfläche in m^2", den zu erwartenden "Stromertrag in kWh pro Jahr" und den Eignungsgrad.

Alternativ zur direkten Adressselektion konnte auch "per Maus" in einem digitalen Stadtplan oder in einem Satellitenbild gesucht werden. Die Auflösung des Satellitenbildes war relativ hoch, so dass beispielsweise parkende Autos gut zu erkennen waren. Im Bild ließ sich mit der Maus ein Rechteck selektieren, für das dann alle Häuser innerhalb dieser Fläche mit Adresse und Eignungsdaten angezeigt wurden.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die o.g. Eignungsdaten können über den Straßennamen und die Hausnummer in vielen Fällen aufgrund persönlicher Kenntnis, z.B. als Nachbar, oder unter Hinzuziehung von Telefonbüchern etc. den Grundstückseigentümern sowie den Bewohnern zugeordnet werden. Es handelt sich in diesen Fällen, soweit sich die Eignungsdaten auf natürliche Personen beziehen, um personenbezogene Daten im Sinn des i.S.d. Art. 4 Abs. 1 des Bayerischen Datenschutzgesetzes - BayDSG - (sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen). In diesem Zusammenhang verweise ich auch auf einen Beschluss der Obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich (sog. Düsseldorfer Kreis) vom 13./14.11.2008.

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich am 13./14.11.2008
Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet

Bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, handelt es sich in der Regel um personenbezogene Daten, deren Erhebung und Verarbeitung nach dem Bundesdatenschutzgesetz zu beurteilen ist. Die Erhebung, Speicherung und Bereitstellung zum Abruf ist nur zulässig, wenn nicht schutzwürdige Interessen der Betroffenen überwiegen. Bei der Beurteilung schutzwürdiger Interessen ist von Bedeutung, für welche Zwecke die Bilddaten verwendet werden können und an wen diese übermittelt bzw. wie diese veröffentlicht werden. Die obersten Aufsichtsbehörden sind sich einig, dass die Veröffentlichung von georeferenziert und systematisch bereit gestellten Bilddaten unzulässig ist, wenn hierauf Gesichter, Kraftfahrzeugkennzeichen oder Hausnummern erkennbar sind. Den betroffenen Bewohnern und Grundstückeigentümern ist zudem die Möglichkeit einzuräumen, der Veröffentlichung der sie betreffenden Bilder zu widersprechen und dadurch die Bereitstellung der Klarbilder zu unterbinden. Keine schutzwürdigen Interessen bestehen, wenn die Darstellung der Gebäude und Grundstücke so verschleiert bzw. abstrakt erfolgt, dass keine individuellen Eigenschaften mehr erkennbar sind. Um die Möglichkeit zum Widerspruch schon vor der Erhebung zu eröffnen, sollte die geplante Datenerhebung mit einem Hinweis

auf die Widerspruchsmöglichkeit rechtzeitig vorher bekannt gegeben werden. Die Widerspruchsmöglichkeit muss selbstverständlich auch noch nach der Veröffentlichung bestehen.

Danach handelt es sich bei digital erfassten Fotos von Gebäude- und Grundstücksansichten, die über Geokoordinaten eindeutig lokalisiert und damit einer Gebäudeadresse und dem Gebäudeeigentümer sowie den Bewohnern zugeordnet werden können, in der Regel um personenbezogene Daten.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat. Als besondere Rechtsvorschrift über den Datenschutz kommt hier Art. 8 Abs. 1 des Bayerischen Umweltinformationsgesetzes (BayUIG) in Betracht.

Das Umweltinformationsgesetz schafft den rechtlichen Rahmen für den freien Zugang zu Umweltinformationen. Nach meinem Dafürhalten handelt es sich bei der Veröffentlichung von Eignungsdaten zur Solarnutzung um Maßnahmen im Sinn des Art. 2 Abs. 2 Nr. 3 BayUIG. Nach dem BayUIG haben die informationspflichtigen Stellen den Informationszugang u.a. durch die Einrichtung öffentlich zugänglicher Informationsnetze und Datenbanken zu erleichtern.

Der Schutz privater Belange wird durch Art. 8 BayUIG gewährleistet. Nach Art. 8 Abs. 1 Satz 1 Nr. 1 BayUIG ist ein Antrag auf Zugang zu Umweltinformationen abzulehnen, soweit durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Anderes gilt, wenn die Betroffenen zugestimmt haben oder das öffentliche Interesse an der Bekanntgabe überwiegt. Diese Vorschrift findet m.E. nicht nur Anwendung, wenn ein Antrag auf Zugang zu Umweltinformationen gestellt wird, sondern auch, wenn eine Behörde personenbezogene Umweltinformationen in das Internet einstellen will.

Art. 8 Abs. 1 Nr. 1 BayUIG
Soweit

1. *durch das Bekanntgeben der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden,*
2. *Rechte am geistigen Eigentum, insbesondere Urheberrechte, durch das Zugänglichmachen von Umweltinformationen verletzt würden oder*
3. *durch das Bekanntgeben Betriebs- oder Geschäftsgeheimnisse zugänglich gemacht würden oder die Informationen dem Steuergeheimnis oder dem Statistikgeheimnis unterliegen,*

ist der Antrag abzulehnen, es sei denn, die Betroffenen haben zugestimmt oder das öffentliche Interesse an der Bekanntgabe überwiegt. Der Zugang zu Umweltinformationen über Emissionen kann nicht unter Berufung auf die in Nrn. 1 und 3 genannten Gründe abgelehnt werden. Vor der Entscheidung über die Offenbarung der durch Satz 1 Nrn. 1 bis 3 geschützten Informationen sind die Betroffenen anzuhören. Die informationspflichtige Stelle hat in der Regel von einer Betroffenheit im Sinn des Satzes 1 Nr. 3 auszugehen, soweit übermittelte Informationen als Betriebs- und Geschäftsgeheimnisse gekennzeichnet sind. Soweit die informationspflichtige Stelle dies verlangt, haben mögliche Betroffene im Einzelnen darzulegen, dass ein Betriebs- oder Geschäftsgeheimnis vorliegt.

Die betroffenen Grundstückseigentümer haben im vorliegenden Fall ein überwiegendes schutzwürdiges Interesse daran, dass die genannten Daten zur Solareignung ihres Gebäudes nicht ohne ihre Einwilligung im Internet weltweit veröffentlicht werden und sie u.a. von personenbezogener "maßgeschneiderter" Werbung für Hausdach-Solarmodule verschont bleiben. Demgegenüber besteht kein überwiegendes Interesse der Allgemeinheit an einer personenbezogenen Veröffentlichung dieser Daten. Hinzu kommt, dass nach Art. 8 Abs. 1 Satz 3 BayUIG die Betroffenen vor einer Entscheidung über die Offenbarung anzuhören sind.

Im Ergebnis sehe ich danach aus datenschutzrechtlicher Sicht folgende Möglichkeiten, die betroffenen Grundstückseigentümer auf das Solarenergiepotential der Dachflächen ihres Gebäudes aufmerksam zu machen:

- Veröffentlichung der Daten im Internet mit informierter Einwilligung der Betroffenen;
- Nur der jeweilige Grundstückseigentümer erhält mittels individuellem Login/Passwort Zugang zu seinen Daten. Diese Alternative erscheint nicht praktikabel, da es weniger Aufwand wäre, gleich die Ergebnisse (Fläche, Ertrag und Eignung) anstelle von Login/Passwort mitzuteilen;
- Die Gemeinde behält die Eignungsdaten in ihrer Verwaltung und teilt sie nur dem jeweils Betroffenen auf dessen Anfrage hin mit. Auf diese Möglichkeit könnte z.B. im Amtsblatt oder in der örtlichen Tageszeitung hingewiesen werden.

6.6 Bekanntgabe personenbezogener Daten der Einwender im Zusammenhang mit der Aufstellung eines Bebauungsplans

Ein Bürger hat sich bei mir darüber beschwert, dass seine Einwendungen in einem Bebauungsplanverfahren von der Gemeinde personenbezogen an alle anderen Einwender übermittelt wurden. Die Überprüfung der Angelegenheit hat folgenden Sachverhalt ergeben: Die Niederschrift über die in öffentlicher Gemeinderatssitzung behandelten Einwendungen enthält neben den Namen und Vornamen sowie dem Wohnort der Bürger, die sich an dem Verfahren beteiligt haben, ihre Einwendungen, die Stellungnahme der Verwaltung zu dem jeweiligen Vorbringen im Einzelnen und in einer Zusammenfassung die Abstimmung darüber im Gemeinderat. Zu den Sammeleinwendungen wurde der Sitzungsniederschrift eine Namensliste der Einwender beigefügt. Die Gemeinde hat die Sitzungsniederschrift zu diesem Tagesordnungspunkt mit der Namensliste im Folgenden an alle Einwender versandt. Ich habe diesen Sachverhalt wie folgt bewertet:

Die Übersendung der Niederschrift der Gemeinderatssitzung zu dem Tagesordnungspunkt, unter dem die Einwendungen im Bebauungsplanverfahren behandelt wurden, und der Namensliste an die Personen, die im Verfahren nach § 3 Abs. 2 Satz 1 Baugesetzbuch (BauGB) Einwendungen erhoben haben, stellte eine Übermittlung personenbezogener Daten an Dritte dar. Mangels einer Einwilligung der Betroffenen war die Datenübermittlung nur auf der Grundlage einer Rechtsvorschrift zulässig. Dabei gehen besondere Rechtsvorschriften über den Datenschutz den allgemeinen Vorschriften des Bayerischen Datenschutzgesetzes vor. Das Baugesetzbuch enthält solche Regelungen.

Das Verfahren zur Aufstellung der Bauleitpläne ist in den §§ 2 ff. BauGB geregelt. Nach § 3 Abs. 2 Satz 4 BauGB sind die im Rahmen der Beteiligung der Öffentlichkeit fristgemäß abgegebenen Stellungnahmen zu prüfen; das Ergebnis ist mitzuteilen. Nach dem Zweck der Regelung des § 3 Abs. 2 Satz 4 Halbsatz 2 BauGB sollen die Betroffenen darüber unterrichtet werden, ob und wie sich die Gemeinde mit ihren Stellungnahmen auseinandergesetzt hat (Ernst/Zinkahn/Bielenberg/Krautzberger, Baugesetzbuch Band I, Stand: 01.02.2008, § 3 Rdnr. 66). Battis/Krautzberger/Löhr, Baugesetzbuch, Zehnte Auflage 2007, weisen in ihrer Kommentierung zu § 3 in Rdnr. 19 daher zu Recht darauf hin, dass das Ergebnis der Prüfung **dem jeweiligen Betroffenen** mitzuteilen ist. In diesem Zusammenhang weise ich auch darauf hin, dass schon bei der öffentlichen Auslegung nach § 3 Abs. 2 Satz 1 BauGB darauf zu achten ist, dass keine Unterlagen mit personenbezogenen Daten ausgelegt werden (Battis/Krautzberger/Löhr, a.a.O., Rdnr. 5 unter Hinweis auf BVerfGE 77, 121).

Die Übermittlung der Einwendungen und ihrer Behandlung im Gemeinderat jeweils unter Nennung von Namen und Wohnort der betroffenen Einwender an **alle anderen Einwender** war somit von § 3 Abs. 2 Satz 4 Halbsatz 2 BauGB nicht gedeckt und stellte eine unzulässige Datenübermittlung an die jeweils anderen Einwender dar. Dem steht auch nicht entgegen, dass die Einwendungen nach Art. 52 Abs. 2 der Gemeindeordnung grundsätzlich in öffentlicher Sitzung behandelt werden. Diese Vorschrift regelt einen anderen Sachverhalt. Die Betroffenen müssen es danach zur Gewährleistung der Transparenz der gemeindlichen Verwaltungstätigkeit zwar grundsätzlich hinnehmen, dass ihre Einwendungen in öffentlicher Gemeinderatssitzung behandelt werden und zur Feststellung ihrer Betroffenheit ggf. auch ihr Name und ihre Anschrift genannt werden. Allerdings können auch hier berechtigte Ansprüche im Einzelfall eine Behandlung in nichtöffentlicher Sitzung erforderlich machen (Battis/Krautzberger/Löhr, a.a.O., Rdnr. 5). Die Betroffenen müssen es jedoch nicht hinnehmen, dass darüber hinausgehend ihre Einwendungen personenbezogen im Wortlaut, mit der Stellungnahme der Verwaltung dazu und dem Abstimmungsergebnis jedem anderen Einwender schriftlich zugesandt werden. Auch die zusätzliche Übersendung einer Namensliste von Einwendern an jeden einzelnen Einwender war danach unzulässig.

Die Übersendung der Niederschrift der Gemeinderatssitzung zu dem o.b. Tagesordnungspunkt und der Namensliste an die Einwender in dem Verfahren nach § 3 Abs. 2 BauGB zur Aufstellung des Bebauungsplans habe ich nach Art. 31 Abs. 1 BayDSG beanstandet.

6.7 Nennung des Eingabeführers bei der Einholung einer Stellungnahme

Ein durch Lärm- und Geruchsimmissionen einer benachbarten Firma beeinträchtigter Anwohner hatte mehrmals vergeblich durch direkte Beschwerden bei der fraglichen Firma versucht, Abhilfe zu erreichen. Schließlich wandte er sich schriftlich mit seinen Beschwerden an das für den Immissionsschutz zuständige Landratsamt. Das Landratsamt hat die Firma daraufhin zur Stellungnahme aufgefordert und dieser hierbei das Schreiben des Anwohners in nicht-anonymisierter Form zugeleitet. Hierüber wiederum hat sich der Betroffene bei mir beschwert.

Das von mir um Stellungnahme gebetene Landratsamt hielt die Weiterleitung der nicht-anonymisierten Beschwerde an die betreffende Firma für zulässig, da dies

der Aufklärung des Beschwerdefalles gedient habe. Überdies sei der Petent wegen seiner vorherigen direkten Beschwerden der Firma sowieso namentlich bekannt gewesen.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die Weiterleitung der Beschwerde des Petenten ohne deren vorherige Anonymisierung an die betreffende Firma war eine Übermittlung personenbezogener Daten an Dritte. Die Übermittlung personenbezogener Daten an Dritte ist datenschutzrechtlich eine Datenverarbeitung (Art 4 Abs. 6 Satz 1 BayDSG). Die Verarbeitung personenbezogener Daten ist nach Art. 15 Abs. 1 Nrn. 1 und 2 BayDSG nur zulässig, wenn das bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Eine Einwilligung des Petenten in die Weitergabe seines Schreibens an die Firma lag nicht vor. Mangels einer bereichsspezifischer Rechtsgrundlage war für die Beurteilung der Datenübermittlung damit Art. 19 Abs. 1 BayDSG maßgebend.

Nach Art. 19 Abs. 1 Nr. 1 BayDSG ist die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach Art. 17 Abs. 1 Nr. 2, Abs. 2 bis 4 BayDSG zulassen würden. Im vorliegenden Fall war es zur Prüfung und Beantwortung der Eingabe des Petenten schon **nicht erforderlich**, der Firma dessen personenbezogene Daten zu übermitteln. Es hätte genügt, der Firma die genannten Beschwerdepunkte mitzuteilen. Diese waren allgemeiner Natur und nicht an eine bestimmte Person gebunden. Auch ist nicht ersichtlich, inwiefern durch die ungefilterte Weiterleitung eine schnellere Aufklärung erreicht werden konnte. Die Datenübermittlung war daher nicht nach Art. 19 Abs. 1 Nr. 1 BayDSG zulässig.

Auch Art. 19 Abs. 1 Nr. 2 BayDSG bot keine ausreichende Rechtsgrundlage. Danach ist eine Datenübermittlung an nicht-öffentliche Stellen zulässig, wenn die nicht-öffentliche Stelle ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Ein **berechtigtes Interesse** der Firma an der Kenntnis, wer sich über Lärm- und Geruchsbelästigungen beschwert hat, bestand **nicht**. Außerdem hatte der Petent ein **schutzwürdiges Interesse**, dass ihm durch eine Eingabe beim Landratsamt keine Nachteile entstehen. Ein Bürger muss grundsätzlich darauf vertrauen können, dass mit seinem Anliegen nur die zuständigen Stellen befasst werden, ein Schreiben an das zuständige Amt also im internen Verhältnis zwischen Bürger und Verwaltung verbleibt und jedenfalls nicht ohne besondere Rechtsgrundlage Dritten zugänglich gemacht wird. Dies gilt unabhängig davon, ob der Informant ausdrücklich um vertrauliche Behandlung gebeten hat. Dies ist letztlich auch im Behördeninteresse, da diese zur ordnungsgemäßen Erfüllung ihrer Aufgaben auf derartige Informationen angewiesen sind.

Da mir das Landratsamt versichert hat, künftig in ähnlichen Fällen auf eine Anonymisierung zu achten bzw. eine schriftliche Einwilligung des Beschwerdeführers einzuholen, habe ich im Rahmen des mir nach Art. 31 Abs. 3 BayDSG zustehenden Ermessens von einer förmlichen Beanstandung des Datenschutzverstoßes abgesehen.

6.8 Veröffentlichung personenbezogener Daten im amtlichen Mitteilungsblatt zur Benachrichtigung von Bürgern

Durch Eingaben und die Presse wurde mir bekannt, dass einige Gemeinden Bürger, für die ein neues Ausweisdokument ausgestellt wurde, im amtlichen Mitteilungsblatt darüber informierten, dass sie das Dokument abholen können. Die Einwilligung der Betroffenen in die Veröffentlichung ihrer Namen erfolgte in der Regel mündlich. Personen, die einer Veröffentlichung nicht zustimmten, wurden telefonisch verständigt.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

Die Veröffentlichung der Namen von Bürgern im amtlichen Mitteilungsblatt verbunden mit dem Hinweis, sie können ihr beantragtes Ausweisdokument abholen, stellt eine Datenübermittlung an die Allgemeinheit dar. Eine solche Datenübermittlung ist nach Art. 15 Abs. 1 Nrn. 1 und 2 BayDSG nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift sie erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Da im vorliegenden Fall eine Rechtsgrundlage nicht vorlag, kam nur eine Einwilligungslösung in Betracht. Die Einwilligung bedarf der Schriftform, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist (Art. 15 Abs. 3 Satz 1 BayDSG). Solche Umstände waren hier nicht ersichtlich, da es beispielsweise ohne weiteres möglich wäre, eine vorformulierte Einwilligungserklärung durch den Antragsteller unterzeichnen zu lassen. Weiterhin muss es sich um eine informierte Einwilligung des Betroffenen handeln, d.h. diese muss alle wesentlichen Informationen beinhalten, die der Antragsteller benötigt, um die Tragweite seiner Entscheidung beurteilen zu können. Wenn das Formular neben der Einwilligung noch andere Erklärungen des Betroffenen enthält, ist diese deutlich hervorzuheben (Art. 15 Abs. 4 BayDSG). Auf das Schriftformerfordernis konnte vorliegend nicht verzichtet werden. Aus Gründen der Nachweisbarkeit dürfte es auch im Interesse der Gemeinde liegen.

Unabhängig davon möchte ich auf die Gefahr missbräuchlicher Nutzung hinweisen. Gerade bei Reisepässen könnten beispielsweise Einbrecher ein Interesse daran haben, zu wissen, wer möglicherweise bald in Urlaub fährt.

Selbst wenn unter Einhaltung der genannten Voraussetzungen eine Benachrichtigung in den amtlichen Bekanntmachungen aus datenschutzrechtlicher Sicht zulässig wäre, halte ich sie aus den dargelegten Erwägungen dennoch nicht für empfehlenswert. Eine telefonische oder schriftliche Benachrichtigung (z.B. per E-Mail) wäre meines Erachtens vorzuziehen. Alternativ dazu könnte die Gefahr missbräuchlicher Nutzung begrenzt werden, indem die Benachrichtigung nicht mit dem Namen des Passinhabers, sondern mit einem Kennwort erfolgt. Dieses Kennwort könnte jeder Passinhaber bei der Antragstellung bestimmen.

6.9 Herausgabe eines Schreibens mit strafbarem Inhalt an den betroffenen Amtsträger

Durch eine Eingabe bin ich mit folgendem Vorgang befasst worden:

In einer Gemeinde hat die vom Gemeinderat beschlossene Ausdehnung des Anschluss- und Benutzungszwangs an die gemeindliche Wasserversorgung und

-entsorgung auf diesem Zwang bislang nicht unterliegende Anwesen zu erheblichen Meinungsverschiedenheiten zwischen einem Teil der hiervon Betroffenen und der Gemeinde geführt. Im Rahmen dieser Meinungsverschiedenheiten hat sich eine Bürgerin mit einer schriftlichen Eingabe an übergeordnete Behörden gewandt. In dieser Petition wurde dem ersten Bürgermeister der betroffenen Gemeinde u.a. Bestechlichkeit vorgeworfen und dieser zugleich als "Napoleon" und "Möchtegern-Diktator" bezeichnet. Auf Verlangen des ersten Bürgermeisters, der von der Existenz des Schreibens erfahren hatte, wurde ihm dieses behördlicherseits aufgrund des strafbaren Inhalts unter Berufung auf § 17 Abs. 1 Satz 3 der Allgemeinen Geschäftsordnung für die Behörden des Freistaats Bayern (AGO) herausgegeben. Nach dieser Bestimmung bleiben die Abgabe von Schreiben mit groben Beschimpfungen oder Beleidigungen u.a. von Behördenangehörigen an andere Behörden und die Möglichkeit strafrechtlicher Verfolgung unberührt. Der Bürgermeister hat daraufhin Strafanzeige wegen Beleidigung gestellt. Die betroffene Bürgerin wiederum hat sich an mich gewandt und das Vorliegen eines Datenschutzverstoßes gerügt.

Der Sachverhalt gibt Anlass, aus datenschutzrechtlicher Sicht auf Folgendes hinzuweisen: Die Herausgabe des Schreibens durch die übergeordnete Behörde an den in amtlicher Eigenschaft betroffenen Bürgermeister erfolgte, um diesem eine Strafverfolgung zu ermöglichen (Beleidigung nach § 185 StGB ist gem. § 194 Abs. 1 Satz 2 StGB ein Antragsdelikt) und damit das beschädigte Ansehen des Bürgermeisteramtes wiederherzustellen. Es lag damit eine Datenübermittlung an eine öffentliche Stelle vor, welche im konkreten Fall mit Art. 18 Abs. 1 i.V.m. Art. 17 Abs. 2 Nr. 10 BayDSG vereinbar war. Danach ist eine Übermittlung personenbezogener Daten an andere öffentliche Stellen zulässig, wenn dies u.a. zur Verfolgung von Straftaten erforderlich ist. In der Herausgabe des Schreibens mit strafbarem Inhalt an den betroffenen Amtsträger lag damit kein Verstoß gegen den Datenschutz.

§ 17 Abs. 1 AGO
Enthält ein Eingang grobe Beschimpfungen oder Beleidigungen von Behörden, Behördenangehörigen oder Dritten und ist er nicht an eine Frist gebunden, wird dem Absender mitgeteilt, dass der Eingang wegen der ungehörigen Form nicht bearbeitet wird. Die Mitteilung kann unterbleiben, wenn kein bestimmter Antrag gestellt ist. Die Abgabe an andere Behörden und die Möglichkeit strafrechtlicher Verfolgung bleiben unberührt.

6.10 Auskunftserteilung über Behördeninformanten

Eine Bürgerin hat sich bei mir darüber beschwert, dass einer Hundehalterin seitens der Verwaltungsgemeinschaft, der ihre Wohnortgemeinde angehört, Auskunft über den Namen und die Anschrift ihres 12-jährigen Sohnes erteilt worden war. Das Kind war zuvor von den nicht angeleinten Hunden dieser Hundehalterin bedrängt worden und hatte den Vorfall der Verwaltungsgemeinschaft gemeldet. Die Verwaltungsgemeinschaft hatte daraufhin die Hundehalterin auf die bestehende Anleinpflicht hingewiesen. Auf deren Frage nach dem Anzeigeerstatter gab ihr die Verwaltungsgemeinschaft Name und Anschrift des Kindes bekannt. Die Hundehalterin wiederum suchte das Kind in Abwesenheit der Eltern auf und griff es im Folgenden verbal an.

Die von mir zu der Auskunftserteilung befragte Verwaltungsgemeinschaft nahm anfänglich nur dahingehend Stellung, Name und Anschrift des Kindes seien der

Hundehalterin mitgeteilt worden, da bei Bußgeldverfahren grundsätzlich Zeugen zu benennen seien. Im weiteren Verlauf meiner Prüfung konkretisierte die Verwaltungsgemeinschaft dies und führte ergänzend aus, die Hundehalterin habe die Sachverhaltsschilderung des Kindes bestritten und zudem einen Rechtsanwalt beauftragt, welcher von der Verwaltungsgemeinschaft Akteneinsicht verlangte.

Die Vorgehensweise habe ich aus folgenden Gründen beanstandet:

Teilt die Behörde den Namen und die Anschrift des Anzeigeerstatters mit, so stellt dies eine Übermittlung personenbezogener Daten an Dritte und damit eine Datenverarbeitung dar. Nach Art. 15 Abs. 1 BayDSG ist eine solche Verarbeitung personenbezogener Daten nur zulässig, wenn das Bayerische Datenschutzgesetz oder eine andere Rechtsvorschrift diese erlaubt oder anordnet (Nr. 1) oder der Betroffene eingewilligt hat (Nr. 2). Mangels Einwilligung des Betroffenen bzw. seiner Erziehungsberechtigten in die Datenverarbeitung kam es insoweit darauf an, ob sich die Auskunftserteilung auf Art. 15 Abs. 1 Nr. 1 BayDSG stützen ließ. Insoweit ging der Hinweis der Verwaltungsgemeinschaft auf das ordnungswidrigkeitenrechtliche Bußgeldverfahren schon deswegen fehl, da ein solches offensichtlich nicht eingeleitet, sondern die Hundehalterin nur allgemein auf die bestehende Anleinpflicht hingewiesen werden sollte. Im Übrigen kommt es auch im Bußgeldverfahren in Betracht, den Namen des Anzeigeerstatters vertraulich zu behandeln (vgl. dazu näher Gohler, Ordnungswidrigkeitengesetz, 15. Auflage, Rdnr. 31 vor § 59).

In datenschutzrechtlicher Hinsicht entscheidend war daher die Frage, ob sich die erfolgte Auskunftserteilung auf Art. 29 Bayerisches Verwaltungsverfahrensgesetz (BayVwVfG) stützen ließ. Unmittelbar war diese Norm nicht anwendbar, da mit dem bloßen Hinweis auf die Anleinpflicht weder ein auf den Erlass eines Verwaltungsaktes abzielendes Verwaltungsverfahren im Sinne des BayVwVfG in Gang gesetzt noch mit der Auskunftserteilung eine Akteneinsicht im eigentlichen Sinne gewährt wurde. Jedoch kann Art. 29 BayVwVfG als Ausdruck eines allgemeinen Rechtsgedankens auch analog für behördliche Auskünfte herangezogen werden (vgl. Kopp/Ramsauer, Verwaltungsverfahrensgesetz, 11. Auflage, § 29 Rdnr. 5). Überdies kommt auch außerhalb eines Verwaltungsverfahrens ein Akteneinsichtsrecht im Rahmen einer Ermessensentscheidung in Betracht, wenn der Anspruchsteller ein berechtigtes Interesse hieran geltend macht (vgl. BayVGH, Urteil vom 17.12.1998, BayVBl 1998, 693 ff. m.w.N.). Zur Gewährung von Akteneinsicht hat eine Behörde ihre Ermessensentscheidung so zu treffen, dass unter Berücksichtigung des Grundprinzips des rechtsstaatlichen und fairen Verfahrens eine beiderseits sachgerechte Interessenwahrung möglich ist. Außerdem muss die Kenntnis des Akteninhalts Voraussetzung für eine wirksame Rechtsverfolgung sein.

Die von der Verwaltungsgemeinschaft demnach zu treffende Ermessensentscheidung hätte unter Berücksichtigung dieser Vorgaben zur Ablehnung der begehrten Auskunft führen müssen. So wurde die Hundehalterin lediglich allgemein auf die Anleinpflicht hingewiesen und hätte auch ohne Kenntnis des Namens des Anzeigeerstatters der Verwaltungsgemeinschaft ihre Sichtweise darlegen können. Die Auskunftserteilung war damit nicht zur Geltendmachung oder Verteidigung ihrer **rechtlichen Interessen** erforderlich. Daran ändert auch die Beauftragung eines Rechtsanwalts nichts. Auf der anderen Seite hatte der Anzeigeerstatter ein **schutzwürdiges Interesse** an der Geheimhaltung seines Namens durch die Behörde. Dem Bürger, der eine Behörde auf tatsächliche oder ver-

meintliche Missstände und Verstöße gegen Rechtsvorschriften hinweist, sollen dadurch keine Nachteile entstehen. Dies ist letztlich auch im Interesse von Behörden, die zur ordnungsgemäßen Erfüllung ihrer Aufgaben auf derartige Informationen angewiesen sind. Der Anzeigeerstatter vertraut darauf, dass seine Hinweise im Bereich der Verwaltung verbleiben. Dies gilt unabhängig davon, ob der Informant ausdrücklich um vertrauliche Behandlung gebeten hat. Er ist nur dann nicht schutzwürdig, wenn es sich um haltlose, grob unwahre oder gar verleumderische Angaben handelt, gegen die sich der Angezeigte zur Wehr setzen will (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 10 Rdnr. 49 a - k). Derartige Anhaltspunkte konnten im konkreten Fall auch der unterschiedlichen Sachverhaltsschilderung seitens Anzeigeerstatter und Angezeigten nicht entnommen werden.

Da es sich hierbei um einen nicht unerheblichen Datenschutzverstoß handelt, der zudem zu nachteiligen Folgen für ein Kind geführt hat, war er zu beanstanden.

6.11 Nachträgliche Bekanntgabe von in nichtöffentlicher Gemeinderatssitzung gefassten Beschlüssen

Im Rahmen meiner Beratungstätigkeit für bayerische öffentliche Stellen bin ich wiederholt mit der Frage befasst worden, ob **und inwieweit** in nichtöffentlicher Gemeinderatssitzung gefasste Beschlüsse der Allgemeinheit bekanntgegeben werden dürfen. Die Antwort auf diese Frage war anhand des Art. 52 Abs. 3 der Gemeindeordnung für den Freistaat Bayern (im Folgenden: GO) zu geben. Maßgeblich für Zeitpunkt und Umfang der Bekanntgabe der in nichtöffentlicher Sitzung gefassten Beschlüsse ist daher nach Art. 52 Abs. 3 GO, wann **und inwieweit** die Gründe für die Geheimhaltung weggefallen sind.

Geheimhaltungsgründe sind nach Art. 52 Abs. 2 Satz 1 GO das Wohl der Allgemeinheit und "berechtigte Ansprüche Einzelner". Bei solchen berechtigten Ansprüchen Einzelner muss es sich um keinen Anspruch im Sinne des Bürgerlichen Gesetzbuchs handeln, vielmehr genügt die Beeinträchtigung rechtlich geschützter oder anerkannter Interessen. Hierzu zählen insbesondere die persönlichen und wirtschaftlichen Verhältnisse der Bürger, an deren öffentlicher Erörterung die Allgemeinheit kein berechtigtes Interesse hat und deren Bekanntgabe dem Einzelnen nachteilig sein kann.

Nur insoweit, als die Gründe, welche ursprünglich zur Behandlung der Thematik in nichtöffentlicher Sitzung geführt haben, zwischenzeitlich weggefallen sind, ist eine Bekanntgabe nach Art. 52 Abs. 3 GO zulässig.

So dürfen z.B. bei Personalentscheidungen Name und Amtsbezeichnung des künftigen Mitarbeiters nur dann bekanntgegeben werden, wenn dieser nach Tätigkeitsbeginn eine Funktion mit Außenwirkung wahrnehmen wird. Handelt es sich dagegen um eine Funktion ohne Außenwirkung, so darf schon die Person des neuen Mitarbeiters nicht bekanntgegeben werden. Diese Unterscheidung nach der jeweiligen Funktion der Beschäftigten ergibt sich aus der Fürsorgepflicht der Gemeinde als Dienstherrin. Ich verweise hierzu auch auf meine Ausführungen im 23. Tätigkeitsbericht, Nr. 21.4, und im 22. Tätigkeitsbericht, Nr. 19.1.

Von vornherein unzulässig ist dagegen die namentliche Bekanntgabe unterlegener Mitbewerber sowie der Privatanschrift des zukünftigen Mitarbeiters. Die Be-

troffenen haben insoweit ein schutzwürdiges Interesse, dass diese personenbezogenen Daten nicht der Öffentlichkeit zugänglich gemacht werden.

Art. 52 Abs. 1 - 3 GO
(1) Zeitpunkt und Ort der Sitzungen des Gemeinderats sind unter Angabe der Tagesordnung, spätestens am dritten Tag vor der Sitzung, ortsüblich bekanntzumachen. Ausnahmen bedürfen der Genehmigung des Gemeinderats.
(2) Die Sitzungen sind öffentlich, soweit nicht Rücksichten auf das Wohl der Allgemeinheit oder auf berechtigte Ansprüche Einzelner entgegenstehen. Über den Ausschluss der Öffentlichkeit wird in nichtöffentlicher Sitzung beraten und entschieden.
(3) Die in nichtöffentlicher Sitzung gefassten Beschlüsse sind der Öffentlichkeit bekanntzugeben, sobald die Gründe für die Geheimhaltung weggefallen sind.

6.12 Anfertigen von Kopien von Unterstützungsunterschriften für Wahlkreisvorschläge

Nach dem Landeswahlgesetz (LWG) müssen Wahlkreisvorschläge unter den gesetzlich genannten Voraussetzungen mit Unterstützungsunterschriften von Stimmberechtigten versehen sein. § 31 Abs. 3 Nr. 3 der Landeswahlordnung (LWO) bestimmt dazu, dass für jeden Unterzeichner auf einem amtlichen Formblatt oder gesondert eine Bescheinigung der Gemeinde, bei der der Unterzeichner im Wählerverzeichnis eingetragen ist, beizufügen ist, dass er im betreffenden Wahlkreis stimmberechtigt ist. Eine politische Partei hat sich nun im Vorfeld der Landtags- und Bezirkstagswahl 2008 mit dem Vorbringen an mich gewandt, eine Stadt habe Unterstützungsunterschriften für die Partei fotokopiert und damit gegen die Landeswahlordnung verstoßen. Danach dürfe die Kommune nicht festhalten, für welchen Wahlkreisvorschlag eine erteilte Bescheinigung bestimmt sei. Die von mir daraufhin durchgeführte Überprüfung hat folgenden Sachverhalt ergeben:

Die Bescheinigung der Unterstützungsunterschriften erfolgte an allen Meldeschaltern der Stadt. Um sicherzustellen, dass keine Doppelbescheinigungen ausgestellt werden, wurde von den zuständigen Mitarbeitern eine Kopie der jeweils getätigten Bescheinigung angefertigt. Das entsprechende Formblatt für eine Unterstützungsunterschrift wurde dabei ab dem Bereich "Angaben zur Person" kopiert; dazu wurde das Formblatt in der Mitte ab "Familienname" geknickt. Die Kopie wurde den anderen Meldeschaltern zur Kenntnisnahme und Beachtung vorgelegt und anschließend vernichtet; eine EDV- oder papiermäßige Speicherung der Daten wurde nicht vorgenommen.

Diesen Sachverhalt habe ich aus datenschutzrechtlicher Sicht wie folgt bewertet:

§ 31 Abs. 5 Satz 2 der Landeswahlordnung (LWO) sieht vor, dass die Gemeinde für jede stimmberechtigte Person die Bescheinigung des Stimmrechts nur einmal zu einem Wahlkreisvorschlag erteilen darf; dabei darf sie nicht festhalten, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt ist. In der Wahlanweisung für die Landtagswahl und die Bezirkswahl 2008 - Gemeinde WA3 - wird unter Ziffer F.I.1.c) auf die Vorschrift des § 31 Abs. 5 LWO hingewiesen und klargestellt, dass es zweckmäßig ist, die Unterzeichner in einer alphabetischen Liste oder einer Datei zu führen oder in einem alphabetischen Verzeichnis aller Stimmberechtigten entsprechend zu kennzeichnen. Weiter heißt es in der Wahlanweisung, dass das Anfertigen von Kopien der Unterstützungsunterschrif-

ten auch dann nicht zulässig ist, wenn der Name der unterstützenden Partei abgedeckt oder geschwärzt wird. Die Erteilung der Bescheinigung darf auch nicht im Wählerverzeichnis vermerkt werden.

Bei dem von der Stadt bei der Landtagswahl und Bezirkswahl 2008 praktizierten Verfahren wurden zwar Kopien angefertigt und damit personenbezogene Angaben (hier: Familienname, Vorname, Geburtsdatum, Anschrift und Unterschrift) des Stimmberechtigten für Kontrollzwecke, nämlich der Vermeidung einer mehrfachen Unterstützung von Wahlkreisvorschlägen durch den Betroffenen, erhoben. Allerdings wurde dabei nicht festgehalten, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt war, da nach Aussage der Stadt dieser Teil des Formblatts jeweils nicht mitkopiert worden war. Ein Verstoß gegen § 31 Abs. 5 Satz 2 LWO, wonach es unzulässig ist, festzuhalten, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt ist, liegt damit nicht vor.

Auch wenn ein Verstoß gegen wahlgesetzliche Vorschriften somit nicht vorliegt, wäre es aus datenschutzrechtlicher Sicht jedoch wünschenswert gewesen, wenn die Stadt ein Kontrollverfahren gewählt hätte, das der Wahlanweisung des Bayerischen Staatsministeriums des Innern für die Landtagswahlen und Bezirkswahlen 2008 - WA 3 - entsprochen hätte. Dort wird unter anderem darauf hingewiesen, es seien auch dann keine Kopien von den Unterstützungsunterschriften anzufertigen, wenn der Name der unterstützenden Partei abgedeckt oder geschwärzt wird. Laut Auskunft des Bayerischen Staatsministeriums des Innern wurde die Wahlanweisung als Handlungsanweisung für die Gemeinden, insbesondere zum Zwecke eines einheitlichen Verwaltungsvollzugs bei der Durchführung der Landtags- und Bezirkswahl 2008, erlassen. Die Stadt hat mir zugesichert, bei künftigen Wahlen keine Kopien mehr zu fertigen, sondern nur noch solche Aufzeichnungen über stimmberechtigte Personen (z.B. in Form von Excel-Tabellen) zu führen, wie dies in der Wahlanweisung des Bayerischen Staatsministeriums des Innern für den Fall der Bescheinigung der Unterstützung eines Wahlkreisvorschlags vorgesehen ist.

Die beschriebene Vorgehensweise war kein Einzelfall. Dies zeigte sich an einer weiteren Eingabe, diesmal im Vorfeld der Europawahl 2009. § 32 Abs. 5 Satz 2 der Europawahlordnung enthält dazu eine § 31 Abs. 5 Satz 2 der Landeswahlordnung entsprechende Regelung. Da der Eingabeführer in diesem Fall die betroffene Gemeinde nicht genannt hat, konnte ich ihn nur allgemein auf die Rechtslage hinweisen und anregen, sich an den behördlichen Datenschutzbeauftragten der Kommune zu wenden.

Art. 31 Abs. 3 Nrn. 2 - 4 und Abs. 5 LWO
(3) Die nach Art. 27 Abs. 1 Nr. 4 Satz 2 LWG erforderlichen Unterstützungsunterschriften von Stimmberechtigten sind auf amtlichen Formblättern nach Anlage 5 unter Beachtung folgender Vorschriften zu erbringen:

2. Die Stimmberechtigten, die einen Wahlkreisvorschlag unterstützen, müssen die Erklärung auf dem Formblatt persönlich unterzeichnen; neben der Unterschrift sind Familienname, Vorname, Tag der Geburt und Anschrift (Hauptwohnung) des Unterzeichners anzugeben.

3. Für jeden Unterzeichner ist auf dem Formblatt oder gesondert eine Bescheinigung der Gemeinde, bei der er im Wählerverzeichnis einzutragen ist, beizufügen, dass er im betreffenden Wahlkreis stimmberechtigt ist. Gesonderte Bescheinigungen des Stimmrechts sind vom Träger des Wahlkreisvorschlags bei der Einreichung des Wahlkreisvorschlags mit den Unterstützungsunterschriften zu verbinden. Wer für einen anderen eine Be-

scheinigung des Stimmrechts beantragt, muss nachweisen, dass der Betreffende den Wahlkreisvorschlag unterstützt.

4. *Eine stimmberechtigte Person darf nur einen Wahlkreisvorschlag unterzeichnen. Hat jemand mehrere Wahlkreisvorschläge unterzeichnet, so ist seine Unterschrift auf allen Wahlkreisvorschlägen ungültig.*

(5) Die Bescheinigung des Stimmrechts (Abs. 3 Nr. 3) und die Bescheinigung der Wählbarkeit (Abs. 4 Nr. 2) sind kostenfrei zu erteilen. Die Gemeinde darf für jede stimmberechtigte Person die Bescheinigung des Stimmrechts nur einmal zu einem Wahlkreisvorschlag erteilen; dabei darf sie nicht festhalten, für welchen Wahlkreisvorschlag die erteilte Bescheinigung bestimmt ist.

6.13 Melderegisterauskünfte in besonderen Fällen

Nach Art. 32 des Meldegesetzes können die Betroffenen der Weitergabe ihrer Meldedaten an politische Parteien für Wahlwerbezwecke, an Adressbuchverlage zur Herausgabe eines Adressbuchs und der Daten über Alters- und Ehejubiläen an die in der Vorschrift genannten Stellen widersprechen. Hierauf sind sie bei der Anmeldung hinzuweisen; auf ihr Widerspruchsrecht gegen die Erteilung von Melderegisterauskünften für Wahlwerbezwecke sind sie zusätzlich spätestens acht Monate vor den Wahlen durch öffentliche Bekanntmachung hinzuweisen.

Wie schon in früheren Jahren haben mich auch im Berichtszeitraum wieder Anfragen und Beschwerden von Bürgern erreicht, denen ihr Widerspruchsrecht nicht bekannt war. Die Praxis zeigt seit langem, dass hier eine effektive Wahrnehmung des Grundrechts auf informationelle Selbstbestimmung durch die Bürger nur bei einer Einwilligungslösung möglich ist. Darauf haben die Datenschutzbeauftragten des Bundes und der Länder bereits auf ihrer 56. Konferenz am 05./06.10.1998 in Wiesbaden und auch in der Folgezeit immer wieder hingewiesen (siehe hierzu 18. Tätigkeitsbericht 1998, Anlage 16).

6.14 Weitergabe von Melderegisterdaten Jugendlicher an die Freiwillige Feuerwehr zur Nachwuchswerbung

Dürfen die Einwohnermeldeämter Melderegisterdaten Jugendlicher an die Freiwilligen Feuerwehren übermitteln? Diese Frage bekomme ich von vielen Gemeinden gestellt, die solche Meldedaten zur Nachwuchswerbung nutzen wollen. Ich vertrete dazu folgende Rechtsauffassung:

Die Weitergabe der Anschriften der Jugendlichen an die Freiwillige Feuerwehr als gemeindliche Einrichtung ist zulässig, wenn dies zur rechtmäßigen Erfüllung der in der Zuständigkeit der Feuerwehr liegenden Aufgaben erforderlich ist (Art. 28 Abs. 7 Satz 1 i.V.m. Art. 28 Abs. 1 Satz 1 Meldegesetz).

Aufgabe der Freiwilligen Feuerwehr als gemeindliche Einrichtung sind nach dem Bayerischen Feuerwehrgesetz (BayFwG) der abwehrende Brandschutz und der technische Hilfsdienst. Für diese Aufgabe wird eine ausreichende Anzahl Feuerwehrdienstleistender benötigt. Sofern absehbar ist, dass in Zukunft nicht genügend Feuerwehrdienstleistende zur Verfügung stehen, kann die gezielte Werbung von Nachwuchskräften erforderlich sein.

Dies gilt auch für die Werbung von Jugendlichen, die seit der Gesetzesänderung vom 10.07.1998 bereits ab dem vollendeten 12. Lebensjahr Feuerwehrdienst

leisten dürfen (Art. 7 Abs. 1 BayFwG). Sie dürfen zwar noch nicht zur Aufgabenerfüllung eingesetzt werden (Art. 7 Abs. 2 Satz 2 BayFwG), um aber zu gewährleisten, dass sie zu dem Zeitpunkt, zu dem sie uneingeschränkt zum Feuerwehrdienst herangezogen werden können, vollständig ausgebildet sind, kann auch die Gewinnung von Jugendlichen, die das 12. Lebensjahr vollendet haben, als Feuerwehranwärter erforderlich sein. Gegen die Bekanntgabe ihrer Namen und Anschriften zur Nachwuchswerbung an den Kommandanten der Freiwilligen Feuerwehr bestehen daher keine Einwände sofern feststeht, dass bei der jeweiligen Feuerwehr ein Bedarf an Feuerwehrnachwuchskräften besteht.

In diesem Zusammenhang möchte ich auch auf meinen Beitrag im 18. Tätigkeitsbericht 1998, Nr. 9.2, hinweisen, in dem ich mich allgemein zur Weitergabe von Melderegisterdaten an die Freiwillige Feuerwehr zur Nachwuchswerbung geäußert habe.

Art. 7 BayFwG
(1) Jugendliche können vom vollendeten 12. bis zum vollendeten 18. Lebensjahr als Feuerwehranwärter Feuerwehrdienst leisten.
(2) Feuerwehranwärter sind den Feuerwehrdienstleistenden gleichgestellt, soweit sich aus diesem Gesetz nicht anderes ergibt. Sie dürfen nur zu Ausbildungsveranstaltungen und erst ab vollendetem 16. Lebensjahr bei Einsätzen zu Hilfeleistungen außerhalb der unmittelbaren Gefahrenzone herangezogen werden.

6.15 Veröffentlichung von Gewerberegisterdaten im Sinne des § 14 Abs. 6 Satz 2 GewO auf der Homepage einer Gemeinde

Im Berichtszeitraum wurde ich durch die Anfrage einer Gemeinde mit dem Problem befasst, ob eine Veröffentlichung der in § 14 Abs. 6 Satz 2 Gewerbeordnung (GewO) genannten Gewerberegisterdaten - Name, betriebliche Anschrift und angezeigte Tätigkeit des Gewerbetreibenden - auf der gemeindlichen Homepage aus datenschutzrechtlicher Sicht zulässig ist. Weiter wollte die anfragende Gemeinde auch wissen, ob der Begriff der "betrieblichen Anschrift" in diesem Sinne neben der postalischen Anschrift zusätzlich Telefon- und Faxnummer sowie E-Mail-Adresse des Gewerbetreibenden umfasst, so dass gegebenenfalls auch die Veröffentlichung dieser Angaben auf der Homepage zulässig wäre. Motivierend für die Anfrage der Gemeinde war die Förderung der ortsansässigen Wirtschaft.

Hierbei handelt es sich um eine Problematik, mit der ich mich zuletzt in meinem 18. Tätigkeitsbericht aus dem Jahr 1998, Nr. 13.4, befasst habe. Damals bin ich zu dem Ergebnis gekommen, dass die mit der Einstellung von Gewerberegisterdaten ins Internet verbundene Veröffentlichung personenbezogener Daten nur zulässig ist, wenn der Gewerbetreibende ausdrücklich vorher zugestimmt hat. Mittlerweile hat sich jedoch die Rechtslage geändert. So wurde durch das Zweite Gesetz zum Abbau bürokratischer Hemmnisse insbesondere in der mittelständischen Wirtschaft vom 07.09.2007 geregelt, dass gemäß § 14 Abs. 6 Satz 2 GewO der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden allgemein zugänglich gemacht werden dürfen.

Aus datenschutzrechtlicher Sicht bin ich insoweit der Meinung, dass der neue § 14 Abs. 6 Satz 2 GewO keinen zwingenden Auskunftsanspruch begründet, sondern vielmehr die Auskunftserteilung im pflichtgemäßen Ermessen der Behörde steht (so auch Martinez in Pielow u.a.; Kommentar zur Gewerbeordnung,

§ 14 Rdnr. 72). Dieses Ermessen muss die Gemeinde vor einer Veröffentlichung der in § 14 Abs 6 Satz 2 GewO genannten Angaben auf ihrer Homepage auch nachweisbar - z.B. dokumentiert durch einen Aktenvermerk - ausüben. Diese Ermessensausübung wird jedoch nur in ganz besonders gelagerten Einzelfällen dazu führen, dass eine Internetveröffentlichung unzulässig ist. Eine besondere Schutzwürdigkeit in Bezug auf die in § 14 Abs. 6 Satz 2 GewO genannten Daten besteht nämlich grundsätzlich nicht, da der Gewerbetreibende mit diesen Angaben auch in der Öffentlichkeit auftritt (so im Ergebnis auch Martinez a.a.O.). Die in meinem 18. Tätigkeitsbericht aus dem Jahr 1998 unter Nr. 13.4 geforderte ausdrückliche Zustimmung des Gewerbetreibenden mit der Internetveröffentlichung von Gewerberegisterdaten ist daher seit der Gesetzesänderung aus dem Jahr 2007 nicht mehr notwendig, soweit es nur um die Veröffentlichung des Namens, der betrieblichen Anschrift und der angezeigten Tätigkeit geht. Hierbei ist aber zu beachten, dass unter den Begriff der "betrieblichen Anschrift" nur die eigentliche postalische Anschrift, also Straße und Hausnummer sowie Postleitzahl fallen. In Übereinstimmung mit dem Bayerischen Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie sowie dem Bundesministerium für Wirtschaft und Technologie vertrete ich die Auffassung, dass § 14 Abs. 6 Satz 2 GewO insoweit gerade auch aus datenschutzrechtlicher Sicht restriktiv zu interpretieren ist. Die Internetveröffentlichung von Telefon- und Faxnummer sowie E-Mail-Adresse ist datenschutzrechtlich also auch weiterhin nur mit ausdrücklicher Zustimmung des Gewerbetreibenden zulässig.

§ 14 Abs. 1 und 6 GewO

(1) Wer den selbständigen Betrieb eines stehenden Gewerbes, einer Zweigniederlassung oder einer unselbständigen Zweigstelle anfängt, muss dies der zuständigen Behörde gleichzeitig anzeigen. Das Gleiche gilt, wenn

1. der Betrieb verlegt wird,
2. der Gegenstand des Gewerbes gewechselt oder auf Waren oder Leistungen ausgedehnt wird, die bei Gewerbebetrieben der angemeldeten Art nicht geschäftsüblich sind, oder
3. der Betrieb aufgegeben wird.

Steht die Aufgabe des Betriebes eindeutig fest und ist die Abmeldung nicht innerhalb eines angemessenen Zeitraums erfolgt, kann die Behörde die Abmeldung von Amts wegen vornehmen.

(6) Die erhobenen Daten dürfen nur für die Überwachung der Gewerbeausübung sowie statistische Erhebungen verwendet werden. Der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden dürfen allgemein zugänglich gemacht werden.

7 Gesundheitswesen

7.1 Krebsregistrierung - Klinikregister datenschutzgerecht ausgestalten!

Die Krebsregistrierung ist in Bayern im Gesetz über das bevölkerungsbezogene Krebsregister Bayern (BayKRG) geregelt (siehe hierzu 19. Tätigkeitsbericht, Nr. 3.3). Das bevölkerungsbezogene Krebsregister besteht aus einer Vertrauensstelle und einer Registerstelle, die jeweils räumlich, organisatorisch und personell voneinander getrennt sind. Daneben kennt das BayKRG auch die Klinikregister. Diesen kommt vor allem die Aufgabe zu, die eingegangenen Meldungen von Ärzten und Zahnärzten - ggf. nach einer Überprüfung und Berichtigung - an die Vertrauensstelle des bevölkerungsbezogenen Krebsregisters weiterzuleiten. Daneben dürfen die Klinikregister die epidemiologischen Daten für ihre Zwecke verarbeiten und nutzen, die auf die Person bezogenen Identitätsdaten der Betroffenen jedoch nur mit deren Einwilligung.

Art. 6 Abs. 1 Sätze 4 und 5 BayKRG
[4]Die Klinikregister dürfen die epidemiologischen Daten (Art. 4 Abs. 2) dieser Meldungen für ihre Zwecke verarbeiten und nutzen. [5]Eine Verarbeitung und Nutzung der Identitätsdaten (Art. 4 Abs. 1) ist nur mit Einwilligung der Betroffenen zulässig.

In den Klinikregistern dürfen deshalb keine Identitätsdaten aus den Meldungen mehr gespeichert sein, sobald die Übermittlung der Daten an die Vertrauensstelle abgeschlossen ist, es sei denn, es liegt eine ausdrückliche Einwilligung der Betroffenen vor. Zu den Identitätsdaten gehören Familienname, Vornamen, frühere Namen, Geschlecht, Anschrift, Geburtsdatum, Datum der ersten Tumordiagnose und Sterbedatum.

Im Berichtszeitraum erreichte mich ein Gesetzentwurf des Staatsministeriums für Umwelt und Gesundheit, der einen regelmäßigen Abgleich der Daten der Klinikregister mit den Daten der Melderegister vorsah. In der Gesetzesbegründung hieß es hierzu, dass die Klinikregister Kenntnis über den Sterbetag der Patienten haben müssten. Aufgrund therapiebedingter jahrelanger Krankheitsverläufe, zunehmender Mobilität und Namensänderungen werde es für die Klinikregister zunehmend schwieriger, Todesbescheinigungen mit der Erstdiagnose in Verbindung zu bringen. Es sei daher erforderlich, die bei den Klinikregistern vorhandenen personenbezogenen Daten mit Hilfe der von den Meldebehörden übermittelten Daten regelmäßig zu aktualisieren.

In Besprechungen mit den beteiligten Ministerien sowie mit Verantwortlichen der Klinikregister wurde deutlich, dass bezüglich der Klinikregister offenbar erhebliche Unterschiede zwischen der Konzeption des BayKRG einerseits und der tatsächlichen Praxis sowie den Vorstellungen der Verantwortlichen der Klinikregister andererseits bestehen. Insbesondere trat offen zu Tage, dass in den Klinikregistern die Identitätsdaten der Krebspatienten auch ohne deren Einwilligung dauerhaft gespeichert werden.

Ich forderte daraufhin das Staatsministerium für Umwelt und Gesundheit auf, dafür Sorge zu tragen, dass die Diskrepanz zwischen Gesetz und Wirklichkeit in den

Klinikregistern beendet wird. Hierzu müssen entweder die ohne Einwilligung der Betroffenen in den Klinikregistern gespeicherten Identitätsdaten gelöscht werden und ein personenbezogener Datenabgleich mit dem Melderegister weiterhin unterbleiben. Alternativ könnte der Gesetzgeber die Konzeption der Krebsregistrierung in den Klinikregistern umfassend neu regeln. Um datenschutzrechtlichen Anforderungen zu genügen, wäre dann jedoch insbesondere vorzusehen, dass die medizinischen Daten der Krebspatienten im Klinikregister nach Weiterleitung an die Vertrauensstelle nur pseudonymisiert, also ohne Identitätsdaten, gespeichert werden. Für die Weiterleitung der Daten an die Vertrauensstelle und die Löschung der Identitätsdaten durch das Klinikregister wären zeitliche Vorgaben erforderlich, welche die Verweildauer der Identitätsdaten im Bereich der Klinikregister weitestgehend minimiert. Der Datenabgleich mit dem Melderegister dürfte nur mit Hilfe pseudonymisierter Daten erfolgen. Für die Auswertungen dürfte nur mit anonymisierten Daten gearbeitet werden.

Ein mir daraufhin vorgelegter weiterer Gesetzentwurf des Staatsministeriums für Umwelt und Gesundheit sah vor, dass die Klinikregister nach Einholung der grundsätzlich erforderlichen Einwilligung als personenbezogenes Klinikregister geführt werden sollen. Ein personenbezogenes Klinikregister, das auf jegliche Pseudonymisierung bzw. Anonymisierung von Daten verzichtet, entspricht jedoch nicht einer datenschutzkonformen Krebsregistrierung. Dies habe ich in meiner Stellungnahme zu dem vorgelegten Gesetzentwurf sehr deutlich gemacht. Nach meiner Auffassung sind geeignete und angemessene Verschlüsselungsverfahren dringend erforderlich.

7.2 Schulgesundheitspflege - Pflicht zur Vorlage des Impfausweises und des gelben Kinderuntersuchungshefts?

Muss ich bei der Schuleingangsuntersuchung meines Kindes den Impfausweis und das sogenannte gelbe Kinderuntersuchungsheft vorlegen? Muss ich bei der Impfberatung in der 6. Klasse meinem Kind den Impfausweis mitgeben? Diese von vielen Eltern an mich gerichteten Fragen sind ein Beispiel für die datenschutzrechtlichen Themen aus dem Bereich der Schulgesundheitspflege, mit denen ich mich im Berichtszeitraum beschäftigt habe.

Gesetzlich gilt derzeit Folgendes: Die Schulgesundheitspflege nehmen die Gesundheitsämter in Zusammenarbeit mit der Schule und den Personensorgeberechtigten wahr. Im Rahmen der Schuleingangsuntersuchung haben die Personensorgeberechtigten den Nachweis über die Teilnahme an der U9-Früherkennungsuntersuchung vorzulegen.

Art. 14 Abs. 5 Satz 4 Gesundheitsdienst- und Verbraucherschutzgesetz
Im Rahmen der nach Art. 80 Satz 1 des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen von den unteren Behörden für Gesundheit, Veterinärwesen, Ernährung und Verbraucherschutz durchzuführenden Schuleingangsuntersuchung haben die Personensorgeberechtigten den Nachweis über die nach Abs. 1 vorgeschriebene Teilnahme an der U9-Früherkennungsuntersuchung vorzulegen.

Zum 01.01.2009 trat hierzu eine Schulgesundheitspflegeverordnung in Kraft, die das Staatsministerium für Umwelt und Gesundheit erlassen hatte - leider ohne mir zuvor Gelegenheit zur Stellungnahme einzuräumen. In dieser Verordnung war bestimmt, dass die Personensorgeberechtigten verpflichtet sind, bei der

Schuleingangsuntersuchung die notwendigen Unterlagen, insbesondere das gelbe Kinderuntersuchungsheft und den Impfausweis, vorzulegen. Bezüglich des Impfausweises war ferner vorgesehen, dass dieser auch später im Rahmen der in den Schulen durchzuführenden jahrgangsweisen Impfberatungen und der Erhebungen zu Impfraten vorzulegen ist.

Ich war mit dieser Fassung der Schulgesundheitspflegeverordnung nicht einverstanden. Denn zum einen war die Vorlage von Unterlagen wie dem gelben Kinderuntersuchungsheft und dem Impfausweis bislang freiwillig gewesen. Gründe, von dieser jahrzehntelangen, bewährten und mit mir abgestimmten Regelung abzuweichen und eine Verpflichtung zur Vorlage von Unterlagen vorzusehen, konnte ich nicht erkennen. Zu bedenken war dabei auch, dass im gelben Kinderuntersuchungsheft mitunter auch äußerst sensible medizinische Daten der Mutter enthalten sein können, die im Rahmen der Schulgesundheitspflege keine Rolle spielen. Darüber hinaus habe ich erhebliche Zweifel geäußert, ob die Bestimmungen in der Schulgesundheitspflegeverordnung vollumfänglich von einer Ermächtigungsgrundlage in einem Parlamentsgesetz gedeckt sind. Denn Art. 14 Abs. 5 Satz 4 des Gesundheitsdienst- und Verbraucherschutzgesetzes bestimmt lediglich, dass ein Nachweis über die Teilnahme an der U9 - Früherkennungsuntersuchung vorzulegen ist. Hingegen enthält das Gesetz keine Verpflichtung zur Vorlage weiterer Unterlagen wie dem vollständigen gelben Kinderuntersuchungsheft (U1 bis U9) oder dem Impfausweis.

Aufgrund meiner Intervention hat das Staatsministerium für Umwelt und Gesundheit die Schulgesundheitspflegeverordnung geändert. In der seit 01.10.2009 geltenden aktuellen Fassung ist nunmehr bestimmt, dass die Personensorgeberechtigten verpflichtet sind, das Kind bei der Schuleingangsuntersuchung vorzustellen und einen geeigneten Nachweis über die Teilnahme des Kindes an der U9 - Früherkennungsuntersuchung zu führen. Diesen Nachweis können die Personsorgeberechtigten dadurch führen, dass sie das gelbe Kinderuntersuchungsheft vorlegen, es stehen ihnen jedoch auch andere geeignete Möglichkeiten wie z.B. ein ärztliches Attest offen. Die Vorschriften, wonach der Impfausweis bei der Schuleingangsuntersuchung und auch später bei der Impfberatung verpflichtend vorzulegen ist, wurden gestrichen. Die Vorlage des Impfbuchs erfolgt daher derzeit wieder auf freiwilliger Basis.

Allerdings hat mir das Staatsministerium für Umwelt und Gesundheit einen Gesetzentwurf zur Ergänzung des Gesundheitsdienst- und Verbraucherschutzgesetzes vorgelegt, der eine Pflicht zur Vorlage des Impfausweises beinhaltet. Ich habe in meiner Stellungnahme darauf hingewiesen, dass keine Pflicht zur Impfung und zum Besitz eines Impfausweises besteht. Eine Verpflichtung zur Vorlage des Impfausweises im Rahmen der Schulgesundheitspflege stünde hierzu im Widerspruch und liefe ins Leere, wenn Betroffene über keinen Impfausweis verfügen.

7.3 Videoüberwachung in den Aufzügen eines Krankenhauses

Aufgrund einer Eingabe habe ich erfahren, dass in den Patientenaufzügen eines Krankenhauses Überwachungskameras angebracht sind.

Das Krankenhaus hat mir in seiner Stellungnahme mitgeteilt, dass die Aufzüge öffentlich zugänglich seien und sowohl von Besuchern, Patienten als auch Beschäftigten genutzt würden. In den Aufzügen würden auch Patienten in Betten

befördert. Die in den Aufzügen installierten Kameras seien jedoch nicht eingeschaltet. Eine Inbetriebnahme sei aber möglich. Die Videokameras dienten - sowohl im aktivierten wie im inaktivierten Zustand - der Abschreckung vor Vandalismus. Später ergänzte das Krankenhaus, dass weiterer Zweck der Videokameras in den Aufzügen die optische Kontaktaufnahme und Einschätzung bei Notfällen sei, so z.B. wenn Personen bei einem technischen Ausfall der Aufzüge oder im Brandfall eingeschlossen seien.

Da es sich bei dem betroffenen Krankenhaus um ein Wettbewerbsunternehmen handelte, kam für die Videoüberwachung der öffentlich zugänglichen Aufzüge grundsätzlich die Vorschrift des § 6 b BDSG zur Anwendung. Von einer Beobachtung im Sinne des § 6 b Abs. 1 BDSG kann jedenfalls dann gesprochen werden, wenn die Videokameras in Betrieb genommen sind. Fraglich ist jedoch, ob § 6 b BDSG auch gilt, solange die Videokameras in den Aufzügen nicht aktiviert sind, es sich also gleichsam um bloße Kameraattrappen handelt. Bei Kameraattrappen bzw. inaktiven Kameras findet an sich keine Beobachtung im Sinne des § 6 b Abs. 1 BDSG statt und liegt damit an sich auch keine Datenerhebung vor (Bizer in Simitis, Bundesdatenschutzgesetz, Rdnr. 39; ebenso zur Parallelvorschrift in Art. 21 a BayDSG: Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Art. 21 a Rdnr. 9). Da allerdings eine Kameraattrappe bzw. eine inaktive Kamera beim Betroffenen die Vorstellung einer funktionsfähigen Anlage erzeugen soll, um ihn von einem unerwünschten Verhalten abzuhalten, unterscheidet sie sich hinsichtlich des Überwachungsdrucks und des verhaltenslenkenden Zwecks nicht von einer in Betrieb befindlichen Videokamera. Es spricht deshalb viel dafür, § 6 b Abs. 1 BDSG auch auf Kameraattrappen und inaktive Kameras zumindest entsprechend anzuwenden (so zu Art. 21 a Abs. 1 BayDSG auch Wilde/Ehmann/Niese/Knoblauch, a.a.O.).

Zumindest wäre festzustellen, dass durch das Anbringen einer Kameraattrappe - gleiches muss für eine inaktive Kamera gelten - jedenfalls in das allgemeine Persönlichkeitsrecht der Betroffenen eingegriffen wird (so auch eine Vielzahl von Entscheidungen der Zivilgerichte, z.B. LG Bonn, Urteil vom 16.11.2004, Az. 8 S 139/04; LG Darmstadt, Urteil vom 17.03.1999, Az. 8 O 42/99; LG Braunschweig, Urteil vom 18.03.1998, Az. 12 S 23/97). Bei der Prüfung der Rechtmäßigkeit eines solchen Eingriffs in das allgemeine Persönlichkeitsrecht müsste wie bei § 6 b BDSG insbesondere eine Abwägung mit den schutzwürdigen Interessen der Betroffenen vorgenommen werden. Insoweit kommt es im Ergebnis also letztlich nicht darauf an, ob § 6 b BDSG auf Kameraattrappen bzw. hier inaktive Kameras entsprechend anwendbar ist oder nicht. Eine Interessenabwägung ist in jedem Fall vorzunehmen.

Daran gemessen bin ich in dem konkreten Fall der Videoüberwachung in den Aufzügen des Krankenhauses zu folgenden Ergebnissen gelangt:

Der Gesichtspunkt der Abschreckung vor Vandalismus kann den Einsatz der Videokameras in den Aufzügen - unabhängig davon, ob sich die Kameras in aktivierten oder inaktivierten Zustand befinden - nicht rechtfertigen. Denn im Rahmen der Abwägung überwiegen die schutzwürdigen Interessen der Betroffenen. Dabei kommt es maßgeblich darauf an, dass in den Aufzügen auch Patienten in ihren Betten transportiert werden. Diese Betroffenen können durch die Videoüberwachung in ihrer Intimsphäre betroffen sein, wenn sie sich liegend, nicht vollständig bekleidet, krank, hilflos und/oder an Apparate angeschlossen beobachtet fühlen. Hinzu kommt, dass sich dieser Personenkreis der Videobeobachtung nicht entziehen kann, denn die in ihren Betten transportierten Patienten

können nicht wie etwa Besucher oder Personal stattdessen die Treppe benutzen. Ein derart schwerwiegender Eingriff in die Persönlichkeitsrechte der Betroffenen könnte zur Abwehr von Gefahren für Rechtsgüter von erheblichem Gewicht gerechtfertigt sein. Dagegen reicht es hierfür nicht aus, wenn - noch dazu ohne nähere Angaben zu evtl. früheren Schadensfällen - die Überwachung lediglich dem Schutz von Sachwerten von nicht besonderer Bedeutung gegen Beschädigung dienen soll.

Hingegen handelt es sich bei dem vom Krankenhaus im weiteren Verlauf zusätzlich vorgebrachten Zweck, mit Hilfe der Videokameras in Notfällen (technischer Ausfall, Brandfall) optisch Kontakt aufnehmen und die Lage einschätzen zu können, um eine Videoüberwachung zum Schutz von Leib und Leben und damit von Rechtsgütern von erheblichem Gewicht. Allerdings reicht zur Abwehr dieser Gefahren eine Videobeobachtung im konkreten Notfall aus, z.B. sobald der Alarmknopf im Aufzug betätigt oder der Ausbruch eines Brandes gemeldet wird. Dagegen ist eine dauerhafte Videobeobachtung oder gar eine Speicherung der Aufnahmen (Videoaufzeichnung) auch zu diesem Zweck nicht erforderlich.

Im Ergebnis konnten die Videokameras deshalb zwar grundsätzlich in den Aufzügen verbleiben, dürfen jedoch nur im konkreten Notfall eingeschaltet werden, eine Speicherung der Aufnahmen muss in jedem Fall unterbleiben. Für die Betroffenen muss dies aus dem nach § 6 b Abs. 2 BDSG erforderlichen Hinweis auf die Videoüberwachung erkennbar sein. Das Krankenhaus muss also die Betroffenen darauf hinweisen, dass die Videokameras in den Aufzügen nur im konkreten Notfall eingeschaltet werden und keine Speicherung der Aufnahmen stattfindet.

7.4 Einsichtsrecht eines Angehörigen in Patientenakten eines Verstorbenen

Ein Krankenhaus fragte bei mir an, ob und unter welchen Voraussetzungen einem Angehörigen ein Einsichtsrecht in die Patientenakten eines Verstorbenen zusteht. Anlass war die konkrete Anfrage eines Angehörigen, der die Wahrheit über seinen 1924 zwangsweise in das Krankenhaus eingewiesenen und 1940 von den Nationalsozialisten umgebrachten Onkel herausfinden wollte.

Bei Patientendaten Verstorbener stellt sich zunächst die (umstrittene) Frage, inwieweit datenschutzrechtliche Vorschriften auch noch nach dem Tod des Betroffenen zur Anwendung kommen. Unbeschadet dessen ist allerdings allgemein anerkannt, dass Art. 1 Abs. 1 Grundgesetz einen postmortalen Persönlichkeitsschutz gewährleistet (grundlegend Bundesverfassungsgericht vom 24.02.1971, Az. 1 BvR 435/68). Darüber hinaus bestimmt § 9 Abs. 1 der Berufsordnung für die Ärzte Bayerns - diese berufsrechtliche Vorschrift ist zugleich als bereichsspezifische Datenschutzbestimmung anzusehen -, dass die ärztliche Schweigepflicht ausdrücklich auch über den Tod des Patienten hinaus gilt.

§ 9 Abs. 1 Berufsordnung für die Ärzte Bayerns
Der Arzt hat über das, was ihm in seiner Eigenschaft als Arzt anvertraut oder bekannt geworden ist, - auch über den Tod des Patienten hinaus - zu schweigen. Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde.

Strafrechtlich ist der postmortale Geheimnisschutz durch § 203 Abs. 1 Nr. 1 und Abs. 4 Strafgesetzbuch sichergestellt.

§ 203 Strafgesetzbuch
(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als 1. Arzt … anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft …
(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

Gleichwohl erkennt die Rechtsordnung vom Einsichtsrecht des Patienten in seine Patientenakte abgeleitete Einsichtsrechte der Erben und der nächsten Angehörigen in Patientenakten des Verstorbenen unter bestimmten Voraussetzungen an (grundlegend das Urteil des Bundesgerichtshofs vom 31.05.1983, Az. VI ZR 259/81; vgl. auch das aktuelle Urteil des Bundesarbeitsgerichts vom 23.02.2010, Az. 9 AZN 876/09). Das Einsichtsrecht eines Erben kommt in Betracht, wenn vermögensrechtliche Interessen wie z.B. die Geltendmachung von Schadensersatzleistungen im Raum stehen. Geht es hingegen um die Wahrnehmung ideeller Interessen des Verstorbenen, so gewährt die Rechtsprechung unabhängig von der Erbenstellung den nächsten Angehörigen eines Verstorbenen ein Einsichtsrecht, wenn sie nachweisen, dass es "nachwirkenden Persönlichkeitsbelangen" des Verstorbenen dient. Auch insoweit ist allerdings die ärztliche Schweigepflicht zu beachten. Nach der Rechtsprechung muss der Arzt prüfen, ob Anhaltspunkte dafür bestehen, dass der Verstorbene die Offenlegung der Unterlagen mutmaßlich missbilligt hätte. Er hat eine Gewissensentscheidung zu treffen.

Im konkreten Fall ging es dem Angehörigen darum, die Wahrheit über seinen 1924 zwangsweise in das Krankenhaus eingewiesenen und 1940 von den Nationalsozialisten umgebrachten Onkel herauszufinden. Dies konnte meiner Auffassung nach als Wahrnehmung ideeller Interessen des Verstorbenen aufgefasst werden, die dessen nachwirkenden Persönlichkeitsbelangen dient. Auch habe ich es für vertretbar gehalten, den anfragenden Neffen des Verstorbenen noch zum Kreis der nächsten Angehörigen zu zählen. Bei der Prüfung der Frage, ob der Verstorbene die Übermittlung seiner Patientendaten an seinen Neffen mutmaßlich missbilligt hätte, waren meiner Auffassung nach insbesondere das Anliegen des Angehörigen, das Schicksal des Verstorbenen im Nationalsozialismus aufzudecken, und der doch erhebliche zeitliche Abstand zum Tod des Betroffenen zu berücksichtigen. Letztlich war das Krankenhaus jedoch auch im konkreten Fall auf die maßgebliche Gewissensentscheidung des Arztes hinzuweisen, der in Kenntnis aller Umstände darüber zu entscheiden hat, ob und ggf. in welchem Umfang dem Angehörigen ein Einsichtsrecht gewährt wird. Der Arzt muss sich dabei bewusst sein, dass er die Einsicht nach der Rechtsprechung nur verweigern darf, wenn gegen sie von seiner Schweigepflicht her zumindest vertretbare Bedenken bestehen. Er muss ggf. auch darlegen, dass und unter welchem allgemeinen Gesichtspunkt er sich durch die Schweigepflicht an der Offenlegung gehindert sieht.

7.5 Weitergabe von Behandlungsunterlagen an Rechtsanwälte

Ich bin gefragt worden, ob ich es für datenschutzrechtlich zulässig halte, dass Krankenhäuser Patientendaten zur Wahrnehmung eigener Interessen an ihren

Rechtsanwalt übermitteln. Im konkreten Fall handelte es sich um die Weitergabe vollständiger psychiatrischer und psychotherapeutischer Behandlungsunterlagen.

Grundsätzlich hatte ich schon bislang die Auffassung vertreten, dass es nach allgemeinen Rechtsgrundsätzen auch öffentlichen Stellen nicht generell verwehrt werden kann, soweit im Einzelfall notwendig einen Rechtsanwalt einzuschalten und diesem dabei auch die erforderlichen personenbezogenen Daten zu übermitteln.

Speziell für den Bereich der ärztlichen Schweigepflicht wird in der Literatur (Laufs/Uhlenbruck, Handbuch des Arztrechts, 4. Auflage 2010, § 68 Rdnr. 18; vgl. ferner Laufs/Katzenmeier/Lipp, Arztrecht, 6. Auflage 2009, IX Rdnr. 31) die meiner Auffassung nach zutreffende Rechtsauffassung vertreten, dass es nach dem Rechtsgrundsatz der "Wahrnehmung berechtigter Interessen" gerechtfertigt ist, wenn ein Arzt Angaben über die Krankheit und Behandlung seines Patienten weitergibt, um z.B. eine Honorarforderung gegen den Patienten gerichtlich durchzusetzen.

In aller Regel wird es dabei nicht ausreichen, die Krankenunterlagen in anonymisierter Form zu übergeben. Denn die Identität des Betroffenen muss einem Rechtsanwalt z.B. für die Korrespondenz oder ggf. die Klageerhebung bekannt sein.

Für die Frage, ob die personenbezogenen Krankenunterlagen vollständig oder nur teilweise übermittelt werden dürfen, kommt es meiner Auffassung nach entscheidend darauf an, inwieweit dies zur Aufgabenerfüllung erforderlich ist. Daran gemessen dürfen einem Rechtsanwalt die Krankenunterlagen nur dann vollständig übergeben werden, wenn dies der jeweilige Zweck tatsächlich erfordert. Soll aber beispielsweise der Rechtsanwalt eine Honorarforderung wegen einer Behandlung im Jahr 2010 durchsetzen, hielte ich es für unzulässig, ihm auch Unterlagen über Behandlungen in früheren Jahren zu übermitteln, die mit der aktuellen Honorarforderung nichts zu tun haben. Soweit - um das Beispiel fortzusetzen - bei der Behandlung im Jahr 2010 Aufzeichnungen über ein bestimmtes Therapiegespräch angefertigt wurden, die der Rechtsanwalt für die Durchsetzung der Honorarforderung gar nicht benötigt, dürfen diese Unterlagen gleichfalls nicht übermittelt werden.

Im Hinblick darauf, dass alle Daten über die Gesundheit besonders schutzwürdig sind, gelten diese Grundsätze für alle Krankenunterlagen unabhängig von der Art der Erkrankung, wobei deren Beachtung sicherlich besonders wichtig ist, wenn wie im konkreten Fall sensible psychiatrische und psychotherapeutische Behandlungsunterlagen betroffen sind. Wegen der besonderen Schutzwürdigkeit der Daten kann grundsätzlich auch keine Rolle spielen, dass der Arbeitsaufwand für das Krankenhaus erhöht ist, wenn die Krankenunterlagen nicht vollständig übermittelt werden dürfen.

7.6 Veröffentlichung eines Notarzteinsatzprotokolls in Fernsehen und Internet

Ein bayerisches Fernsehteam begleitete einen Tag lang ein Notarzteinsatzfahrzeug bei allen Notarzteinsätzen. Dem Filmteam wurden dabei personenbezogene Daten bekannt, da sie bei der Übernahme des Einsatzes zugegen waren und

dabei von der Rettungsleitstelle an den Notarzt übermittelte Namen und Adressen von Patienten über Funk mithören konnten. Darüber hinaus konnten sie die Namen an Tür und Klingelschild am Einsatzort erkennen.

Die Mitarbeiter des Fernsehteams wurden vor den Filmaufnahmen über die ärztliche Schweigepflicht belehrt und verpflichtet, eine Verschwiegenheitserklärung zu unterschreiben. Dennoch filmte das Fernsehteam während der Dokumentationstätigkeit des Notarztes ohne dessen Kenntnis die Daten des Notarzteinsatzprotokolls. Der Filmbeitrag wurde im Fernsehen ausgestrahlt und im Internetportal des Fernsehsenders eingestellt. Dabei waren insbesondere die Daten einer zwischenzeitlich verstorbenen Patientin zu erkennen.

Ich habe den Träger des Notarztdienstes aufgefordert, zur Wahrung der ärztlichen Schweigepflicht und zum Schutz von Patientengeheimnissen keine Fernsehteams oder sonstige Presse mehr an Notarzteinsätzen zu beteiligen, soweit keine Offenbarungsbefugnis durch eine Einwilligung von Patienten vorliegt.

Bereits die durch die Begleitung des Notarztteams ermöglichte Kenntnisnahme von Patientendaten durch das Fernsehteam stellt eine unbefugte Datenübermittlung und somit eine Verletzung der ärztlichen Schweigepflicht dar. Auf die Nichtbeachtung der Verschwiegenheitserklärung durch die Mitarbeiter des Fernsehteams und auf das Filmen des Notarzteinsatzprotokolls ohne Kenntnis des zuständigen Notarztes kommt es insofern nicht an. Aus dem Schutzzweck des § 203 Strafgesetzbuch (StGB) und der ausdrücklichen Regelung in § 203 Abs. 4 StGB folgt der uneingeschränkte Geheimnisschutz und damit die Pflicht zur Verschwiegenheit des Arztes in vollem Umfang, auch nach dem Tode eines Patienten.

§ 203 Strafgesetzbuch
(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als 1. Arzt … anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft …
(4) Die Absätze 1 bis 3 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

Eine ausdrückliche Erklärung über die Entbindung von der Schweigepflicht der Ärzte durch betroffene Patienten lag zu keinem Zeitpunkt vor. Auch waren keine Anhaltspunkte erkennbar, die eine konkludente oder mutmaßliche Einwilligung von Notfallpatienten nahe gelegt hätten. Gesetzliche Vorschriften, die eine Offenlegung von Patientendaten gegenüber dem Filmteam zugelassen hätten, konnten ebenso wenig geltend gemacht werden. Entsprechende Offenbarungsbefugnisse haben sich hier weder aus Art. 4 Abs. 1 Bayerisches Pressegesetz (BayPrG) ergeben, der einen Auskunftsanspruch der Presse nur insoweit gewährt als keine gesetzliche Verschwiegenheitspflicht (hier: ärztliche Schweigepflicht) besteht (Art. 4 Abs. 2 Satz 2 BayPrG), noch aus § 9 Abs. 2 Satz 1 der Bayerischen Berufsordnung für die Ärzte Bayerns zum Schutz höherwertiger Rechtsgüter, da nicht anzunehmen war, dass das öffentliche Informationsinteresse an Notarzteinsätzen das Recht von Notfallpatienten auf Schutz ihrer Intimsphäre überwiegt.

Art. 4 Bayerisches Pressegesetz
(1) Die Presse hat gegenüber Behörden ein Recht auf Auskunft. Sie kann es nur durch Redakteure oder andere von ihnen genügend ausgewiesene Mitarbeiter von Zeitungen oder Zeitschriften ausüben.
(2) Das Recht auf Auskunft kann nur gegenüber dem Behördenleiter und den von ihm Beauftragten geltend gemacht werden. Die Auskunft darf nur verweigert werden, soweit auf Grund beamtenrechtlicher oder sonstiger gesetzlicher Vorschriften eine Verschwiegenheitspflicht besteht.

§ 9 Abs. 2 Berufsordnung für die Ärzte Bayerns
Der Arzt ist zur Offenbarung befugt, soweit er von der Schweigepflicht entbunden worden ist oder soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes erforderlich ist …

Wegen Art. 2 Abs. 9 Bayerisches Datenschutzgesetz (BayDSG) konnten im Bereich der ärztlichen Schweigepflicht die allgemeinen Vorschriften des BayDSG von vornherein nicht herangezogen werden.

Wie eine mögliche Verletzung von Verschwiegenheitserklärungen oder die Verwendung von Patientendaten im Fernsehen und im Internet durch Mitarbeiter des Fernsehsenders zu beurteilen ist, konnte ich mangels eigener Kontrollzuständigkeit nicht selbst bewerten. Ich habe jedoch den Datenschutzbeauftragten des Fernsehsenders unterrichtet.

7.7 Verbundverfahren TIZIAN

Bereits in meinem 23. Tätigkeitsbericht, Nr. 3.14 und Nr. 14.1, habe ich mich mit dem Verbundverfahren "TIZIAN" befasst. Ich habe darauf hingewiesen, dass aufgrund des erheblichen Eingriffs in das informationelle Selbstbestimmungsrecht für die Verbunddatei "TIZIAN" eine gesetzliche Grundlage erforderlich ist. Zum Zeitpunkt der damaligen Beurteilung fehlte eine hinreichend klare und bestimmte gesetzliche Grundlage.

Zwischenzeitlich liegt ein Gesetzentwurf vor, an dem ich maßgeblich beteiligt war. Der Gesetzentwurf regelt zum einen die allgemeinen Anforderungen an ein Verbundverfahren im Bayerischen Datenschutzgesetz und zum anderen die spezifischen Anforderungen an "TIZIAN" im Gesundheitsdienst- und Verbraucherschutzgesetz. Der Gesetzentwurf befindet sich noch im Gesetzgebungsverfahren.

8 Sozialwesen

8.1 Hausbesuche bei Eltern anlässlich der Geburt von Kindern

Ich war im Berichtszeitraum intensiv mit einem kommunalen Modellprojekt "Begrüßung von Neugeborenen" befasst. Ein Begrüßungsschreiben des Bürgermeisters an die Eltern sollte außer der Gratulation zur Geburt und der Ankündigung von Familiengutscheinen und Informationsunterlagen, insbesondere die Ankündigung eines ersten Hausbesuchs durch eine beim städtischen Jugendamt angestellte Kinderkrankenschwester mit Terminvorschlag sowie die Aufklärung über den Zweck des Hausbesuchs enthalten. Bei dem ersten Hausbesuch - auf dessen Freiwilligkeit hingewiesen wurde - sollte es sich um ein rein informatives Gespräch handeln. Für weitere Hausbesuche war eine schriftliche Einwilligungserklärung der Eltern vorgesehen, weil dabei Daten erhoben, gespeichert und gegebenenfalls weitergegeben werden sollten.

Ich habe die Auffassung vertreten, dass die Zielrichtung des Projekts, junge Eltern in einer Umbruchsituation zu unterstützen, zu fördern und ihnen Hilfe anzubieten, durchaus nachvollziehbar sei. Dennoch ist dieses Projekt ambivalent. Das Jugendamt hat nicht nur die Funktion, Eltern Angebote zu unterbreiten, wie es sie in ihrer Erziehungsarbeit und ihrem Erziehungsauftrag unterstützen kann, sondern es hat auch die Funktion, ein Wächteramt auszuüben. Vor allem die umfangreiche Rechtsprechung des Bundesverfassungsgerichts zur Sorgerechtsentziehung auf Antrag von Jugendämtern zeigt, dass diese beiden Funktionen nicht gänzlich voneinander getrennt werden können. Wenn ein Mitarbeiter des Jugendamts zu Hause bei den Eltern Besuche macht, um sie zu informieren, wie sie ihre Kinder besser pflegen oder erziehen können, dann kann nicht ausgeschlossen werden, dass dabei - auch wenn es nicht beabsichtigt sein mag - auch Erkenntnisse gewonnen werden, wie denn die Wohnung der besuchten Eltern aussieht oder wo und wie das neu geborene Kind untergebracht ist. Der vom Jugendamt als Service gedachte Besuch hat in dieser Kehrseite den Charakter eines Grundrechtseingriffs. Beeinträchtigt wird das Grundrecht auf Unverletzlichkeit der Wohnung und das Elterngrundrecht. Dies erfordert eine ausreichende Rechtsgrundlage, dies gilt auch dann, wenn es sich bei einem ersten Hausbesuch lediglich um ein reines Beratungsgespräch handelt.

Für die Durchführung eines Hausbesuchs besteht jedoch keine ausreichende gesetzliche Rechtsgrundlage. Ein Hausbesuch ist nur zulässig, wenn die Eltern nach ausreichender Information vor einem solchen Hausbesuch gemäß § 67 b SGB X ausdrücklich, freiwillig und schriftlich gegenüber dem Jugendamt einwilligen. Aus dem Gebot der Schriftform folgt, dass bloßes Schweigen der Eltern gegenüber dem Jugendamt dafür nicht reicht. Es genügt nach meiner Auffassung auch nicht, die Einwilligung an der Haustüre der Eltern einzuholen, weil hier nicht mehr in jedem Fall die Freiwilligkeit der Einwilligung unterstellt werden kann.

Ich habe - auch im sozialpolitischen Ausschuss des Bayerischen Landtags - deutlich gemacht, dass eine entsprechende gesetzliche Regelung jedenfalls sicherstellen müsste, dass die Eltern sich freiwillig für oder gegen einen Hausbesuch entscheiden könnten. Insbesondere dürfte eine Verweigerung eines Hausbesuchs nicht vermerkt werden oder andere Sanktionen zur Folge haben.

8.2 Vorlage eines ärztlichen Untersuchungsbogens durch Tagesbetreuungspersonen

Ein Jugendamt hat von Tagesmüttern und Tagesvätern im Rahmen der Erlaubnisprüfung nach § 43 SGB VIII verlangt, dass jede Tagesbetreuungsperson zum Zweck des Nachweises der persönlichen Eignung einen ausgefüllten und vom Arzt unterschriebenen "Ärztlichen Untersuchungsbogen" vorlegen müsse. In dem vom Arzt auszufüllenden Untersuchungsbogen war vorgesehen, Angaben über die Tagesbetreuungsperson zu schwerwiegenden, vor allem ansteckenden oder chronischen Erkrankungen, körperlichen und psychischen Beeinträchtigungen, Klinikaufenthalten, notwendigen Medikamenten, zum Gebrauch von Nikotin, Alkohol und Drogen und zu derzeitigen und weiteren Behandlungen zu machen. Abschließend sollte der Arzt dazu Stellung nehmen, ob keine Bedenken gegen die Tätigkeit als Betreuungsperson bzw. welche Bedenken hinsichtlich der Eignung als Tagesbetreuungsperson bestehen.

Ich bin zu dem Ergebnis gelangt, dass das Jugendamt nach den Vorschriften des SGB VIII eine Datenerhebungsbefugnis hat, weil die Vorlage eines ärztlichen Untersuchungsbogens im Rahmen der Eignungsprüfung nach § 43 Abs. 2 SGB VIII erforderlich sein kann. Eine solche Erhebungsbefugnis genügt jedoch nicht, um eine Vorlagepflicht für die betroffenen Tagesbetreuungspersonen zu begründen. Erforderlich sind vielmehr auch entsprechende Mitwirkungs- oder Auskunftspflichten von Tagesbetreuungspersonen, die dem Gesetz nicht zu entnehmen sind. Deshalb sind die Tagesbetreuungspersonen auf die Freiwilligkeit ihrer Angaben hinzuweisen.

§ 67 a Abs. 3 Satz 3 SGB X
Werden Sozialdaten beim Betroffenen auf Grund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, ist der Betroffene hierauf sowie auf die Rechtsvorschrift, die zur Auskunft verpflichtet, und die Folgen der Verweigerung von Angaben, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen.

Ich habe daher gebeten, in einem Anschreiben an die Tagesmütter und Tagesväter den Hinweis auf die Freiwilligkeit der Abgabe eines ärztlichen Untersuchungsbogens aufzunehmen. Vorsorglich habe ich darauf hingewiesen, dass eine Erlaubnis zur Kindertagespflege nicht deshalb vom Jugendamt versagt werden könne, weil kein ärztlicher Untersuchungsbogen vorgelegt werde. Andernfalls würde "durch die Hintertür" doch eine Mitwirkungspflicht eingeführt werden, die gerade nicht vorgesehen sei. Hierauf soll ebenfalls hingewiesen werden.

§ 43 SGB VIII (Erlaubnis zur Kindertagespflege)
(1) Eine Person, die ein Kind oder mehrere Kinder außerhalb des Haushalts des Erziehungsberechtigten während eines Teils des Tages und mehr als 15 Stunden wöchentlich gegen Entgelt länger als drei Monate betreuen will, bedarf der Erlaubnis.
(2) Die Erlaubnis ist zu erteilen, wenn die Person für die Kindertagespflege geeignet ist. Geeignet im Sinne des Satzes 1 sind Personen, die
1. sich durch ihre Persönlichkeit, Sachkompetenz und Kooperationsbereitschaft mit Erziehungsberechtigten und anderen Tagespflegepersonen auszeichnen und
2. über kindgerechte Räumlichkeiten verfügen.

Sie sollen über vertiefte Kenntnisse hinsichtlich der Anforderungen der Kindertagespflege verfügen, die sie in qualifizierten Lehrgängen erworben oder in anderer Weise nachgewiesen haben …

8.3 Überprüfung von Laborabrechnungen durch ein "Kompetenzzentrum Labor" bei der Kassenärztlichen Vereinigung Bayerns

Im Bereich der Kassenärztlichen Vereinigungen war im Berichtszeitraum eine bislang nicht zu beobachtende Entwicklung auszumachen, die dazu führen könnte, dass eine Konzentration von Aufgaben Kassenärztlicher Vereinigungen auf eine Kassenärztliche Vereinigung stattfände. Die Kassenärztlichen Vereinigungen erwarten sich davon insbesondere Kosteneinsparungen und eine Steigerung der Einheitlichkeit der Verwaltungspraxis aller Kassenärztlichen Vereinigungen. Aus datenschutzrechtlicher Sicht habe ich erhebliche Bedenken gegen eine solche Konzentration von Aufgaben, weil diese eine Ansammlung von Sozialdaten aller Kassenärztlichen Vereinigungen der Länder bei einer Kassenärztlichen Vereinigung zur Folge haben könnte. Die Datenschutzbeauftragten des Bundes und der Länder teilen meine Auffassung.

Ein Beispiel ist die Errichtung eines "Kompetenzzentrums Labor" bei der Kassenärztlichen Vereinigung Bayerns. Ich habe von diesem Vorhaben durch eine Anfrage der Landesbeauftragten für Datenschutz und Informationsfreiheit der Freien Hansestadt Bremen erfahren. Darin wurde mir mitgeteilt, dass durch eine Eingabe eines medizinischen Labors bekannt geworden sei, dass die Kassenärztliche Vereinigung Bremen die Aufgabe der Überprüfung von Honorarabrechnungen ihrer Mitglieder auf Plausibilität und auf deren sachliche und rechnerische Richtigkeit auf die Kassenärztliche Vereinigung Bayerns übertragen habe.

Meine daraufhin erfolgte Prüfung bei der Kassenärztlichen Vereinigung Bayerns hat folgendes ergeben:

Die Kassenärztliche Bundesvereinigung und die Kassenärztlichen Vereinigungen der Länder haben durch Vertrag die Arbeitsgemeinschaft "K(B)V-Kompetenzzentrum Labor" gegründet. Innerhalb dieser Arbeitsgemeinschaft wurde die Kassenärztliche Vereinigung Bayerns vertraglich mit der Durchführung der Aufgaben des "K(B)V-Kompetenzzentrums Labor" beauftragt. Aufgabe des "Kompetenzzentrum Labor" ist es insbesondere, andere Kassenärztliche Vereinigungen bei der Prüfung der Abrechnung von Laborleistungen zu unterstützen, beispielsweise die sachlich-rechnerische Richtigkeit zu prüfen, eine erweiterte Plausibilitätsprüfung vorzunehmen sowie bei Wirtschaftlichkeitsprüfungen gutachtlich tätig zu werden und sozialgerichtliche Verfahren zu begleiten. Die Kassenärztliche Vereinigung, die sich an das "Kompetenzzentrum Labor" wendet, sollte für das unmittelbare Verwaltungsverfahren verantwortlich bleiben.

Im Ergebnis habe ich festgestellt, dass die beabsichtigte Übertragung von Aufgaben der zuständigen Kassenärztlichen Vereinigungen auf das "Kompetenzzentrum Labor" bei der Kassenärztlichen Vereinigung Bayerns nicht mit den gesetzlichen Vorschriften des Sozialgesetzbuchs vereinbar ist. Grundsätzlich ergibt sich die gesetzliche Erlaubnis für die Bildung einer Arbeitsgemeinschaft zur gemeinsamen Aufgabenwahrnehmung zwar aus § 77 Abs. 6 SGB V. In entsprechender Anwendung des § 94 Abs. 1 a SGB X können die Kassenärztlichen Vereinigungen und die Kassenärztliche Bundesvereinigung "insbesondere zur gegenseitigen Unterrichtung, Abstimmung, Koordinierung und Förderung der engen Zu-

sammenarbeit im Rahmen der ihnen gesetzlich übertragenen Aufgaben Arbeitsgemeinschaften bilden". Die genannten Zwecke (gegenseitige Unterrichtung, Abstimmung, Koordinierung und Förderung der engen Zusammenarbeit) lassen jedoch erkennen, dass solche Arbeitsgemeinschaften in erster Linie der Verbesserung des Zusammenwirkens der verschiedenen Stellen, hier der Kassenärztlichen Vereinigungen der Länder und des Bundes, dienen sollen, nicht aber der Aufgabenerledigung der an der Arbeitsgemeinschaft beteiligten Einrichtungen (siehe Hauck/Noftz, Sozialgesetzbuch SGB X, K § 94 Rdnr. 6). Daraus habe ich geschlossen, dass die Übertragung der Aufgabe "Plausibilitätsprüfung von Laborleistungen" auf die Arbeitsgemeinschaft, sowie die Einsetzung der Kassenärztlichen Vereinigung Bayerns als Kompetenzzentrum zur Erledigung der Aufgabe für andere Kassenärztliche Vereinigungen, nicht dem mit der Bildung einer Arbeitsgemeinschaft beabsichtigten gesetzlichen Zweck des § 94 Abs. 1 a SGB X entspricht, weil die eigentliche Aufgabenerledigung zwar durch gegenseitige Unterrichtung, Abstimmung, Koordinierung und Förderung der engen Zusammenarbeit durch die Arbeitsgemeinschaft optimiert werden kann, aber im Ergebnis nicht dazu führen darf, dass die Aufgabe durch die Arbeitsgemeinschaft selbst bzw. durch eine von der Arbeitsgemeinschaft bestimmte und an ihr beteiligte Einrichtung an Stelle der zuständigen Institution wahrgenommen wird.

Auch für eine wirksame Einzelbeauftragung der KVB durch eine Kassenärztliche Vereinigung fehlen die Voraussetzungen. Als Rechtsgrundlagen kommen § 88 SGB X (Funktionsübertragung) oder § 80 SGB X (Auftragsdatenverarbeitung) in Betracht.

a) Die Voraussetzungen für eine Funktionsübertragung nach § 88 SGB X liegen jedoch nicht vor. Zum einen haben die KVB und die KVHB im Rahmen des Pilotprojekts eine "Vereinbarung über die Auftragsdatenverarbeitung nach § 80 SGB X" getroffen und eine Funktionsübertragung auf die KVB ausdrücklich ausgeschlossen. Zum anderen setzt eine unmittelbare Anwendung des § 88 Abs. 1 Satz 1 SGB X eine Funktionsübertragung durch einen "Leistungsträger" voraus. Die Kassenärztlichen Vereinigungen sind jedoch keine Leistungsträger gemäß § 12 SGB I (vgl. Hauck/Noftz, Sozialgesetzbuch X, K § 88 Rdnr. 15,18). Darüber hinaus müsste die Aufgabe durch die KVB nicht nur durchgeführt werden, sondern sie müsste nach außen auch die Verantwortung tragen; hier sollte jedoch die Verantwortung bei der beauftragenden Stelle bleiben.

   § 88 SGB X (Auftrag)
   (1) Ein Leistungsträger (Auftraggeber) kann ihm obliegende Aufgaben durch einen anderen Leistungsträger oder seinen Verband (Beauftragter) mit dessen Zustimmung wahrnehmen lassen, wenn dies
   1. wegen des sachlichen Zusammenhangs der Aufgaben vom Auftraggeber und Beauftragten,
   2. zur Durchführung der Aufgaben und
   3. im wohlverstandenen Interesse der Betroffenen zweckmäßig ist …

b) Die Regelungen zur Auftragsdatenverarbeitung sind hier ebenfalls nicht einschlägig. Eine Auftragsdatenverarbeitung nach § 80 SGB X setzt voraus, dass die beauftragte Stelle lediglich Hilfsfunktionen zur Erfüllung der Aufgaben des verantwortlichen Auftraggebers leistet (siehe Hauck/Noftz, Sozialgesetzbuch X, K § 80 Rdnr. 20). Die beauftragende KV soll zwar nach der vertraglichen Regelung weiterhin für das unmittelbare Verwaltungsverfahren verantwortlich bleiben, die KVB übernimmt aber nicht nur

Unterstützungsarbeiten für die beauftragende Kassenärztliche Vereinigung in deren Auftrag, sondern soll maßgeblich die Laborprüfungen durchführen, wie sich aus den angebotenen Leistungspaketen der Broschüre der KVB ergibt.

c) Im Ergebnis liegt hier weder eine Funktionsübertragung noch eine Auftragsdatenverarbeitung vor. Die Konstellation, dass eine Kassenärztliche Vereinigung eine ihr obliegende Aufgabe zur Erledigung auf eine andere Kassenärztliche Vereinigung überträgt, aber die rechtliche Verantwortung behält, sieht die gesetzliche Systematik des SGB V und SGB X derzeit nicht vor. Es ist darüber hinaus grundsätzlich zweifelhaft, ob der Gesetzgeber eine Spezialisierung der Kassenärztlichen Vereinigungen zulassen wollte, mit der Folge, dass ein Kompetenzzentrum eine bestimmte Aufgabe für alle anderen Kassenärztlichen Vereinigungen erfüllen soll. Dies würde bedeuten, dass bei der grundsätzlich unzuständigen Kassenärztlichen Vereinigung versicherten- und arztbezogene Daten von allen Kassenärztlichen Vereinigungen erhoben, verarbeitet und genutzt würden. Dies würde wohl alle gesetzlich Versicherten und Vertragsärzte betreffen, somit mehr als 70 Millionen Bundesbürger. Da das Kompetenzzentrum Labor wohl nur ein erstes Beispiel für eine Spezialisierung einer Kassenärztlichen Vereinigung wäre, müsste damit gerechnet werden, dass künftig Sozialdaten den Bereich der eigentlich zuständigen Kassenärztlichen Vereinigung verlassen und bei der beauftragten Kassenärztlichen Vereinigung gebündelt verwertet werden würden.

Ich habe die Kassenärztliche Vereinigung Bayerns deshalb aufgefordert, keine Abrechnungsdaten von anderen Kassenärztlichen Vereinigungen mehr zu erheben, verarbeiten oder zu nutzen und zu diesem Zweck gespeicherte Abrechnungsdaten aus dem Zuständigkeitsbereich anderer Kassenärztlicher Vereinigungen umgehend zu löschen.

Die immer häufiger zu beobachtende Tendenz zur Zentralisierung von Aufgaben und von personenbezogenen Daten im Bereich der Kassenärztlichen Vereinigungen ist aus datenschutzrechtlicher Sicht besorgniserregend. Ich sehe es deshalb als meine vordringliche Aufgabe, hierauf ein besonderes Augenmerk zu legen und diese Entwicklung kritisch zu verfolgen.

8.4 Elektronische Dokumentation und Abrechnung von Notarzteinsätzen ("emDoc")

Ich habe die zwischen Notärzten in Bayern und der Kassenärztlichen Vereinigung Bayerns öffentlich ausgetragene Auseinandersetzung über die elektronische Dokumentation und Abrechnung von Notarzteinsätzen zum Anlass für eine Überprüfung des Konzepts "emDoc" bei der KVB genommen.

Das Bayerische Rettungsdienstgesetz verpflichtet die Notärzte in Bayern, Einsätze und die dabei getroffenen aufgabenbezogenen Feststellungen und Maßnahmen zu dokumentieren. Diese Dokumentation hat nach einheitlichen Grundsätzen zu erfolgen, um eine bayernweit einheitliche Auswertung für Zwecke der Bedarfsfeststellung, für das Qualitätsmanagement, für die Weiterentwicklung des Rettungsdienstes und zur notfallmedizinischen Forschung zu ermöglichen. Die KVB hat hingegen die Aufgabe, die Versorgung von Notfallpatienten sicherzustellen.

Vor diesem Hintergrund hat die KVB Anfang Januar 2010 die elektronische Dokumentation und Abrechnung von Notarzteinsätzen eingeführt. Die Notärzte werden danach verpflichtet, der KVB die personenbezogenen Dokumentationen über ein Online-Portal zur Verfügung zu stellen.

Dagegen haben Notärzte datenschutzrechtliche Bedenken geäußert, weil sie durch die Übermittlung der Daten eines Notarzteinsatzes ohne ausdrückliches Einverständnis von Betroffenen insbesondere das Patientengeheimnis und die ärztliche Schweigepflicht gefährdet sahen. Zudem wurde die Erforderlichkeit des Umfangs der angeforderten Daten in Frage gestellt.

Das Ergebnis meiner rechtlichen Prüfung war, dass nach dem Bayerischen Rettungsdienstgesetz Arzt- und Patientendaten sowie nichtärztliche Personaldaten in den Notarzteinsatz-Dokumentationen im erforderlichen Umfang durch die KVB personenbezogen erhoben und gespeichert werden dürfen. Die KVB hat die Erforderlichkeit des Umfangs der zu meldenden Daten nachvollziehbar begründet. Die tatsächliche Notwendigkeit der Daten kann allerdings erst anhand von praktischen Fällen nachhaltig überprüft werden. Deshalb konnte ich insoweit nur eine Plausibilitätsprüfung vornehmen und habe mir vorbehalten, ggf. nachträglich eine Anpassung des Datenumfangs zu fordern.

Art. 46 Bayerisches Rettungsdienstgesetz (Dokumentation)
(1) Das im Rettungsdienst mitwirkende ärztliche und nichtärztliche Personal ist verpflichtet, Einsätze und die dabei getroffenen aufgabenbezogenen Feststellungen und Maßnahmen zu dokumentieren. …
(2) Die Unternehmer, die Durchführenden des Rettungsdienstes, die Kassenärztliche Vereinigung Bayerns und die mit der Sicherstellung der Mitwirkung von Verlegungsärzten Beauftragten haben die Einhaltung der Dokumentationsverpflichtung nach Abs. 1 gegenüber den in ihrem Einwirkungsbereich tätigen Personen durchzusetzen, die Dokumentation fortdauernd auszuwerten und zusammen mit den Ergebnissen der Auswertung als Grundlage des Qualitätsmanagements nach Art. 45 zu verwenden. Die in Abs. 1 genannten Personen sind verpflichtet, ihnen ihre Dokumentation zur Verfügung zu stellen.
(3) Die Dokumentation hat nach einheitlichen Grundsätzen zu erfolgen, um eine bayernweit einheitliche Auswertung für Zwecke der Bedarfsfeststellung, für die Nutzung zum Qualitätsmanagement, für die Weiterentwicklung des Rettungsdienstes und zur notfallmedizinischen Forschung zu ermöglichen …

Art. 47 Bayerisches Rettungsdienstgesetz (Datenschutz)
(1) Personenbezogene Daten dürfen durch die in Art. 46 Abs. 1 und 2 genannten Personen und Stellen erhoben, verarbeitet oder genutzt werden, wenn dies zur Erfüllung rettungsdienstlicher Aufgaben, insbesondere
1. …,
2. zur Abwicklung des Einsatzes, insbesondere der Abrechnung der erbrachten Leistungen,
3. …,
oder für Zwecke der wissenschaftlichen notfallmedizinischen Forschung erforderlich ist oder die betroffene Person eingewilligt hat.

Zu technischen Aspekten meiner Prüfung verweise ich auf Nr. 2.2.11.

8.5 Bereitstellung eines Internetdienstes "Arztsuche"

Ein Arzt hatte sich wegen der Veröffentlichung seiner personenbezogenen Daten auf der Homepage der KVB im Rahmen einer "Arztsuche" an mich gewandt. Er habe der Veröffentlichung dieser Daten nicht zugestimmt. Insbesondere seien dabei auch Daten wie beispielsweise seine lebenslang zugeordnete Arztnummer (LANR) veröffentlicht, die von keinem allgemeinen Interesse seien und nicht öffentlich im Internet zugänglich sein sollen.

Auf meine Bitte um Stellungnahme zur dortigen "Arztsuche" hat mir die KVB mitgeteilt, sie habe bereits vor Jahren eine "Arztsuche" im Internet über die Homepage der KVB implementiert. Über die Einrichtung der Arztsuche seien die zu dieser Zeit niedergelassenen Vertragsärzte durch eine Veröffentlichung in einem der Landesrundschreiben der KVB informiert worden. Dabei seien sie darauf hingewiesen worden, dass sie einer Veröffentlichung widersprechen können.

Ärzte, die erst nach dieser Veröffentlichung zur vertragsärztlichen Versorgung zugelassen wurden, hätten zusammen mit einem "Erstausstattungspaket" ein Informationsblatt über die Veröffentlichung arztbezogener Daten im Internetauftritt der KVB erhalten, u.a. mit dem Hinweis der Widerspruchsmöglichkeit.

Später habe die KVB dann im Zusammenhang mit Anpassungen bei der Arztsuche ein neues Informationsblatt und eine Einwilligungserklärung formuliert und u.a. im "Erstausstattungspaket" bereit gestellt. Auch hierüber habe die KVB u.a. in der Mitgliederzeitschrift informiert.

Ich habe im Hinblick auf diese "Arztsuche" der KVB im Wesentlichen folgende Punkte bemängelt:

- Eine Einwilligungserklärung ist erst nach einem bestimmten Zeitpunkt von niedergelassenen Vertragsärzten eingeholt worden. Die Einräumung einer Widerspruchsmöglichkeit für die anderen Vertragsärzte ist rechtlich nicht mit einer Einwilligung gleichzusetzen.
- Eine Einwilligung ist nur in die Veröffentlichung aller von der KVB vorgesehenen Daten möglich, also entweder in diese Veröffentlichung oder keine. Darunter sind auch Daten, die keinen ersichtlichen Bezug zu einer allgemeinen Information über den Arzt und dessen Kontaktdaten haben. Dies betrifft etwa die lebenslang zugeordnete Arztnummer (LANR).

Nach entsprechendem Schriftwechsel hat die KVB die von mir kritisch gesehenen Punkte aufgegriffen und das Konzept der "Arztsuche" entsprechend angepasst.

Das neue Konzept sieht vor, dass von allen Vertragsärzten, deren Daten im Rahmen der "Arztsuche" der KVB veröffentlicht werden, Einwilligungserklärungen eingeholt werden. Zudem soll dann neben der Veröffentlichung eines verkleinerten Datensatzes an Grunddaten (Basiskontaktdaten, fachliche Informationen und sonstige Informationen wie Sprechzeiten) für die Vertragsärzte auch die Möglichkeit bestehen, weitere Zusatzdaten (u.a. lebenslange Arztnummer, persönliche E-Mail-Adresse, Fremdsprachen) gesondert freizugeben. Letzteres ist aber keine Voraussetzung für die Veröffentlichung der Grunddaten.

Die Einholung der Einwilligungen soll noch im Jahr 2010 anlaufen. Nach einer Übergangsphase sollen dann die (Basis-)Daten derjenigen Vertragsärzte gesperrt werden, die keine Einwilligung abgegeben haben.

8.6 Erinnerung an Impfungstermin (Impf-Recall)

Die Kassenärztliche Vereinigung Bayerns hat mich um Bewertung eines Pilotprojekts "Masern-Impferinnerungsservice - Wirksamkeitsnachweis" gebeten. Das Pilotprojekt sah vor, dass die KVB im Namen und Auftrag eines teilnehmenden Arztes dessen Patienten, die bereits eine erste Masernimpfung erhalten haben und eine zweite Masernimpfung erhalten sollen, mittels Erinnerungsschreiben per Post an den Termin der zweiten Impfung erinnert.

Der teilnehmende Arzt sollte die KVB beauftragen, die übermittelten Patientendaten zu analysieren, um die Patienten zu identifizieren, bei denen die 2. Masernimpfung noch aussteht und die im Rahmen des Projektes an die Impfung erinnert werden sollen. Danach sollte der Arzt eine Aufstellung der identifizierten Patienten erhalten und eine Liste mit den Patienten an die KVB zurücksenden, die angeschrieben werden sollten. Die KVB hätte dann den Versand der Impferinnerung an die ausgewählten Patienten organisiert.

Ich habe die Auffassung vertreten, dass für die Weitergabe von Patientendaten durch einen Arzt und die Nutzung dieser Gesundheitsdaten durch die KVB eine Einwilligung der betroffenen Patienten erforderlich ist.

Gesetzliche Bestimmungen, die das Pilotprojekt ohne ausdrückliche Einwilligung der Betroffenen zugelassen hätten, habe ich weder im Sozialgesetzbuch - Fünftes Buch - (SGB V) noch im Bundesdatenschutzgesetz (BDSG) oder in sonstigen Rechtsvorschriften erkennen können:

- Nach meiner Einschätzung kann die Weitergabe von Gesundheitsdaten durch einen Arzt an die KVB und die Nutzung dieser Patientendaten nicht auf die Vereinbarung eines Auftragsdatenverhältnisses nach § 11 BDSG oder § 80 Zehntes Sozialgesetzbuch (SGB X) gestützt werden, da ansonsten der Schutz sensibler Gesundheitsdaten der Patienten, der insbesondere durch die ärztliche Schweigepflicht nach § 203 Abs. 1 Strafgesetzbuch (StGB) sichergestellt werden soll, durch eine bloße Vereinbarung Dritter ausgehebelt und so umgangen werden könnte. Aus Sicht des Patienten würde das eine Vereinbarung zu seinen Lasten darstellen, die dazu führt, dass seine von einem Arzt zu Behandlungszwecken erhobenen Gesundheitsdaten, insbesondere auch für andere Zwecke, vom Arzt an Dritte weitergegeben werden könnten, ohne seine Einwilligung einholen zu müssen.

- Darüber hinaus können die zu Abrechnungszwecken vom Arzt an die KVB übermittelten Patientendaten nicht ohne Einwilligung der Patienten für andere Zwecke, hier für das Pilotprojekt "Masern-Impferinnerungsservice" genutzt werden. Es wurde insoweit vorgetragen, dass § 75 Abs. 6 SGB V eine Rechtsvorschrift sei, die eine solche Zweckänderung zulassen würde.

  § 75 Abs. 6 SGB V:
  Mit Zustimmung der Aufsichtsbehörden können die Kassenärztlichen Vereinigungen und Kassenärztlichen Bundesvereinigungen weitere Aufgaben

der ärztlichen Versorgung insbesondere für andere Träger der Sozialversicherung übernehmen.

Nach meiner Auffassung wird ein Impferinnerungsservice der KVB nicht von dieser Vorschrift gedeckt. Nach ihr sollte die KVB nicht damit beauftragt werden, in den ärztlichen Aufgabenbereich fallende Tätigkeiten anstelle von Vertragsärzten selbst auszuführen, z.B. die Erinnerung von Patienten an eine ausstehende Impfung. Die Vorschrift ist im Zusammenhang mit der Sicherstellungs- und Gewährleistungspflicht der KVB für die vertragsärztliche Versorgung zu beurteilen. Danach hat die KVB den Auftrag, die ärztliche Versorgung insbesondere mit Hilfe von zugelassenen Ärzten zu organisieren. Eine Übernahme der originären Arztaufgaben durch die KVB ist damit jedoch nicht verbunden.

Ich habe die KVB darauf hingewiesen, dass eine solche beabsichtigte Dienstleistung für Ärzte, die durch den Gesetzgeber nicht vorgesehen ist, nur aufgrund einer vorherigen Einwilligung der betroffenen Patienten zulässig ist.

8.7 Datenübermittlung an Taxiunternehmen im Zusammenhang mit vertragsärztlichem Bereitschaftsdienst

Ich bin gebeten worden, die Vorgehensweise der Kassenärztlichen Vereinigung Bayerns bei der Vermittlung von ärztlichen Hausbesuchen im Rahmen des vertragsärztlichen Bereitschaftsdienstes datenschutzrechtlich zu beurteilen.

Im Normalfall werden die Personalien des anrufenden Patienten, dessen Wohn- bzw. Aufenthaltsort und Angaben zum medizinischen Meldebild von den Vermittlungs- und Beratungszentralen (VBZ) der KVB an den Dienst habenden Arzt telefonisch übermittelt. Dies begegnet keinen rechtlichen Bedenken, denn die KVB hat den gesetzlichen Auftrag, die vertragsärztliche Versorgung in Bayern sicherzustellen; dazu gehört auch die vertragsärztliche Versorgung zu den sprechstundenfreien Zeiten.

§ 75 Abs. 1 Satz 2 SGB V
Die Sicherstellung umfasst auch die vertragsärztliche Versorgung zu den sprechstundenfreien Zeiten (Notdienst), nicht jedoch die notärztliche Versorgung im Rahmen des Rettungsdienstes, soweit Landesrecht nichts anderes bestimmt.

Zur Organisation dieses Notdienstes ist die Erhebung und Weitergabe von Patientendaten an den Dienst habenden Arzt erforderlich. Entsprechende Datenerhebungs- und -übermittlungsbefugnisse enthält § 285 SGB V:

§ 285 Abs. 1 Nr. 2, Abs. 2, Abs. 3 Satz 1 SGB V
(1) Die Kassenärztlichen Vereinigungen dürfen Einzelangaben über die persönlichen und sachlichen Verhältnisse der Ärzte nur erheben und speichern, soweit dies zur Erfüllung der folgenden Aufgaben erforderlich ist: …
2. Sicherstellung und Vergütung der vertragsärztlichen Versorgung einschließlich der Überprüfung der Zulässigkeit und Richtigkeit der Abrechnung, …
(2) Einzelangaben über die persönlichen und sachlichen Verhältnisse der Versicherten dürfen die Kassenärztlichen Vereinigungen nur erheben und speichern, soweit dies zur Erfüllung der in Abs. 1 Nr. 2 … genannten Aufgaben erforderlich ist.

(3) Die rechtmäßig erhobenen und gespeicherten Sozialdaten dürfen nur für die Zwecke der Aufgaben nach Abs. 1 in dem jeweils erforderlichen Umfang verarbeitet oder genutzt werden, für andere Zwecke, soweit dies durch Rechtsvorschriften des Sozialgesetzbuchs angeordnet oder erlaubt ist ...

Diese Rechtsgrundlagen sind auch für die Organisation von ärztlichen Hausbesuchen in Ballungsräumen anwendbar. Die Besonderheit besteht diesbezüglich darin, dass die Dienst habenden Ärzte aufgrund der wesentlich häufigeren Anforderungen von Hausbesuchen, mangelnder Ortskenntnisse und Parkmöglichkeiten und zur organisatorischen Entlastung durch gewerbliche Fahrdienste (Taxiunternehmen) unterstützt werden. Dabei werden die Patientenangaben häufig von den jeweiligen Fahrern entgegengenommen und von dort an den Dienst habenden Arzt weitergegeben. Ich habe der KVB mitgeteilt, dass die Zwischenschaltung von Taxizentrale und Taxifahrern, die in dem rechtlichen System des ärztlichen Bereitschaftsdienstes nicht vorgesehen sind, rechtlichen Bedenken begegnet:

Nach § 10 Abs. 3 Buchst. b) der Bereitschaftsdienstordnung der Kassenärztlichen Vereinigung Bayerns (BDO-KVB) vom April 2008 muss der Dienst habende Arzt während der gesamten Dienstzeit innerhalb seines Bereitschaftsdienstbereiches, in dem er als Dienst habender Arzt eingeteilt ist, anwesend und ständig erreichbar sein. Er soll zur Sicherstellung seiner persönlichen Erreichbarkeit ein Mobiltelefon mit sich führen. Eine Weitergabe des (Bereitschaftsdienst-) Handys des Dienst habenden Arztes an einen Taxifahrer ist mit dieser Regelung nicht vereinbar. Die Formulierung "Der Diensthabende ist verpflichtet, die ihm von der VBZ mitgeteilten Behandlungsfälle ..." in § 10 Abs. 3 Buchst. d) BDO-KVB lässt den Schluss zu, dass der Dienst habende Arzt für die VBZ unmittelbar und ständig erreichbar sein muss. Meines Erachtens muss deshalb die Information über einen Patienten von der VBZ unmittelbar an den Dienst habenden Arzt übermittelt werden, nicht auf einem Umweg über die Taxizentrale oder den Taxifahrer an den Arzt. Eine Datenübermittlung von der VBZ mittels Taxizentrale und Taxifahrer als Auftragnehmer bzw. Unterauftragnehmer (§ 80 SGB X) an den Dienst habenden Arzt wäre nach meiner Auffassung eine unzulässige Umgehung der genannten Bestimmung.

Nur sofern die Regelung des § 10 Abs. 3 Buchst. b) BDO-KVB nicht bestehen würde, käme gegebenenfalls eine Entgegennahme und Weitergabe der patientenbezogenen Einsatzdaten durch eine Taxizentrale bzw. Taxifahrer im Rahmen einer Auftragsdatenverarbeitung in Betracht. Dazu müssten jedoch insbesondere die umfangreichen Voraussetzungen des § 80 SGB X erfüllt sein.

Einer daraufhin vorgenommenen Änderung bzw. Ergänzung der Bereitschaftsdienstordnung der KVB, die eine Beteiligung von Fahrdiensten ermöglicht, habe ich nicht widersprochen. Bei der Vereinbarung von Auftragsverhältnissen werde ich beratend zur Seite stehen.

8.8 Pflegeservice Bayern

Der Medizinische Dienst der Krankenversicherung in Bayern (MDK Bayern) betreibt im Auftrag der gesetzlichen Pflegekassen in Bayern den "Pflegeservice Bayern", eine kostenlose Rufnummer für Pflegebedürftige. Der Pflegeservice Bayern dient als erste Informations- und Anlaufstelle für alle gesetzlich Versicherten zu Fragen rund um das Thema Pflege. Hauptaufgaben sind die Unterstüt-

zung beim Verbleib in der Häuslichkeit, der Umgang mit Überforderung, die Aufnahme und Weiterleitung von Beschwerden, eine Fachinformation mit dem Ziel der Verbesserung der Lebensqualität, die Verbesserung der Rahmenbedingungen durch Aufzeigen von Hilfsangeboten, sowie das Vorbeugen von Missständen bei nicht sichergestellter Pflege. Vorrangiges Ziel ist es, die Selbstständigkeit und die Lebensqualität der Pflegebedürftigen zu erhalten, zu fördern und zu verbessern.

Ich bin durch Nutzer des Pflegeservice Bayern darauf aufmerksam gemacht worden, dass erst am Ende des Telefonats und eher beiläufig mitgeteilt werde, dass das Gespräch zur Sicherheit der Anrufer aufgezeichnet worden sei. Nur wenn der Anrufer einer Aufzeichnung ausdrücklich widerspreche, werde das Gespräch gelöscht.

Auf meine Intervention hin, dass das von Art. 2 Abs. 1 und Art. 1 Abs. 1 Grundgesetz geschützte Recht am gesprochenen Wort berührt sei und zumindest am Anfang des Gesprächs auf die Aufzeichnung hingewiesen werden müsse sowie eine Aufzeichnung nur nach ausdrücklicher Einwilligung durch den Anrufer zulässig sei, hat sich der MDK Bayern dazu bereit erklärt, auf die Aufzeichnung gänzlich zu verzichten, da insbesondere zu befürchten sei, dass ein Hinweis auf die Aufzeichnungsmöglichkeit zu Beginn des Beratungsgesprächs bei einigen Ratsuchenden zum Abbruch des Gesprächs führen könnte. Darüber hinaus sei noch kein Fall aufgetreten, der einen Abruf der Aufzeichnung nötig gemacht habe - dies deutet darauf hin, dass insoweit auch keine Erforderlichkeit der Aufzeichnung von Gesprächen gegeben sei.

8.9 Unzulässige Datenübermittlung durch einen Rentenversicherungsträger

Rentenversicherungsträger führen im Rahmen ihrer Zuständigkeit Betriebsprüfungen durch. In einer solchen Angelegenheit hatte sich ein Bevollmächtigter des betroffenen Betriebsinhabers mit einem Widerspruchs- und Beschwerdeschreiben an den zuständigen Rentenversicherungsträger gewandt. Dieser Rentenversicherungsträger hat sein Antwortschreiben an den Bevollmächtigten auch in Abdruck an dessen Vorgesetzten bei dessen Arbeitgeber - ein anderer Rentenversicherungsträger - gesandt und dies gegenüber dem Bevollmächtigten im Schreiben so begründet: "…, da ich Inhalt und Diktion Ihres Schreibens an mich nicht für angemessen halte, auch wenn Sie hier nicht dienstlich, sondern privat als Bevollmächtigter gehandelt haben." Der Betroffene hat sich darauf hin bei mir über dieses Vorgehen beschwert. Und das zu Recht.

Auch die Tatsache, dass ein Bediensteter eines Rentenversicherungsträgers privat als Bevollmächtigter ein Widerspruchs- und Beschwerdeschreiben an einen anderen Rentenversicherungsträger gerichtet hat, unterfällt grundsätzlich dem Sozialdatenschutz nach § 35 Abs. 1 SGB I, § 67 Abs. 1 Satz 1 SGB X.

§ 35 Abs. 1 Satz 1 SGB I
Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Abs. 1 Zehntes Buch) von den Leistungsträgern nicht unbefugt erhoben, verarbeitet oder genutzt werden (Sozialgeheimnis) …

§ 67 Abs. 1 Satz 1 SGB X
Sozialdaten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener), die von

einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch erhoben, verarbeitet oder genutzt werden.

Dies gilt zudem auch für die weiteren Inhalte des Schreibens, etwa die enthaltenen (auch personenbezogenen) Daten zum zugrundeliegenden Verfahren. Auch auf wiederholte Nachfrage hat mir der Rentenversicherungsträger keine Rechtsgrundlage für die erfolgte Mitteilung an den Vorgesetzten des Betroffenen benannt. Weder die in der Antwort angeführte Begründung, dass das Schreiben nach Inhalt und Diktion nicht für angemessen gehalten wird, noch die weiteren im Rahmen einer Stellungnahme erfolgten Ausführungen können die Bennennung einer Rechtsgrundlage und die Darlegung des Vorliegens der entsprechenden Tatbestandsvoraussetzungen ersetzen. Den Verstoß des Rentenversicherungsträgers gegen den Datenschutz habe ich beanstandet.

8.10 Antrag auf Betreuungsleistungen

Im Berichtszeitraum bin ich von einem ambulanten Pflegedienst auf ein Formular einer Pflegekasse aufmerksam gemacht worden, mit dem Versicherte Betreuungsleistungen zu beantragen haben. Der ambulante Pflegedienst hatte - offensichtlich anders als die Pflegekasse - erkannt, dass das Antragsformular nicht den gesetzlichen Vorgaben entspricht.

Die Pflegekasse hatte im Antragsformular eine Einwilligungserklärung von den Versicherten eingefordert, dass die Pflegekasse vom behandelnden Arzt, von Krankenhäusern und den betreuenden Pflegepersonen ärztliche Unterlagen, Auskünfte sowie in deren Besitz befindliche Fremdbefunde anfordern kann, soweit diese für die Begutachtung und Entscheidung über den Antrag auf Betreuungsleistungen erforderlich sind. Die Einwilligung hat sich zudem ausdrücklich auf eine Einsichtnahme der Pflegekasse in diese Unterlagen (und eine Weiterleitung an den Medizinischen Dienst der Krankenversicherung -MDK-) bezogen. Weiterhin umfasste die Erklärung eine entsprechende Entbindung von der Schweigepflicht im Hinblick auf die genannten Stellen. Im Antragsformular hat die Pflegekasse außerdem auf Mitwirkungspflichten und die Möglichkeit von Nachteilen bzw. einer Ablehnung bei Verstoß gegen die Mitwirkungspflichten hingewiesen.

Zwar wird über die Leistung - auch der Höhe nach - von der Pflegekasse entschieden. Der Gesetzgeber hat in den hier maßgeblichen Regelungen gemäß § 45 b SGB XI allerdings zum Ausdruck gebracht, dass der MDK hier Leistungsvoraussetzungen zu ermitteln und zu beurteilen hat. Ich konnte daher hier keine Erforderlichkeit einer Einsichtnahme in die genannten Unterlagen durch die Pflegekasse erkennen. Auf meine Bitte um Stellungnahme hat mir die Pflegekasse mitgeteilt, dass der entsprechende Antrag zwischenzeitlich überarbeitet worden sei. Die Einwilligungserklärung sei für die Belange des MDK textlich angepasst und neu aufgelegt worden. Auch ein weiterer Fehler, auf den ich die Pflegekasse hingewiesen hatte, war nunmehr behoben worden: In der früheren Version war die "Unterschrift" oberhalb des Textes der Einwilligungserklärung vorgesehen. Eine unterschriebene Einwilligungserklärung läge bei einer solchen Formulargestaltung gar nicht vor.

Nach zweifacher Aufforderung änderte die Pflegekasse auch das bis dahin unverändert gebliebene im Internet zum Herunterladen vorgesehene Formular. Dann hat mir die Pflegekasse immerhin mitgeteilt, dass sie meine Schreiben "er-

neut" (?) zum Anlass genommen hat, alle Anträge auf Pflegeleistungen, die Online zur Verfügung stehen, mit den Formularen in Papierform abzugleichen und gegebenenfalls anzupassen.

Als Fazit bleibt festzuhalten, dass die Pflegekasse in mehrfacher Hinsicht kein gutes Bild abgegeben hat.

8.11 Jobcenter-Reform - Wechsel in der Zuständigkeit der Datenschutzkontrolle

Das Bundesverfassungsgericht hat die Zuständigkeit von Bundes- und Kommunalbehörden bei den Arbeitsgemeinschaften (ARGEn) im Bereich der Grundsicherung für Arbeitssuchende (Zweites Buch Sozialgesetzbuch - SGB II) für nicht mit der Verfassung der Bundesrepublik Deutschland vereinbar erklärt.

Der Bundesgesetzgeber hat daraufhin eine Neuorganisation der ARGEn vorgenommen, die eine erhebliche Auswirkung auf die Zuständigkeit bei der Datenschutzkontrolle der von der Agentur für Arbeit und den Kommunen gemeinsam getragenen gemeinsamen Einrichtungen (Jobcenter) hat. Mit dem 01.01.2011 ist ausschließlich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit für die datenschutzrechtliche Kontrolle der „gemeinsamen Einrichtungen“ (§ 44 b SGB II) zuständig (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Handbuch XVIII. 13). Durch die Neuregelung wird der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die nicht unerhebliche Anzahl an Beschwerden gegenüber Jobcentern, die bislang an die Landesbeauftragten für den Datenschutz herangetragen und dort geprüft worden sind, alleine bearbeiten müssen.

Allerdings wird durch die gesetzliche Neuregelung die Zuständigkeit der Landesbeauftragten für den Datenschutz im Bereich der Grundsicherung für Arbeitssuchende nicht gänzlich entfallen. Für die sogenannten Optionskommunen, die Leistungen des SGB II ohne Beteiligung der Agentur für Arbeit erbringen (§ 6 a SGB II), bleibt die Zuständigkeit der Landesbeauftragten für den Datenschutz bestehen (vgl. Wilde/Ehmann/Niese/Knoblauch, Bayerisches Datenschutzgesetz, Handbuch XVIII. 14). Meine Prüfungen werden sich deshalb im Bereich des SGB II künftig auf die sog. Optionskommunen in Bayern beschränken.

8.12 Mangelnde Unterstützung des Landesbeauftragten für den Datenschutz

Die Kooperationsbereitschaft der bislang meiner Zuständigkeit unterliegenden ARGEn ist regelmäßig gegeben. Diskussionspunkte sind normalerweise allenfalls inhaltliche Fragen.

Bei einer ARGE lag dies leider anders. Diese ARGE hat weder auf meine Anforderung einer Stellungnahme noch auf die folgende Mahnung reagiert. Auch eine weitere Mahnung unter Setzung einer Frist und dem Hinweis auf eine mögliche Beanstandung wegen Verstoß gegen die gesetzliche Pflicht, mir Auskünfte zu erteilen, ließ die ARGE unbeachtet.

Ich habe die ARGE daher beanstandet und dies dem Bayerischen Staatsministerium für Arbeit und Sozialordnung, Familie und Frauen mitgeteilt. Das Staatsministerium hat hierauf schnell und gezielt reagiert. In der Folge hat die ARGE dann

die angeforderte Stellungnahme abgegeben und sich für "die verspätete Beantwortung" meiner "Anfrage" entschuldigt. Warum die ARGE hier erst nach einer Beanstandung ihrer gesetzlichen Unterstützungspflicht nachgekommen ist, bleibt mir unerklärlich. Sie hat dabei - sogar trotz Hinweis und Fristsetzung - gegen ihre gesetzlichen Pflichten verstoßen und außer einem negativen Bild bei den Beteiligten nichts gewonnen.

Inhaltlich war die dann abgegebene Stellungnahme übrigens eher einfacher Art. Die ARGE musste sich letztlich nur zum vorgetragenen Sachverhalt äußern. Es hat sich im weiteren Verlauf herausgestellt, dass ein bestimmtes personenbezogenes Datum gerade nicht von der ARGE an einen Dritten weitergegeben worden ist. Die Angelegenheit wäre damit bei einer zeitnahen Stellungnahme ohne größeren Aufwand erledigt gewesen.

8.13 Weitergabe von Sozialdaten an eine Betriebskrankenkasse

Eine ARGE hat im Zusammenhang mit dem Verdacht auf Leistungsmissbrauch durch einen Leistungsempfänger insbesondere wegen der Inanspruchnahme einer Haushaltshilfe Sozialdaten des Leistungsempfängers an dessen Betriebskrankenkasse weitergegeben, um ggf. eine Strafanzeige gegen den Leistungsempfänger vorbereiten zu können.

Die Betriebskrankenkasse wurde insbesondere darüber informiert, dass der Leistungsempfänger wegen Leistungsmissbrauchs gegenüber der ARGE bereits von einem Amtsgericht zu 90 Tagessätzen verurteilt worden sei. Es wurde auch mitgeteilt, dass der Leistungsempfänger und seine Frau seit Jahren Leistungen nach dem SGB II bezögen und keiner Arbeit nachgingen. Ferner bestünde eine fast 1000-seitige Akte, weil der Leistungsempfänger gegen jede Entscheidung der ARGE in Widerspruch gehe und darüber hinaus auch die Sozialgerichte beschäftige.

Ich habe der ARGE dargelegt, dass Datenübermittlungen nur zulässig sind, wenn eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift im Sozialgesetzbuch vorliegt (§ 67 d Abs. 1 SGB X). Auch nach mehrmaliger Aufforderung konnte mir die ARGE keine entsprechende Rechtsgrundlage benennen. Sie hat sich lediglich dahingehend geäußert, dass die Daten im Zusammenhang mit der Bekämpfung von Leistungsmissbrauch übermittelt worden und für den Leistungsträger (Betriebskrankenkasse) erforderlich gewesen seien, um eine Strafanzeige stellen zu können. Insoweit könne nicht von einer Verletzung des Datenschutzes ausgegangen werden.

Als Rechtsgrundlage für die Datenübermittlungen an die Betriebskrankenkasse wäre allenfalls § 69 Abs. 1 Nr. 1 2. oder 3. Alternative SGB X in Betracht gekommen. Dies hätte vorausgesetzt, dass die Übermittlungen dieser Informationen über den Leistungsempfänger für die Erfüllung einer gesetzlichen Aufgabe der ARGE oder der Betriebskrankenkasse erforderlich gewesen wären. Auch wenn die Bekämpfung von Leistungsmissbrauch zu den Aufgaben von ARGE oder Krankenkasse im weiteren Sinne gerechnet werden kann, sind die von der ARGE übermittelten Sozialdaten des Leistungsempfängers nicht in dem erfolgten Umfang erforderlich gewesen, um einen eventuellen Leistungsmissbrauch des Leistungsempfängers zur Strafanzeige zu bringen. Es wäre allenfalls die Information erforderlich gewesen, dass bzw. ob der Leistungsempfänger Leistungen nach

dem SGB II und zeitgleich Leistungen für eine Haushaltshilfe erhalten habe. Insbesondere die Verurteilung des Leistungsempfängers in anderer Angelegenheit oder der Hinweis auf Widerspruchs- und Klageverfahren waren nicht erforderlich, um eine Strafanzeige wegen Verdacht auf Leistungsmissbrauch vorzubereiten.

Ich habe die ARGE beanstandet, weil sie Sozialdaten eines Leistungsempfängers in nicht erforderlichem Umfang und somit ohne ausreichende Rechtsgrundlage an eine Betriebskrankenkasse übermittelt hatte.

8.14 Lebensmittelgutscheine

Ein Leistungsbezieher hatte von der zuständigen ARGE Lebensmittelgutscheine erhalten. Er hat sich insbesondere dagegen gewandt, dass die Lebensmittelgutscheine mit seinem Namen, seiner Anschrift und seiner Personalausweisnummer personalisiert waren. Unter Vorlage seines Personalausweises und Aushändigung des Gutscheins konnte er dann bei bestimmten Händlern Lebensmittel ("ohne alkoholische Getränke") bis zum Gegenwert des Gutscheins einkaufen. Der Händler hat dann im Anschluss den Gutschein mit der ARGE abgerechnet. Der Betroffene hat geltend gemacht, es sei nicht erforderlich, die Lebensmittelgutscheine zu personalisieren. Der Händler erhalte so seinen Namen, seine Adresse und seine Personalausweisnummer zusammen mit der Information des Sozialleistungsbezugs. Zudem werde aufgrund der Gegenprüfung der Daten durch den Lebensmittelhändler anhand des vorzulegenden Ausweises auch bei anderen Kunden zusätzliche Aufmerksamkeit hierauf gelenkt.

Ich habe die ARGE daraufhin um Stellungnahme gebeten. Die ARGE hat sich zum einen auf Rechtsprechung berufen, nach der die Verfahrensweise zulässig sei. Der Betroffene hatte außerdem auch eine einstweilige Anordnung beim zuständigen Sozialgericht beantragt. Im Verlauf des Schriftwechsels mit der ARGE ergab sich, dass das im konkreten Fall angerufene Sozialgericht den Erlass einer einstweiligen Anordnung gegen die ARGE - auch aus inhaltlichen Gründen - abgelehnt hat.

ARGE und Sozialgericht argumentieren im Wesentlichen damit, dass nur auf diese Weise sichergestellt werden kann, dass nur der Berechtigte den Lebensmittelgutschein einlöst und eine effektive Missbrauchskontrolle erfolgen kann. Zudem sei der Händler über die Regelung in § 78 SGB X ebenfalls der Geheimhaltungspflicht unterworfen. Auch wird von der ARGE darauf hingewiesen, dass erst Verhaltenweisen des Betroffenen zu Minderungen der Leistungen und der Erbringung geldwerter Leistungen bzw. Sachleistungen in angemessenem Umfang geführt haben.

Ich vertrete hingegen die Auffassung, dass ein pauschales Verfahren der Ausgabe von personalisierten Lebensmittelgutscheinen nicht nötig ist. Bei der grundlegenden Verfahrensweise der Ausgabe von personalisierten Lebensmittelgutscheinen erfolgt keine auf den Einzelfall bezogene Prüfung der Erforderlichkeit der Personalisierung. In Fallgestaltungen des § 23 Abs. 2 SGB II wird bereits in den Tatbestandsvoraussetzungen daran angeknüpft, dass sich der jeweilige Leistungsempfänger als ungeeignet erweist, mit der Regelleistung seinen Bedarf zu decken.

§ 23 Abs. 2 SGB II
Solange sich der Hilfebedürftige, insbesondere bei Drogen- oder Alkoholabhängigkeit sowie im Falle unwirtschaftlichen Verhaltens, als ungeeignet erweist, mit der Regelleistung nach § 20 seinen Bedarf zu decken, kann die Regelleistung in voller Höhe oder anteilig in Form von Sachleistungen erbracht werden.

In solchen Fällen kann die grundlegende Erforderlichkeit einer Personalisierung begründet werden. Demgegenüber lässt das wie im vorliegenden Fall nach § 31 SGB II sanktionierte Verhalten nicht notwendigerweise auf eine Unzuverlässigkeit im Hinblick auf die eigene Bedarfsdeckung schließen. Ich halte daher die Personalisierung von Lebensmittelgutscheinen in den Fällen des § 31 Abs. 3 Satz 6 SGB II ("Bei einer Minderung des Arbeitslosengeldes II um mehr als 30 vom Hundert der nach § 20 maßgebenden Regelleistung kann der zuständige Träger in angemessenem Umfang ergänzende Sachleistungen oder geldwerte Leistungen erbringen") nur dann für erforderlich, wenn in der Person des Betroffenen spezifische Anhaltspunkte für eine missbräuchliche Verwendung nicht personalisierter Lebensmittelgutscheine vorliegen.

Zudem sollten die Lebensmittelgutscheine, wenn sie nach einer Einzelfallprüfung ausgegeben werden, unauffällig gestaltet sein, um eine Stigmatisierung des Betroffenen zu vermeiden. Insbesondere auffällige Farben und eine große Beschriftung z.B. mit dem Logo der ARGE sollten vermieden werden.

Angesichts der vorliegenden Rechtsprechung, die ähnlich wie die ARGE argumentiert, habe ich die ARGE nicht beanstandet. Im Verlauf des Schriftwechsels und aufgrund meiner Hinweise hat mir die ARGE immerhin mitgeteilt, dass für die Abrechnung mit dem Lebensmittelhandel ein Kassenbon mit Auflistung der eingekauften Lebensmittel nicht benötigt und daher nun auch nicht mehr zur Akte genommen wird. Insofern hat die ARGE die Verfahrensweise umgestellt.

8.15 Vorlage von Kontoauszügen

Ein Dauerbrenner bei telefonischen und schriftlichen Beratungen bzw. Beschwerden ist nach wie vor die Frage, ob und in welchem Umfang eine ARGE die Kontoauszüge des Antragtellers bzw. Leistungsbeziehers verlangen darf bzw. diese vorgelegt werden müssen.

Die Sozial- und Landessozialgerichte hatten diese Frage zunächst uneinheitlich beurteilt, so dass mit Spannung eine Entscheidung des Bundessozialgerichts erwartet wurde. Der Text der dann am 19.09.2008 ergangenen Entscheidung (Az. B 14 AS 45/07 R) kann über einen Link auf meiner Homepage nachgelesen werden.

Gemäß dieser Entscheidung besteht die Obliegenheit zur Vorlage von Kontoauszügen jedenfalls für die letzten drei Monate. Dies ergibt sich aus

§ 60 Abs. 1 Satz 1 Nr. 3 SGB I
Wer Sozialleistungen beantragt oder erhält, hat …
3. Beweismittel zu bezeichnen und auf Verlangen des zuständigen Leistungsträgers Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen.

Schwärzungen sind bei Buchungen auf der Ausgabenseite zulässig, wenn es sich um besondere Arten personenbezogener Daten handelt. Dies sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (§ 67 Abs. 12 SGB X). Das Bundessozialgericht hat weiter ausgeführt, dass die Grundsicherungsträger bereits bei ihren Mitwirkungsbegehren auf diese Möglichkeiten der Schwärzung gesondert hinweisen müssen. Beispielsweise bei Beitragszahlungen an eine politische Partei, Gewerkschaft oder Religionsgemeinschaft kann daher der Empfänger geschwärzt werden. Würde sich aus den insoweit geschwärzten Kontoauszügen eines Leistungsempfängers ergeben, dass in auffälliger Häufung oder Höhe Beträge überwiesen werden, so wäre gemäß dem Bundessozialgericht jeweils im Einzelfall zu entscheiden, inwieweit ausnahmsweise nicht doch eine Offenlegung auch des bislang geschwärzten Adressaten gefordert werden kann.

8.16 Verräterischer Zusatz bei der Ablehnung von Auskünften an Dritte

Die Übermittlung von Informationen kann nicht nur ausdrücklich, sondern auch indirekt "zwischen den Zeilen" erfolgen. So hat ein Rechtsanwalt bei einer ARGE angefragt, ob eine namentlich benannte Person zu einem bestimmten Zeitpunkt Leistungen nach dem SGB II bezogen hat. Zu diesem Zeitpunkt sei von dieser Person ein Kaufvertrag über ein Grundstück abgeschlossen, der Kaufpreis dann jedoch nicht bezahlt worden. Die ARGE hat dem Rechtsanwalt daraufhin zutreffend mitgeteilt, dass die ARGE den datenschutzrechtlichen Bestimmungen des Sozialgesetzbuchs unterliegt und dem Auskunftsersuchen nicht entsprechen könne. So weit, so gut. Allerdings hat die ARGE im Schreiben weiterhin mitgeteilt, dass die gewünschten Auskünfte im Rahmen eines polizeilichen Ermittlungsverfahrens wegen Betrugsverdachts erteilt werden könnten. Weiterhin hat sie diesbezüglich auf die Erforderlichkeit einer entsprechenden Anfrage durch die Polizei und § 68 SGB X hingewiesen.

Meine "Anfrage" hierzu (tatsächlich: meine Bitte um Stellungnahme unter Darlegung meiner datenschutzrechtlichen Bedenken) hat die ARGE "mit großer Verwunderung" aufgenommen. Sie hat mir mitgeteilt, die zusätzlichen Ausführungen seien im Rahmen der allgemeinen Informations- und Beratungspflicht nach dem SGB I aufgenommen worden und enthielten keinerlei inhaltliche Aussage. Die ARGE hat mir weiterhin mitgeteilt, sie sehe die Angelegenheit als erledigt an.

Ich halte es allerdings für fernliegend, dass Behörden anfragenden Rechtsanwälten "im Rahmen einer Beratung nach dem SGB I" einen Hinweis auf die Möglichkeit einer Auskunft in einem polizeilichen Ermittlungsverfahren wegen Betrugs geben, ohne dass derartige Zusatzausführungen zumindest indirekt auf einen Leistungsbezug schließen lassen bzw. jedenfalls so verstanden werden. Es ist kaum verwunderlich, wenn daraufhin eine Strafanzeige erstattet wird.

Im Übrigen waren die Zusatzausführungen der ARGE unter Hinweis auf § 68 SGB X auch inhaltlich unrichtig, da diese Vorschrift keine Befugnis für die Erteilung der gewünschten Auskunft an die Polizei enthält.

Die Angelegenheit war demnach für mich (und damit auch für die ARGE) noch nicht erledigt. Ich habe die ARGE aufgefordert, sich bei Auskunftsersuchen Dritter, die aus sozialdatenschutzrechtlichen Gründen nicht inhaltlich beantwortet werden dürfen, auf diese Aussage zu beschränken und mir mitzuteilen, dass sie

dies zukünftig beachtet. Die ARGE hat mir dies dann auch zugesichert. Die Unrichtigkeit der Zusatzausführungen unter Hinweis auf § 68 SGB X hat sie ebenfalls eingeräumt.

8.17 Private Nutzung von Sozialdaten durch Mitarbeiter

Ein Bezieher von Leistungen nach dem SGB II hatte aus persönlichen Gründen den Kontakt zu seiner Mutter bereits vor Jahren abgebrochen. Seine Mutter habe immer wieder ihre Tätigkeit bei Behörden ausgenutzt, um an seine aktuellen Adressdaten zu gelangen. Dann habe sie ihn mit Briefen, Postkarten und auch per E-Mail "belästigt". Auch nach einem Umzug habe der Betroffene erneut Post von seiner Mutter erhalten, in der sie ihm sogar mitteilte, dass sie seine neuen Adressdaten von der ARGE habe, bei der sie nun arbeite.

Auf Wunsch des Betroffenen habe ich die ARGE angeschrieben. Diese hat mir mitgeteilt, dass dort bereits eine Beschwerde über den Vorgang vorliege. Die Mitarbeiterin sei bereits in einem persönlichen Gespräch eingehend darüber informiert worden, dass die Verwendung der dortigen Datenbestände für persönliche Zwecke untersagt ist. Der Mitarbeiterin seien die Konsequenzen aufgezeigt worden und sie bedauere ihr Verhalten. Eine nochmalige missbräuchliche Nutzung der personenbezogenen Daten werde ausgeschlossen.

Ich habe dies dem Betroffenen mitgeteilt. Eine neuerliche Beschwerde wegen der Nutzung der Adressdaten des Betroffenen durch dessen Mutter habe ich in dieser Angelegenheit nicht mehr erhalten. Die Beschaffung und die Nutzung entsprechender Sozialdaten zu privaten Zwecken ist selbstverständlich unzulässig.

8.18 Zusatzerklärung zum Leistungsantrag

Eine Antragstellerin hat sich an mich gewandt, da sie bei einer ARGE neben dem Antragsformular noch ein Beiblatt mit Erklärungen, Hinweisen und einer Einwilligungserklärung (zu Datenerhebungen bzw. -übermittlungen) unterzeichnen sollte. Sie sei unter Androhung von Sanktionen zur Unterschrift aufgefordert worden.

Eine gesetzlich festgelegte Pflicht zur Unterzeichnung der Erklärungen und Hinweise bzw. eine Möglichkeit zu Sanktionen seitens der ARGE bestanden tatsächlich nicht. Die Einwilligungserklärung, die zusammen mit anderen Erklärungen abgegeben werden sollte, war außerdem entgegen § 67 b Abs. 2 Satz 4 SGB X im äußeren Erscheinungsbild nicht hervorgehoben. Weiterhin war etwa ein Hinweis zu Hausbesuchen enthalten, der in seiner allgemeinen und voraussetzungslosen Formulierung nicht zutreffend war ("Die persönlichen Verhältnisse können durch unangemeldete Hausbesuche des Ermittlers des Jobcenters überprüft werden.").

Die ARGE hat mir auf meine Bitte um Stellungnahme zunächst mitgeteilt, dass die dortigen Mitarbeiter nicht angewiesen seien, bei Nichtunterschrift Sanktionen anzudrohen. Dazu gäbe es keine Rechtsgrundlage.

Nach weiterem Schriftverkehr mit mir hat die ARGE dann auch ihre Hinweise, etwa zu Hausbesuchen, und das Formular als solches umgestaltet. Nunmehr ist

die Einwilligung räumlich abgesetzt und kann durch eine eigene, hierauf bezogene Unterschrift erteilt werden. Zudem ist nun ein eindeutiger Hinweis auf die Freiwilligkeit der Abgabe der Einwilligungserklärung enthalten.

8.19 Einzelne ARGE-Mitarbeiter: furcht- oder doch eher gedankenlos?

"Ich fürchte keine Hölle: Ich bin ARGE Mitarbeiter" so hat sich eine Gruppe von ARGE-Mitarbeitern in einem öffentlich zugänglichen Internetportal genannt. Ob diese - vermeintlich humorvolle - Gruppenbezeichnung lustig oder in irgendeiner Weise angebracht ist, habe ich aus datenschutzrechtlicher Sicht nicht zu bewerten. Im Rahmen des Themas "Kindernamen der Leistungsempfänger" haben sich Mitglieder dieser Gruppe im Wesentlichen über aus ihrer Sicht bemerkenswerte Vornamen der Kinder im Leistungsbezug ausgetauscht und diese vermeintlich humorvoll kommentiert. Der "Spaß" hört datenschutzrechtlich spätestens dann auf, wenn durch die Nennung der Vornamen die betroffenen Kinder und Familien öffentlich als Leistungsbezieher identifizierbar werden. Mir ist ein Fall bekannt geworden, in dem eine ARGE-Mitarbeiterin ungewöhnliche Vornamen, noch dazu verbunden mit der Information "Zwillinge", veröffentlicht hat. Der Eintrag endet außerdem mit der Formel "Grüße aus der ARGE …", wobei die betreffende ARGE konkret benannt worden ist. Schon bei der Übersendung entsprechender Ausdrucke aus dem Internet wurde mir mitgeteilt, dass die Gruppe bereits gelöscht sei.

Aufgrund der veröffentlichten Angaben sind die genannten Kinder bzw. diese Familie für deren Umfeld als Leistungsbezieher identifizierbar. Es versteht sich von selbst, dass die ARGE-Mitarbeiterin keine Daten veröffentlichen durfte, die einzelne Personen als Leistungsbezieher identifizierbar machen.

Ich habe die genannte ARGE über den Vorgang informiert und um Stellungnahme sowie Mitteilung der veranlassten Maßnahmen gebeten. Die Mitarbeiterin der ARGE hat dargelegt, sie sei sich der Tragweite des entstandenen Schadens bzw. der Verletzung des Datenschutzes zum damaligen Zeitpunkt nicht bewusst gewesen und hat sich ausdrücklich hierfür entschuldigt. Sie hat versichert, dass dies nicht wieder vorkommen werde. Auch die ARGE selbst hat sich für die unbedachte Nennung entschuldigt und alle Mitarbeiter entsprechend informiert und instruiert.

8.20 Beiblatt zum Sozialhilfeantrag

In schöner Regelmäßigkeit erhalte ich Eingaben zu Antragsformularen und anderen Datenerhebungsbögen, die von Sozialleistungsträgern verwendet werden. Dabei wird oft geltend gemacht, dass der Leistungsträger im Formular Daten abfragt, die er nicht benötigt. Zur Ausgestaltung von Fragebögen hatte ich mich u.a. in meinem 22. Tätigkeitsbericht unter Nr. 14.3.2 geäußert. Leider muss ich nach wie vor feststellen, dass mittels Formularen teilweise Daten erhoben werden, die tatsächlich gar nicht benötigt werden. Besondere Aufmerksamkeit sollte man dabei angefertigten "Zusatzblättern" oder "Beiblättern" widmen.

Im Berichtszeitraum hatte beispielsweise ein Sozialamt einen Betroffenen - angeblich unter Hinweis auf eine sonst mögliche Leistungseinstellung - zum Ausfüllen eines Beiblatts zum Sozialhilfeantrag im Hinblick auf unterhaltspflichtige Angehörige aufgefordert. Auf die erbetene Stellungnahme hin wurden mir als

Begründung für die detaillierten Datenerhebungen zu den unterhaltspflichtigen Angehörigen Vorschriften benannt. Das Sozialamt hat mir weiter mitgeteilt, dass man dort immer das monierte Formblatt verwende, wenn geprüft werden muss, ob Unterhaltsverhandlungen zu führen seien.

Da die erhaltene Stellungnahme einige Fragen offen ließ, habe ich nochmals beim Sozialamt nachgehakt und konkretere Begründungen erbeten. Darauf hin hat mir das Sozialamt mitgeteilt, dass entgegen der bisherigen Ausführungen das angesprochene Beiblatt üblicherweise überhaupt nicht mehr verwendet werde. Es sei ursprünglich einem Antrag nach dem (früher geltenden) BSHG beigefügt worden. Es sei nicht mehr nachvollziehbar, warum das Formblatt in diesem Fall doch benutzt wurde. Zudem hat mir das Sozialamt das aktuelle, eigentliche Antragsformular übersandt, das entsprechend weniger detaillierte Daten abfragt.

Ich habe das Sozialamt aufgefordert, durch geeignete Maßnahmen sicherzustellen, dass das angesprochene Beiblatt zum Sozialhilfeantrag zukünftig tatsächlich nicht mehr verwendet wird.

8.21 Verstoß gegen das Sozialgeheimnis

Durch eine Eingabe bin ich darüber unterrichtet worden, dass eine Mitarbeiterin des Sozialamts einer Gemeinde Informationen über den Bezug von Sozialleistungen und über die Wohnverhältnisse von Gemeindebürgern an eine Privatperson weitergegeben hat. Offenkundig wurde dieser Vorgang, als der Rechtsanwalt der Gemeindebürger in einem mietrechtlichen Rechtsstreit gegen diese Privatperson Akteneinsicht beim Amtsgericht genommen hatte und in den Akten ein Schreiben der Gemeinde an die Beklagte vorfand, das die genannten Auskünfte über seine Mandanten enthielt. Die Gemeinde hat eingeräumt, dass sie die personenbezogenen Daten (Sozialdaten) ohne Beachtung der geltenden Datenschutzbestimmungen an eine Dritte herausgegeben habe.

Ich habe die Übermittlung der personenbezogenen Daten durch die Gemeinde beanstandet, weil darin ein Verstoß gegen das grundsätzlich bestehende Übermittlungsverbot gemäß Art. 15 Abs. 1 Bayerisches Datenschutzgesetz sowie eine Verletzung des Sozialgeheimnisses gemäß § 78 Abs. 1 Satz 2 SGB X bestand. Von der grundsätzlich bestehenden Möglichkeit nach Art. 31 Abs. 3 Bayerisches Datenschutzgesetz, von einer Beanstandung abzusehen, habe ich keinen Gebrauch gemacht, weil es sich nicht um einen unerheblichen Verstoß gehandelt hat. Insbesondere die Mitteilung über den Bezug von Sozialleistungen ist ein sensibles Datum, das den besonderen Schutzbestimmungen und dem Sozialgeheimnis des Sozialgesetzbuchs unterliegt.

9 Steuer- und Finanzverwaltung

9.1 eGovernment in der Steuerverwaltung

In der Vergangenheit habe ich bereits mehrfach über die vielfältigen Bestrebungen der Steuerverwaltung berichtet, den Automationsgrad in den Finanzämtern zu verbessern; diese werden seit einigen Jahren unter dem länderübergreifenden eGovernment-Projekt KONSENS (Koordinierte neue Software-Entwicklung der Steuerverwaltung) zusammengefasst und stark vorangetrieben (siehe hierzu 23. Tätigkeitsbericht, Nr. 11.1). Im Berichtszeitraum war ich in erster Linie mit den Fachverfahren RMS (Risikomanagementsysteme), ELSTEROnline und ELSTERLohn II (Elektronische Steuererklärung) befasst.

9.1.1 Projekt RMS

Um das Risiko von Steuerausfällen zu minimieren, werden im Rahmen des Projekts RMS von den Ländern Nordrhein-Westfalen und Bayern **Risikomanagementsysteme** entwickelt. Das Staatsministerium der Finanzen hat mir auf meine Bitte hin eine ausführliche Übersicht sowohl über die bereits weitgehend fertig gestellten als auch über die in Planung oder Entwicklung befindlichen Produkte übermittelt. Nach Durchsicht dieser Unterlagen haben sich für mich keine grundsätzlichen datenschutzrechtlichen Bedenken ergeben. Unabhängig davon werde ich aber zu gegebener Zeit den Echteinsatz einzelner Produkte vor Ort datenschutzrechtlich überprüfen.

9.1.2 Projekt ELSTEROnline

Um ausschließlich elektronisch Steuererklärungen abgeben zu können, ist eine **Registrierung bei ELSTEROnline** erforderlich. **Steuerberatungskanzleien** in der Rechtsform eines Einzelunternehmens u.ä. müssen dabei auch zur elektronischen Abgabe von Steuererklärungen ihrer Mandanten die persönliche Steuernummer des Kanzleiinhabers angeben. Diese Angabe ist dann datenschutzrechtlich problematisch, wenn dadurch Dritte - beispielsweise Angestellte der Steuerberatungskanzlei - die persönliche Steuernummer des Kanzleiinhabers zur Kenntnis nehmen und in der Folge u.U. entsprechende Abfragen vornehmen können.

Ich habe in dem genannten Zusammenhang eine ausführliche Stellungnahme des Staatsministeriums der Finanzen eingeholt. Zur Lösung der Problematik hat das Finanzministerium vorgeschlagen, im Rahmen der Registrierung bei ELSTEROnline ein nicht-persönliches "Organisationszertifikat" zu beantragen. Dazu muss der Kanzleiinhaber den Namen und die E-Mail-Adresse des/der mit der elektronischen Abgabe von Steuererklärungen betrauten Mitarbeiter(s) als Ansprechpartner angeben. Zwar ist bei der Erst-Registrierung sodann immer noch die persönliche Steuernummer des Kanzleiinhabers mitzuteilen. Diese Steuernummer wird aber nur zur Ermittlung der Adressdaten für die Zustellung

des Registrierungsbriefes verwendet; sie ergibt sich aber nicht aus dem Zertifikat selbst. Diese vom Staatsministerium der Finanzen aufgezeigte Alternative scheint mir ein durchaus gangbarer Weg.

9.1.3 Projekt ELSTERLohn II

In Nr. 11.1.3 meines 23. Tätigkeitsberichts habe ich mich eingehend zur beabsichtigten Ablösung der bisher bekannten (Papier-) Lohnsteuerkarte durch ein elektronisches Abrufverfahren geäußert (Projekt ELSTERLohn II). In diesem Zusammenhang habe ich auch auf die Risiken hingewiesen, die mit der Einrichtung der dafür notwendigen zentralen Steuerdatei verbunden sind. Insbesondere stellt sich hier die Problematik der zuverlässigen Vermeidung von sogenannten "Neugierabfragen" durch nicht berechtigte Arbeitgeber.

Im Berichtszeitraum musste die ursprünglich für das Jahr 2011 geplante Ersetzung der (Papier-) Lohnsteuerkarte durch elektronische Lohnsteuerabzugsmerkmale (ELStAM) wegen Verzögerungen in der Verfahrensentwicklung auf das Jahr 2012 verschoben werden. Das Jahressteuergesetz 2010 enthält die dafür notwendigen Übergangsregelungen, sieht darüber hinaus aber auch die Erweiterung der zentralen Steuerdatenbank um die für den Lohnsteuerabzug erforderlichen Angaben zu Religionszugehörigkeit und Familienangehörigen vor. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mit der Entschließung "Erweiterung der Steuerdatenbank enthält große Risiken" vom 24.06.2010 ihre grundsätzliche Kritik an dem Vorhaben erneuert, dem Bundesgesetzgeber aber auch die aus Datenschutzsicht notwendigen Nachbesserungen aufgezeigt. So sollte beispielsweise zur Vermeidung von "Neugierabfragen" der Abruf generell nur unter Mitwirkung des jeweils betroffenen Arbeitnehmers möglich sein.

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.06.2010
Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale (ELStAM), wie z.B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- *Vorherige Information der Arbeitnehmer*
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- *Keine Speicherung auf Vorrat*
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- *Verhindern des unzulässigen Datenabrufs*
  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- *Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept*
  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

9.2 Nochmals: Auskunftsanspruch in der Abgabenordnung

Schon mehrfach habe ich über die Bemühungen der Datenschutzbeauftragten des Bundes und der Länder berichtet, einen Auskunftsanspruch für Steuerpflichtige in der Abgabenordnung zu verankern. Zuletzt habe ich in Nr. 11.3 meines 23. Tätigkeitsberichts auf eine Entscheidung des Bundesverfassungsgerichts vom 10.03.2008 (1 BvR 2388/03) hingewiesen, in der das Gericht klar gestellt hat, dass § 19 BDSG, der den Auskunftsanspruch eines Betroffenen im Geltungsbereich des Bundesdatenschutzgesetzes regelt, auch gegenüber der Steuerverwaltung gilt.

Auf diese Entscheidung des höchsten deutschen Gerichts hat das **Bundesministerium der Finanzen** im Einvernehmen mit den obersten Finanzbehörden der Länder mit einer einfachen **Verwaltungsanweisung** (BMF-Schreiben vom 17.12.2008, IV A 3 - S 0030/08/10001) reagiert. Diese Verwaltungsanweisung macht die Auskunftserteilung zudem von einem "berechtigten Interesse" abhängig, was zu einer weitgehenden Einschränkung des Auskunftsrechts führt.

Die Datenschutzbeauftragten des Bundes und der Länder haben diese Vorgehensweise der Finanzverwaltung auf ihrer 77. Konferenz am 26./27.03.2009 in Berlin mit der Entschließung "Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!" als **Aushebelung des verfassungsrecht-**

lich garantierten Auskunftsrechts scharf kritisiert. Sie haben eine unverzügliche Aufhebung der Verwaltungsanweisung und eine eindeutige Regelung des Auskunftsanspruchs in der Abgabenordnung gefordert.

Mittlerweile sind bei der Steuerverwaltung Tendenzen erkennbar, den Auskunftsanspruch für Steuerpflichtige endlich doch gesetzlich in der Abgabenordnung zu regeln. Ein mir vorliegender Diskussionsentwurf macht die Geltendmachung eines Auskunftsanspruchs allerdings immer noch von der Darlegung eines "Informationsinteresses" abhängig. Aus datenschutzrechtlicher Sicht ist aber auch diese Einschränkung des verfassungsrechtlich gewährleisteten Auskunftsanspruchs nicht akzeptabel.

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009
Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem "berechtigten Interesse" abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10.03.2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17.12.2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

9.3 Datenschutz bei Alterseinkünften

Mitte des Jahres 2009 häuften sich Presseberichte, dass Rentner bald mit genaueren Kontrollen bezüglich der Versteuerung ihrer Alterseinkünfte zu rechnen hätten. Die Finanzämter könnten künftig beispielsweise feststellen, ob jemand mehrere Renten erhalten, aber keine Steuererklärung abgegeben habe. Diese Presseartikel haben datenschutzrechtliche Fragen bei zahlreichen betroffenen Bürgerinnen und Bürgern aufgeworfen.

Rechtliche Grundlage für die Besteuerung von Renten bildet das Alterseinkünftegesetz vom 05.07.2004. Das Gesetz sieht vor, dass - beginnend mit dem Jahr

2005 - die Bezüge aus Alterseinkünften (z.B. die gesetzliche Rente) verstärkt steuerpflichtig werden. Im Gegenzug werden die in der Erwerbsphase in eine Altersvorsorge eingezahlten Beträge zunehmend von der Einkommensteuer befreit.

Das Alterseinkünftegesetz verpflichtet die Rentenversicherungsträger und Lebensversicherungsunternehmen (bei Vorliegen einer Leibrentenversicherung) dazu, jährlich sog. **Rentenbezugsmitteilungen** an eine zentrale Stelle zu übermitteln. Dabei handelt es sich um die Deutsche Rentenversicherung Bund. Diese übermittelt die Daten nach einer internen Plausibilitätsprüfung an das Bundeszentralamt für Steuern. Von dort werden sie an das für den jeweiligen Leistungsempfänger zuständige Finanzamt weitergeleitet. Die vom Alterseinkünftegesetz bereits ab dem Frühjahr 2006 (für das Jahr 2005) vorgesehenen Datenübermittlungen wurden aufgrund der Verzögerungen bei der Vergabe der Steueridentifikationsnummer nach § 139 b AO (siehe hierzu 23. Tätigkeitsbericht, Nr. 11.1.1) immer wieder zurückgestellt; sie wurden nunmehr ab Herbst 2009 aufgenommen.

Durch das Alterseinkünftegesetz erhalten die Finanzämter von den Rentenversicherungsträgern und Lebensversicherungsunternehmen über den Umweg der zentralen Stelle Mitteilungen über die Höhe der gesetzlichen Rente, der betrieblichen Altersvorsorge oder einer privat abgeschlossenen Rentenversicherung "ihrer" Rentner. Das zuständige **Finanzamt prüft** anhand der erhaltenen Angaben, **ob** nach den Regelungen des Einkommensteuergesetzes **bereits ergangene Steuerbescheide zu korrigieren sind oder ein Leistungsempfänger zur Abgabe einer Steuererklärung verpflichtet ist.**

Aus datenschutzrechtlicher Sicht sieht das Alterseinkünftegesetz somit eine gesetzliche Durchbrechung des Grundsatzes der Direkterhebung vor. Nach diesem Grundsatz hat eine öffentliche Stelle personenbezogene Daten im Regelfall direkt beim Betroffenen - hier dem steuerpflichtigen Rentner - und nicht bei Dritten zu erheben. Der jeweilige **Rentner** - im Gesetz wird er Leistungsempfänger genannt - **ist allerdings von der Datenübermittlung an die zentrale Stelle zu unterrichten.**

Erkenntnisse zur praktischen Umsetzung des Alterseinkünftegesetzes durch die Finanzämter liegen mir noch nicht vor. Ich werde die Problematik aber weiterhin aufmerksam beobachten. Nicht unerwähnt möchte ich dabei lassen, dass bereits vor Inkrafttreten des Alterseinkünftegesetzes Rentner oberhalb bestimmter Grenzen ihre Alterseinkünfte zu versteuern hatten.

9.4 Bürgerentlastungsgesetz Krankenversicherung

Mit dem Gesetz zur verbesserten steuerlichen Berücksichtigung von Vorsorgeaufwendungen (Bürgerentlastungsgesetz Krankenversicherung) vom 16.07.2009 hat der Bundesgesetzgeber die steuerliche Abziehbarkeit von Beiträgen zur Kranken- und Pflegeversicherung umfassend reformiert. Im Zusammenhang mit dem nunmehr im Einkommensteuergesetz diesbezüglich vorgeschriebenen Verfahren haben sich mehrere Bürgerinnen und Bürger an mich gewandt. Hierzu nehme ich wie folgt Stellung:

- Bereits durch das Jahressteuergesetz 2008 vom 20.12.2007 wurden die Weichen für die schrittweise Ablösung der bisherigen (Papier-) Lohn-

steuerkarte durch ein elektronisches Übermittlungssystem gestellt (siehe hierzu 23. Tätigkeitsbericht, Nr. 11.1.3). Dazu wurde beim Bundeszentralamt für Steuern ein Datenpool eingerichtet, in dem die für das Lohnsteuerabzugsverfahren erforderlichen Lohnsteuerabzugsmerkmale jedes Steuerpflichtigen unter der steuerlichen Identifikationsnummer nach § 139 b AO (siehe hierzu 23. Tätigkeitsbericht, Nr. 11.1.1) gespeichert werden: Nach Beendigung des Arbeitsverhältnisses oder am Ende des Kalenderjahres hat der Arbeitgeber eine elektronische Lohnsteuerbescheinigung an die Finanzverwaltung zu übermitteln (§ 41 b Abs. 1 Satz 1 EStG). Als Ordnungsmerkmal ist dabei die Steueridentifikationsnummer vorgesehen. Bei dieser handelt es sich um eine "nichtsprechende" Nummer, deren Verwendung vom Gesetzgeber auf steuerliche Verfahren beschränkt wurde; eine anderweitige Verwendung ist strafbewehrt (siehe §§ 139 b Abs. 2, 383 a AO).

Der Nachweis über die gezahlten Kranken- und Pflegeversicherungsbeiträge der gesetzlich Krankenversicherten wird damit künftig bereits im Rahmen des elektronischen Lohnsteuerverfahrens durch die Arbeitgeber an die Finanzverwaltung übermittelt (§ 41 b Abs. 1 Satz 2 Nr. 13 EStG).

- Das Bürgerentlastungsgesetz Krankenversicherung sieht nunmehr vor, dass auch die Kranken- und Pflegeversicherungsbeiträge der privat Krankenversicherten nur dann steuerlich als Sonderausgaben abzugsfähig sind, wenn ihre Zahlung von den Krankenversicherungsunternehmen unter Verwendung der steuerlichen Identifikationsnummer elektronisch gegenüber den Finanzbehörden bestätigt wird. Voraussetzung dafür ist allerdings, dass die privat Krankenversicherten in diese Datenübermittlung einwilligen (siehe § 10 Abs. 2 Satz 3, Abs. 2 a EStG).

  § 10 Abs. 2 Satz 3 EStG
  Vorsorgeaufwendungen nach Abs. 1 Nr. 3 werden nur berücksichtigt, wenn der Steuerpflichtige gegenüber dem Versicherungsunternehmen, dem Träger der gesetzlichen Kranken- und Pflegeversicherung oder der Künstlersozialkasse in die Datenübermittlung nach Abs. 2 a eingewilligt hat; die Einwilligung gilt als erteilt, wenn die Beiträge mit der elektronischen Lohnsteuerbescheinigung (§ 41 b Abs. 1 Satz 2) oder der Rentenbezugsmitteilung (§ 22 a Abs. 1 Satz 1 Nr. 5) übermittelt werden.

  Für die steuerliche Berücksichtigung von Kranken- und Pflegeversicherungsbeiträgen war bisher - wie auch für die Berücksichtigung anderer steuerlicher Abzugsbeträge - die Vorlage der entsprechenden Papierbelege notwendig. Stattdessen ist nunmehr die Einwilligung in die elektronische Datenübermittlung unumgänglich. Sollte ein Steuerbürger einen steuerlichen Abzug dieser Versicherungsbeiträge nicht wünschen, so kann er die Einwilligung in die Datenübermittlung verweigern. Eine steuerliche Berücksichtigung ist dann aber auch nicht durch Vorlage der entsprechenden Papierbelege möglich.

- Aus datenschutzrechtlicher Sicht ist das nunmehr gesetzlich vorgeschriebene Einwilligungsverfahren nicht unproblematisch: Nachdem der betroffene Steuerbürger keine wirkliche Wahlmöglichkeit hat, ist das Vorliegen einer "echten" Freiwilligkeit der Einwilligung zweifelhaft. Andererseits ist aber zu bedenken, dass in dem bisher angewandten (Papier-)Verfahren die geltend gemachten Beiträge in der Steuererklärung anzugeben und

die entsprechenden Belege beizufügen waren; dies entspricht im Ergebnis einer Einwilligung. Wurden - vergleichbar mit der Nichterteilung einer Einwilligung - keine Beiträge erklärt und keine Belege beigefügt, erfolgte auch bisher keine steuerliche Berücksichtigung.

Unabhängig davon wäre die Finanzverwaltung meiner Ansicht nach aber gut beraten, den betroffenen Steuerbürgern **im Falle der Verweigerung der Einwilligung** einen **alternativen (Papier-) Nachweis der gezahlten Beiträge** zu ermöglichen. Dies nicht zuletzt deshalb, um die in breiten Bevölkerungskreisen vorhandenen Bedenken und Befürchtungen gegenüber einer immer weiteren Verbreitung der Steueridentifikationsnummer zu begegnen.

9.5 Nochmals: Automatisierte Kontenabfrage im Besteuerungsverfahren

Bereits in Nr. 11.2 meines 23. Tätigkeitsberichts habe ich zur automatisierten Kontenabfrage im Besteuerungsverfahren aus datenschutzrechtlicher Sicht ausführlich Stellung genommen. In diesem Zusammenhang habe ich auch über die Ergebnisse einer detaillierten Einzelfallprüfung bei einem bayerischen Finanzamt berichtet. Dabei habe ich insbesondere die nach meinen Feststellungen oftmals unterbliebene Unterrichtung der von einer automatisierten Kontenabfrage betroffenen Steuerbürger kritisiert.

Nach meinen damaligen Feststellungen war die Unterrichtung der von einer automatisierten Kontenabfrage Betroffenen vielfach gerade in den Fällen unterblieben, in denen nicht die veranlagende Stelle, sondern eine andere Organisationseinheit des Finanzamts - etwa die Betriebsprüfungsstelle - die Kontenabfrage veranlasst hatte. Denn diese Fallkonstellation (Auseinanderfallen von abrufender und veranlagender Stelle) war nach meinen Feststellungen durch eine nicht ausreichend klare Aufgabenzuweisung und durch das Fehlen von Kontrollmechanismen gekennzeichnet. Zur Sicherstellung der Benachrichtigung habe ich deshalb in meinem Prüfbericht dem Staatsministerium der Finanzen geraten, bei allen bayerischen Finanzämtern im Sinne eines Vier-Augen-Prinzips eine Kontrolle durch den verantwortlichen Hauptsachgebietsleiter Abgabenordung vorzusehen.

Zwar hat das Staatsministerium der Finanzen "wegen des damit verbundenen Verwaltungsaufwands" zunächst die Einführung einer derartigen Kontrolle abgelehnt. Nach einer vom Finanzministerium angeordneten internen Prüfung, welche meine Prüfungsfeststellungen vollumfänglich bestätigte, hat mir das **Staatsministerium der Finanzen** jedoch Ende 2009 mitgeteilt, dass es **zur Sicherstellung der Benachrichtigung allen bayerischen Finanzämtern** inzwischen **aufgegeben** habe, die von mir geforderte **Vier-Augen-Kontrolle durch den Hauptsachgebietsleiter Abgabenordnung** durchzuführen. Zudem hat das Finanzministerium mir zugesichert, dass die fehlenden Unterrichtungen unverzüglich nachgeholt werden.

Den nach längeren und intensiven Verhandlungen schließlich eingetretenen Sinneswandel des Staatsministeriums der Finanzen begrüße ich ausdrücklich. Ich gehe davon aus, dass die aus Transparenz- und Rechtsschutzgründen gesetzlich in § 93 Abs. 9 AO **grundsätzlich vorgeschriebene Information der von einem Kontenabruf betroffenen Steuerpflichtigen künftig sichergestellt** ist.

§ 93 Abs. 9 AO Auskunftspflicht der Beteiligten und anderer Personen
Vor einem Abrufersuchen nach Abs. 7 oder Abs. 8 ist der Betroffene auf die Möglichkeit eines Kontenabrufs hinzuweisen; dies kann auch durch ausdrücklichen Hinweis in amtlichen Vordrucken und Merkblättern geschehen. Nach Durchführung eines Kontenabrufs ist der Betroffene vom Ersuchenden über die Durchführung zu benachrichtigen. Ein Hinweis nach Satz 1 erster Halbsatz und eine Benachrichtigung nach Satz 2 unterbleiben, soweit

1. *sie die ordnungsgemäße Erfüllung der in der Zuständigkeit des Ersuchenden liegenden Aufgaben gefährden würden,*
2. *sie die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würden oder*
3. *die Tatsache des Kontenabrufs nach einer Rechtsvorschrift oder seinem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden muss*

und deswegen das Interesse des Betroffenen zurücktreten muss; § 19 Abs. 5 und 6 des Bundesdatenschutzgesetzes in der Fassung der Bekanntmachung vom 14.01.2003 (BGBl. I S. 66), das zuletzt durch Art. 1 des Gesetzes vom 22.08.2006 (BGBl. I S. 1970) geändert worden ist, in der jeweils geltenden Fassung gilt entsprechend, soweit gesetzlich nichts anderes bestimmt ist.

9.6 Adressierung von Steuerbescheiden

Immer wieder erreichen mich Eingaben, die eine fehlerhafte Adressierung von Steuerbescheiden zum Gegenstand haben. Aus allen diesen Fällen lassen sich im Wesentlichen zwei Problemschwerpunkte herauskristallisieren: zum Teil wird der Adressat zwar im Grunde zutreffend angegeben, das Adressfeld aber mit nicht zulässigen Zusätzen versehen. Teilweise kommt es aber auch zu einer vollständigen Fehladressierung. In beiden Fallgruppen sind Fragen der Wahrung des Steuergeheimnisses im Sinne des § 30 AO berührt. Im Einzelnen möchte ich aus datenschutzrechtlicher Sicht auf Folgendes hinweisen:

Die gesetzliche Grundlage für die Bekanntgabe eines Steuerbescheides findet sich in § 122 AO. Nähere Erläuterungen zu den Bekanntgaberegeln - einschließlich verschiedener beispielhafter Fallgestaltungen - enthält der Anwendungserlass zu § 122 AO. Hiernach ist **grundsätzlich zu unterscheiden,** an wen ein Steuerbescheid bekanntgegeben werden soll **(Bekanntgabeadressat)** und welcher Person er zu übermitteln ist **(Empfangsadressat).**

§ 122 AO Bekanntgabe des Verwaltungsakts
(1) Ein Verwaltungsakt ist demjenigen Beteiligten bekannt zu geben, für den er bestimmt ist oder der von ihm betroffen wird. § 34 Abs. 2 ist entsprechend anzuwenden. Der Verwaltungsakt kann auch gegenüber einem Bevollmächtigten bekannt gegeben werden.
...
(6) Die Bekanntgabe eines Verwaltungsakts an einen Beteiligten zugleich mit Wirkung für und gegen andere Beteiligte ist zulässig, soweit die Beteiligten einverstanden sind; diese Beteiligten können nachträglich eine Abschrift des Verwaltungsakts verlangen.
(7) Betreffen Verwaltungsakte Ehegatten oder Ehegatten mit ihren Kindern oder Alleinstehende mit ihren Kindern, so reicht es für die Bekanntgabe an alle Beteiligten aus, wenn ihnen eine Ausfertigung unter ihrer gemeinsamen Anschrift

übermittelt wird. Die Verwaltungsakte sind den Beteiligten einzeln bekannt zu geben, soweit sie dies beantragt haben oder soweit der Finanzbehörde bekannt ist, dass zwischen ihnen ernstliche Meinungsverschiedenheiten bestehen.

- Mehrere Eingaben hatten die Zustellung von Steuerbescheiden im Rahmen einer **(Gesamt-)Rechtsnachfolge** zum Inhalt. Das jeweilige Finanzamt hatte in diesen Fällen im Anschriftenfeld den Zusatz "als Rechtsnachfolger des/der verstorbenen …" angebracht. Ich habe hier die Auffassung vertreten, dass die Empfängeranschrift derartige Zusätze nicht enthalten darf, diese vielmehr in dem - für Außenstehende nicht sichtbaren - Bescheidkopf aufgeführt werden müssen.

  Die zur Stellungnahme aufgeforderten Leiter der betroffenen Finanzämter haben sich meiner Rechtsauffassung unmittelbar angeschlossen. Sie haben die fehlerhafte Bekanntgabe jeweils zum Anlass genommen, im Wege einer Amtsverfügung alle Bediensteten auf die Problematik hinzuweisen, um solche Fehler für die Zukunft auszuschließen.

- In anderen mir vorliegenden Eingaben kam es seitens der jeweils zuständigen Finanzämter zu **vollständigen Fehladressierungen.** Zumeist wurden aufgrund von Büroversehen Adressen von Steuerbürgern vertauscht. In einem Fall wurde im Anschriftenfeld als Adressat allein das Seniorenheim, in dem die Steuerbürgerin lebte, angegeben. Ein Hinweis auf die eigentliche Bekanntgabeadressatin erfolgte nur im Bescheidkopf, so dass das Seniorenheim zunächst in die Lage versetzt wurde, den Steuerbescheid der Heimbewohnerin zur Kenntnis zu nehmen.

  Auch in diesen Fällen haben die zuständigen Finanzamtsleiter unmittelbar reagiert, sich bei den betroffenen Steuerbürgern für die Fehlzustellungen ausdrücklich entschuldigt und die Finanzamtsbediensteten für die Problematik sensibilisiert, um derartige Fehler in der Zukunft zu vermeiden.

Festzuhalten bleibt, dass es sich in den angeführten Fällen jeweils um "Ausreißer" handelte; eine Häufung ähnlicher Fehlzustellungen in der Vergangenheit war bei keinem der betroffenen Finanzämter festzustellen. An dieser Stelle möchte ich aber **an alle bayerischen Finanzämter appellieren, im Interesse der Wahrung des Steuergeheimnisses auf die** - zugegebenermaßen nicht immer einfach zu beantwortende - **Problematik der Adressierung von Steuerbescheiden besonderes Augenmerk zu legen.**

9.7 Prüfung des Servicezentrums des Finanzamts München

Seit der Jahrtausendwende haben zur Verbesserung der Servicequalität alle bayerischen Finanzämter sukzessive sog. Servicezentren eingerichtet. Als erste Anlauf- und Informationsstellen für alle Besucher sollen sie den Publikumsverkehr möglichst vollständig abwickeln und damit auch den übrigen Finanzamtsbediensteten ein ungestörtes und konzentriertes Arbeiten ermöglichen. In datenschutzrechtlicher Hinsicht stellt für ein Servicezentrum die Wahrung des Steuergeheimnisses eine besondere, beständige Herausforderung dar. Im Berichtszeitraum habe ich beispielhaft beim Servicezentrum des Finanzamts München die Einhaltung datenschutzrechtlicher Vorschriften geprüft.

Die Prüfung erbrachte folgende Ergebnisse:

9.7.1 Tätigkeiten im Servicezentrum

Die Bediensteten des der Abteilung IV des Finanzamts München zugeordneten Servicezentrums üben in erster Linie Tätigkeiten im Zusammenhang mit der Aufgabe des Servicezentrums als **zentrale Anlaufstelle** aus. Dabei erfolgen im Regelfall nur eine Durchsicht und Vorprüfung, aber keine abschließende Bearbeitung eines Steuerfalles. In **Stoßzeiten** übt das Servicezentrum nur die Funktion einer **Annahmestelle** aus. Auf den eingereichten Unterlagen wird dann vermerkt, dass eine Durchsicht und Vorprüfung nicht erfolgt sind.

Nur in vergleichsweise sehr geringem Umfang werden **Veranlagungen** von einfach gelagerten Steuerfällen vorgenommen, dies insbesondere um in publikumsschwachen Zeiten eine gleichmäßige Arbeitsauslastung sicherzustellen.

Neben den einzelnen Schaltern ist im Servicezentrum eine sog. "**Vorinfo**"**-Stelle** eingerichtet, die allgemeine Auskünfte erteilt, Vordrucke ausgibt etc. und auch (gebäude-)organisatorische Aufgaben erfüllt.

9.7.2 Zugriffsrechte der Bediensteten auf Steuerdaten

Die Zugriffsrechte der Bediensteten im Bereich des Servicezentrums auf die Steuerdaten werden im Rahmen des Verfahrens ACUSTIG (Arbeitsplatz-Computer-Unterstützung in der Geschäftsstelle) durch die Geschäftsstelle der Abteilung IV vergeben. Danach haben die Mitarbeiter des Servicezentrums keine unterschiedlichen Zugriffsberechtigungen im Hinblick auf Tätigkeiten, die der Funktion des Servicezentrums als zentraler Anlaufstelle zuzuordnen sind, und im Hinblick auf Veranlagungstätigkeiten; vielmehr werden **insgesamt einheitliche Zugriffsrechte** vergeben.

Davon abweichend wird den Mitarbeitern im Bereich der "**Vorinfo**"**-Stelle** in der Hauptsache lediglich ein lesender Zugriff ermöglicht.

9.7.3 Zugriffsrecht auf die zentrale Datenbank ZAUBER

Nach meinem bisherigen Kenntnisstand wurde beim Bundeszentralamt für Steuern die Datenbank ZAUBER (Zentrale Datenbank zur Speicherung und Auswertung von Umsatzsteuer-Betrugsfällen und Entwicklung von Risikoprofilen) eingerichtet, um länderübergreifend den **Umsatzsteuerbetrug** zu bekämpfen. Ausweislich der Aufgabenbeschreibung ist das Servicezentrum des Finanzamts München im Bereich der Umsatzsteuer allenfalls für die Annahme von Umsatzsteuer-Voranmeldungen zuständig. Nach Aussagen von Mitarbeitern des Servicezentrums ist jedoch selbst die bloße Abgabe von Umsatzsteuer-Voranmeldungen in der Vergangenheit praktisch nicht vorgekommen.

Gegenüber dem Staatsministerium der Finanzen habe ich deshalb keine Notwendigkeit dafür gesehen, den Bediensteten des Servicezentrums Abfragen in der Datenbank ZAUBER generell zu ermöglichen. Das Finanzministerium hat sich meiner Auffassung angeschlossen und umgehend veranlasst, dass die **Zugriffsberechtigung zur Datenbank ZAUBER für die Bediensteten des Servicezentrums München entfernt** wird.

9.7.4 Freie Suche nach Lohndaten - "Neugierabfragen"

Aufgrund von früheren Aussagen des Staatsministeriums der Finanzen war ich bisher davon ausgegangen, dass nach Einführung der Steueridentifikationsnummer eine freie - und damit auch namensbezogene - Suche der Finanzamtsbediensteten nach Lohndaten nicht mehr erforderlich sein wird. Im Zuge der Prüfung habe ich jedoch den Eindruck gewonnen, dass die **freie Suche nach Lohndaten im Bereich der Servicezentren auch weiterhin möglich** sein soll.

Diesbezüglich hat mir das Finanzministerium mitgeteilt, dass die im Rahmen der freien Suche nach Lohndaten in den Servicezentren getätigten Datenabrufe **vollständig protokolliert** würden. Die Protokolldaten würden auch durch die beauftragten Sachgebietsleiter **stichprobenartig überprüft.** Aufgrund der Erfahrungsberichte der mit den Protokollauswertungen betrauten Sachgebietsleiter sei festzuhalten, dass die Protokollierung eine nicht unerhebliche abschreckende Wirkung im Hinblick auf sogenannte "**Neugierabfragen**" entfalte.

Auch wenn die Anstrengungen des Staatsministeriums der Finanzen zur Wahrung des Steuergeheimnisses innerhalb der Finanzverwaltung anzuerkennen sind, bleibt aus datenschutzrechtlicher Sicht festzuhalten, dass eine stichprobenartige Überprüfung von Protokolldaten zu Datenabrufen immer **nur ein nachträgliches Korrektiv** darstellen kann.

9.7.5 Veranlagung von Steuerfällen

Wie oben dargestellt, werden im Servicezentrum des Finanzamts München gelegentlich auch Veranlagungen einfach gelagerter Steuerfälle vorgenommen. Diese Steuerfälle werden ausschließlich aus dem Zuständigkeitsbereich der Abteilung IV des Finanzamts München zur Verfügung gestellt. Aus einer - mir vorgelegten - Statistik über die der Prüfung vorhergehenden Monate hat sich jedoch ergeben, dass **insgesamt nur sehr vereinzelt Veranlagungen vorgenommen** wurden.

Ich habe dem Staatsministerium der Finanzen daher die Frage gestellt, ob angesichts der äußerst geringen Fallzahlen eine generelle Berechtigung der Servicezentrums-Mitarbeiter in ACUSTIG zur Durchführung von Veranlagungen - mit all den damit verbundenen Rechten - zur Aufgabenerfüllung des Servicezentrums überhaupt erforderlich ist. Ich habe dem Finanzministerium dementsprechend vorgeschlagen, diese Berechtigung im Einzelfall - je nach Bedarf - nur temporär einzuräumen. Das Staatsministerium der Finanzen hat meinen Vorschlag übernommen und angeordnet, dass **künftig die zu bearbeitenden Steuerfälle einzeln durch temporäre Zuständigkeitsübertragung für die Bearbeiter des Servicezentrums des Finanzamts München frei geschaltet** werden.

Das Finanzministerium will jedoch in den Servicezentren der übrigen bayerischen Finanzämter, in denen in erheblichem Umfang Veranlagungen von Arbeitnehmerfällen vorgenommen werden, die bisherigen Berechtigungen beibehalten. Dies ist aus datenschutzrechtlicher Sicht hinnehmbar.

9.7.6 Diskretionsräume

Die Namensschilder aller Sachbearbeiter des Servicezentrums enthalten auch den Hinweis, dass auf Wunsch die Angelegenheit des Besuchers in einem Diskretionsraum besprochen werden kann. Die zur Verfügung stehenden Diskretionsräume habe ich in Augenschein genommen.

Das **Vorhalten derartiger Diskretionsräume** ermöglicht auf Wunsch des Steuerpflichtigen die ungestörte Führung besonders sensibler Gespräche und ist **aus datenschutzrechtlicher Sicht ausdrücklich zu begrüßen.**

Insgesamt ist festzustellen, dass die datenschutzrechtliche Prüfung des Servicezentrums des Finanzamts München zu einer Anhebung des Datenschutzniveaus geführt hat.

10 Schulen und Hochschulen

10.1 Und nochmals: eGovernment-Projekt "Amtliche Schuldaten"

Bereits mehrfach habe ich zu dem eGovernment-Projekt "Amtliche Schuldaten" des Staatsministeriums für Unterricht und Kultus in meinen Tätigkeitsberichten eingehend Stellung genommen (siehe hierzu 23. Tätigkeitsbericht, Nr. 23.1, und 22. Tätigkeitsbericht, Nr. 21.1). Auch im Berichtszeitraum hat mich die datenschutzrechtliche Begleitung dieses eGovernment-Großprojekts wiederum stark in Anspruch genommen.

Im Rahmen der eGovernment-Initiative der Staatsregierung hat das Staatsministerium für Unterricht und Kultus im Jahr 2005 eine vollständige Neukonzeption des Verfahrens "Amtliche Schuldaten" in Angriff genommen. Gegenstand dieses Projekts ist zum einen eine umfassende Restrukturierung der Geschäftsprozesse der Kultusverwaltung mit dem Ziel eines effektiven, netzbasierten Schulverwaltungsverfahrens und zum anderen eine Neukonzeption der Schulstatistik, die insbesondere durch die Ermöglichung von Bildungsverlaufsuntersuchungen die längerfristige Bildungsplanung verbessern soll. So sehr ich auch eine Rationalisierung von Arbeitsprozessen befürworte, stellt doch die mit einem derart umfangreichen, multifunktionalen eGovernment-Großprojekt entstehende Dateninfrastruktur besondere datenschutz- und statistikrechtliche Anforderungen, die von den vorhandenen Rechtsvorschriften (Art. 85, 113 Abs. 1 BayEUG) nicht mehr abgedeckt werden.

Seit dem Start des eGovernment-Projekts "Amtliche Schuldaten" im Jahre 2005 habe ich daher beim Staatsministerium für Unterricht und Kultus **wiederholt die Schaffung einer normenklaren und umfassenden gesetzlichen Rechtsgrundlage angemahnt,** in der nicht nur die Datenschutzrechte der Schüler und Lehrer, sondern auch die mit der Umstellung der Schulstatistik von Summendaten auf Individualdaten verbundenen erhöhten statistikrechtlichen Anforderungen sichergestellt werden müssen.

Anfang des Jahres 2007 hat mir das Staatsministerium für Unterricht und Kultus erstmals einen umfassenden Gesetzentwurf für das Gesamtprojekt "Amtliche Schuldaten" vorgelegt. Seitdem konnte ich im Zuge einer mehrjährigen, kritischen und intensiven Diskussion mit dem Staatsministerium für Unterricht und Kultus erhebliche datenschutz- und statistikrechtliche Verbesserungen gegenüber den ursprünglichen Planungen erreichen. Am 19.05.2010 hat der **Landtag** schließlich mit dem "Gesetz zur Änderung des Bayerischen Gesetzes über das Erziehungs- und Unterrichtswesen" die **Rechtsgrundlage für das eGovernment-Projekt "Amtliche Schuldaten" beschlossen,** die im Wesentlichen am 01.06.2010 in Kraft getreten ist (GVBl S. 230).

Aus datenschutz- und statistikrechtlicher Sicht möchte ich insbesondere folgende Verbesserungen herausgreifen:

10.1.1 Schulverwaltung (Art. 85 a, 113 a BayEUG):

- Alle personenbezogenen **Schüler-, Eltern und Lehrerdaten** werden im Gesetz **abschließend** aufgeführt.
- Der Umfang der Schüler-, Eltern und Lehrerdaten wurde **deutlich reduziert.** Insbesondere entfällt die ursprünglich vorgesehene "Schüler-ID".
- Es werden **strenge Zugriffsrechte** festgelegt. Die bisherigen Befugnisse insbesondere der Schulaufsichtsbehörden werden nicht ausgeweitet. Es bestehen keine Zugriffsrechte von außerhalb der Schulverwaltung.
- Nur die im jeweiligen Einzelfall **zuständige Schule** hat Zugriff auf die personenbezogenen Daten "ihrer" Schüler und Erziehungsberechtigten. Ein Datenzugriff der Schulaufsichtsbehörden einschließlich des Staatsministeriums für Unterricht und Kultus ist insoweit ausgeschlossen.
- Für das **Lehrpersonal** ist die Wahrung der personalaktenrechtlichen Bestimmungen sichergestellt.
- Unmittelbar im Gesetz werden **strenge Löschungsfristen** festgelegt.
- Die **Datenbanken** werden nicht beim Staatsministerium für Unterricht und Kultus, sondern beim Landesamt für Statistik und Datenverarbeitung - **Rechenzentrum Süd** angesiedelt.

10.1.2 Schulstatistik (Art. 113 b BayEUG):

- Die bisher nur als Geschäftsstatistik erstellte Schulstatistik wird künftig als **amtliche Landesstatistik** im Sinne des Art. 9 BayStatG vom Landesamt für Statistik und Datenverarbeitung durchgeführt. Damit gilt das strenge **Statistikgeheimnis** des Art. 17 BayStatG.
- Die **Erhebungs- und Hilfsmerkmale** werden im Gesetz im Einzelnen festgelegt. Es erfolgt eine frühestmögliche Pseudonymisierung/Anonymisierung.
- Das zur Erstellung von Bildungsverlaufsstatistiken notwendige **Pseudonym** wird im Wege einer unumkehrbaren Einwegverschlüsselung erzeugt, um einen Rückschluss auf Einzelpersonen zuverlässig auszuschließen.
- **Schulübergreifende Geschäfts- oder Ergebnisstatistiken** werden ausschließlich von den - vom Verwaltungsvollzug strikt abgeschotteten - Statistikstellen des Staatsministeriums für Unterricht und Kultus und des Staatsinstituts für Schulqualität und Bildungsforschung erstellt.

Darüber hinaus verpflichtet das Gesetz die Staatsregierung, die **Auswirkungen der Neuregelung insbesondere in datenschutzrechtlicher Hinsicht** spätestens fünf Jahre nach Inkrafttreten **zu evaluieren** und dem Landtag darüber zu berichten.

10.1.3 Zusammenfassung und Ausblick

Im Ergebnis kann ich daher feststellen, dass die nunmehr vorliegende, mit mir abgestimmte gesetzliche **Rechtsgrundlage für das eGovernment-Projekt "Amtliche Schuldaten" den datenschutz- und statistikrechtlichen Erfordernissen genügt.** Zu respektieren habe ich dabei die politische Entscheidung von Staatsregierung und Landtag, Bildungsverlaufsuntersuchungen auf der Grundlage einer - jetzt immerhin durch das Statistikgeheimnis geschützten - Totalerhe-

bung statt auf der Grundlage einer - von mir seit jeher grundsätzlich bevorzugten - wissenschaftlich basierten repräsentativen Stichprobenerhebung durchzuführen.

Nach Abschluss des Gesetzgebungsverfahrens gilt es, die korrekte praktische Umsetzung des Verfahrens aus datenschutzrechtlicher Sicht zu überprüfen. Ich sehe deshalb von meiner Seite auch in den nächsten Jahren noch Handlungsbedarf beim eGovernment-Projekt "Amtliche Schuldaten".

10.2 Nochmals: Internetauftritt von Schulen

Bereits im letzten Berichtszeitraum hatte ich mich intensiv mit datenschutzrechtlichen Problemen im Zusammenhang mit Schulhomepages befasst (siehe hierzu 23. Tätigkeitsbericht, Nr. 12.2.3 und Nr. 12.4). Auch in diesem Berichtszeitraum haben mich wieder zahlreiche Fragen rund um den Internetauftritt von Schulen beschäftigt.

10.2.1 Grundsatz: schriftliche Einwilligung

Für die weltweite Veröffentlichung personenbezogener Daten von Lehrkräften, Schülerinnen und Schülern, Erziehungsberechtigten und sonstigen am Schulleben Beteiligten auf der Schulhomepage - dazu gehören insbesondere auch Fotos - bedarf es grundsätzlich einer **freiwilligen, informierten und schriftlichen Einwilligung des jeweiligen Betroffenen**. Eine Ausnahme besteht nur hinsichtlich der dienstlichen Kommunikationsdaten (Name, Namensbestandteile, Vorname(n), Funktion, Amtsbezeichnung, Lehrbefähigung, dienstliche Anschrift, dienstliche Telefonnummer, dienstliche E-Mail-Adresse) der Schulleitung und von Lehrkräften, die an der Schule eine Funktion mit Außenwirkung wahrnehmen; lediglich insoweit ist keine Einwilligung erforderlich. Sind die Betroffenen noch minderjährig, so muss die Einwilligung bis zur Vollendung des 14. Lebensjahres durch die Erziehungsberechtigten und ab Vollendung des 14. Lebensjahres durch die Minderjährigen selbst **und** deren Erziehungsberechtigte erfolgen (siehe im Einzelnen Anlage 9 Nr. 3 der Verordnung des Staatsministeriums für Unterricht und Kultus zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes - im Folgenden: Durchführungsverordnung).

10.2.2 Kein bloßes Widerspruchsrecht

Bei der datenschutzrechtlichen Prüfung eines städtischen Gymnasiums der Landeshauptstadt München habe ich festgestellt, dass das Gymnasium lediglich im ersten Elternbrief zu Schuljahresbeginn in einem Unterpunkt auf die Veröffentlichung personenbezogener Daten auf der Schulhomepage hingewiesen und den Eltern ein befristetes Widerspruchsrecht eingeräumt hatte. Eine solche Verfahrensweise genügt den in Art. 15 Abs. 2 bis 4, 7 BayDSG aufgestellten **datenschutzrechtlichen Anforderungen an eine Einwilligung** keinesfalls. Vielmehr muss eine ausdrückliche schriftliche Einwilligung eingeholt werden. Dabei sind die Betroffenen darüber zu informieren, welche personenbezogenen Daten zu welchem Zweck auf die Homepage eingestellt werden sollen. Ferner ist im Einwilligungsformular darauf hinzuweisen, dass die Einwilligung freiwillig und widerruflich ist sowie dass den Betroffenen keine Nachteile entstehen, wenn sie die Einwilligung verweigern oder widerrufen.

10.2.3 Landeshauptstadt München: Einwilligungsformulare

Um den bei der Prüfung festgestellten datenschutzrechtlichen Mangel zu beheben, hat die für das städtische Gymnasium zuständige Datenschutzbeauftragte des Schul- und Kultusreferats der Landeshauptstadt München **mehrere Formblätter für Einwilligungserklärungen** - je eines für minderjährige Schülerinnen und Schüler, volljährige Schülerinnen und Schüler, Lehrkräfte und Verwaltungspersonal sowie Mitglieder des Elternbeirats - entwickelt. Diese Einwilligungsformulare regeln umfassend die Problematik der Veröffentlichung personenbezogener Daten durch die Schule, nicht nur auf der Schulhomepage, sondern auch im **Jahresbericht** und in der örtlichen **Tagespresse**. Die mit mir abgestimmten Formblätter hat die Datenschutzbeauftragte des Schul- und Kultusreferats u.a. allen in der Landeshauptstadt München gelegenen Schulen aller Schularten zur Verfügung gestellt, so dass erfreulicherweise eine große Breitenwirkung erzielt werden konnte.

10.2.4 Passwortgeschützter Bereich

Im Zusammenhang mit schulischen Homepages wurde ich des Öfteren mit der Frage konfrontiert, ob auf eine Einwilligung verzichtet werden könne, wenn die personenbezogenen Daten in einen passwortgeschützten Bereich der Schulhomepage eingestellt würden, auf den nur berechtigte Lehrkräfte, Schülerinnen und Schüler sowie Erziehungsberechtigte Zugriff hätten.

Hierzu ist aus datenschutzrechtlicher Sicht Folgendes festzustellen:

- Bei der Veröffentlichung in einem passwortgeschützten Bereich der Schulhomepage kann eine Einwilligung nur insoweit entfallen, als das Einwilligungserfordernis gerade darauf beruht, dass die personenbezogenen Daten weltweit im Internet veröffentlicht werden und damit eine Datenübermittlung an die Allgemeinheit vorliegt. Soweit hingegen personenbezogene Daten betroffen sind, deren Bekanntgabe - unabhängig von der Veröffentlichungsform - auch dann einer Einwilligung bedarf, wenn diese lediglich an Lehrkräfte, Schülerinnen und Schüler sowie Eltern weitergegeben werden, wird eine Einwilligung durch die Einrichtung eines passwortgeschützten Bereichs auf der Internetseite nicht entbehrlich.

- Daran gemessen können z.B. **Sprechstundenlisten** und **Vertretungspläne** (siehe hierzu 23. Tätigkeitsbericht, Nr. 12.4) auch ohne schriftliche Einwilligung der Betroffenen in einen nur Lehrkräften, Schülerinnen und Schülern sowie Eltern zugänglichen, geschützten Bereich der Schulhomepage eingestellt werden. Denn nur die weltweite Übermittlung dieser Daten an die Allgemeinheit wäre mit dem Datenschutz nicht vereinbar; hingegen ist die Bekanntgabe an Lehrkräfte, Schülerinnen und Schüler sowie Eltern der jeweiligen Schule - wie bei herkömmlichen, papiergebundenen Sprechstundenlisten und Vertretungsplänen - gem. Art. 85 Abs. 1 Satz 1 BayEUG datenschutzrechtlich möglich. Bei **Elternbriefen** und sonstigen klassen- und fachbezogenen Informationen kommt es auf den Inhalt an. Enthalten diese personenbezogene Daten, deren Bekanntgabe an Lehrkräfte, Schülerinnen und Schüler sowie Eltern nur mit Einwilligung der Betroffenen möglich ist (z.B. die Schwangerschaft einer Lehrkraft), ist auch bei einer Veröffentlichung in einem geschützten Bereich der Homepage eine Einwilligung erforderlich.

- Aus **technischer und organisatorischer Datenschutzsicht** sind die Inhalte eines geschützten Bereichs bei der Übertragung durch geeignete Verschlüsselung zu sichern (https). Der Zugriff ist durch ein Passwort zu schützen, das mindestens zu Beginn jedes Schuljahres zu wechseln ist und auf geeignete Weise sicher den Zugriffsberechtigten mitzuteilen ist. Die Art der betroffenen Daten kann es erlauben, ausnahmsweise von der Forderung nach einem individuellen Login/Passwort pro Benutzer, das auch nur diesem Benutzer bekannt ist, abzuweichen. Sollte es bei dieser Vorgehensweise zu Sicherheitsproblemen kommen (z.B. Bekanntwerden des Passworts für eine Vielzahl von Nichtberechtigten, etwa durch unerlaubte Publizierung im Internet), so ist das Passwort unverzüglich zu wechseln. Sollte es auch dann erneut zu Problemen kommen, sind allerdings individuelle Passwörter für die einzelnen Benutzer unumgänglich.

- Schließlich ist zu beachten, dass die Veröffentlichung personenbezogener Daten in einem geschützten Bereich der Schulhomepage einer **datenschutzrechtlichen Freigabe** des Internetauftritts **durch den für die Schule zuständigen behördlichen Datenschutzbeauftragten** bedarf. Denn die Einrichtung eines geschützten Bereichs auf der Schulhomepage ist in Anlage 9 der Durchführungsverordnung nicht vorgesehen und damit auch vom Staatsministerium für Unterricht und Kultus nicht generell freigegeben. Einen geschützten Bereich einzurichten, kommt deshalb vor allem für Schulen in kommunaler Trägerschaft in Betracht, da in diesen Fällen der behördliche Datenschutzbeauftragte der Kommune tätig werden kann. Schwieriger erweist sich die Umsetzung hingegen bei staatlichen Schulen, die - gestützt auf § 2 der Durchführungsverordnung - leider oftmals keinen behördlichen Datenschutzbeauftragten bestellt haben. Außerdem bedarf nach Nr. 9 der "Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus und Wissenschaft, Forschung und Kunst vom 19.04.2001, KWMBl S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl S. 354) die Einrichtung eines geschützten Bereichs auf der Schulhomepage **bei staatlichen Schulen der Genehmigung durch das Staatsministerium für Unterricht und Kultus**.

10.3 Passwortgeschützte Lernplattformen wie "BayernMoodle"

Im schulischen Bereich hat E-Learning - das Lehren und Lernen unter Einsatz elektronischer Medien - mittlerweile auch zur Entwicklung "**virtueller Klassenzimmer", sog. Lernplattformen,** geführt. So wird den bayerischen Gymnasien beispielsweise von den Ministerialbeauftragten für die Gymnasien in Bayern die Lernplattform "BayernMoodle" kostenfrei zur Verfügung gestellt. "BayernMoodle" hat inzwischen deutlich über 30.000 Nutzer. Ebenso kostenfrei können die bayerischen Realschulen im Rahmen des Bayerischen Realschulnetzes die Lernplattform "BRN-Moodle" nutzen. Bei Moodle (modular object-oriented dynamic learning environment) handelt es sich um eine Lernplattform auf Open-Source-Basis, die nicht nur als bloße "Materialverteilstation" fungiert, sondern einen "Online-Kursraum" zur Verfügung stellt. In diesem können u.a. Arbeitsmaterialien und Lernaktivitäten bereitgestellt sowie vielfältige Kommunikationsmöglichkeiten unter den Nutzern eröffnet werden. In aller Regel kostenpflichtige Lernplattformen können daneben auch von privaten Anbietern bezogen werden.

10.3.1 Datenschutzrechtliche Problematik

Aus datenschutzrechtlicher Sicht sind derartige Lernplattformen durchaus problematisch. Zum einen, weil sich die Nutzer in aller Regel personalisiert anmelden müssen. Zum anderen, weil alle Nutzungsbewegungen protokolliert werden können. So kann beispielsweise festgehalten werden, welcher Nutzer wann auf welche Seite zugegriffen hat oder sich ob und wie an Tests beteiligt hat. Damit besteht die Möglichkeit, detaillierte Verhaltensprofile der einzelnen Nutzer anzulegen.

Dem hierdurch ausgelösten datenschutzrechtlichen Regelungsbedarf ist das Staatsministerium für Unterricht und Kultus - in Abstimmung mit mir - durch Erlass der Anlage 10 "Passwortgeschützte Lernplattform" der Verordnung zur Durchführung des Art. 28 Abs. 2 des Bayerischen Datenschutzgesetzes (im Folgenden: Durchführungsverordnung) nachgekommen (siehe hierzu 23. Tätigkeitsbericht, Nr. 12.2.4). **In Anlage 10 der Durchführungsverordnung finden sich detailliert die rechtlichen Rahmenbedingungen für den Einsatz von passwortgeschützten Lernplattformen an bayerischen Schulen**, beispielsweise im Hinblick auf den zulässigen Umfang der Datenspeicherung sowie die zulässige Speicherdauer.

Unter diesem spezifisch bayerischen Datenschutzregime wurden "BayernMoodle" und "BRN-Moodle" von der bayerischen Kultusverwaltung entwickelt. Insoweit gebotene datenschutzrechtliche Verbesserungen konnte ich in Zusammenarbeit mit dem Staatsministerium für Unterricht und Kultus erreichen.

10.3.2 Rechtsgrundlage: Einwilligung

Nach Nr. 3.2 und 3.3 der Anlage 10 der Durchführungsverordnung **müssen die Schulen für den Einsatz von passwortgeschützten Lernplattformen grundsätzlich die Einwilligung der Lehrkräfte sowie der Schüler und/oder Erziehungsberechtigten einholen.** Diese Einwilligungserklärungen müssen unter Beachtung der vom bayerischen Gesetzgeber in Art. 15 Abs. 2 bis 4 und 7 BayDSG aufgestellten, strengen Anforderungen erfolgen. Danach stellt eine Einwilligung insbesondere nur dann eine tragfähige Rechtsgrundlage dar, wenn sie **freiwillig, informiert und grundsätzlich schriftlich** erfolgt.

Im Berichtszeitraum bin ich von verschiedener Seite darauf aufmerksam gemacht worden, dass zahlreiche Schulen die geforderte Einwilligung pauschal - beispielsweise im Rahmen eines (Unterpunktes eines) Elternbriefes - einholen, also ohne die Betroffenen vorher auch nur ansatzweise über Gegenstand und Einsatzzweck der passwortgeschützten Lernplattform sowie Art, Umfang, Verarbeitung, Nutzung und Löschung der dort gespeicherten personenbezogenen Daten aufzuklären. Diese Vorgehensweise hat nicht nur bei vielen Schülern und Erziehungsberechtigten zu Unklarheiten und Unsicherheiten geführt; sie genügt auch nicht den gesetzlichen Anforderungen an eine informierte Einwilligung.

10.3.3 Rundschreiben des Kultusministeriums

Vor diesem Hintergrund habe ich das Staatsministerium für Unterricht und Kultus gebeten, im Rahmen seiner datenschutzrechtlichen Gesamtverantwortung gem. Art. 25 Abs. 1 BayDSG die Schulen für die schul- und datenschutzrechtliche

Problematik des Einsatzes von passwortgeschützten Lernplattformen zu sensibilisieren. Gebeten habe ich das Kultusministerium insbesondere darum, dafür zu sorgen, dass die Schulen den Anforderungen des Bayerischen Datenschutzgesetzes und der Anlage 10 der Durchführungsverordnung Rechnung tragen. Zudem habe ich beim Kultusministerium angeregt, den Schulen je eine Muster-Einwilligungserklärung für Lehrkräfte und Schüler/Erziehungsberechtigte zur Verfügung zu stellen.

Das **Staatsministerium für Unterricht und Kultus** ist meiner Bitte mit **Rundschreiben vom 18.08.2010** (Az. I.5-5 L 0572.2/28/16) **an alle öffentlichen Schulen und staatlich anerkannten Ersatzschulen** sowie an alle nachgeordneten Schulaufsichtsbehörden rechtzeitig vor dem Unterrichtsbeginn des Schuljahres 2010/2011 nachgekommen; in diesem Zusammenhang hat es den Schulen auch die mit mir abgestimmten **Muster-Einverständniserklärungen** zur künftigen Verwendung übersandt.

10.4 Weitergabe von Schülerdaten zu Werbezwecken

Gleich in einer Reihe von Fällen wurde ich im Berichtszeitraum darauf aufmerksam, dass noch immer Daten und Unterlagen über Schülerinnen und Schüler sowie deren Erziehungsberechtigte von Schulen an außerschulische Stellen für kommerzielle Zwecke weitergegeben werden. Dabei macht es keinen Unterschied, ob die Schulen die Daten selbst weitergeben oder ob sie Datenerhebungen durch außerschulische Stellen - oftmals getarnt als **Geschenkauslobungen** oder **(Wissens-)Wettbewerbe** - in der Schule dulden. Aufgefallen in diesem Zusammenhang sind mir vor allem **Kreditinstitute, Krankenkassen und (Buch-) Direktvertriebsunternehmen**, aber auch nichtgewerbliche Akteure wie beispielsweise **Musikchöre**, die an Schulen um neue Mitglieder werben.

Als besonders anschauliches Beispiel greife ich folgenden Fall heraus: Die Erziehungsberechtigten eines ABC-Schützen haben mich darüber informiert, dass die Eltern aller künftigen Schulanfänger noch vor dem ersten Schultag persönlich adressierte Anschreiben der örtlichen **Sparkasse** erhalten hatten. In diesen Schreiben hatte die Sparkasse Glückwünsche zur Einschulung des Kindes übermittelt und eine - persönlich von Sparkassenmitarbeitern in der Schule zu überreichende - Trinkflasche ausgelobt. "Daneben" hatte die Sparkasse auf die Bedeutung des richtigen Umgangs mit Geld hingewiesen und insoweit sogleich ihre Beratung angeboten. Die für die Anschreiben erforderlichen Adress- und Namensdaten der Erziehungsberechtigten der künftigen Schulanfänger hatte die Sparkasse von der Grundschule erhalten.

Obwohl es sich nicht nur in diesem Beispielsfall um eine Problematik handelt, die ich in der Vergangenheit schon mehrmals aufgegriffen habe (siehe hierzu 16. Tätigkeitsbericht 1994, Nr. 16.1), werden offensichtlich die insoweit zu beachtenden schul- und datenschutzrechtlichen Vorgaben noch nicht von allen Schulen eingehalten. Ich nehme dies daher zum Anlass, nochmals aus schul- und datenschutzrechtlicher Sicht auf Folgendes hinzuweisen:

Nach Art. 85 Abs. 1 Satz 1 und Abs. 2 Satz 1 BayEUG ist den Schulen die Weitergabe von Daten und Unterlagen über Schülerinnen und Schüler und Erziehungsberechtigte an außerschulische Stellen untersagt, es sei denn, die Weitergabe erfolgt zur Erfüllung der den Schulen durch Rechtsvorschriften jeweils zugewiesenen Aufgaben oder es besteht ein rechtlicher Anspruch auf die Herausgabe der

Daten. In Konkretisierung dieser gesetzlichen Bestimmung ist es gem. Nr. 4.4 Buchstabe b) Satz 4 Spiegelstrich 1 der mit mir abgestimmten und für die Schulen verbindlichen "Erläuternden Hinweise für die Schulen zum Vollzug des Bayerischen Datenschutzgesetzes" (Bekanntmachung des Bayerischen Staatsministeriums für Unterricht und Kultus und Wissenschaft, Forschung und Kunst vom 19.04.2001, KWMBl S. 112, geändert durch Bekanntmachung vom 10.10.2002, KWMBl S. 354) **den Schulen verboten, Schülerdaten zu Werbezwecken weiterzugeben.** Diese Bestimmung korrespondiert mit dem in Art. 84 Abs. 1 BayEUG vom bayerischen Gesetzgeber aufgestellten Verbot der kommerziellen Werbung an Schulen. So sind nach Art. 84 Abs. 1 BayEUG der Vertrieb von Gegenständen aller Art, Ankündigungen und Werbung hierzu, das Sammeln von Bestellungen sowie der Abschluss sonstiger Geschäfte in der Schule grundsätzlich untersagt.

Art. 84 Abs. 1 BayEUG Kommerzielle und politische Werbung
Der Vertrieb von Gegenständen aller Art, Ankündigungen und Werbung hierzu, das Sammeln von Bestellungen sowie der Abschluss sonstiger Geschäfte sind in der Schule untersagt. [2] Ausnahmen im schulischen Interesse insbesondere für Sammelbestellungen regelt die Schulordnung.

Art. 85 Abs. 1 Satz 1 und Abs. 2 Satz 1 BayEUG Erhebung und Verarbeitung von Daten
(1) Die Schulen dürfen die zur Erfüllung der ihnen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlichen Daten erheben, verarbeiten und nutzen.
(2) Die Weitergabe von Daten und Unterlagen über Schülerinnen und Schüler und Erziehungsberechtigte an außerschulische Stellen ist im Übrigen untersagt, falls nicht ein rechtlicher Anspruch auf die Herausgabe der Daten nachgewiesen wird.

In dem von mir eingangs herausgegriffenen Beispielsfall war die Übermittlung der Schülerdaten durch die Grundschule an die örtliche Sparkasse weder zur Erfüllung der den Schulen durch Rechtsvorschriften zugewiesenen Aufgaben erforderlich, noch hatte die Sparkasse einen rechtlichen Anspruch auf die Herausgabe dieser Daten. Ich habe die Schule daher darauf hingewiesen, dass die Datenübermittlung unzulässig war. Die Grundschule hat unverzüglich ihren Fehler eingeräumt und mir für die Zukunft die genaue Beachtung der schul- und datenschutzrechtlichen Vorgaben zugesichert.

Um den notwendigen Schutz personenbezogener Daten von Schülerinnen und Schülern sowie deren Erziehungsberechtigten sicherzustellen, habe ich - über meine einzelfallbezogene Kontrolltätigkeit hinaus - das Staatsministerium für Unterricht und Kultus eindringlich gebeten, alle bayerischen Schulen für die Problematik nochmals eingehend zu sensibilisieren. Das **Staatsministerium für Unterricht und Kultus** hat meiner Bitte mit **Rundschreiben** vom 30.04.2009 (Az. II.1-5 O 4101.2-6.46827) und vom 09.06.2010 (Az. II.1-5 O 4101.2-6.141716) jeweils **an alle bayerischen öffentlichen Schulen** entsprochen.

In diesem Zusammenhang möchte ich noch auf zwei Punkte aufmerksam machen: Zum einen, dass auf die zur Rechtfertigung der Übermittlung von Schülerdaten an Kreditinstitute in der Vergangenheit (fälschlicherweise) gerne herangezogene "Pflege des Spargedankens in den Schulen" schon deswegen nicht mehr abgestellt werden kann, weil die zugrundeliegende Bekanntmachung aus dem Jahr 1978 mit Wirkung vom 01.09.2009 aufgehoben wurde. Zum anderen, dass

die vorgenannten Grundsätze auch dann gelten, wenn die außerschulischen Akteure mit den Schülerdaten grundsätzlich billigenswerte Zwecke, wie etwa die Förderung der Musikalität von Schülerinnen und Schülern, verfolgen.

10.5 Meldungen von Erkrankungen an der Neuen Grippe durch Schulen

Ende 2009 wurde ich durch eine Eingabe darauf aufmerksam, dass einige Schulen - unter Berufung auf eine entsprechende Anweisung des Staatsministeriums für Unterricht und Kultus - an der Neuen Grippe (sog. "Schweine-Grippe") erkrankte Schüler namentlich sowohl an das jeweils zuständige Gesundheitsamt als auch an das Kultusministerium gemeldet hatten. Meine umgehend eingeleitete Sachverhaltsaufklärung ergab, dass das Staatsministerium für Unterricht und Kultus - nach Abstimmung mit dem Staatsministerium für Umwelt und Gesundheit - die Schulen in der Tat mit Schreiben vom 08.09.2009 darauf hingewiesen hatte, dass Erkrankungen an der Neuen Grippe gemäß § 34 Abs. 6 Infektionsschutzgesetz (IfSG) namentlich dem zuständigen Gesundheitsamt zu melden sind. Derartige Erkrankungen stellten auch besondere Vorkommnisse im Sinne des § 35 Lehrerdienstordnung (LDO) dar und seien entsprechend den dort genannten öffentlichen Stellen (vorgesetzte Behörde und Aufwandsträger, ggf. Kultusministerium, ggf. Ministerialbeauftragter) zu melden.

§ 34 Abs. 6 IfSG Gesundheitliche Anforderungen, Mitwirkungspflichten, Aufgaben des Gesundheitsamtes
Werden Tatsachen bekannt, die das Vorliegen einer der in den Absätzen 1, 2 oder 3 aufgeführten Tatbestände annehmen lassen, so hat die Leitung der Gemeinschaftseinrichtung das zuständige Gesundheitsamt unverzüglich zu benachrichtigen und krankheits- und personenbezogene Angaben zu machen. Dies gilt auch beim Auftreten von zwei oder mehr gleichartigen, schwerwiegenden Erkrankungen, wenn als deren Ursache Krankheitserreger anzunehmen sind. Eine Benachrichtigungspflicht besteht nicht, wenn der Leitung ein Nachweis darüber vorliegt, dass die Meldung des Sachverhalts durch eine andere in § 8 genannte Person bereits erfolgt ist.

§ 35 LDO Besondere Vorkommnisse
Bei Vorkommnissen von besonderer Bedeutung für die Schule, wie Bränden, großen Wasserschäden, Einbrüchen im Schulhaus, schweren Unfällen während des Unterrichts oder im Schulbereich usw. ist der vorgesetzten Behörde und dem Aufwandsträger unverzüglich zu berichten. In besonders schwerwiegenden Fällen ist das Staatsministerium für Unterricht und Kultus fernmündlich zu verständigen. Von schriftlichen Berichten ist bei Realschulen, Fachoberschulen, Berufsoberschulen und Gymnasien dem Ministerialbeauftragten ein Abdruck vorzulegen.

Die Rechtslage war in diesem Schreiben jedoch zumindest sehr missverständlich wiedergegeben worden. Da Erkrankungen an der Neuen Grippe nicht unter die in § 34 Abs. 1 bis 3 IfSG aufgezählten Tatbestände fallen, besteht für die betroffene Schule keine einzelfallbezogene Meldepflicht an das Gesundheitsamt nach § 34 Abs. 6 Satz 1 IfSG. Dem Gesundheitsamt sind von der betroffenen Schule nach § 34 Abs. 6 Satz 2 IfSG Erkrankungen an der Neuen Grippe vielmehr nur dann namentlich zu melden, wenn in zeitlichem Zusammenhang mindestens zwei gleichartige, schwerwiegende Krankheitsfälle aufgetreten sind. Keinesfalls aber dürfen unter Berufung auf § 35 LDO personenbezogene Angaben, insbesondere die Namen der Erkrankten, an die dort genannten öffentlichen Stellen

gemeldet werden. Denn die Übermittlung dieser personenbezogenen Gesundheitsdaten ist allenfalls zur Aufgabenerfüllung der Gesundheitsämter erforderlich; die Namen der Erkrankten benötigen zur Erfüllung ihrer gesetzlich zugewiesenen Aufgaben aber weder die Kultusverwaltung noch gar die schulischen Aufwandsträger. Meiner Auffassung nach können der Kultusverwaltung und den Aufwandsträgern unter den in § 35 LDO genannten Voraussetzungen daher höchstens die Tatsache und ggf. die Anzahl der Erkrankungen an der Neuen Grippe in einer bestimmten Schule mitgeteilt werden.

Nach Abstimmung mit dem Staatsministerium für Umwelt und Gesundheit hat sich das Staatsministerium für Unterricht und Kultus meiner Rechtsauffassung angeschlossen. In seiner Stellungnahme hat es mir ausdrücklich versichert, dass es zu keinem Zeitpunkt seine Absicht gewesen sei, die Namen erkrankter Personen zu sammeln bzw. in Erfahrung zu bringen. Vielmehr wollte das Kultusministerium lediglich über die Anzahl der aufgetretenen Fälle informiert sein, um bei Bedarf entsprechende Maßnahmen einleiten zu können. Im Übrigen sei es nur in wenigen Einzelfällen zu namentlichen Meldungen durch Schulen gekommen.

Da die Neue Grippe zwischenzeitlich stark abgeflaut war, habe ich auf die Versendung eines klarstellenden Schreibens durch das Kultusministerium an alle Schulen in Bayern verzichtet. Ich habe aber das Staatsministerium für Unterricht und Kultus gebeten, diejenigen Schulen, die datenschutzrechtlich unzulässige Meldungen erstattet hatten, schriftlich auf die Rechtslage hinzuweisen. Dieser Bitte ist das Kultusministerium umgehend nachgekommen.

Im Falle etwaiger zukünftiger Pandemien habe ich das Staatsministerium für Unterricht und Kultus ebenso wie das Staatsministerium für Umwelt und Gesundheit gebeten, die **Schulen über Art und Umfang der gesundheits- und schulrechtlichen Meldepflichten rechtzeitig, klar und unmissverständlich zu unterrichten.** Dies betrifft insbesondere die Fragen, unter welchen Voraussetzungen eine gesetzliche Meldepflicht der Schulen besteht und ob und an wen die Schulen personenbezogene Daten übermitteln dürfen. Dabei sollten die Schulen auch darauf hingewiesen werden, ob die Schüler bzw. deren Sorgeberechtigte gegenüber der Schule zur Meldung verpflichtet sind (§ 34 Abs. 5 IfSG).

Gesundheitsdaten stellen besonders schutzwürdige Daten dar. Sie dürfen von den Schulen nur unter den gesetzlich geregelten Voraussetzungen erhoben und übermittelt werden.

10.6 Datenschutz beim "Nationalen Bildungspanel"

Im Berichtszeitraum habe ich mich intensiv mit dem Datenschutz beim "Nationalen Bildungspanel" für die Bundesrepublik Deutschland (National Educational Panel Study - NEPS) auseinandergesetzt. Diese Längsschnittstudie wird von einem Konsortium unter Federführung der Otto-Friedrich-Universität Bamberg durchgeführt. Beteiligt sind zahlreiche weitere Universitäten und Forschungseinrichtungen; mit den tatsächlichen Befragungen sind verschiedene Erhebungsinstitute beauftragt. Ziel des "Nationalen Bildungspanels" ist es nach eigener Darstellung, Längsschnittdaten zu Kompetenzentwicklungen, Bildungsprozessen, Bildungsentscheidungen und Bildungsrenditen über die gesamte Lebensspanne zu erheben. NEPS umfasst acht Etappen (u.a. zu den Bereichen Kindergarten, Schule, Hochschule und Berufsausbildung) mit ca. 144 Einzelbefragungen. Die NEPS-Daten sollen der nationalen und internationalen Wissenschaft in anonymi-

sierter Form zugänglich gemacht werden; sie sollen auch die Grundlagen für eine verbesserte Bildungsberichterstattung und Politikberatung in Deutschland schaffen. Nähere Informationen zu NEPS sind auf der Homepage der Otto-Friedrich-Universität Bamberg unter www.uni-bamberg.de/neps/ zu finden.

NEPS ist derart umfassend und vielgestaltig, dass es mir nicht möglich ist, an dieser Stelle über alle bei meiner Tätigkeit aufgetretenen datenschutzrechtlichen Problemstellungen erschöpfend zu berichten. Aufgreifen möchte ich nachfolgend nur einige der Punkte, die bei meiner - leider zumeist unter äußerst engen zeitlichen Vorgaben von NEPS vorgenommenen - datenschutzrechtlichen Bewertung von NEPS eine besondere Rolle gespielt haben und die zudem auch für vergleichbare Langzeit-Forschungsprojekte von Bedeutung sein können:

10.6.1 Einwilligung

Die Erhebung personenbezogener Daten ist bei Befragungen wie NEPS nur auf der Grundlage einer Einwilligung der Betroffenen möglich. Die Einwilligung muss insbesondere freiwillig, widerrufbar, informiert und in aller Regel schriftlich erfolgen (vgl. Art. 15 Abs. 2 bis 4 und 7 BayDSG).

Im Einzelnen stellten sich bei NEPS diesbezüglich vor allem folgende Probleme:

- Bei einem Teil der Befragungen möchte NEPS auch Daten zu Personen erfahren, die keine Einwilligung erteilt haben, diese mitunter sogar ausdrücklich verweigert haben, und deshalb nicht an der Befragung teilnehmen (Nichtteilnehmer). Auf diese Weise sollen Aussagen über die sog. **Grundgesamtheit** getroffen werden können. Da die Erhebung personenbezogener Daten eine Einwilligung des jeweiligen Betroffenen voraussetzt, ist ein solches Vorgehen nur zulässig, wenn die **Daten zu den Nichtteilnehmern** zu keinem Zeitpunkt einer bestimmten oder bestimmbaren Person zugeordnet werden können, also von Anfang an anonymisiert sind (vgl. Art. 4 Abs. 8 BayDSG).

  Auf meine entsprechende Forderung hin hat NEPS verbesserte Verfahrensweisen entwickelt, mit denen eine erhebliche Reduzierung des Identifizierungsrisikos erreicht werden konnte.

- Bei verschiedenen Etappen von NEPS werden Telefoninterviews mit einem Elternteil durchgeführt. Dabei stellt NEPS dem Gesprächspartner auch zahlreiche **Fragen zu seinem (Ehe-)Partner.** Da auf diese Weise personenbezogene Daten des Partners erhoben werden, muss auch der Partner mit der Befragung einverstanden sein.

  Nach einer längeren und intensiven Diskussion mit NEPS konnte ich erreichen, dass nunmehr in den betreffenden Einwilligungsformularen die Möglichkeit vorgesehen ist, dass beide (Ehe-)Partner die Einwilligungserklärung unterzeichnen. Unterschreibt trotzdem nur eine Person, muss diese zusätzlich erklären, dass sie von ihrem Partner bevollmächtigt ist, die Einwilligungserklärung auch in dessen Namen zu unterschreiben, und dass der Partner insbesondere damit einverstanden ist, dass auch die Fragen zu seiner Person beantwortet werden.

- Teilweise ist bei NEPS vorgesehen, dass die Teilnehmer an der Befragung **Sach- und Geldgeschenke (sog. Incentives)** erhalten sollen. Incentivierungen sind datenschutzrechtlich bedenklich, weil die Gefahr besteht, dass die Einwilligung nicht mehr freiwillig ist. Datenschutzrechtlich unzulässig sind deshalb insbesondere Geschenke, mit denen ein Gruppendruck aufgebaut wird. Dies wäre z.B. dann der Fall, wenn die Höhe eines einer Schulklasse gewährten Geldbetrags von der Zahl der teilnehmenden Schüler abhängig gemacht würde.

  NEPS hat mir zugesichert, dass es bei den Befragungen allenfalls kleinere, individuelle Belohnungen für einzelne Teilnehmer verteilen wird. Hingegen wird keine auf die Klasse oder die Jahrgangsstufe bezogene oder von der Teilnahmequote abhängige Incentivierung stattfinden.

- Die Betroffenen müssen darauf hingewiesen werden, dass die Teilnahme an der NEPS-Befragung freiwillig ist. **Freiwilligkeit** bedeutet dabei auch, dass Betroffene, die grundsätzlich ihr Einverständnis mit der Befragung erklärt haben, das Recht haben, einzelne Fragen nicht zu beantworten.

  Auf meinen Hinweis hin hat NEPS in verschiedene Dokumente eine entsprechende Erläuterung für die Befragten aufgenommen.

- Eine Einwilligung ist nur wirksam, wenn der Betroffene ausreichend über die Datenumgänge bei NEPS informiert ist. Verschiedentlich hatte ich deshalb angemahnt, dass die **Information der Betroffenen** erweitert und verbessert wird; so sind z.B. die genauen Themen der Befragung anzugeben.

  Soweit im Rahmen von NEPS besonders sensible personenbezogene Daten - wie z.B. über die rassische oder ethnische Herkunft, die religiöse Überzeugung, die Gesundheit oder das Sexualleben - erhoben werden, muss sich die Einwilligungserklärung ausdrücklich auch auf derartige Daten beziehen (siehe Art. 15 Abs. 7 Satz 2 Nr. 2 BayDSG).

10.6.2 Umgang mit den erhobenen Daten

Im Hinblick auf die Verarbeitung und Nutzung personenbezogener Daten, die für Zwecke der wissenschaftlichen Forschung erhoben oder gespeichert worden sind, sieht Art. 23 BayDSG - Datenschutzgesetze anderer Bundesländer enthalten im Wesentlichen vergleichbare Bestimmungen - wichtige Regelungen vor: So dürfen diese Daten nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden. Die erhobenen personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale, mit denen eine Identifizierung einer bestimmten oder bestimmbaren Person möglich ist (also insbesondere Name, Adresse etc.), von den inhaltlichen Einzelangaben gesondert zu speichern. Die Identifizierungsmerkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

Im Einzelnen ergibt sich daraus für NEPS vor allem Folgendes:

- Da es sich bei NEPS um eine sog. **Panelstudie** handelt, also dieselben Personen über einen längeren Zeitraum hinweg mehrfach befragt werden

und die zu den verschiedenen Zeitpunkten erhobenen Daten zusammengeführt werden müssen, ist eine sofortige Anonymisierung der Daten nicht möglich. Nach den genannten Bestimmungen muss NEPS die Identifizierungsmerkmale und die Einzelangaben allerdings gesondert speichern. Spätestens nach Abschluss der letzten Befragung zu einer Person müssen die Daten anonymisiert werden.

- Darauf hingewirkt habe ich, dass die **Namen und Adressen der Teilnehmer** nur bei den von NEPS mit der Befragung beauftragten Erhebungsinstituten, nicht hingegen bei der Otto-Friedrich-Universität Bamberg selbst gespeichert sind, um das Risiko einer unzulässigen Reidentifizierung zu verringern.

- Ziel von NEPS ist es u.a., für die nationale und internationale Wissenschaft Forschungsdaten zur Verfügung zu stellen. Entscheidend aus datenschutzrechtlicher Sicht ist, dass nur anonymisierte Daten weitergegeben und veröffentlicht werden. Um dies sicherzustellen, hat NEPS eine **differenzierte Anonymisierungs- und Verwertbarkeitsstrategie** entwickelt.

10.6.3 Fazit und Ausblick

Insgesamt betrachtet ist festzustellen, dass die Verantwortlichen von NEPS datenschutzrechtlichen Belangen schon im Ansatz einen hohen Stellenwert beimessen. Darüber hinaus konnte ich durch mein - wenn auch oft unter extremem Zeitdruck stehendes - Tätigwerden zahlreiche datenschutzrechtliche Verbesserungen erreichen. Im Komplex der Schuletappe habe ich zudem eng und vertrauensvoll mit dem Staatsministerium für Unterricht und Kultus zusammengearbeitet, das die Befragungen im Schulbereich zu genehmigen hatte und dabei seinerseits besonders auf den Schutz der Persönlichkeitsrechte der betroffenen Schüler, Eltern und Lehrer geachtet hat.

Für die Zukunft bleibt abzuwarten, ob bei der praktischen Umsetzung des "Nationalen Bildungspanels" für die Bundesrepublik Deutschland (weitere) datenschutzrechtliche Probleme erkennbar werden, die - im Rahmen meiner Kontrollkompetenz für bayerische öffentliche Stellen - mein erneutes Tätigwerden erfordern.

10.7 Neuregelung der studentischen Evaluation der Lehre

Durch eine Erweiterung des Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG hat der Bayerische Landtag mit Wirkung vom 15.07.2009 die bayerischen Hochschulen ermächtigt, die konkreten personenbezogenen Ergebnisse der studentischen Einzelevaluationen der Lehrveranstaltungen nicht nur - wie bisher - allein dem Fakultätsrat und der Hochschulleitung, sondern auch allen Studierenden der Fakultät bekannt zu geben. Diese Ausweitung des Empfängerkreises soll zur Verbesserung des Instruments der studentischen Evaluation der Lehre und damit zur Verbesserung der Qualität der Lehre insgesamt führen.

Art. 10 BayHSchG Bewertung der Forschung, Lehre, Förderung des wissenschaftlichen Nachwuchses und der Gleichstellung der Geschlechter
(3) Im Rahmen der Bewertung der Lehre können die Studierenden als Teilnehmer und Teilnehmerinnen von Lehrveranstaltungen anonym über Ablauf sowie

Art und Weise der Darbietung des Lehrstoffs befragt und die gewonnenen Daten verarbeitet werden; eine Auskunftspflicht besteht nicht. Die personenbezogenen Daten dürfen nur dem Fakultätsrat, den Studierenden der Fakultät und der Hochschulleitung bekannt gegeben und für die Bewertung der Lehre verwendet werden; die wesentlichen Ergebnisse der studentischen Befragungen werden den Mitgliedern der Hochschule, gegebenenfalls unter Hinzufügung der Stellungnahme der betreffenden Lehrperson (Satz 3), zugänglich gemacht. Den betroffenen Lehrpersonen ist in den Fällen des Satzes 2 Gelegenheit zur Stellungnahme zu den Bewertungsergebnissen zu geben.

Mit der Problematik der studentischen Evaluation der Lehre habe ich mich bereits in der Vergangenheit mehrfach kritisch auseinandergesetzt. Hierzu verweise ich insbesondere auf meine Ausführungen in meinem 22. Tätigkeitsbericht, Nr. 12.1, in meinem 21. Tätigkeitsbericht, Nr. 20.2.1, und in meinem 19. Tätigkeitsbericht, Nr. 15.4. Zwar verkenne ich nicht, dass der Verbesserung der Qualität der Lehre an den Hochschulen ein hohes Gewicht zukommt, nicht zuletzt seitdem sich die Studierenden mit Studiengebühren auch unmittelbar an den Kosten der Hochschulausbildung beteiligen. Im Ressortanhörungsverfahren habe ich dennoch **verfassungs- und datenschutzrechtliche Bedenken gegen die massive Ausweitung des Empfängerkreises der personenbezogenen Einzelergebnisse der studentischen Evaluationen** geltend gemacht, mit denen ich mich aber leider nicht durchsetzen konnte.

Im Einzelnen:

Die bisherige Regelung beruhte weitgehend auf einem austarierten Kompromiss, der dem verfassungsrechtlich erforderlichen Ausgleich zwischen dem Informationsinteresse der Hochschule einschließlich der Studierenden einerseits und dem Recht der Lehrpersonen auf Wahrung ihrer Persönlichkeitsrechte andererseits diente. Vor diesem Hintergrund sah Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG alte Fassung (a.F.) vor, dass die bei der Evaluierung von Lehrveranstaltungen durch die teilnehmenden Studierenden erhobenen personenbezogenen Daten **vollständig** nur dem Fakultätsrat und der Hochschulleitung bekannt gegeben werden durften. Darüber hinaus gestattete der (insoweit weiterhin geltende) Art. 10 Abs. 3 Satz 2 Halbsatz 2 BayHSchG nur die Weitergabe der **wesentlichen** Ergebnisse der studentischen Befragungen an alle Mitglieder der Hochschule und damit auch an die Studierenden. Dies bedeutete, dass den Studierenden der Fakultät bereits nach der früheren Rechtslage eine personenbezogene Zusammenfassung der Bewertungen - etwa in Form einer "Benotung" - bekannt gegeben werden durfte.

Die Neuregelung in Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG sieht nunmehr vor, dass die personenbezogenen Daten **vollständig** auch an alle Studierenden der Fakultät weitergegeben werden dürfen. Ich halte dies für einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung des Lehrpersonals. Mir wurde - auch in direkten Gesprächen mit dem federführenden Staatsministerium für Wissenschaft, Forschung und Kunst - kein einziges Argument genannt, das belegt hätte, dass eine konsequente Umsetzung der bestehenden Möglichkeit zur Bekanntgabe einer personenbezogenen Zusammenfassung an die Studierenden als milderes Mittel nicht ausgereicht hätte und deshalb eine Weitergabe der vollständigen personenbezogenen Daten an die Studierenden erforderlich ist. Vor der Schaffung erweiterter Veröffentlichungsbefugnisse sollten meiner Auffassung nach jedoch erst die bestehenden Möglichkeiten ausgeschöpft werden.

Darüber hinaus habe ich zu bedenken gegeben, dass der Evaluationsprozess ohne die konstruktive Mitwirkung des Lehrpersonals nicht gelingen kann. Primäres Ziel einer Evaluation sollte es sein, der betroffenen Lehrperson eine eigene Einschätzung der Qualität der von ihr angebotenen Lehrveranstaltung zu ermöglichen, um diese ggf. zu verbessern. Durch die Bekanntgabe der vollständigen Ergebnisse an alle Studierenden einer Fakultät wird jedoch einer weitergehenden Veröffentlichung der vollständigen personenbezogenen Daten (z.B. weltweit über das Internet) Tür und Tor geöffnet. Daran vermag auch die Tatsache nichts zu ändern, dass die Daten den Studierenden zunächst nur im Intranet gegen Eingabe eines Passwortes zugänglich gemacht werden sollen, da einzelne Studierende diese Daten anschließend unschwer weiterverbreiten können. Vor diesem Hintergrund habe ich auch die beamtenrechtliche Fürsorgepflicht als betroffen angesehen. Müssen die Lehrpersonen aber befürchten, dass ihre bei der studentischen Evaluation von den Hochschulen erhobenen personenbezogenen Daten detailliert weltweit verbreitet werden, wird ihre Bereitschaft, die Evaluation als Instrument zur Verbesserung von Lehre und Studium einzusetzen, spürbar abnehmen. Weltweit öffentlich "an den Pranger" gestellt zu werden, muss kein Dozent hinnehmen (so auch Bayerischer Verwaltungsgerichtshof, Urteil vom 10.03.2010, Az. 7 B 09.1906, zur Eröffnung eines Internet-Lehrerbewertungsforums durch einen Schüler).

Meiner Auffassung nach ist es den Hochschulen allerdings auch nach der Neufassung des Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG durchaus **weiterhin möglich**, mit Rücksicht auf die Persönlichkeitsrechte des Lehrpersonals die **Bekanntgabe der Evaluationsergebnisse an die Studierenden der Fakultät auf die wesentlichen Ergebnisse zu beschränken**. Denn nach Art. 10 Abs. 3 Satz 1 BayHSchG können - nicht müssen - die Studierenden befragt werden und nach Art. 10 Abs. 3 Satz 2 Halbsatz 1 BayHSchG dürfen - nicht müssen - die personenbezogenen Daten den Studierenden der Fakultät bekannt gegeben werden. Dies eröffnet die Möglichkeit einer verfassungskonformen, restriktiven Auslegung. Insbesondere haben die Hochschulen im Rahmen ihres Ermessensspielraums darauf zu achten, dass unsachliche oder gar herabwürdigende Aussagen nicht weitergegeben werden.

Ich würde es daher sehr begrüßen, wenn die Hochschulen von der Möglichkeit Gebrauch machen, den Studierenden der Fakultät weiterhin lediglich eine personenbezogene Zusammenfassung der wesentlichen Ergebnisse der studentischen Befragungen bekanntzugeben.

10.8 Zugriff auf elektronische Notenkonten von Studierenden

Im Hochschulbereich wurde mir im Berichtszeitraum u.a. **folgender Sachverhalt** vorgetragen:

Für jeden Studierenden einer Fakultät einer bayerischen Universität existiere ein elektronisches Notenkonto, in dem alle erbrachten Prüfungsleistungen erfasst würden. Für den internen Zugang zu diesen Daten seien keine Einschränkungen bekannt.

Bedenklich sei insbesondere, dass bei mündlichen Prüfungen dem Prüfer vorab ein vollständiger Kontoauszug zur Verfügung gestellt werde. Auf diese Weise erhalte der Prüfer Einblick in alle Noten, die der Studierende bislang erhalten habe.

Für die Abnahme der Prüfung sei es jedoch unerheblich, welche Noten ein Studierender im Einzelnen erzielt habe. Vielmehr werde die Gefahr begründet, dass der Prüfer die Prüfung voreingenommen durchführe.

Darüber hinaus komme es oft vor, dass sich Dozenten ohne Wissen und ohne Einwilligung den Kontoauszug eines Studierenden besorgten, etwa wenn sich der Studierende um einen Praktikumsplatz oder ein Stipendium bewerbe. Es sei verständlich, dass der Dozent über den Leistungsstand des jeweiligen Bewerbers Bescheid wissen müsse. Allerdings solle er den Kontoauszug nur mit Einwilligung des betroffenen Studierenden erhalten können.

Die betroffene Fakultät habe ich unverzüglich um eine ausführliche Stellungnahme zu dem vorgetragenen Sachverhalt gebeten. Im Rahmen meiner **datenschutzrechtlichen Bewertung des Zugangs zu den in den Notenkonten gespeicherten personenbezogenen Daten der Studierenden** - sei es durch Gewährung eines elektronischen Zugriffs auf die Daten oder durch Weitergabe eines Kontoauszugs - habe ich sodann Folgendes ausgeführt:

Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Studierenden bestimmt sich nach den jeweils geltenden Vorschriften über den Schutz personenbezogener Daten (Art. 42 Abs. 4 Satz 1 BayHSchG). Werden personenbezogene Daten Studierender innerhalb der Hochschule weitergegeben oder zugänglich gemacht, handelt es sich datenschutzrechtlich um eine Datennutzung im Sinne des Art. 4 Abs. 7 BayDSG. Eine solche Datennutzung ist u.a. nur zulässig, wenn sie zur Erfüllung der Aufgaben der Hochschule erforderlich ist (Art. 17 Abs. 1 Nr. 1 BayDSG). Inwieweit der Zugang zu den in den Notenkonten gespeicherten Daten erforderlich ist, ist letztlich eine Frage des Einzelfalls.

Art. 42 Abs. 4 Satz 1 BayHSchG Allgemeine Bestimmungen
Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten der Studierenden und Gaststudierenden bestimmt sich nach den jeweils geltenden Vorschriften über den Schutz personenbezogener Daten.

Allerdings lassen sich **folgende allgemeinen Grundsätze** aufstellen:

- Ein **elektronischer Zugang zu den Notenkonten** kann in aller Regel nur für diejenigen Mitarbeiter der Hochschule als erforderlich angesehen werden, die unmittelbar mit der Aufgabe der Prüfungs- und Notenverwaltung befasst sind. Das sind die Mitarbeiter in Prüfungsämtern, Prüfungssekretariaten o.ä., die insbesondere Prüfungen zu organisieren und Zeugnisse auszustellen haben. Sind einzelne Mitarbeiter nur in bestimmten Bereichen tätig, z.B. weil die Mitarbeiter unterschiedliche Studiengänge betreuen, sind die Zugangsberechtigungen entsprechend zu differenzieren.

- Die **Studierenden selbst** können selbstverständlich jederzeit einen vollständigen Auszug ihres Notenkontos erhalten.

- Die **Weitergabe von (vollständigen) Kontoauszügen an andere Personen** als die jeweils betroffenen Studierenden kommt hingegen nur eingeschränkt in Betracht. So ist es z.B. in dem eingangs geschilderten Fall, in dem sich ein Studierender um einen **Praktikumsplatz** oder ein **Stipendium** bewirbt und hierfür von einem Dozenten ein Gutachten erstellt werden soll, ohne Weiteres möglich, dass der Dozent die Daten bei dem betroffe-

nen Studierenden selbst erhebt, indem er den Studierenden auffordert, einen Kontoauszug vorzulegen. Die Weitergabe von Kontoauszügen ohne Wissen und ohne Einwilligung des betroffenen Studierenden ist in diesem Zusammenhang hingegen nicht erforderlich. Gleiches gilt etwa für die **Studienberatung:** auch hier ist es möglich, dass diejenigen Studierenden, die eine Beratung wünschen, ihren Kontoauszug selbst vorlegen oder im Einzelfall in die Weitergabe einer Notenübersicht an den mit der Studienberatung betrauten Hochschulmitarbeiter einwilligen.

- Für **mündliche Prüfungen** reicht es häufig aus, dass die Prüfer eine **eingeschränkte Übersicht über die besuchten Lehrveranstaltungen** erhalten. Hingegen kann es aus den genannten Gründen oftmals nicht als erforderlich angesehen werden, den Prüfern vollumfänglich auch die genauen Einzelleistungen (Noten) und Prüfungsergebnisse bekanntzugeben. In einem solchen Fall wäre es dann datenschutzrechtlich unzulässig, den Prüfern einen vollständigen Auszug aus dem Notenkonto zur Verfügung zu stellen.

Im konkreten Fall hat die betroffene Fakultät aufgrund meines Eingreifens die bisherige Praxis des vergleichsweise unbeschränkten internen Zugangs zu den in den Notenkonten gespeicherten personenbezogenen Daten der Studierenden gestoppt und eine datenschutzgerechte, am Erforderlichkeitsprinzip orientierte Neuregelung getroffen.

11 Personalwesen

11.1 Neues Dienstrecht - Dienstunfallunterlagen und Beamtenversorgung

Im Berichtszeitraum habe ich die im Zuge der Föderalismusreform unter dem Begriff "Neues Dienstrecht" erfolgte grundlegende Neugestaltung des Dienstrechts der bayerischen Beamten aus datenschutzrechtlicher Sicht intensiv begleitet. Besonders erwähnen möchte ich hier die Teilbereiche "Dienstunfallunterlagen" und "Bayerisches Beamtenversorgungsgesetz".

11.1.1 Dienstunfallunterlagen

Vor dem Hintergrund der besonderen Sensibilität gesundheitsbezogener Daten enthält das seit 01.04.2009 geltende Personalaktenrecht der bayerischen Beamten in Art. 105 BayBG besondere Datenschutzbestimmungen für Unterlagen über Beihilfen, Heilfürsorge und Heilverfahren (u.a. getrennte Aufbewahrung von der übrigen Personalakte, Bearbeitung durch eine von der übrigen Personalverwaltung getrennte Organisationseinheit, enge Zweckbindung mit abschließend aufgezählten Ausnahmen). Die bis zum 31.03.2009 geltende Vorgängervorschrift des Art. 100 b Satz 5 BayBG a.F. sah dies darüber hinaus auch für Dienstunfallunterlagen vor. Über den Gesetzentwurf, mit dem die Anwendung der besonderen Datenschutzbestimmungen auf Dienstunfallunterlagen gestrichen wurde, hatte mich das Staatsministerium der Finanzen - unter Verstoß gegen Art. 32 Abs. 3 BayDSG - leider nicht unterrichtet.

Art. 105 BayBG Beihilfeunterlagen
Unterlagen über Beihilfen sind stets als Teilakte zu führen. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben. Die Beihilfeakte darf für andere als für Beihilfezwecke nur verwendet oder weitergegeben werden, wenn der oder die Beihilfeberechtigte und bei der Beihilfegewährung berücksichtigte Angehörige im Einzelfall einwilligen, die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Sätze 1 bis 4 gelten entsprechend für Unterlagen über Heilfürsorge und Heilverfahren.

So habe ich den Gesetzentwurf für das Neue Dienstrecht zum Anlass genommen, beim Staatsministerium der Finanzen im Hinblick auf die **Absenkung des Schutzniveaus für Dienstunfallunterlagen** - auch hier sind besonders sensible Personalaktendaten über den Gesundheitszustand eines Beamten betroffen - meine **erheblichen datenschutzrechtlichen Bedenken** vorzubringen:

- Im Rahmen der Dienstunfallfürsorge ist der Beamte verpflichtet, der hierfür zuständigen Behörde über seinen Gesundheitszustand sehr weitreichende Auskünfte zu erteilen und Unterlagen vorzulegen. Diese einerseits

sehr weitgehende Offenlegungspflicht des Beamten gegenüber dem Dienstherrn erfordert auf der anderen Seite einen besonderen Schutz der Vertraulichkeit seiner sensiblen medizinischen Daten. Notwendig ist die besondere Vertraulichkeit der Dienstunfallunterlagen gerade gegenüber der Personalstelle, um eine **ungerechtfertigte dienstliche Benachteiligung des Beamten** zu vermeiden.

- Darüber hinaus wird die gesetzliche Schutzvorschrift des Art. 67 BayBG, der im Fall einer Untersuchung zur Feststellung der Dienstunfähigkeit die Übermittlung von Gesundheitsdaten an die Personalstelle beschränkt, im Ergebnis ausgehöhlt: Die **Personalstelle** kann nunmehr bezüglich des Gesundheitszustands des Beamten nicht mehr nur die tragenden Feststellungen und Gründe eines medizinischen Gutachtens erfahren, sondern es können ihr **vollumfänglich sensible Daten über die Gesundheit** einschließlich vollständiger ärztlicher Gutachten **zur Kenntnis gelangen.** Für die Beeinträchtigung des Persönlichkeitsrechts eines Betroffenen ist es jedoch gleichgültig, ob die Personalstelle diese sensiblen Informationen aus einer Untersuchung zur Feststellung der Dienstunfähigkeit oder aus einer Untersuchung in einem Dienstunfallverfahren erhält.

  Art. 67 BayBG Mitteilung aus Untersuchungsbefunden
  (1) Wird in den Fällen des Art. 65 eine (amts-)ärztliche Untersuchung durchgeführt, teilt der Arzt oder die Ärztin im Einzelfall auf Anforderung der Behörde die tragenden Feststellungen und Gründe des Gutachtens und die in Frage kommenden Maßnahmen zur Wiederherstellung der Dienstfähigkeit mit, soweit deren Kenntnis für die Behörde unter Beachtung des Grundsatzes der Verhältnismäßigkeit für die von ihr zu treffende Entscheidung erforderlich ist.
  (2) Die ärztliche Mitteilung über die Untersuchungsbefunde nach Abs. 1 ist in einem gesonderten, verschlossenen und versiegelten Umschlag zu übersenden. Die an die Behörde übermittelten Daten dürfen nur für die nach § 26 BeamtStG zu treffende Entscheidung verarbeitet oder genutzt werden. Die Mitteilung ist verschlossen zur Personalakte zu nehmen.
  (3) Die Behörde hat vor der Untersuchung auf den Zweck der Untersuchung und auf die ärztliche Befugnis zur Übermittlung der Untersuchungsbefunde nach Abs. 1 an die Behörde hinzuweisen. Der Arzt oder die Ärztin übermittelt dem Beamten oder der Beamtin oder, soweit dem ärztliche Gründe entgegenstehen, dem Vertreter oder der Vertreterin eine Ablichtung der auf Grund dieser Vorschrift an die Behörde erteilten Auskünfte.

Anlass für die Gesetzesänderung war nach Mitteilung des Staatsministeriums der Finanzen **ein (!) Einzelfall**, in dem durch die Weitergabe der Daten von der Dienstunfallbehörde an die Personalstelle die Unrichtigkeit der Feststellungen eines Amtsarztes erkannt werden konnte. Dieser Einzelfall **vermag** aber die **generelle Absenkung des Schutzniveaus für Dienstunfallunterlagen nicht zu rechtfertigen.**

Ich habe das Staatsministerium der Finanzen deshalb im Rahmen des Gesetzentwurfs für das Neue Dienstrecht gebeten, die bereits zum 01.04.2009 erfolgte Gesetzesänderung zurückzunehmen. Allenfalls - so meine Auffassung - könnte darüber nachgedacht werden, eine Rechtsgrundlage dafür zu schaffen, dass bei begründeten Zweifeln an der Richtigkeit des amtsärztlichen Gutachtens in einem Verfahren über die Feststellung der Dienstunfähigkeit die Unfallfürsorgestelle auf

Anforderung der Personalstelle im Einzelfall die tragenden Feststellungen und Gründe eines im Dienstunfallverfahren eingeholten ärztlichen Gutachtens weiterleitet und in diesem Zusammenhang die Art. 67 Abs. 2 und 3 BayBG entsprechend gelten.

Das Staatsministerium der Finanzen war allerdings leider nicht bereit, die Gesetzesänderung zurückzunehmen und darüber nachzudenken, an geeigneter Stelle eine Rechtsgrundlage des vorgeschlagenen Inhalts zu schaffen. Es stellte sich dabei auf den Standpunkt, es ergebe sich bereits aus Art. 103 BayBG (Zugang zur Personalakte), dass Dienstunfallunterlagen als getrennte Teilakte geführt, von einer besonderen Organisationseinheit bearbeitet und nicht routinemäßig, sondern nur in begründeten Einzelfällen und im erforderlichen Umfang an die Personalstelle weitergeleitet werden dürfen. Immerhin hat sich das Staatsministerium der Finanzen nach einer längeren Diskussion dazu bereiterklärt, dies zur Sicherstellung eines angemessenen Datenschutzniveaus bei Dienstunfallunterlagen in einem Schreiben an die für die Dienstunfallfürsorge im staatlichen und nichtstaatlichen Bereich zuständigen Behörden klarzustellen. Diesen Vorschlag habe ich - wenn auch mit Bedenken - als Kompromiss akzeptiert.

Als ich nach einiger Zeit nachfragte, musste ich dann leider feststellen, dass das Staatsministerium der Finanzen bereits ein Schreiben an die für die staatliche Dienstunfallfürsorge zuständige Dienststelle Regensburg des Landesamts für Finanzen versandt hatte, dessen Inhalt ich nicht als Umsetzung des Kompromisses akzeptieren konnte. Denn die aus Sicht des Datenschutzes wesentlichen Aussagen fehlten; teilweise enthielt das Schreiben sogar kontraproduktive Ausführungen.

Auf meine erneute Intervention hin hat das **Staatsministerium der Finanzen** schließlich in einem ergänzenden Schreiben an das Landesamt für Finanzen **klar gestellt,** dass

- **Dienstunfallakten als getrennter Teilakt der Personalakten** zu führen sind sowie
- die **Auskunft aus bzw. die Vorlage von Dienstunfallakten an die personalverwaltende Stelle nicht routinemäßig, sondern nur in begründeten Einzelfällen** (namentlich bei Missbrauchs- und Täuschungsverdacht) und
- nur **im erforderlichen Umfang** erfolgen darf.

Ein entsprechendes Schreiben an die Dienstherrn im nichtstaatlichen Bereich soll noch gesondert ergehen.

11.1.2 Bayerisches Beamtenversorgungsgesetz

Aufgrund der Föderalismusreform sind nunmehr die Länder u.a. für die Regelung des Versorgungsrechts ihrer Richterinnen und Richter sowie der Beamtinnen und Beamten ihres Landes, ihrer Kommunen und der sonstigen ihrer Aufsicht unterstehenden Dienstherrn selbst zuständig. Der bayerische Gesetzgeber hat von dieser neuen Gesetzgebungskompetenz Gebrauch gemacht und als Teil des Neuen Dienstrechts das Bayerische Beamtenversorgungsgesetz (BayBeamtVG) erlassen, das mit Wirkung vom 01.01.2011 an die Stelle des bislang geltenden Bundesrechts tritt.

Der Gesetzentwurf des Staatsministeriums der Finanzen zum Bayerischen Beamtenversorgungsgesetz gab Anlass, diverse Anmerkungen und Verbesserungsvorschläge aus Sicht des Datenschutzes vorzubringen:

- In Bezug auf die **Anzeige- und Mitwirkungspflichten** des Art. 10 Abs. 2 BayBeamtVG habe ich das Staatsministerium der Finanzen insbesondere darum gebeten, im Gesetzestext klarer zum Ausdruck zu bringen, dass nach allgemeinen datenschutzrechtlichen Grundsätzen

  - Daten vorrangig beim betroffenen Versorgungsempfänger mit seiner Kenntnis zu erheben sind, eine Datenerhebung bei Dritten hingegen nur nachrangig in Betracht kommt,

  - erforderliche Zustimmungen im konkreten Einzelfall erklärt werden müssen, da eine pauschale Zustimmung zu einer Vielzahl unbestimmter Datenerhebungen nicht datenschutzgerecht ist und

  - die Datenerhebung auch bezüglich der Vorlage von Beweisurkunden am Maßstab der Erforderlichkeit zu messen ist.

  Insoweit habe ich dem Finanzministerium konkrete Formulierungsvorschläge vorgelegt.

Art. 10 BayBeamtVG Anzeige- und Mitwirkungspflichten
(1) Die Beschäftigungsstelle hat der Pensionsbehörde jede Verwendung von Versorgungsberechtigten unter Angabe der gewährten Bezüge, ebenso jede spätere Änderung der Bezüge oder die Zahlungseinstellung sowie die Gewährung einer Versorgung unverzüglich anzuzeigen.
(2) Versorgungsberechtigte haben der Pensionsbehörde unverzüglich
1. alle Tatsachen anzugeben, die für die Versorgung erheblich sind, und auf Verlangen der Pensionsbehörde der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen,
2. Änderungen in den Verhältnissen, die für die Versorgung erheblich sind oder über die im Zusammenhang mit der Versorgung Erklärungen abgegeben worden sind, mitzuteilen,
3. Beweismittel zu bezeichnen und auf Verlangen der Pensionsbehörde Beweisurkunden vorzulegen oder ihrer Vorlage zuzustimmen.
Satz 1 gilt entsprechend für Personen, die Versorgungsleistungen zu erstatten haben. Die Pensionsbehörde kann Erkenntnisse und Beweismittel an Sachverständige weitergeben, soweit dies zur Entscheidung über die Versorgung notwendig ist.
(3) Kommen Versorgungsberechtigte den ihnen nach Abs. 2 oder nach anderen Bestimmungen dieses Gesetzes auferlegten Mitwirkungsverpflichtungen schuldhaft nicht nach, so kann ihnen die Versorgung ganz oder teilweise auf Zeit oder auf Dauer entzogen werden. Beim Vorliegen besonderer Verhältnisse kann die Versorgung ganz oder teilweise wieder zuerkannt werden. Die Entscheidung trifft die Pensionsbehörde.

- Ferner habe ich das Staatsministerium der Finanzen darauf aufmerksam gemacht, dass die allgemeinen Anzeige- und Mitwirkungspflichten in Art. 10 Abs. 2 BayBeamtVG insbesondere auch sensible Daten über die Gesundheit betreffen. Die **Erhebung sensibler medizinischer Daten** stellt einen vergleichsweise schwerwiegenden Eingriff in das Grundrecht

auf informationelle Selbstbestimmung dar; sie muss deshalb vom Gesetzgeber selbst angeordnet und unter Beachtung des Grundsatzes der Verhältnismäßigkeit geregelt werden.

Orientiert an Art. 67 BayBG habe ich dem Staatsministerium der Finanzen konkrete Formulierungsvorschläge unterbreitet, durch welche gesetzlichen Maßgaben erreicht werden kann, dass beim Umgang mit Daten über die Gesundheit dem Grundrecht auf informationelle Selbstbestimmung der betroffenen Beamtinnen und Beamten ausreichend Rechnung getragen wird (u.a. Beschränkung der Anzeige- und Mitwirkungspflichten auf die tragenden Feststellungen, besondere organisatorische Maßnahmen für die Aufbewahrung und Übermittlung der medizinischen Daten, Information der Betroffenen im Fall einer Datenerhebung bei Dritten).

- Im Hinblick auf die in Art. 10 Abs. 3 BayBeamtVG enthaltenen **Sanktionen** habe ich angeregt, im Gesetzestext klarzustellen, dass ein vollständiger oder teilweiser Entzug von Versorgungsansprüchen nicht schon bei einer geringfügigen und unbedeutenden Verletzung der Anzeige- und Mitwirkungspflicht, sondern regelmäßig nur bei schwerwiegenden Verstößen gerechtfertigt ist. Ferner habe ich moniert, dass der Gesetzeswortlaut den Verlust des Leistungsanspruchs auch dann vorsieht, wenn eine (evt. unbedeutende) formale Pflichtverletzung überhaupt keinen Einfluss auf die Feststellung des materiellen Versorgungsanspruchs hat, und auch diesbezüglich eine Klarstellung im Gesetz für notwendig gehalten.

- Im Bereich der Unfallfürsorge verpflichtet Art. 45 Abs. 3 Satz 1 BayBeamtVG die Beteiligten, sich ärztlich oder psychologisch untersuchen oder beobachten zu lassen. Mit einer solchen Verpflichtung ist ein erheblicher Grundrechtseingriff verbunden. Ich habe deshalb kritisiert, dass Art. 45 Abs. 3 Satz 1 BayBeamtVG diese Verpflichtung allgemein auf den gesamten Bereich der Unfallfürsorge ausweitet. Im bislang geltenden Bundesrecht war eine Verpflichtung zur ärztlichen Untersuchung nur für bestimmte Fallgestaltungen vorgesehen. Eine für den gesamten Bereich der Unfallfürsorge geltende **Untersuchungspflicht** habe ich schon nicht für erforderlich gehalten. Denn können die Voraussetzungen eines Anspruchs auf Unfallfürsorge nicht nachgewiesen werden, weil sich der Betroffene einer ärztlichen Untersuchung verweigert, so geht dies nach materiellen Beweislastregeln ohnehin zu seinen Lasten. Darüber hinaus fehlt es an der Angemessenheit des Grundrechtseingriffs, wenn die Untersuchungspflicht umfassend auf den gesamten Bereich der Unfallfürsorge ausgeweitet wird. Daran gemessen habe ich das Staatsministerium der Finanzen gebeten, im Gesetzentwurf die Untersuchungspflicht auf die schon bislang im Bundesrecht vorgesehenen Tatbestände zu begrenzen und im Übrigen eine Untersuchung nur mit Einwilligung der Betroffenen vorzusehen.

Art. 45 Abs. 3 BayBeamtVG Allgemeines
Auf Verlangen der Pensionsbehörde haben sich die Beteiligten von einer von dieser bestimmten Person ärztlich oder psychologisch untersuchen oder beobachten zu lassen und die erforderlichen Auskünfte zu erteilen, soweit dies zur Entscheidung über die Gewährung von Unfallfürsorge erforderlich ist. Die Pensionsbehörde ist zur Weitergabe von Erkenntnissen und Beweismitteln an die mit der Begutachtung beauftragte Person berechtigt.

- Zu Art. 45 Abs. 3 Satz 2 BayBeamtVG, der die zuständigen Pensionsbehörden zur **Übermittlung personenbezogener Daten an einen Gutachter** berechtigt, habe ich das Staatsministerium der Finanzen gebeten, im Gesetzestext klarzustellen, dass diese Übermittlung nur zulässig ist, soweit sie zur Entscheidung über die Gewährung von Unfallfürsorge erforderlich ist.

- Moniert habe ich außerdem, dass in Art. 45 Abs. 3 BayBeamtVG eine datenschutzrechtliche **Rechtsgrundlage für die Übermittlung aus Untersuchungs- oder Beobachtungsbefunden von den Gutachtern an die Pensionsbehörde** fehlt, und diesbezüglich vorgeschlagen, Art. 67 BayBG für entsprechend anwendbar zu erklären.

- Schließlich habe ich kritisiert, dass Art. 50 Abs. 2 Satz 1 BayBeamtVG die **Verpflichtung von Verletzten, sich Maßnahmen des Heilverfahrens zu unterziehen,** im Vergleich zum bislang geltenden Bundesrecht ausweitet. Da mit einer solchen Verpflichtung ebenfalls ein erheblicher Grundrechtseingriff verbunden ist und keine Gründe für deren Ausweitung erkennbar waren, habe ich das Staatsministerium der Finanzen gebeten, auf die Ausweitung zu verzichten.

Leider war das Staatsministerium der Finanzen nicht bereit, meine Anmerkungen und (konkreten) Formulierungsvorschläge aufzugreifen. Es bleibt zu hoffen, dass es der Praxis gelingt, den Persönlichkeitsrechten der Betroffenen durch eine grundrechtskonforme Auslegung des Bayerischen Beamtenversorgungsgesetzes Rechnung zu tragen. Dafür werde ich mich jedenfalls auch weiterhin einsetzen.

11.2 eGovernment-Großprojekte im Personalbereich - VIVA, BayZeit und BayRMS

Im Berichtszeitraum habe ich drei staatliche eGovernment-Großprojekte im Personalbereich von bayernweiter Bedeutung datenschutzrechtlich intensiv begleitet: das Personal- und Stellenmanagementsystem VIVA, das Zeitmanagementsystem BayZeit und das Reisekostenmanagementsystem BayRMS.

11.2.1 Personal- und Stellenmanagementsystem VIVA

VIVA ist ein automatisiertes Verfahren zur Personal- und Stellenverwaltung, das unter Federführung des Staatsministeriums der Finanzen insbesondere für den landesweiten Einsatz in allen Behörden, Gerichten und sonstigen Stellen des Freistaats Bayern entwickelt wurde. Am 06.05.2009 hat das Staatsministerium der Finanzen das Verfahren im Einvernehmen mit der Staatskanzlei, den übrigen Staatsministerien, dem Obersten Rechnungshof und dem Landtagsamt für den bayernweiten Einsatz datenschutzrechtlich freigegeben; die Freigabe ist im Bayerischen Behördennetz (BYBN) auf der Seite des Staatsministeriums der Finanzen unter der Rubrik "Datenschutz" - "Datenschutzrechtliche Freigaben" abrufbar. Nicht nur in die datenschutzrechtliche Freigabe, sondern auch in die langjährige Entwicklung des Verfahrens war ich eingebunden.

Auf Folgendes möchte ich besonders hinweisen:

- **Automatisierte Datenabrufe von Personalaktendaten** durch andere Behörden, die über den Datenfluss zwischen Grundakt, Nebenakten und Teilakten hinausgehen, sind unzulässig, soweit durch besondere Rechtsvorschriften nichts anderes bestimmt ist (Art. 111 Abs. 1 Satz 3 BayBG). Es liegt in der Verantwortung der Ressorts, der Staatskanzlei, des Obersten Rechnungshofs und des Landtagsamts, dafür Sorge zu tragen, dass bei VIVA die automatisierten Datenabrufe für ihren Bereich rechtlich zulässig sind.

  Art. 111 BayBG Automatisierte Verarbeitung und Nutzung von Personalaktendaten
  (1) Personalaktendaten dürfen in Dateien nur für Zwecke der Personalverwaltung oder der Personalwirtschaft verarbeitet und genutzt werden. Ihre Übermittlung ist nur nach Maßgabe des Art. 108 zulässig. Ein automatisierter Datenabruf durch andere Behörden ist unzulässig, soweit durch besondere Rechtsvorschrift nichts anderes bestimmt ist.
  (2) Personalaktendaten im Sinn des Art. 105 dürfen automatisiert nur im Rahmen ihrer Zweckbestimmung und nur von den übrigen Personaldateien technisch und organisatorisch getrennt verarbeitet und genutzt werden.
  (3) Von den Unterlagen über medizinische oder psychologische Untersuchungen und Tests dürfen im Rahmen der Personalverwaltung nur die Ergebnisse automatisiert verarbeitet oder genutzt werden, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten oder der Beamtin dient.
  (4) Beamtenrechtliche Entscheidungen dürfen nicht ausschließlich auf Informationen und Erkenntnisse gestützt werden, die unmittelbar durch automatisierte Verarbeitung und Nutzung personenbezogener Daten gewonnen werden.
  (5) Bei erstmaliger Speicherung ist dem oder der Betroffenen die Art der über ihn oder sie gemäß Abs. 1 gespeicherten Daten mitzuteilen, bei wesentlichen Änderungen ist er oder sie zu benachrichtigen. Ferner sind die Verarbeitungs- und Nutzungsformen automatisierter Personalverwaltungsverfahren zu dokumentieren und einschließlich des jeweiligen Verwendungszwecks sowie der regelmäßigen Empfänger und des Inhalts automatisierter Datenübermittlung allgemein bekanntzugeben.

- **Zugang zu Personalaktendaten** dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren (Art. 103 BayBG). Diese Vorgaben gelten uneingeschränkt für den Zugang zu den bei VIVA gespeicherten Personalaktendaten. Die Zugriffsrechte auf diese Daten sind in einem detaillierten Rechte- und Rollenkonzept beschrieben und festgelegt. Die Berechtigten dürfen nur insoweit Zugriff auf die Daten erhalten, als dies zur Erfüllung der oben genannten Aufgaben erforderlich ist. Dies gilt selbstverständlich auch im Verhältnis zwischen übergeordneter und nachgeordneter Behörde. Die Ressorts, die Staatskanzlei, der Oberste Rechnungshof und das Landtagsamt tragen die Verantwortung dafür, dass das Rechte- und Rollenkonzept in ihrem jeweiligen Geschäftsbereich präzise umgesetzt und in der Praxis eingehalten wird.

Art. 103 BayBG Zugang zur Personalakte
Zugang zur Personalakte dürfen nur Beschäftigte haben, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind, und nur soweit dies zu Zwecken der Personalverwaltung oder der Personalwirtschaft erforderlich ist; dies gilt auch für den Zugang im automatisierten Abrufverfahren.

- Speichernde Stelle im Sinne des Art. 4 Abs. 9 BayDSG und damit **datenschutzrechtlich verantwortlich** ist jeweils die personalverwaltende Stelle des betroffenen Beamten, Richters etc. Im technischen Sinne gespeichert sind die Daten beim Landesamt für Finanzen, das im Auftrag der jeweiligen personalverwaltenden Stelle als Auftragnehmer einer Auftragsdatenverarbeitung gem. Art. 6 BayDSG tätig wird.

11.2.2 Zeitmanagementsystem BayZeit

Das unter Federführung des Staatsministeriums der Finanzen entwickelte Verfahren "Basiskomponente Integriertes Zeitmanagement - BayZeit" soll als Gesamtsystem die Verwaltung der Bereiche Zeiterfassung, Erledigung von Korrekturbuchungen und Beantragung von Abwesenheitszeiten, Zutrittskontrolle, Dienst-/Abwesenheitsplanung und Abwesenheitsübersicht sowie Planung von Schicht- und Wechselschichtdienst automatisiert durchführen. BayZeit ist für den landesweiten Einsatz in grundsätzlich allen Behörden, Gerichten und sonstigen Stellen des Freistaats Bayern vorgesehen; im Polizeibereich soll die Variante "BayZeit-Polizei" verwendet werden. Am 12.04.2010 hat das Staatsministerium der Finanzen das Verfahren im Einvernehmen mit der Staatskanzlei, den übrigen Staatsministerien, dem Obersten Rechnungshof und dem Landtagsamt datenschutzrechtlich freigegeben; die Freigabe ist im Bayerischen Behördennetz (BYBN) auf der Seite des Staatsministeriums der Finanzen unter der Rubrik "Datenschutz" - "Datenschutzrechtliche Freigaben" abrufbar. Auch die Entwicklung von BayZeit habe ich über viele Jahre hinweg datenschutzrechtlich begleitet.

Von besonderer datenschutzrechtlicher Relevanz erscheinen mir folgende Punkte:

- BayZeit enthält ein **Anwesenheitstableau**, bei dem einem (Fach-) Vorgesetzten der aktuelle An-/Abwesenheitsstatus der ihm zugeordneten Mitarbeiter auf den jeweiligen Tag bezogen angezeigt wird. Dies begegnet keinen durchgreifenden datenschutzrechtlichen Bedenken.

  Problematisiert habe ich allerdings, dass die Vorgesetzten im Anwesenheitstableau darüber hinaus offenbar über Sortierungsfunktionen verfügen sollten (z.B. nach der Reihenfolge der Kommenden). Hierzu hat mir das Staatsministerium der Finanzen versichert, dass von den standardmäßig von der Hersteller-Software angebotenen Sortierfunktionen bei BayZeit nur mehr eine Sortierung nach "Name" - ggf. in Verbindung mit "Abteilung" oder "Kostenstelle" -, hingegen insbesondere nicht mehr nach "Kommt Uhrzeit" oder "Anwesenheitszeit" enthalten ist. Gegen die verbliebenen Sortierungsmöglichkeiten habe ich keine Einwände mehr erhoben.

- Datenschutzrechtlich problematisch ist, dass BayZeit einen **graphischen Abwesenheitsplaner** enthält, der dem Fachvorgesetzten einen Überblick

über die Abwesenheiten seiner Mitarbeiter in den zurückliegenden sechs Monaten gewährt. Derartige Kenntnisse über die Abwesenheiten in der Vergangenheit benötigt die Personalverwaltung, nicht hingegen der Fachvorgesetzte. Für bedenklich halte ich insbesondere, dass sich der Fachvorgesetzte damit jederzeit einen Überblick über die Zahl der Krankheitstage eines Mitarbeiters in der Vergangenheit verschaffen kann. Dies geht erheblich über den Informationsstand hinaus, den der Fachvorgesetzte durch die Krankmeldung eines Mitarbeiters am Tag der Erkrankung erhält.

Das Staatsministerium der Finanzen hat den graphischen Abwesenheitsplaner damit begründet, dass der Fachvorgesetzte dafür Sorge zu tragen habe, dass die Urlaubsgenehmigung innerhalb der Organisationseinheit ausgewogen erfolge. Dies sei insbesondere von Bedeutung für die Urlaubsgenehmigung an Brückentagen oder in Ferienzeiten. Darüber hinaus werde vom Fachvorgesetzten erwartet, dass er auch die Aspekte der Gesundheitsfürsorge mit im Auge behalte.

Ich konnte hingegen keine überzeugenden Gründe dafür erkennen, warum der Fachvorgesetzte zur Erfüllung seiner Aufgaben den durch den graphischen Abwesenheitsplaner vermittelten Überblick über die Abwesenheiten seiner Mitarbeiter in der Vergangenheit benötigen sollte. Die Überlegung, der Vorgesetzte könne hiermit Brückentage besonders gerecht unter den Mitarbeitern verteilen, halte ich nicht für ausreichend. Differenzen zwischen Mitarbeitern über die Urlaubsplanung in Ferienzeiten können meiner Meinung nach besser durch ein Gespräch mit den Betroffenen als durch einen Blick in einen Abwesenheitsplan gelöst werden. Auch benötigt der Fachvorgesetzte keinen taggenauen Überblick über die Abwesenheiten in den letzten sechs Monaten, damit er etwaige allgemeine Aufgaben im Bereich der Gesundheitsfürsorge erfüllen kann. Zu bedenken ist dabei, dass es nicht Aufgabe des Fachvorgesetzten, sondern der Personalverwaltung ist, bei längerer krankheitsbedingter Abwesenheit eines Mitarbeiters die nötigen Maßnahmen - wie z.B. ein Angebot zum Betrieblichen Eingliederungsmanagement oder eine ärztliche Untersuchung beim Amtsarzt - einzuleiten.

Dem Datenschutz wurde immerhin wenigstens dadurch Rechnung getragen, dass der im System ursprünglich unbegrenzt angelegte Datenzugriff in die Vergangenheit jetzt nurmehr die letzten sechs Monate umfasst und über die graphische Darstellung hinaus keine weiteren Auswertungsmöglichkeiten bestehen.

- Hingewiesen habe ich ferner darauf, dass dem **Vertreter eines Vorgesetzten** Zugriff auf die Mitarbeiterdaten nicht zeitlich unbegrenzt, sondern nur beschränkt auf den konkreten Vertretungsfall eingeräumt werden darf. Das Staatsministerium der Finanzen hat mir zugesichert, dass diese Vorgabe schnellstmöglich technisch umgesetzt wird.

11.2.3 Reisekostenmanagementsystem BayRMS

Bei dem vom Landesamt für Finanzen betriebenen Verfahren BayRMS handelt es sich um ein elektronisches Reisekostenmanagementsystem, mit dem Dienstreiseanträge gestellt und genehmigt sowie genehmigungsfreie Reisen angezeigt werden können und auch die Reisekostenvergütung beantragt werden kann.

Auch BayRMS wurde unter Federführung des Staatsministeriums der Finanzen für den landesweiten Einsatz bei allen Behörden, Gerichten und sonstigen Stellen des Freistaats Bayern entwickelt. Die bayernweite Freigabe für BayRMS hat das Staatsministerium der Finanzen im Einvernehmen mit der Staatskanzlei, den übrigen Staatsministerien, dem Obersten Rechnungshof und dem Landtagsamt am 02.03.2010 erteilt; sie ist im Bayerischen Behördennetz (BYBN) auf der Seite des Staatsministeriums der Finanzen unter der Rubrik "Datenschutz" - "Datenschutzrechtliche Freigaben" abrufbar. In die Entwicklung und datenschutzrechtliche Freigabe von BayRMS war ich ebenfalls eingebunden.

Auf folgende Punkte möchte ich besonders eingehen:

- Die **datenschutzrechtlichen Verantwortlichkeiten** sind bei BayRMS wie folgt verteilt: Bezüglich der im Zusammenhang mit der Antragstellung, Genehmigung bzw. Anzeige anfallenden Daten sind die jeweiligen Beschäftigungs- bzw. Genehmigungsbehörden speichernde Stellen im Sinne von Art. 4 Abs. 9 BayDSG. Das Landesamt für Finanzen wird in Bezug auf diese Daten im Auftrag der jeweiligen Beschäftigungs- bzw. Genehmigungsbehörde als Auftragnehmer einer Auftragsdatenverarbeitung gem. Art. 6 BayDSG tätig. Die für die Abrechnung einer Dienstreise zusätzlich erforderlichen Daten werden vom Landesamt für Finanzen durch den Abrechnungsantrag erhoben; insoweit ist das Landesamt für Finanzen speichernde Stelle im rechtlichen Sinn. Dem Landesamt für Finanzen werden zusätzlich, soweit für Abrechnungszwecke erforderlich, die im Rahmen der Antragstellung, Genehmigung bzw. Anzeige bereits erhobenen und gespeicherten Daten von den Genehmigungsbehörden durch ein automatisiertes Abrufverfahren übermittelt. In beiden Fällen (Antragstellung/Genehmigung/Anzeige sowie Abrechnung) beauftragt das Landesamt für Finanzen seinerseits das Bayerische Landesamt für Steuern, Rechenzentrum Nord, mit dem technischen Systembetrieb. Das Landesamt für Steuern ist damit Unterauftragnehmer bzw. Auftragnehmer einer Auftragsdatenverarbeitung.

- In inhaltlicher Hinsicht habe ich insbesondere darauf hingewiesen, dass die **Löschfristen** mit den gesetzlichen Vorgaben in Art. 110 Abs. 5 BayBG in Einklang gebracht werden müssen. Hierzu hat mir das Staatsministerium der Finanzen mitgeteilt, dass die Löschfristen überarbeitet und deutlich verkürzt worden sind.

Insgesamt kann ich feststellen, dass bei der Konzeption der dargestellten drei staatlichen eGovernment-Großprojekte im Personalbereich datenschutzrechtliche Belange - auch in Folge meiner jeweiligen Einbindung - im Wesentlichen berücksichtigt wurden. Die Umsetzung dieser Projekte in der Praxis bleibt allerdings abzuwarten; ich werde sie aufmerksam beobachten.

11.3 Drogentests bei der Einstellung neuer Mitarbeiter

In den letzten Jahren wurde vielfach diskutiert, ob bei der Einstellung neuer Mitarbeiter Urin- oder gar Bluttests erlaubt sind. Auch ich war im Berichtszeitraum mit dieser Problematik befasst. Konkret ging es um die Frage, ob es zulässig ist, dass ein meiner Kontrollkompetenz unterstehendes Wettbewerbsunternehmen aus dem Bereich der Daseinsvorsorge von sämtlichen neu einzustellenden Mitarbeitern einen Urintest für ein Drogenscreening verlangt.

Meine Prüfung der Rechtslage hat ergeben, dass es **datenschutzrechtlich nur zulässig ist, neu einzustellende Mitarbeiter mit deren schriftlicher Einwilligung auf Alkohol- oder Drogenabhängigkeit untersuchen zu lassen, sofern dies erforderlich ist, um die Eignung für die konkret vorgesehene Tätigkeit festzustellen.** Eine solche Arbeitsplatzrelevanz liegt allerdings nur vor, wenn der neu einzustellende Mitarbeiter durch ein abhängigkeitsbedingtes Fehlverhalten sich selbst, Leben und Gesundheit Dritter oder bedeutende Sachwerte gefährden könnte. Dem Dienstherrn/Arbeitgeber darf dabei als Ergebnis der Eignungsuntersuchung vom untersuchenden (Betriebs-/Amts-)Arzt nur mitgeteilt werden, ob der Betroffene für die konkret vorgesehene Tätigkeit geeignet oder nicht geeignet ist; nicht mitgeteilt werden dürfen ihm hingegen ärztliche Diagnosen oder sonstige einzelne Untersuchungsergebnisse.

Im Einzelnen gilt Folgendes:

- Ausgangspunkt für die datenschutzrechtliche Bewertung der Zulässigkeit von Urintests bei der Einstellung neuer Mitarbeiter ist stets die Frage, inwieweit die Erhebung personenbezogener Daten für die Entscheidung über die Einstellung **erforderlich** ist - gleichgültig, ob im konkreten Fall Art. 102 Bayerisches Beamtengesetz (analog) oder eine andere Erhebungsbefugnis zur Anwendung kommt. Bei der Prüfung der Erforderlichkeit ist zwischen dem berechtigten Informationsinteresse des Dienstherrn/Arbeitgebers und dem Anspruch des Betroffenen auf Schutz seines Persönlichkeitsrechts abzuwägen. Für diese datenschutzrechtliche Bewertung kann maßgeblich auf die **arbeitsrechtlichen Grundsätze zum Fragerecht des Arbeitgebers** zurückgegriffen werden.

- Nach weit überwiegender Rechtsaufassung sind bei der Einstellung Fragen und damit auch Untersuchungen bezüglich einer Alkohol- und Drogenabhängigkeit lediglich insoweit zulässig, als im Hinblick auf besondere Gefahren für Leib und Leben des Betroffenen oder Dritter oder bedeutende Sachwerte eine Relevanz für den konkret zu besetzenden Arbeitsplatz besteht. Daran gemessen habe ich es für **rechtswidrig** gehalten, dass das von mir überprüfte Unternehmen **unterschiedslos bei allen neu einzustellenden Mitarbeitern einen Urintest für ein Drogenscreening durchführen** lässt. **Vielmehr** muss bezogen auf die **konkret vorgesehene Tätigkeit** geprüft werden, ob durch ein abhängigkeitsbedingtes Fehlverhalten Gefahren für Leib und Leben des Betroffenen oder Dritter oder für bedeutende Sachwerte drohen. Es mag durchaus sein, dass dies im konkreten Einzelfall auf viele Tätigkeiten in dem Unternehmen zutraf; trotzdem darf es - gerade im Verwaltungsbereich - keinen Automatismus geben.

- Darüber hinaus habe ich das Unternehmen darauf hingewiesen, dass unter den oben genannten Voraussetzungen **bei der Einstellung lediglich** Fragen und Untersuchungen anerkannt sind, die sich auf eine Alkohol- und Drogen**abhängigkeit** beziehen; hingegen darf es **nicht** bloß darum gehen, den Alkohol- oder Drogen**konsum** zu ermitteln. Denn bei der Einstellungsuntersuchung ist darauf abzustellen, ob der Bewerber aufgrund einer Alkohol- oder Drogenabhängigkeit für die konkret vorgesehene Tätigkeit nicht geeignet ist. Deshalb sind bei der Einstellung nur solche Un-

tersuchungen zulässig, die Ergebnisse bezüglich einer Abhängigkeit bringen können, nicht hingegen die in der Praxis weit verbreiteten Tests, die nur den Konsum nachweisen können.

- Auch für einen nach den genannten Grundsätzen rechtmäßigen Urintest kann auf eine schriftliche **Einwilligung** der Betroffenen nicht verzichtet werden. Vor dem Hintergrund der Problematik der Freiwilligkeit einer Einwilligung in einer Bewerbungssituation ist es allerdings keinesfalls möglich, den Urintest über die **Grenzen des Arbeitgeberfragerechts** hinaus allein auf eine Einwilligung der neu einzustellenden Mitarbeiter zu stützen.

Das betroffene Unternehmen habe ich aufgefordert, die von mir aufgezeigten datenschutzrechtlichen Anforderungen an Urintests für ein Drogenscreening bei der Einstellung neuer Mitarbeiter zukünftig zu beachten. Nach einer längeren und intensiven Diskussion hat mir das Unternehmen schließlich zugesichert, dass es bei der Durchführung von Drogenscreenings von der grundsätzlichen, automatischen Durchführung bei Neueinstellungen auf eine differenzierte, auf die konkreten Aufgaben der jeweiligen Stelle bezogene Durchführung umgestellt hat.

11.4 Polizeiliche Daten zur Überprüfung von Bewerbern, Praktikanten und Fremdpersonal in der bayerischen Staatsverwaltung

Ein Jura-Student wollte sein nach der Ausbildungs- und Prüfungsordnung für Juristen vorgeschriebenes Praktikum bei einem bayerischen Staatsministerium ableisten. Dazu sollte er sich damit einverstanden erklären, dass sich das Ministerium die über ihn bei der Polizei gespeicherten Daten beschafft.

Dieser Fall hat mich veranlasst, das für die Polizei - und zudem innerhalb der Staatsregierung für das Datenschutzrecht federführend zuständige - Staatsministerium des Innern um Stellungnahme zu bitten.

In tatsächlicher Hinsicht interessierte mich vor allem, an welche Behörden der bayerischen Staatsverwaltung die Polizei ihre Daten zum Zweck der Überprüfung von Bewerbern, Praktikanten und Fremdpersonal (z.B. Reinigungskräfte) herausgibt.

In rechtlicher Hinsicht habe ich **datenschutzrechtliche Bedenken gegen eine umfassende Erhebung polizeilicher Daten über Fremdpersonal, Praktikanten und Bewerber durch Behörden der bayerischen Staatsverwaltung** geltend gemacht, v.a.:

- Nur ausnahmsweise erlauben bereichsspezifische gesetzliche Vorschriften in eng begrenzten Fällen die Erhebung polizeilicher Daten zu diesem Zweck (siehe z.B. § 7 Luftsicherheitsgesetz, § 12 b Atomgesetz oder Art. 16 Bayerisches Sicherheitsüberprüfungsgesetz); im Allgemeinen fehlen hingegen normenbestimmte und normenklare Rechtsgrundlagen.
- Die Wertentscheidungen des Bundeszentralregistergesetzes werden umgangen, da die Polizei auch Daten speichert, die in das Bundeszentralregister nicht eingetragen werden, die im Bundeszentralregister bereits getilgt sind oder die nach dem Bundeszentralregistergesetz nicht übermittelt werden dürfen.

- Die polizeilichen Daten enthalten nicht immer gesicherte Kenntnisse; teilweise liegen auch unbewiesene, objektiv unzutreffende Verdachtsmomente vor.
- Die polizeilichen Daten werden für polizeiliche Aufgaben gespeichert, nicht jedoch für den Zweck der Auswahl von Fremdpersonal, Praktikanten und Bewerbern durch die gesamte bayerische Staatsverwaltung.
- Und schließlich: Eine Einwilligung vermag die Datenerhebung mangels echter Freiwilligkeit nicht zu rechtfertigen.

Eine abschließende Stellungnahme des Staatsministeriums des Innern steht noch aus. Meine datenschutzrechtliche Überprüfung ist deshalb noch nicht beendet.

11.5 Gesundheitsdaten von bayerischen Polizeibeamten

Fragen zum Umgang des Dienstherrn mit sensiblen Gesundheitsdaten seiner Beschäftigten sind zurzeit besonders aktuell. Im Berichtszeitraum zeigte sich hier auch bei der Bayerischen Polizei in einigen Punkten Handlungsbedarf:

- So habe ich erfahren, dass im Bereich einzelner Polizeipräsidien **Krankenblätter** verwendet wurden, auf denen auch die Art der Erkrankung von Polizeibeamten festgehalten wurde. Die beamtenrechtlichen Vorschriften (Art. 95 Abs. 1 Satz 2 BayBG, § 21 Abs. 1 Sätze 2, 3 und Abs. 2 Urlaubsverordnung) gestatten es allerdings nur, die Tatsache und die Dauer der Erkrankung einer Beamtin oder eines Beamten zu erfassen. Hingegen ist es **nicht zulässig,** die **Art der Erkrankung** zu erheben.

  Auf meine Bitte hin hat das Staatsministerium des Innern die Polizeiverbände über die Rechtslage informiert und mir zugesichert, dass die Erhebung der Art der Erkrankung von Polizeibeamten eingestellt wird sowie bestehende Krankenblätter entsprechend angepasst werden.

- Darüber hinaus musste ich feststellen, dass die **Aktenhaltung des Ärztlichen Dienstes der Bayerischen Polizei** immer noch nicht datenschutzkonform ist. Dem Ärztlichen Dienst obliegt u.a. die allgemein- und zahnmedizinische Versorgung der Polizeibeamtinnen und Polizeibeamten in Ausbildung und in der Einsatzstufe; er ist aber auch als besonderes Gesundheitsamt z.B. für ärztliche Begutachtungen im Rahmen des Bewerberauswahlverfahrens, zur Dienstunfähigkeit oder nach Dienstunfällen zuständig. Der Ärztliche Dienst verfügt damit über sensibelste Gesundheitsdaten zahlreicher Polizeibeamtinnen und Polizeibeamten. Deren Weitergabe an die Personalverwaltungen ist durch die bestehenden gesetzlichen Vorschriften vielfach beschränkt, z.B. nach Art. 5 Abs. 4 Satz 1, Art. 11 Abs. 1 i.V.m. Art. 30 und Art. 31 Abs. 8 GDVG, insbesondere auch nach Art. 128 Abs. 1 Satz 4 i.V.m. Art. 67 BayBG. Trotzdem werden die Sachakten des Ärztlichen Dienstes der Bayerischen Polizei immer noch bei der jeweiligen personalaktenführenden Dienststelle im sog. Unterordner "C" der Personalakte aufbewahrt (wenn auch in einer Verschlusstasche versehen mit dem Hinweis, dass diese nur vom Ärztlichen Dienst zu öffnen ist).

  Hinzu kommt, dass in allen Polizeiverbänden die Funktion eines sog. **Ärztlichen Sachbearbeiters** eingerichtet ist, der als Bindeglied zwischen dem

Ärztlichen Dienst, dem Dienstherrn und dem jeweils betroffenen Polizeibeamten den Polizeiarzt unterstützen soll. Unklar war, ob der Ärztliche Sachbearbeiter Mitarbeiter des Ärztlichen Dienstes sein soll - dann müsste er organisatorisch in diesen eingegliedert sein und wäre bezüglich der Datenweitergabe an die Mitarbeiter der Personalverwaltung vielfach beschränkt - oder ob er selbst Mitarbeiter der Personalverwaltung ist - dann dürfte er allerdings die Verschlusstaschen nicht öffnen.

Nach einem längeren, intensiven Schriftwechsel hat mir das Staatsministerium des Innern letztlich mitgeteilt, dass der Ärztliche Sachbearbeiter künftig allein den Personalverwaltungen zugeordnet sein soll und damit die in der Personalakte enthaltenen Verschlusstaschen nicht öffnen darf. Diese Lösung ist für eine Übergangsphase akzeptabel. Wirklich datenschutzgerecht ist es allerdings allein, die Unterlagen mit den sensiblen Gesundheitsdaten nicht mehr in den einzelnen Personalakten, sondern in einer **Zentralen Medizinischen Registratur beim Ärztlichen Dienst der Bayerischen Polizei** aufzubewahren. Ich habe das Staatsministerium des Innern gedrängt, dem Aufbau einer solchen Registratur höchste Priorität zuzuweisen. Dies hat mir das Innenministerium schließlich zugesagt.

11.6 DNA-Reihentests im Finanzamt

Im Frühjahr 2009 informierte mich der Personalrat eines Finanzamtes darüber, dass die Amtsleitung die Durchführung von DNA-Reihentests unter den Mitarbeitern beabsichtige. Seit einigen Jahren seien im Finanzamt wiederholt anonyme, vorgeblich von Beschäftigten an Kolleginnen und Kollegen gesandte Briefe aufgetaucht. Die zum Teil obszönen und beleidigenden Briefe hätten zu gegenseitigen Verdächtigungen und in der Folge zu einer deutlichen Verschlechterung des Betriebsklimas geführt. Da die polizeilichen Ermittlungen im Sande verlaufen seien, wolle nun die Finanzamtsleitung die Sache selbst in die Hand nehmen und eigene Ermittlungen anstellen. Dazu sollten die ggf. auf den Briefen vorhandenen DNA-Spuren "mit der DNA einiger Kollegen verglichen werden".

Trotz allem Verständnis für die Lage habe ich die Amtsleitung des Finanzamtes darauf hingewiesen, dass sie nicht berechtigt ist, DNA-Spuren auf den anonymen Briefen mit der DNA von Mitarbeitern abzugleichen, um den im Kreis der Mitarbeiter vermuteten Absender der Briefe zu ermitteln. **Derartige DNA-Untersuchungen sind allein dem strafrechtlichen Ermittlungsverfahren vorbehalten.** Sie dürfen nur unter engen Voraussetzungen beim tatsachenbegründeten Verdacht, dass ein Verbrechen gegen das Leben, die körperliche Unversehrtheit, die persönliche Freiheit oder die sexuelle Selbstbestimmung begangen worden ist, und überdies erst nach gerichtlicher Anordnung durchgeführt werden (vgl. dazu § 81 h StPO). Außerhalb eines strafrechtlichen Ermittlungsverfahrens bestehen keine Rechtsgrundlagen für derartige DNA-Reihenuntersuchungen: Die allgemeinen datenschutzrechtlichen Vorschriften stellen keine normenklaren und normenbestimmten Befugnisnormen für einen derart massiven Grundrechtseingriff dar; zudem fehlte es an der Verhältnismäßigkeit. Die DNA-Untersuchungen können aber auch nicht mit dem Einverständnis der betroffenen Mitarbeiter vorgenommen werden, da derartige Einwilligungen allein schon mangels echter Freiwilligkeit unwirksam wären; zudem würden dadurch die strikten gesetzlichen Vorgaben der Strafprozessordnung umgangen.

Das betroffene Finanzamt teilte mir daraufhin mit, dass es zwar von einem Abgleich der DNA-Spuren mit der DNA von Mitarbeitern Abstand nehme. Allerdings habe es eine Untersuchung zur Feststellung von DNA-Spuren auf den Briefen in Auftrag gegeben, um herauszufinden, ob nur ein oder mehrere Täter in Frage kommen und ob der/die Täter männlich oder weiblich ist/sind. Der Täterkreis solle auf diese Weise eingeschränkt werden, einerseits um verdächtige Mitarbeiter zu entlasten, andererseits um der Polizei Anstoß zu weiteren Ermittlungen zu geben.

Meiner Auffassung nach ist aber **auch eine (bloße) Untersuchung der Briefe auf DNA-Spuren ohne Abgleich mit der DNA verdächtiger Mitarbeiter unzulässig.** Die oben angeführten Argumente gelten hier entsprechend. Insbesondere sind auch derartige DNA-Untersuchungen dem strafrechtlichen Ermittlungsverfahren vorbehalten und bedürfen grundsätzlich einer gerichtlichen Anordnung (vgl. § 81 e f. StPO). Solche Untersuchungen wären überdies untauglich, weil die auf den Briefen gefunden DNA-Spuren auch von unbeteiligten Dritten, wie z.B. den Mitarbeitern der Poststelle des Finanzamts, stammen könnten.

Um die DNA-Untersuchungen endgültig zu stoppen und die bereits ermittelten DNA-Identifizierungsmuster löschen zu lassen, bedurfte es letztlich meiner unmittelbaren Intervention beim Amtschef des Staatsministeriums der Finanzen.

Dies nehme ich zum Anlass, nochmals ausdrücklich darauf hinzuweisen, dass die **Strafprozessordnung abschließend regelt, unter welchen inhaltlichen und verfahrensmäßigen Voraussetzungen genetische Untersuchungen zum Zwecke der Aufklärung von Straftaten zulässig sind.** Diese strengen Voraussetzungen können weder durch eine Einverständniserklärung der betroffenen Mitarbeiter noch durch eine Berufung auf die Fürsorgepflicht des Dienstherren umgangen werden.

Meine Rechtsauffassung wird mittlerweile durch das größtenteils zum 01.02.2010 in Kraft getretene Gendiagnostikgesetz (GenDG) bestätigt, in dessen Anwendungsbereich gerade auch genetische Untersuchungen im Arbeitsleben fallen (§ 2 Abs. 1 GenDG). In Bezug auf - gem. § 22 GenDG selbstverständlich auch öffentlich-rechtliche - Beschäftigungsverhältnisse verbietet es § 19 GenDG dem Arbeitgeber ausdrücklich, sowohl vor als auch nach Begründung eines Beschäftigungsverhältnisses die Vornahme genetischer Untersuchungen oder Analysen zu verlangen bzw. die Mitteilung von Ergebnissen bereits vorgenommener genetischer Untersuchungen oder Analysen zu verlangen, solche Ergebnisse entgegenzunehmen oder zu verwenden. Verstöße hiergegen stellen nach den §§ 25 Abs. 1 Nr. 5 und 26 Abs. 1 Nr. 8 GenDG Straftaten bzw. bußgeldbewehrte Ordnungswidrigkeiten dar.

11.7 Durchsicht der persönlichen Laufwerke aller Mitarbeiter

Große Aufregung unter den Bediensteten verursachte die EDV-Abteilung einer öffentlichen Stelle, als sie die persönlichen Laufwerke aller Mitarbeiter elektronisch durchsuchte.

Die EDV-Abteilung hatte einen fundierten Hinweis erhalten, dass auf das EDV-System unzulässig zugegriffen wird. Daraufhin hatte sie mit der Windows-Explorer-Funktion sämtliche ".exe"-Dateien aufgelistet und auf ein evt. Schadprogramm überprüft. Dabei fiel der EDV-Abteilung eine verdächtige Datei auf.

Umgehend stellte sie fest, auf dem Laufwerk welchen Mitarbeiters diese Datei gespeichert war. Anschließend setzte sie die Dienststellenleitung in Kenntnis; diese informierte dann den Personalratsvorsitzenden.

Die Erhebung personenbezogener Mitarbeiterdaten ist nach der - auf die nichtverbeamteten Beschäftigten des bayerischen öffentlichen Dienstes entsprechend anzuwendenden - Vorschrift des Art. 102 Satz 1 BayBG u.a. zulässig, soweit dies zur Durchführung des Dienstverhältnisses erforderlich ist. Im Rahmen der Prüfung der Erforderlichkeit ist abzuwägen zwischen dem Informationsinteresse des Dienstherrn und dem Persönlichkeitsrecht der Beschäftigten.

Art. 102 Satz 1 BayBG Erhebung personenbezogener Daten
Der Dienstherr darf personenbezogene Daten über Bewerber, Bewerberinnen, Beamte und Beamtinnen sowie ehemalige Beamte und Beamtinnen nur erheben, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes, erforderlich ist oder eine Rechtsvorschrift dies erlaubt.

Daran gemessen wäre es z.B. datenschutzrechtlich **unzulässig**, die Laufwerke der Mitarbeiter einer **ständigen Vollkontrolle** über Verhalten und Leistung der Beschäftigten zu unterziehen. Dabei spielt es keine Rolle, ob den Bediensteten die private Nutzung des EDV-Systems vom Dienstherrn gestattet oder verboten ist. **In Anbetracht des konkreten, tatsachengestützten Verdachts** eines unzulässigen Zugriffs auf das EDV-System war es in dem gegenständlichen Einzelfall hingegen mangels anderer Aufdeckungsmöglichkeiten als **erforderlich** anzusehen, dass die EDV-Abteilung die Laufwerke der Mitarbeiter nach Schadprogrammen durchsucht und den verdächtigen Mitarbeiter ausfindig gemacht hat.

Derartige Überprüfungen führen allerdings zu einer erheblichen Verunsicherung der Beschäftigten. Denn für die Beschäftigten sind Anlass, Zweck und Ausmaß von Überwachungsmaßnahmen der EDV-Abteilung nicht überschaubar. Vielfach und zu Recht fühlen sich Mitarbeiter einem ungerechtfertigten Überwachungsdruck ausgesetzt.

Ich rate deshalb dringend dazu, Maßnahmen wie eine Durchsicht der Laufwerke der Bediensteten in einer **Dienstvereinbarung** zu regeln. Darin sollte insbesondere bestimmt sein, welche Überprüfungen aus welchen Gründen und zu welchen Zwecken zulässig sind. Hinsichtlich einer personenbezogenen Auswertung von Verhalten und Leistung der Beschäftigten sollte vorgesehen sein, dass diese nur im Einzelfall mit Zustimmung des Personalrats und bei Anwesenheit eines Mitglieds des Personalrats und des behördlichen Datenschutzbeauftragten stattfinden darf. Über den konkreten Inhalt der Dienstvereinbarung sind die Bediensteten natürlich auch eingehend zu informieren.

In diesem Zusammenhang weise ich erneut darauf hin, dass die Einführung, Anwendung und erhebliche Änderung technischer Einrichtungen, die dazu geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, nach Art. 75 Abs. 1 Nr. 1 BayPVG der Mitbestimmung durch den **Personalrat** unterliegen.

12 Spezielle datenschutzrechtliche Themen

12.1 Vorbereitung der Volkszählung 2011

In meinem 23. Tätigkeitsbericht, Nr. 23.3, und in meinem 22. Tätigkeitsbericht, Nr. 21.5, habe ich bereits darauf aufmerksam gemacht, dass sich Deutschland an der kommenden Volkszählungsrunde der Europäischen Union 2010/2011 mit einem registergestützten Zensus beteiligen wird. Derzeit laufen die Vorbereitungen des Zensus auf Hochtouren:

12.1.1 Bundesebene

In das Gesetzgebungsverfahren für ein "Gesetz zur Anordnung des Zensus 2011 (Zensusgesetz 2011) sowie zur Änderung von Statistikgesetzen" war ich eingebunden. Ich habe mehrfach gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und auch gegenüber dem Staatsministerium des Innern Stellung genommen. Das Gesetz ist am 16.07.2009 in Kraft getreten (BGBl. I S. 1781).

- Bereits in meinem 23. Tätigkeitsbericht, Nr. 23.3, habe ich deutlich gemacht, dass die in § 8 Zensusgesetz 2011 vorgesehene **personenscharfe Erhebung in sogenannten Sonderbereichen** (u.a. Krankenhäuser, Justizvollzugsanstalten, siehe § 2 Abs. 5 Zensusgesetz 2011) aus datenschutzrechtlicher Sicht bedenklich ist.

  Mit meinem Kompromissvorschlag, nur in wenig sensiblen Sonderbereichen (wie z.B. Studentenwohnheimen) eine personenscharfe Erhebung durchzuführen, in sensiblen Sonderbereichen (wie z.B. Behindertenheimen oder Justizvollzugsanstalten) es aber bei einer summarischen Erhebung zu belassen, konnte ich mich leider nicht durchsetzen.

  Das Statistische Bundesamt ist allerdings bestrebt, durch besondere Maßnahmen in sensiblen Sonderbereichen eine frühzeitige Trennung und Löschung der Hilfsmerkmale Name, Vorname, Tag der Geburt und Geburtsort von den Erhebungsmerkmalen zu erreichen.

  Dies stellt zwar sicherlich aus datenschutzrechtlicher Sicht eine Verbesserung dar; vorzugswürdig wäre aber der Verzicht auf eine personenscharfe Erhebung (zumindest) in (sensiblen) Sonderbereichen gewesen.

- Nicht zuletzt das Staatsministerium des Innern hatte im Gesetzgebungsverfahren vorgeschlagen, das Merkmal "Anschrift" als Erhebungsmerkmal und nicht als - frühestmöglich von den Erhebungsmerkmalen zu trennendes und zu löschendes - Hilfsmerkmal zu qualifizieren. Diesen Vorschlag hat der Bundesgesetzgeber aufgrund des damit verbundenen Deanonymisierungsrisikos erfreulicherweise nicht aufgegriffen.

Das Zensusgesetz 2011 enthält allerdings in § 22 Abs. 2 eine Aufweichung: danach ist eine **temporäre anschriftengenaue Speicherung von Erhebungsmerkmalen in den kommunalen Statistikstellen** möglich. Diese Speicherung erfolgt zwar im abgeschotteten (kommunal-) statistischen Bereich; gerade auf kommunaler Ebene ist jedoch eine Reidentifizierung einzelner Personen nicht gänzlich unwahrscheinlich.

Aus datenschutzrechtlicher Sicht wäre die ursprüngliche Formulierung einer Speicherung von "Einzelangaben ohne Hilfsmerkmale" oder "auf der Grundlage von Blockseiten" vorzugswürdig gewesen.

- Die **Erhebung der "Zugehörigkeit zu einer Religionsgemeinschaft"** - dabei handelt es sich um ein äußerst sensibles Erhebungsmerkmal - habe ich mehrfach problematisiert (siehe hierzu 23. Tätigkeitsbericht, Nr. 23.3).

  Dabei habe ich stets darauf hingewiesen, dass es sich bei diesem Merkmal nach der **Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 09.07.2008 über Volks- und Wohnungszählungen** nicht um ein Pflichtmerkmal handelt. Zudem hatte das Europäische Parlament in seiner Sitzung vom 20.02.2008 mit überwältigender Mehrheit dafür gestimmt, die von der Europäischen Kommission ursprünglich vorgeschlagene freiwillige Abfrage bestimmter sensibler Merkmale - dazu zählte u.a. die Religionszugehörigkeit - vollständig zu streichen.

  Das Zensusgesetz 2011 enthält nunmehr insoweit einen Kompromiss, als es die "rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft" - dieses Merkmal ist aufgrund der Kirchensteuerpflicht bereits im Meldedatensatz enthalten - zu einer Pflichtangabe im Rahmen der Haushaltsstichprobe erklärt (§ 7 Abs. 4 Nr. 18 Zensusgesetz 2011), die Angabe "Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung (sunnitischer Islam, schiitischer Islam, alevitischer Islam, Buddhismus, Hinduismus und sonstige Religionen, Glaubensrichtungen und Weltanschauungen)" in § 7 Abs. 4 Nr. 19 Zensusgesetz 2011 hingegen zu einer freiwilligen Angabe (siehe § 18 Abs. 1 Zensusgesetz 2011). Insoweit wird es entscheidend darauf ankommen, dass bei der praktischen Durchführung der Haushaltsstichprobe die Freiwilligkeit der Angabe für den Befragten klar erkennbar gemacht wird.

  § 7 Abs. 4 Zensusgesetz 2011 Haushaltebefragung auf Stichprobenbasis
  Erhebungsmerkmale sind:

  . . .

  18. rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgesellschaft,

  19. Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung (sunnitischer Islam, schiitischer Islam, alevitischer Islam, Buddhismus, Hinduismus und sonstige Religionen, Glaubensrichtungen oder Weltanschauungen).

  Aus datenschutzrechtlicher Sicht wäre aber der Verzicht auf die Erhebung des Merkmals "Zugehörigkeit zu einer Religionsgesellschaft" vorzugswürdig gewesen.

12.1.2 Landesebene

Im Zensusgesetz 2011 hat der Bundesgesetzgeber nicht alle zur Durchführung der Volkszählung erforderlichen Regelungen getroffen. Er hat es den Landesgesetzgebern insbesondere überlassen, die **Einrichtung der Erhebungsstellen und die Organisation der durchzuführenden Maßnahmen** näher zu regeln.

- Das Staatsministerium des Innern hat mich in diesem Zusammenhang in das Gesetzgebungsverfahren für ein "Gesetz zur Änderung des Bayerischen Statistikgesetzes" eingebunden. Meine diesbezüglichen Anmerkungen wurden dabei berücksichtigt.

- Ebenfalls eingebunden hat mich das Landesamt für Statistik und Datenverarbeitung in die Abfassung eines Informationsschreibens zur näheren Ausgestaltung der bei den kreisfreien Städten und Landkreisen einzurichtenden **kommunalen Erhebungsstellen** (Rundschreiben "Wichtige Informationen für die Erhebungsstelle" vom 15.07.2010).

  In diesem Schreiben hat das Landesamt für Statistik und Datenverarbeitung insbesondere die bei der Auswahl des Erhebungspersonals und bei der räumlichen und organisatorischen Abschottung der Erhebungsstellen zu beachtenden Anforderungen, die aufgrund des verfassungsrechtlichen Gebots der Trennung von Statistik und Verwaltungsvollzug zu erfüllen sind, im Einzelnen dargestellt. Meine diesbezüglichen Anmerkungen wurden auch hier berücksichtigt.

12.1.3 Ausblick

Als Stichtag für den geplanten Zensus ist der 09.05.2011 vorgesehen. Ich werde die praktische Durchführung der Zensusarbeiten aus datenschutzrechtlicher Sicht auch weiterhin aufmerksam begleiten.

12.2 Einheitlicher Ansprechpartner nach der EU-Dienstleistungsrichtlinie

Am 12.12.2006 hat die Europäische Gemeinschaft die **EU-Dienstleistungsrichtlinie** (Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt) erlassen, welche von den Mitgliedstaaten bis zum 28.12.2009 in nationales Recht umzusetzen war. Zweck der Dienstleistungsrichtlinie ist die Schaffung eines einheitlichen Rechtsrahmens, insbesondere für den freien Dienstleistungsverkehr zwischen den Mitgliedstaaten. Im Rahmen dieser Zwecksetzung fordert die Richtlinie von den Mitgliedstaaten unter anderem auch die Schaffung sogenannter Einheitlicher Ansprechpartner. Diese sollen Dienstleistern aus dem europäischen Ausland die Erbringung grenzüberschreitender Dienstleistungen erleichtern. Insbesondere soll es ausländischen Dienstleistern möglich sein, eventuell erforderliche Genehmigungsverfahren in anderen Mitgliedstaaten über den Einheitlichen Ansprechpartner abzuwickeln. Dem Einheitlichen Ansprechpartner kommt insoweit eine gleichsam koordinierende und überwachende Funktion zu.

In Bayern wurden die Aufgaben des Einheitlichen Ansprechpartners durch das **Gesetz über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern vom 22.12.2009-BayEAG** (GVBl S.626) grundsätzlich den Kammern der gewerblichen und freien Berufe zugewiesen.

Den Landkreisen und kreisfreien Gemeinden wurde aber zugleich die Option eröffnet, durch Abgabe einer entsprechenden Erklärung gegenüber dem Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie selbst die Aufgaben des Einheitlichen Ansprechpartners zu übernehmen, wovon eine Reihe von Kommunen auch Gebrauch gemacht haben.

Datenschutzrechtlich relevant ist die Einführung des Einheitlichen Ansprechpartners deswegen, weil hierdurch in bestehende Genehmigungsverfahren gleichsam eine zusätzliche neue Stelle eingeführt wird, welche - neben der eigentlichen Genehmigungsbehörde - eine Vielzahl personenbezogener Daten erhebt, verarbeitet und speichert. Da der beim Einheitlichen Ansprechpartner im Laufe der Zeit entstehende Datenpool naturgemäß geeignet ist, Begehrlichkeiten auszulösen, ist es datenschutzrechtlich unumgänglich, klare Regeln für die Verwendung und Speicherung dieser Daten aufzustellen. Im Gesetzgebungsverfahren konnte ich insoweit erreichen, dass in das Umsetzungsgesetz eine diesbezügliche Verordnungsermächtigung für das Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie aufgenommen wurde. Dieses wurde in Art. 5 Abs. 1 Nr. 3 BayEAG ermächtigt, durch Rechtsverordnung nähere Regelungen über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Einheitlichen Ansprechpartner, insbesondere über die Zweckbindung dieser Daten sowie über die getrennte Verarbeitung der Daten aus sachlich nicht zusammengehörenden Verwaltungsvorgängen zu treffen.

Im Vollzug dieser Verordnungsermächtigung hat das Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie die **Verordnung zur Ausführung des Gesetzes über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern (Ausführungsverordnung Einheitlicher Ansprechpartner - AVBayEAG) vom 28.04.2010** (GVBl S. 224) erlassen. Im Erlassverfahren konnte ich insbesondere erreichen, dass anders als ursprünglich vorgesehen, eine bereichsspezifische Datenschutzregelung - in § 5 AVBayEAG - aufgenommen und es damit nicht bei der bloßen Geltung des allgemeinen Bayerischen Datenschutzgesetzes (BayDSG) belassen wurde. Entsprechend meiner Forderung regelt § 5 Abs. 1 AVBayEAG nunmehr ausdrücklich, dass der Einheitliche Ansprechpartner personenbezogene Daten getrennt von anderen Verfahren/Aufgaben verarbeiten muss, was insbesondere dann wichtig ist, wenn der Einheitliche Ansprechpartner und die für die Antragsbearbeitung zuständige Behörde identisch sind. Durchsetzen konnte ich mich insbesondere auch mit meiner Forderung, den Umfang des Informationsaustauschs zwischen der fachlich zuständigen Stelle und dem Einheitlichen Ansprechpartner im Hinblick auf dessen Funktion - Auskunftserteilung über den aktuellen Verfahrensstand gegenüber dem Antragsteller - zu begrenzen und klarzustellen, wer für die Entgegennahme und Bearbeitung von Anträgen der Betroffenen - insbesondere auf Berichtigung, Löschung und Sperrung personenbezogener Daten - zuständig ist (vgl. insoweit § 5 Abs. 2 und 3 AVBayEAG). Nicht aufgegriffen wurde meine Empfehlung, den Einheitlichen Ansprechpartner zur Erstellung eines Datenschutz- und Datensicherheitskonzepts zu verpflichten, sowie vor allem ausdrücklich zu regeln, für welche Zwecke personenbezogene Daten des Antragstellers erhoben, verarbeitet oder genutzt werden dürfen und klarzustellen, wann diese zu löschen sind. Eine wesentliche inhaltliche Einbuße für den Datenschutz ist damit jedoch nicht verbunden, da sich die entsprechenden Verpflichtungen letztlich auch aus den Art. 7, 12 und 15 ff. BayDSG ergeben, auf welches § 5 Abs. 4 AVBayEAG ausdrücklich verweist.

§ 5 AVBayEAG
(1) Personenbezogene Daten aus sachlich nicht zusammengehörenden Verwaltungsvorgängen sind getrennt voneinander zu verarbeiten. Handelt es sich beim Einheitlichen Ansprechpartner zugleich um die für die Antragsbearbeitung zuständige Behörde, müssen auch bei sachlich zusammengehörenden Verwaltungsvorgängen personenbezogene Daten getrennt nach dem jeweiligen Aufgabenbereich verarbeitet werden.
(2) Im Rahmen des Informationsaustauschs nach § 3 darf die zuständige Stelle diejenigen personenbezogenen Daten an den Einheitlichen Ansprechpartner übermitteln, die erforderlich sind, um dem Antragsteller jederzeit über den aktuellen Verfahrensstand Auskunft geben zu können.
(3) Sofern die Betroffenen den Einheitlichen Ansprechpartner in Anspruch genommen haben, hat er deren Anträge auf Auskunft und Benachrichtigung, Berichtigung, Löschung und Sperrung nach den Art. 10, 11, 12 und 13 des Bayerischen Datenschutzgesetzes entgegen zu nehmen. Soweit erforderlich, leitet er die Anträge an diejenigen Stellen weiter, denen er personenbezogene Daten des Antragstellers übermittelt hat. Jede dieser Stellen ist zur Bearbeitung der Anträge zuständig, soweit sie personenbezogene Daten verarbeitet hat. Mitteilungen dieser Stellen werden auf Verlangen der Betroffenen über den Einheitlichen Ansprechpartner zugeleitet.
(4) Im Übrigen gelten die Regelungen des Bayerischen Datenschutzgesetzes.

12.3 Weitergabe von personenbezogenen Daten der Einwendungsführer an den Vorhabensträger in Planfeststellungsverfahren

Im Zusammenhang mit der Durchführung eines Planfeststellungsverfahrens für eine 3. Start- und Landebahn am Verkehrsflughafen München haben sich Bürger mit Fragen zur Weitergabe von Einwendungen an den Vorhabensträger an mich gewandt.

Zur Behandlung personenbezogener Daten in Planfeststellungsverfahren erhalte ich immer wieder Anfragen. Bereits im 17. Tätigkeitsbericht 1996, Nr. 8.14, habe ich mich zu dieser Thematik geäußert. Danach halte ich aus datenschutzrechtlicher Sicht die Übermittlung der personenbezogenen Daten der Einwendungsführer an den Träger des Vorhabens grundsätzlich für zulässig, soweit der Träger des Vorhabens zur fachgerechten Vorbereitung auf die Behandlung von Einwendungen im Erörterungstermin die konkret betroffenen individuellen Belange des Einwenders kennen muss. Zu berücksichtigen ist dabei, dass sich ein Einwender mit der form- und fristgerechten Einwendung förmlich am Verwaltungsverfahren beteiligt und damit die Rechtsstellung eines Beteiligten im Sinne des Bayerischen Verwaltungsverfahrensgesetzes mit den daraus sich ergebenden verfahrensrechtlichen Rechtspositionen erhält. Eine Kenntnisnahme der personenbezogenen Daten der Einwender durch den Vorhabensträger ist dagegen nicht erforderlich, wenn diese erkennbar keinen Beteiligtenstatus anstreben, z.B. weil sie nicht die Verletzung eigener Rechte geltend machen, sondern nur allgemein für die Belange des Naturschutzes eintreten.

Auch das Bundesverwaltungsgericht hat in einem Beschluss vom (14.08.2000, Az. 11 VR 10/00) die Auffassung vertreten, dass es grundsätzlich nicht zu beanstanden ist, wenn die Anhörungsbehörde Einwendungen dem Vorhabensträger in nicht anonymisierter Form zur Stellungnahme überlässt. Der Entscheidung zufolge könnte nur dann etwas Anderes gelten, wenn ein Einwender im Einzelfall darlegen kann, dass ihm durch die Weitergabe seiner nicht anonymisierten Ein-

wendung besondere und unzumutbare und mithin von der Funktion des Anhörungsverfahrens nicht mehr gedeckte Nachteile entstehen, die es gebieten, das Verfahrens- und Rechtsverfolgungsinteresse der Vorhabensträger ausnahmsweise hinter dem Recht auf informationelle Selbstbestimmung zurücktreten zu lassen. Damit die zuständige Behörde die besondere Schutzbedürftigkeit der Einwendung noch vor der Weitergabe an den Vorhabensträger erkennen kann, sind solche Umstände vom Einwendungsführer geltend zu machen.

In dem o.g. Vorgang hat mir die Regierung von Oberbayern auf meine Anfrage hin mitgeteilt, dass die Betroffenen mit öffentlicher Bekanntmachung darauf hingewiesen wurden, dass Einwendungen auf Wunsch anonymisiert an die Flughafen München GmbH (FMG) weitergegeben werden. Diese Bekanntmachung wurde auf der Homepage der Regierung von Oberbayern (abrufbar unter www.regierung.oberbayern.de) sowie in allen betroffenen Auslegungsgemeinden durch öffentliche Bekanntmachung (z.B. Anschlagstafel, Amtsblatt) veröffentlicht. Weiter teilte die Regierung von Oberbayern mit, dass bei den Einwendungen, für die ein entsprechender Anomyisierungswunsch vorlag, Name und Anschrift des Eingabeführers entfernt worden seien. Außerdem seien diese Einwendungsschreiben nicht im Original an die FMG weitergegeben worden, sondern der FMG wurden lediglich die - nicht personenbezogenen - Argumente mitgeteilt, um evtl. Rückschlüsse auf die Person des Eingabeführers auszuschließen. Dieses Verfahren setzt die Vorgaben des Bundesverwaltungsgerichts sachgerecht um.

12.4 Nochmals: Mitteilung Daten Reisegewerbetreibender an Industrie- und Handelskammern

Im 18. Tätigkeitsbericht 1998, Nr. 13.3, habe ich berichtet, dass Industrie- und Handelskammern von einigen Gewerbeämtern regelmäßig Mitteilungen über erteilte Reisegewerbekarten bzw. die Ausübung einer reisegewerbefreien Tätigkeit erhalten hatten. Für eine solche Datenübermittlung gibt es keine Rechtsgrundlage. Das Bayerische Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie hatte seinerzeit auf meine Bitte hin die Vollzugsbehörden entsprechend informiert.

Eine bundesweite Umfrage eines anderen Landesbeauftragten für den Datenschutz zu diesem Thema im Berichtszeitraum habe ich zum Anlass genommen, stichprobenartig bei einer Industrie- und Handelskammer nachzufragen, wie dort verfahren wird. Die Industrie- und Handelskammer teilte mir mit, dass sie keine Daten aus dem Reisegewerbe bei den Gewerbeämtern abfrage, jedoch von einigen Landratsämtern regelmäßige Mitteilungen über Erteilung, Rücknahme und Änderung von Reisegewerbekarten (allerdings nicht auch über reisegewerbefreie Tätigkeiten) erhalten würde. Nach Hinweis auf die Unzulässigkeit dieser Datenübermittlungen hat die Industrie- und Handelskammer erklärt, die betroffenen Behörden darüber zu unterrichten. Das von mir eingeschaltete Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie hat darüber hinaus auf meine Bitte hin die nachgeordneten Behörden nochmals auf die Rechtslage hingewiesen.

12.5 Unzulässige Führung einer "Schwarzen Liste" als Entscheidungshilfe für die Verhängung von Fahrtenbuchauflagen

Im Berichtszeitraum habe ich mehrere Fahrerlaubnis- und Zulassungsbehörden einer datenschutzrechtlichen Prüfung unterzogen. Hierbei bin ich bei einer Zulassungsbehörde auf eine datenschutzrechtlich unzulässige Praxis im Bereich der Verhängung von Fahrtenbuchauflagen nach der Straßenverkehrszulassungsordnung (StVZO) aufmerksam geworden.

Bei derartigen Fahrtenbuchauflagen handelt es sich um Maßnahmen zur Abwehr von Gefahren für die Sicherheit und Ordnung des Straßenverkehrs. Mit ihnen soll sichergestellt werden, dass trotz der regelmäßig kurzen Verjährungsfrist von Verkehrsordnungswidrigkeiten - in Zukunft - rechtzeitig ermittelt werden kann, wer diese als Fahrzeugführer begangen hat. Fahrtenbuchauflagen nach § 31 a StVZO können gegenüber dem Fahrzeughalter verhängt werden, wenn eine Verkehrsordnungswidrigkeit nicht geahndet werden konnte, da die Feststellung des Fahrzeugführers nicht möglich war.

Im Zulassungsbereich einer der von mir geprüften Zulassungsbehörden wurden Fahrtenbuchauflagen nicht schon bei einmaligen, sondern nur bei wiederholten - mangels rechtzeitiger Fahrerfeststellung - sanktionslos gebliebenen derartigen Verkehrsordnungswidrigkeiten verhängt. Die Verhängung der Fahrtenbuchauflage im Wiederholungsfall wurde den betreffenden Fahrzeughaltern vorher schriftlich angedroht. Um eventuelle Wiederholungstäter identifizieren zu können, wurden diese Androhungen in einem Aktenordner gesammelt. Diese "schwarze Liste" enthielt zum Zeitpunkt meiner datenschutzrechtlichen Prüfung bis in das Jahr 1998 zurückreichende derartige Vorgänge. Zur tatsächlichen Verhängung einer Fahrtenbuchauflage ist es aufgrund dieser Praxis in den meiner Prüfung vorausgehenden acht Jahren dann nur in einem einzigen Fall gekommen.

Die Beurteilung der Sinnhaftigkeit dieser eben geschilderten Verwaltungspraxis aus straßenverkehrsrechtlicher Sicht steht mir nicht zu. Aus datenschutzrechtlicher Sicht ist es jedoch keinesfalls zulässig, Unterlagen über potentielle Wiederholungstäter derart lange aufzubewahren. Wenn nach § 44 Abs. 2 des Straßenverkehrsgesetzes sogar die Daten über verhängte Fahrtenbuchauflagen nach deren Wegfall zu löschen sind, dürfen Angaben bloß angedrohter Auflagen keinesfalls unbegrenzt lange aufbewahrt bzw. gespeichert werden. Denkbar ist es allein, diese Androhungsfälle für den Zeitraum aufzubewahren bzw. zu speichern, für den auch eine Auflage hätte verhängt werden können. Nach Ablauf dieses Zeitraums sind die Unterlagen dann aber gemäß Art. 12 Abs. 4 Satz 2 des Bayerischen Datenschutzgesetzes zu löschen. Dies habe ich der betreffenden Zulassungsbehörde auch so mitgeteilt, zugleich aber darauf aufmerksam gemacht, dass das Gebrauchmachen von dieser Möglichkeit die Einführung eines Löschfristenkalenders sowie dessen strikte Beachtung voraussetzt.

§ 31 a Abs. 1 StVZO
Die Verwaltungsbehörde kann gegenüber einem Fahrzeughalter für ein oder mehrere auf ihn zugelassene oder künftig zuzulassende Fahrzeuge die Führung eines Fahrtenbuchs anordnen, wenn die Feststellung eines Fahrzeugführers nach einer Zuwiderhandlung gegen Verkehrsvorschriften nicht möglich war. Die Verwaltungsbehörde kann ein oder mehrere Ersatzfahrzeuge bestimmen.

12.6 Regelmäßige Übermittlung personenbezogener Daten über die Entziehung von Fahrerlaubnissen an die Polizei

Im Rahmen einer datenschutzrechtlichen Prüfung bei einer Fahrerlaubnisbehörde habe ich festgestellt, dass von dort regelmäßig die jeweilige örtliche Polizeidienststelle über eine (verwaltungsbehördliche oder gerichtliche) Entziehung einer Fahrerlaubnis unterrichtet wurde. Soweit Fahrerlaubnisbehörden regelmäßig Daten über entzogene Fahrerlaubnisse an die Polizei übermitteln, stellt dies eine unzulässige Datenübermittlung auf Vorrat dar und widerspricht der gesetzlichen Regelung in § 3 Abs. 5 des Straßenverkehrsgesetzes, wonach die Fahrerlaubnisbehörde der Polizei die Entziehung der Fahrerlaubnis nur übermitteln darf, soweit dies im Einzelfall für die polizeiliche Überwachung im Straßenverkehr erforderlich ist. Routinemäßige Mitteilungen sollen nach dem Willen des Gesetzgebers demnach gerade nicht erfolgen, ebenso wenig sind die Fahrerlaubnisbehörden dazu verpflichtet, die Polizei über derartige Maßnahmen zu informieren. Entsprechende Übermittlungen sollen vielmehr auf Ausnahmefälle begrenzt sein, in denen ein Anlass zur Information der Polizei besteht. Dies setzt allerdings im Vorfeld der Datenübermittlung eine Überprüfung der Erforderlichkeit im Einzelfall sowie eine Dokumentation der Erwägungen bei der Fahrerlaubnisbehörde voraus. Erforderlich kann eine Mitteilung an die Polizei z.B. dann sein, wenn damit zu rechnen ist, dass der Betroffene gegen die verhängte Maßnahme verstößt.

12.7 Weitergabe von Fahrzeug- und Halterdaten durch eine Kfz-Zulassungsstelle

Eine Bürgerin hat sich bei mir über die Weitergabe ihrer Fahrzeug- und Halterdaten an eine Privatperson beschwert. Meine Prüfung des Vorgangs hat ergeben, dass eine Privatperson bei der Kfz-Zulassungsstelle eine Halterauskunft die Eingabeführerin betreffend beantragt hatte. Als Begründung hatte sie ausgeführt, dass das fragliche Fahrzeug wiederholt unberechtigterweise auf ihrem Parkplatz abgestellt und sie deshalb an der Nutzung ihres Parkplatzes gehindert worden sei. Um den/die Fahrzeughalterin zur Rechenschaft ziehen zu können, benötige sie dessen/deren Name und Anschrift. Das betreffende Fahrzeug war einem auswärtigen Zulassungsbereich zugeordnet. Deshalb wurde vorab die Zustimmung der örtlich zuständigen Kfz-Zulassungsstelle eingeholt, um die Halterauskunft im Wege der Amtshilfe erteilen zu können. Anschließend führte der Mitarbeiter der Kfz-Zulassungsstelle online über das Zentrale Fahrzeugregister des Kraftfahrtbundesamtes eine Halterabfrage durch und übersandte den kompletten Bildschirmausdruck der durch Abruf im automatisierten Verfahren erhobenen Daten an die Antragstellerin.

Rechtsgrundlage für die Übermittlung von Fahrzeugdaten und Halterdaten zur Verfolgung von Rechtsansprüchen ist § 39 Abs. 1 des Straßenverkehrsgesetzes (StVG). Nach dieser Vorschrift dürfen Fahrzeug- und Halterdaten aus dem Fahrzeugregister durch die Zulassungsstelle oder durch das Kraftfahrt-Bundesamt übermittelt werden, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt. Auskunftsberechtigt ist jeder, der einen Rechtsanspruch geltend machen, sichern, vollstrecken oder befriedigen oder abwehren will. Für die Darlegung des Anspruchs genügt es, wenn der An-

tragsteller den Sachverhalt plausibel behauptet, d.h. schlüssig und widerspruchsfrei vorträgt; Nachweise oder Belege muss er dazu nicht beifügen. Der Rechtsanspruch, der geltend gemacht werden soll, muss im Zusammenhang mit der Teilnahme am Straßenverkehr stehen. Hierfür genügt es, wenn der Anspruch einen Bezug zum straßenverkehrlichen Geschehen hat. Dies ist auch der Fall, wenn das Kraftfahrzeug auf einem Parkplatz abgestellt ist.

Nach § 39 Abs. 1 StVG war die vorliegende Halterabfrage und Auskunftserteilung aus dem Zentralen Fahrzeugregister an die Antragstellerin dem Grunde nach zulässig und durfte (nach erteilter Zustimmung) im Wege der Amtshilfe auch durch die an sich örtlich unzuständige Zulassungsstelle erfolgen.

Allerdings wurde die Halterabfrage durch die Kfz-Zulassungsstelle im automatisierten Abrufverfahren beim Kraftfahrt-Bundesamt eingeholt. Die Zulässigkeit des automatisierten Abrufverfahrens durch die Zulassungsbehörde beurteilt sich nach § 35 Abs. 1 Nr. 1 i.V.m. § 36 Abs. 1 StVG. Nach dieser Vorschrift darf die Übermittlung von Fahrzeug- und Halterdaten aus dem Zentralen Fahrzeugregister durch Abruf im automatisierten Verfahren an die Zulassungsbehörde nur erfolgen, soweit es sich um Aufgaben nach § 32 Abs. 1 Nr. 1 StVG - Zulassung und Überwachung von Fahrzeugen nach dem Straßenverkehrsgesetz oder den darauf beruhenden Rechtsvorschriften - handelt. Einen automatisierten Abruf von Daten durch die Zulassungsbehörde für Zwecke der Verfolgung von Rechtsansprüchen im Sinne des § 39 Abs. 1 StVG, wie dies im vorliegenden Sachverhalt gegeben war, sieht § 36 Abs. 1 StVG dagegen nicht vor.

In § 39 Abs. 1 Satz 1 Ziffern 1 bis 11 StVG ist außerdem abschließend aufgezählt, welche Fahrzeug- und Halterdaten aus dem Fahrzeugregister zur Verfolgung von Rechtsansprüchen an einen privaten Dritten übermittelt werden dürfen. Im vorliegenden Fall wurde der Auskunftsbegehrenden der komplette Bildschirmausdruck über den nach § 36 Abs. 1 StVG eingeholten Datenbestand übermittelt. Damit wurden auch personenbezogene Angaben der Eingabeführerin (u.a. Geburtsdatum und Geburtsort) übermittelt, die nicht im enumerativen Datenkatalog des § 39 Abs. 1 Satz 1 StVG enthalten sind. Die Weitergabe dieser Daten ohne Rechtsgrundlage war unzulässig.

Die unzulässige Einholung der Halterauskunft im automatisierten Abrufverfahren nach § 35 Abs. 1 Nr. 1 i.V.m. § 36 Abs. 1 StVG und die Übermittlung personenbezogener Daten der Eingabeführerin ohne entsprechende Rechtsgrundlage habe ich beanstandet.

§ 39 Abs. 1 StVG
Von den nach § 33 Abs. 1 gespeicherten Fahrzeugdaten und Halterdaten sind
1. *Familienname (bei juristischen Personen, Behörden oder Vereinigungen: Name oder Bezeichnung),*
2. *Vornamen,*
3. *Ordens- und Künstlername,*
4. *Anschrift,*
5. *Art, Hersteller und Typ des Fahrzeugs,*
6. *Name und Anschrift des Versicherers,*
7. *Nummer des Versicherungsscheins, oder, falls diese noch nicht gespeichert ist, Nummer der Versicherungsbestätigung,*
8. *gegebenenfalls Zeitpunkt der Beendigung des Versicherungsverhältnisses,*
9. *gegebenenfalls Befreiung von der gesetzlichen Versicherungspflicht,*

10. Zeitpunkt der Zuteilung oder Ausgabe des Kennzeichens für den Halter sowie

11. Kraftfahrzeugkennzeichen

durch die Zulassungsbehörde oder durch das Kraftfahrt-Bundesamt zu übermitteln, wenn der Empfänger unter Angabe des betreffenden Kennzeichens oder der betreffenden Fahrzeug-Identifizierungsnummer darlegt, dass er die Daten zur Geltendmachung, Sicherung oder Vollstreckung oder zur Befriedigung oder Abwehr von Rechtsansprüchen im Zusammenhang mit der Teilnahme am Straßenverkehr oder zur Erhebung einer Privatklage wegen im Straßenverkehr begangener Verstöße benötigt (einfache Registerauskunft).

13 Datenschutzkommission

Der Datenschutzkommission beim Bayerischen Landtag gehörten in den vergangenen zwei Jahren folgende Mitglieder bzw. stellvertretende Mitglieder an:

Für den Landtag:

Mitglieder:
Eberhard Rotter, CSU
Walter Taubeneder, CSU
Prof. Dr. Winfried Bausback, CSU
Dr. Florian Herrmann, CSU
Florian Ritter, SPD
Florian Streibl, Freie Wähler
Christine Kamm, BÜNDNIS 90/DIE GRÜNEN
Dr. Andreas Fischer, FDP

stellvertretende Mitglieder:
Peter Schmid, CSU
Christian Meißner, CSU
Manfred Ländner, CSU
Dr. Franz Rieger, CSU
Horst Arnold, SPD
Alexander Muthmann, Freie Wähler
Susanna Tausendfreund, BÜNDNIS 90/DIE GRÜNEN
Karsten Klein, FDP

Auf Vorschlag der Staatsregierung:

ab dem 26.03.2009

Mitglied:
Christian Peter Wilde, Ltd. Ministerialrat a.D.
im Bayerischen Staatsministerium des Innern

stellvertretendes Mitglied:
Armin Schwimmbeck, Ministerialrat im Bayerischen Staatsministerium
für Wirtschaft, Infrastruktur, Verkehr und Technologie

Auf Vorschlag der kommunalen Spitzenverbände in Bayern:

Mitglied:
Rudolf Schleyer, Mitglied des Vorstands bei der AKDB

stellvertretendes Mitglied:
Klaus Laumer, Abteilungsleiter bei der AKDB

ab dem 26.03.2009:

Mitglied:
Rudolf Schleyer, Mitglied des Vorstands bei der AKDB

stellvertretendes Mitglied:
Mario Pohl, Abteilungsleiter bei der AKDB

Auf Vorschlag des Staatsministeriums für Arbeit und Sozialordnung, Familie und Frauen aus dem Bereich der gesetzlichen Sozialversicherungsträger:

ab dem 26.03.2009

Mitglied:
Werner Krempl, Direktor und Mitglied der Geschäftsführung der Deutschen Rentenversicherung Nordbayern

stellvertretendes Mitglied:
Dr. Helmut Platzer, Vorstandsvorsitzender der AOK Bayern

Auf Vorschlag des Verbands Freier Berufe in Bayern e.V.:

ab dem 26.03.2009

Mitglied:
Hans-Ulrich Sorge, Notar

stellvertretendes Mitglied:
Dr. Janusz Rat, Vorsitzender der Kassenzahnärztlichen Vereinigung Bayerns

Herr Eberhard Rotter, MdL, führt den Vorsitz in der Datenschutzkommission; stellvertretender Vorsitzender ist Herr Florian Ritter, MdL.

Die Datenschutzkommission beim Bayerischen Landtag tagte im vergangenen Berichtszeitraum sieben Mal. Dabei befasste sie sich u.a. mit folgenden Themen:

- Vorberatung des 23. und 24. Tätigkeitsberichts
- Berichte über Beanstandungen
- Berichte von Datenschutzkonferenzen
- Berichte vom Europäischen Datenschutztag
- Gesetzentwurf der Regierungsfraktionen zur Änderung des Polizeiaufgabengesetzes, des Bayerischen Verfassungsschutzgesetzes und des Bayerischen Versammlungsgesetzes
- Polizeiliche Videoüberwachung und Kriminalaktennachweis
- Hausbesuche bei Eltern anlässlich der Geburt von Kindern (kommunales Modellprojekt)
- Krebsregistrierung - Ausgestaltung von Klinikregistern
- IuK-Zentralisierung im Bayerischen Behördennetz

Anlage 1:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18.02.2009
Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes!

Das Bundeskabinett hat am 14.01.2009 den Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes beschlossen (BR-Drs. 62/09). Mit dem Gesetz sollen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassende Befugnisse eingeräumt werden, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Weiter sollen aber zugleich auch das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG) geändert werden.

Angriffe auf die IT-Sicherheit können nicht nur die ordnungsgemäße Abwicklung von Verwaltungsaufgaben beeinträchtigen, sondern auch Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich bringen. Daher sind Konzepte zu entwickeln und umzusetzen, die sowohl die IT-Sicherheit stärken als auch den Schutz der Privatsphäre gewährleisten.

In weiten Bereichen wurden in der jüngsten Vergangenheit Maßnahmen zur Stärkung der IT-Sicherheit getroffen, die eine detaillierte Registrierung und Auswertung des Nutzerverhaltens und sogar der Inhalte der Kommunikation ermöglichen. Entsprechende Ansätze gibt es nun auch in der Bundesverwaltung. So sieht der Gesetzentwurf vor, dem BSI sehr weitgehende Befugnisse einzuräumen. Kritisch sind insbesondere

- die Ermächtigung des BSI, die gesamte Sprach- und Datenkommunikation aller Unternehmen, Bürgerinnen und Bürger mit Bundesbehörden ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten (§ 5),
- die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und
- die fehlende Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu (erwartenden) Angriffen (Spionage und Sabotage) zu warnen (§ 7).

Äußerst bedenklich ist darüber hinaus die Regelung, dass im Zweifelsfall allein das Bundesministerium des Innern entscheiden darf, ob Daten dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind und wie damit weiter zu verfahren ist (§ 5 Abs. 6). In solchen Zweifelsfällen sollten diese Daten gelöscht oder einem Richter zur Entscheidung vorgelegt werden.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen zwar grundsätzlich alle Aktivitäten, in den gewachsenen, vernetzten IT-Strukturen des Bundes das Niveau der IT-Sicherheit zu erhöhen. Sie fordern aber auch, dass die zur Risikobegrenzung eingeführten Maßnahmen nicht den Datenschutz der Nutzerinnen und Nutzer beeinträchtigen. Deshalb ist schon bei der Konzeption von IT-Sicherheitsmaßnahmen vorzusehen, dass das erforderliche Sicherheitsniveau

nur mit datenschutzgerechten Lösungen gewährleistet wird. Die Datenschutzbeauftragten fordern strengere Sicherheitsstandards und soweit möglich die Protokoll- und Inhaltsdaten vor der Auswertung durch das BSI zu anonymisieren bzw. zu pseudonymisieren. Damit ließen sich eine unnötige Registrierung des Nutzerverhaltens und Überwachung von Kommunikationsinhalten vermeiden. Die Auswertung der Daten durch das BSI muss revisionssicher ausgestaltet werden. Der vorgelegte Gesetzentwurf enthält keine solchen Regelungen.

Die Gesetzesänderung des Telemediengesetzes böte öffentlichen und privaten Anbietern von Telemedien die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer im Internet, da sie entsprechend der Gesetzesbegründung weit auslegbar ist. Der Gesetzgeber muss unmissverständlich klarstellen, dass die Erhebung und Auswertung personenbezogener Daten ultima ratio ist.

Sowohl die Betreiber der "Netze des Bundes" als auch die Verantwortlichen für die übergreifenden Netze der Verwaltung in Europa sind aufgefordert, bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer zu gewährleisten.

Anlage 2:
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009
Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz

Datenskandale der letzten Zeit haben deutlich gemacht, dass bei der Verarbeitung von Beschäftigtendaten weder Transparenz noch Rechtssicherheit besteht. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen.

Ziel des neuen Beschäftigtendatenschutzgesetzes muss sein, Rechtssicherheit herzustellen, Regelungslücken zu schließen und bereits vorhandene Regelungsaspekte sowie Vorgaben der Rechtsprechung in einem Spezialgesetz zusammenzufassen. Die Konferenz der Datenschutzbeauftragten hält deshalb vor allem folgende Eckpunkte für unverzichtbar:

- Die Regelungen des Beschäftigtendatenschutzgesetzes müssen sowohl für die Beschäftigten der Privatwirtschaft als auch für die Beschäftigten im öffentlichen Dienst gelten.
- Es muss klar geregelt werden, welche Daten Unternehmen und öffentliche Stellen im Rahmen des Einstellungsverfahrens und im weiteren Verlauf des Arbeitslebens über ihre Beschäftigten erheben dürfen, wie sie damit verfahren müssen und wozu sie die Daten nutzen dürfen. Es bedarf besonderer Festlegungen im Hinblick auf Gesundheitsdaten (u.a. zur Frage der Zulässigkeit von Drogen-Screening, psychologischen Testverfahren, ärztlichen Untersuchungen, etc.).
- Einen umfassenden anlass- und verdachtslosen Datenabgleich darf es nicht geben. Der Zugriff von Kontrollinstanzen wie z.B. der Innenrevision auf erhobene Personaldaten bedarf enger gesetzlicher Vorgaben.
- Moderne Informations- und Kommunikationstechnologien dürfen nicht zu lückenlosen Verhaltens- und Leistungskontrollen eingesetzt werden. Da

die Nutzung von Telefon, Internet und E-Mail-Diensten nicht mehr aus dem Arbeitsleben wegzudenken ist, sind auch die Voraussetzungen für eine beschäftigtenbezogene Auswertung dieser Kommunikationsmittel eindeutig und restriktiv festzulegen. Dabei ist auch zu regeln, welcher Personenkreis solche Auswertungen durchführen darf und ab welchem Verfahrensstand ggf. Dritte (z.B. Mitarbeitervertretungen oder Datenschutzbeauftragte) hinzugezogen werden müssen. Auswertungen von Datenbeständen der Zugangs- und Personalinformationssysteme sind strikt zu begrenzen.

- Der Einsatz von Überwachungssystemen, wie z.B. Videokameras und Ortungssystemen, ist auf das unbedingt notwendige Maß zu beschränken und unter Wahrung der Beteiligungsrechte der Mitarbeitervertretungen zulässig. Die Verwendung biometrischer Verfahren bedarf besonders enger Vorgaben.
- Es bedarf der Festlegung der Rechte der Beschäftigten, z.B. im Hinblick auf Auskunfts-, Einsichts-, Widerrufs-, Berichtigungs-, Löschungs- und Schadensersatzansprüche.
- Der Schutz von Persönlichkeitsrechten der in Deutschland tätigen Beschäftigten weltweit agierender Unternehmen oder Konzerne ist sicherzustellen.
- Eine effektive Kontrolle durch die zuständigen Datenschutzbehörden muss gewährleistet werden. Die betrieblichen und behördlichen Datenschutzbeauftragten sind bei allen personaldatenschutzrechtlich relevanten Verfahren und Entscheidungen frühzeitig einzubinden und umfassend zu beteiligen. Ihre Rechte und Befugnisse gegenüber den Mitarbeitervertretungen sind gesetzlich festzulegen.
- Verstöße gegen die Bestimmungen des Beschäftigtendatenschutzgesetzes müssen ein gesetzliches Verwertungsverbot der dadurch gewonnenen Daten nach sich ziehen. Zur Abschreckung bedarf es wirksamer Sanktionen.

Anlage 3:
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009
Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!

Das Bundesministerium der Finanzen (BMF) hat mit einer einfachen Verwaltungsanweisung den Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren weitgehend eingeschränkt. Es macht die Auskunftserteilung von einem "berechtigten Interesse" abhängig, was zu einer Einschränkung des Auskunftsrechts führt.

Die Vorgehensweise des BMF steht im krassen Widerspruch zum Beschluss des Bundesverfassungsgerichts vom 10.03.2008 (1 BvR 2388/03). Danach sind auch von der Finanzverwaltung die Grundrechte auf informationelle Selbstbestimmung und auf effektiven Rechtsschutz zu gewährleisten. Der in § 19 Bundesdatenschutzgesetz (BDSG) verankerte umfassende Auskunftsanspruch findet auch im Besteuerungsverfahren unmittelbare Anwendung.

Es ist inakzeptabel, dass verfassungsrechtlich garantierte Auskunftsrechte der Steuerpflichtigen ausgehebelt werden. Auch die Finanzverwaltung ist an Recht und Gesetz gebunden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass das BMF die Verwaltungsanweisung vom 17.12.2008 unverzüglich aufhebt. Die Finanzbehörden des Bundes und der Länder sind zu verpflichten, entsprechend der Rechtslage den Auskunftsanspruch zu erfüllen. Die Datenschutzbeauftragten des Bundes und der Länder appellieren zudem an den Bundesgesetzgeber, den Auskunftsanspruch der Steuerpflichtigen durch eine eindeutige Regelung in der Abgabenordnung klarzustellen, die dem § 19 BDSG entspricht.

Anlage 4:
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009
Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage

Die Speicherung von Daten im polizeilichen Informationssystem INPOL durch die Polizeien des Bundes und der Länder ist nur dann rechtmäßig, wenn eine Rechtsverordnung gemäß § 7 Abs. 6 Bundeskriminalamtsgesetz das Nähere über die Art der Daten bestimmt, die in dieser Datei gespeichert werden dürfen. Eine solche Rechtsverordnung existiert nicht. Mit Urteil vom 16.12.2008 (Az. 11 LC 229/08) hat das Niedersächsische Oberverwaltungsgericht dies in Bezug auf die Verbunddatei "Gewalttäter Sport" bekräftigt. Das Urteil ist nicht nur für die Rechtmäßigkeit der Hooligan-Datei bedeutsam, sondern hat Auswirkung auf alle im Rahmen von INPOL geführten Verbunddateien.

Mit der Entscheidung des Gerichts wird die Auffassung der Datenschutzbeauftragten des Bundes und der Länder bestätigt. Die vom Bundesministerium des Innern bisher vertretene Auffassung, wonach die Rechtsverordnung keine Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien sei, wird durch die einschlägigen Regelungen nicht gestützt.

Ohne eine derartige Rechtsverordnung ist die Gesamtheit der in Verbunddateien stattfindenden polizeilichen Datenverarbeitungen rechtswidrig. Die Datenschutzbeauftragten von Bund und Länder fordern das Bundesministerium des Innern und die Landesregierungen auf, unverzüglich daraus Konsequenzen zu ziehen und die polizeiliche Datenverarbeitung auf den Prüfstand zu stellen.

Anlage 5:
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27.03.2009
Defizite beim Datenschutz jetzt beseitigen!

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Deutschland auf, endlich die nötigen Konsequenzen aus den nicht mehr abreißenden Datenskandalen zu ziehen. Dazu sind mindestens folgende Schritte geboten:

1. Der Deutsche Bundestag wird aufgefordert, noch in dieser Legislaturperiode die von der Bundesregierung vorgelegten Gesetzentwürfe für erste notwendige Korrekturen des Bundesdatenschutzgesetzes im Bereich der Auskunfteien und des Adresshandels zu verabschieden. Ansonsten verlieren die Bürgerinnen und Bürger das Vertrauen in die Zusagen der Bundesregierung nach den Skandalen des Jahres 2008. Insbesondere mit Adressen darf nur noch mit ausdrücklicher Einwilligung der Betroffenen Handel getrieben werden. Der Entwurf für ein Datenschutzauditgesetz muss gründlich überarbeitet werden, damit dieser notwendige Schritt hin zu einem modernen Datenschutzrecht von der Praxis auch umgesetzt werden kann.
2. Mit Beginn der nächsten Legislaturperiode muss endlich eine grundlegende Modernisierung des Datenschutzrechts in Angriff genommen werden, die bereits zu lange aufgeschoben wurde. Nur so kann das Datenschutzrecht den Herausforderungen der Informationsgesellschaft zu Beginn des 21. Jahrhunderts gerecht werden.
3. Der Einsatz datenschutzfreundlicher Technik muss vorangetrieben und rechtlich verpflichtend vorgeschrieben werden. Darin liegt auch eine Chance für den Wirtschaftsstandort Deutschland in Zeiten der Krise.

Anlage 6:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16.04.2009
Datenschutz beim vorgesehenen Bürgerportal unzureichend

Der Gesetzentwurf zur Regelung von Bürgerportalen (BR-Drs. 174/09) soll rechtliche Rahmenbedingungen für eine sichere und vertrauenswürdige elektronische Kommunikation zwischen Bürgerinnen und Bürgern und der Wirtschaft und Verwaltung im Internet schaffen. Private Anbieter sollen die Portale betreiben, über die der sichere E-Mail-Verkehr De-Mail, eine sichere Dokumentenablage De-Safe und ein Identitätsbescheinigungsdienst abgewickelt werden sollen. Eine solche Infrastruktur stellt hohe Anforderungen an die IT-Sicherheit und den Datenschutz.

Der Gesetzentwurf wird diesen Anforderungen noch nicht gerecht und ist zumindest in folgenden Punkten zu korrigieren:

- Der Entwurf sieht vor, dass nur akkreditierte Anbieter Portale betreiben dürfen. Voraussetzung für die Akkreditierung darf nicht allein der Nachweis der technischen und administrativen Sicherheit, sondern muss auch die tatsächliche Einhaltung datenschutzrechtlicher Standards sein. Die dabei zu erfüllenden Mindestanforderungen müssen verbindlich im Gesetz vorgegeben werden. Portalbetreiber sollten zudem erst dann die Akkreditierung erhalten, wenn die Umsetzung dieser Anforderungen durch unabhängige Prüfstellen bescheinigt wurde.
- Die Sicherung der Vertraulichkeit, Integrität und Authentizität von Nachrichteninhalten soll lediglich durch eine Verschlüsselung auf dem Transport zwischen den Diensteanbietern und durch die Sicherung des Zugangs zu den Bürgerportalen erfolgen. Es muss jedoch sichergestellt werden, dass Nachrichten auch bei den Portalbetreibern nicht durch Dritte

gelesen oder verändert werden können. Deshalb muss die Kommunikation standardmäßig durch eine Ende-zu-Ende-Verschlüsselung zwischen Absendenden und Empfangenden nach dem Stand der Technik gesichert und nicht nur als Option angeboten werden.

- Das Bürgerportal soll gerade zwischen Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.
- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.
- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss - entgegen der Stellungnahme des Bundesrates vom 3.4.2009 - erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.
- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen - etwa zur verbindlichen Kommunikation mit staatlichen Stellen - hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.
- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.
- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.
- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

Anlage 7:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z.B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;
- die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;
- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;
- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;
- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;
- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z.B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;
- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;
- die Videoüberwachung in Staat und Gesellschaft einzuschränken;
- den Schutz der Meldedaten zu verbessern;
- ein praktikables Datenschutzaudit zu schaffen;
- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

Anlage 8:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

Anlage 9:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 Krankenhausinformationssysteme datenschutzgerecht gestalten!

- Krankenhausinformationssysteme sind heute zu unverzichtbaren Hilfsmitteln ärztlicher Behandlung in Krankenhäusern geworden. Ein Abruf der darin elektronisch gespeicherten Patientendaten ist jederzeit, ortsungebunden und sekundenschnell möglich und bietet damit die Grundlage für effiziente Behandlungsentscheidungen. Diesen Vorteilen stehen aller-

dings erhebliche Datenschutzrisiken gegenüber. Die Möglichkeiten für Klinikpersonal, Behandlungsdaten von Bekannten, Kolleginnen und Kollegen oder Prominenten einzusehen und privat zu nutzen, sind groß. Prüfungen der Datenschutzaufsichtsbehörden und bekannt gewordene Missbrauchsfälle belegen dies.

- Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.
- Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.
- Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.
- Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

Anlage 10:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009 "Reality-TV" - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

"Reality-TV"-Produktionen über behördliche Einsätze haben in den letzten Jahren erheblich zugenommen. Justiz-, Polizei- und Sozialbehörden scheinen mittlerweile wichtige "Lieferanten" für solche Fernsehsendungen zu sein, die einzelne Bürgerinnen und Bürger bloßstellen und dadurch erheblich in ihre Rechte eingreifen. Das Fernsehpublikum ist dabei, wenn etwa eine Gerichtsvollzieherin versucht, einen Haftbefehl gegen einen Schuldner zu vollziehen - wobei auch schon einmal eine Wohnung zwangsgeöffnet wird - oder wenn die Polizei Verdächtige überprüft oder bei Verkehrsdelikten zur Rede stellt. Es kann vom heimischen Fernsehsessel aus bequem mitverfolgen, ob Betroffene glaubwürdig Einsicht zeigen, unbelehrbar bleibt oder gar ausfällig werden. Aufgrund des Erfolgs derartiger "Unterhaltungssendungen" ist abzusehen, dass die Intensität und die Eingriffstiefe der gezeigten staatlichen Maßnahmen zukünftig immer weiter zunehmen werden.

Presse- und Öffentlichkeitsarbeit sind zwar grundsätzlich notwendig, um die behördliche Aufgabenerfüllung darzustellen und den Informationsanspruch der Öffentlichkeit zu erfüllen. Dabei muss aber das Persönlichkeitsrecht der Betroffenen gewahrt werden, gerade wenn Unterhaltung und Befriedigung von Sensationslust im Vordergrund stehen.

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb alle Behörden auf, grundsätzlich von der Mitwirkung an solchen "Reality"-Reportagen Abstand zu nehmen.

Anlage 11:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009
Datenschutzdefizite in Europa auch nach Stockholmer Programm

Die Europäische Union will im Stockholmer Programm ihre politischen Zielvorgaben zur Entwicklung eines Raums der Freiheit, der Sicherheit und des Rechts für die kommenden fünf Jahre festschreiben. Dazu hat die Kommission der Europäischen Gemeinschaften einen Entwurf vorgelegt.

Zwar erwähnt der Kommissionsentwurf die Wahrung der persönlichen Freiheitsrechte und des Schutzes der Privatsphäre als Prioritäten der Innen- und Sicherheitspolitik in einem "Europa der Bürger". Schritte wie der geplante Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention, Aufklärungs- und Informationskampagnen zum Datenschutz und die Förderung und ggf. Zertifizierung von datenschutzfreundlichen Technologien weisen auch in diese Richtung.

Allerdings bleiben die konkreten Überlegungen für einen verbesserten Datenschutz deutlich hinter den Zielsetzungen für eine verbesserte Sicherheitsarchitektur zurück. Hierzu enthält der Kommissionsentwurf einen umfangreichen Katalog von zum Teil äußerst eingriffsintensiven Maßnahmen, wie z.B. ein elektronisches Registrier- sowie Vorabgenehmigungssystem für Ein- und Ausreisen in oder aus der EU oder den Aufbau eines europäischen Strafregisterinformationssystems. Die ebenfalls angestrebte einheitliche Plattform der Informationsverarbeitung mit beinahe beliebigen Datenverarbeitungsmöglichkeiten gefährdet ohne angemessene Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit die Bürgerrechte.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder bedarf es weiterer Schritte, um in Europa ein ausgewogenes Verhältnis von Sicherheit und Freiheit zu erreichen. Hierzu zählen insbesondere:

- Die Weiterentwicklung des Rahmenbeschlusses 2008/977/JI zu einem harmonisierten und auch für die innerstaatliche Datenverarbeitung verbindlichen Datenschutzrecht, das im Bereich der polizeilichen und justiziellen Zusammenarbeit ein hohes Datenschutzniveau gewährleistet.
- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.
- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.
- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.
- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, sich für diese Forderungen - auch unter Berücksichtigung der Kritik des Bundesrates etwa zu der Schaffung von Exekutivbefugnissen für EUROPOL und EUROJUST - im weiteren Verfahren einzusetzen.

Anlage 12:
Entschließung der 78. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 08./09.10.2009
Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängi-

ge Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebliche Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

Anlage 13:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Klare gesetzliche Regelungen zur Abrechnung durch private Stellen in der gesetzlichen Krankenversicherung

In seinem Urteil vom 10.12.2008 hatte das Bundessozialgericht nach der damals bestehenden Rechtslage die Einschaltung privater Stellen bei der Abrechnung von ärztlichen Leistungen gegenüber den gesetzlichen Krankenkassen für unzulässig erklärt. Es betonte, dass bei der Einbeziehung von privaten Stellen ebenso detaillierte Regelungen über den Umfang der verarbeiteten Daten und über die erlaubten Datenflüsse vorliegen müssten, wie dies für die klassischen Abrechnungen über die Kassenärztlichen Vereinigungen der Fall ist. Es sei nicht nachvollziehbar, dass gerade bei der Einbeziehung von Privaten an diese geringere Anforderungen gestellt würden als an die öffentlich-rechtlichen Körperschaften. Infolge des Urteils war die Einbeziehung der privaten Stellen nur noch für einen Übergangszeitraum erlaubt.

Um die Abrechnung von Leistungen durch private Rechenzentren nicht einstellen zu müssen, hat der Gesetzgeber hierfür durch das Arzneimittelrechtsänderungsgesetz vom 17.07.2009 vorläufige Rechtsgrundlagen in den §§ 120 Abs. 6 und 295 Abs. 1 b SGB V geschaffen, die bis zum 30.06.2010 befristet sind. Die Bundesregierung beabsichtigt nunmehr, die Geltung dieser Übergangsregelungen, die den vom Bundessozialgericht formulierten Anforderungen an den Datenschutz nicht entsprechen, um ein weiteres Jahr zu verlängern.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für dringend geboten, unverzüglich materielle Vorgaben für die Einbeziehung privater Stellen bei der Abrechnung von ärztlichen Leistungen im Gesetz zu verankern. Dabei müssen präzise Regelungen geschaffen werden, die denselben Schutz der Sozialdaten garantieren, gleich ob die Daten unter Einschaltung privater oder öffentlich-rechtlicher Abrechnungsstellen verarbeitet werden. Die für die Abrechnung zu verwendenden Daten müssen wie bei den herkömmlichen Abrechungsregelungen für die Patienten transparent verarbeitet und auf das absolut Erforderliche für den konkreten Zweck normativ begrenzt werden. Weiterhin müssen die Datenflüsse in einer Weise definiert werden, dass die Rechte der Versicherten so wenig wie möglich gefährdet werden. Eine Rechtsaufsicht über die Datenverarbeitung ist sicherzustellen. Es ist zu gewährleisten, dass Krankenkassen bei der Beauftragung privater Abrechnungsstellen nicht mehr Sozialdaten erhalten als bei der Abrechnung über die Kassenärztliche Vereinigung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung auf, unverzüglich inhaltliche Vorschläge für eine verfassungskonforme Regelung zu erarbeiten.

Anlage 14:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Für eine umfassende wissenschaftliche Evaluierung im Sicherheitsbereich

Die Bundesregierung beabsichtigt, nicht nur die in den vergangenen Jahren durch zahlreiche Gesetze neu geschaffenen Befugnisse und die bestehenden Sicherheitsdateien, sondern auch die Kooperationszentren, in denen Polizei und Nachrichtendienste zusammenarbeiten, zu evaluieren.

Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, die Evaluierung zeitnah und vorbehaltlos nach wissenschaftlichen Kriterien durchzuführen. Kein Vorbild darf die im Mai 2005 vorgenommene "Evaluierung" des Terrorismusbekämpfungsgesetzes 2002 sein. Diese war eine inhaltlich und methodisch defizitäre Selbsteinschätzung. Dagegen enthalten die in verschiedenen Gesetzen aufgenommenen Evaluationsklauseln sinnvolle Ansätze, die es weiter zu entwickeln gilt. Dies betrifft etwa die Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag zu bestellen ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt darauf hingewiesen, dass die Ausweitung der Befugnisse von Polizei und Verfassungsschutz, auch in das Vorfeld der Gefahrenabwehr, zur anlasslosen, oftmals massenhaften Erhebung personenbezogener Daten unbescholtener Bürgerinnen und Bürger führen kann.

Aufgrund der Eingriffsintensität der Regelungen ist eine systematische, ergebnisoffene und wissenschaftlich fundierte Überprüfung auf der Grundlage eines umfassenden Bewertungsansatzes erforderlich. Jede Evaluation, auch die landesrechtlicher Vorschriften, muss auf der Grundlage valider, strukturierter Daten unter Mitwirkung aller relevanten Stellen in einem transparenten Verfahren durch

ein unabhängiges Expertengremium erfolgen. Die Nachvollziehbarkeit und Überprüfbarkeit der Evaluierung ist zu gewährleisten. Der Evaluationsbericht muss dem Gesetzgeber eine umfassende Bewertungsgrundlage zur Optimierung bestehender Regelungen zur Verfügung stellen.

Dazu muss insbesondere Folgendes dargelegt und bewertet werden

- die mit der zu evaluierenden Norm intendierten Ziele,
- die tatsächlich erzielten Wirkungen (beabsichtigte und unbeabsichtigte) sowie die Wirkungszusammenhänge,
- die Auswirkungen auf die Grundrechte von Betroffenen und unbeteiligten Dritten (Eingriffsbreite und -tiefe),
- die Gewährleistung eines effektiven Grundrechtsschutzes, insbesondere im Hinblick auf den absolut geschützten Kernbereich der privaten Lebensgestaltung, sowie die Wahrung des Verhältnismäßigkeitsgebots,
- die Umsetzung von organisations-, verfahrens- und technikorientierten Schutzvorkehrungen (z.B. von Kennzeichnungspflichten, differenzierten Zugriffsberechtigungen, Verwertungsverboten, Prüf- und Löschungspflichten, Richtervorbehalten, Benachrichtigungspflichten),
- die Leistung, Wirkung sowie der Erfolg und die Effizienz,
- die Stellung der zu evaluierenden Norm im Gesamtrechtsgefüge sowie ihre Wechselwirkung mit anderen Normen.

Die Evaluierung ist kein statischer, sondern ein dynamischer, entwicklungsoffener Prozess, der einer ständigen Optimierung bedarf.

Anlage 15:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Körperscanner - viele offene Fragen

Der Anschlagsversuch von Detroit am 23.12.2009 hat die Diskussion über den Einsatz von sog. Körperscannern bei der Passagierkontrolle am Flughafen neu entfacht. Mit dieser Technik sollen Sicherheitslücken geschlossen werden. Es ist aber noch weitgehend unklar, was diese Geräte technisch leisten können und wie sie sich in ein konsistentes Gesamtsystem zur Flugsicherheit einfügen lassen. Eine Entscheidung über den Einsatz solcher Geräte, die der Gesetzgeber zu treffen hätte, setzt zumindest die Erfüllung folgender Bedingungen voraus:

1. Es muss geklärt werden, ob mit diesen Geräten ein nennenswerter Sicherheitsgewinn erzielbar ist. Derzeit bestehen zumindest ernsthafte Zweifel an der technischen Leistungsfähigkeit und Effizienz dieser Technologie, vor allem im Hinblick auf die Detektierbarkeit von Materialien mit geringer Dichte, etwa pulverförmigen Substanzen, wie sie im Fall des Anschlagsversuchs von Detroit verwendet worden sind.
2. Es muss sichergestellt sein, dass die beim Einsatz der Körperscanner erhobenen Daten der Kontrollierten über den Scanvorgang hinaus nicht gespeichert werden. Auch die Anzeige der Körperkonturen gegenüber dem Kontrollpersonal und die Speicherung der erstellten Bilder über den Scanvorgang hinaus sind technisch auszuschließen.
3. Selbst wenn die vorstehenden Bedingungen erfüllt werden, darf der Einsatz von Scannern die Grundrechte der Betroffenen, insbesondere die ab-

solut geschützte Menschenwürde und das Recht auf körperliche Unversehrtheit nicht verletzen. So dürften z.B. Geschlechtsmerkmale oder künstliche Körperteile bzw. medizinische Hilfsmittel (etwa Prothesen und künstliche Darmausgänge) nicht angezeigt werden. Gesundheitsschäden sind auszuschließen.

4. Die Erfüllung dieser Bedingungen ist in praktischen Tests und Erprobungen nachzuweisen.

Anlage 16:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Keine Vorratsdatenspeicherung!

Das Bundesverfassungsgericht bewertet in seinem Urteil zur Vorratsdatenspeicherung vom 02.03.2010 (1 BvR 256/08) die anlass- und verdachtslose vorsorgliche Speicherung von Telekommunikationsdaten als einen "besonders schweren Eingriff mit einer Streubreite, wie sie die Rechtsordnung bisher nicht kennt". Weil diese Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch aller Bürgerinnen und Bürger ermöglicht, lehnt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Vorratsdatenspeicherung grundsätzlich ab. Das Verbot der Totalerfassung gehört zur verfassungsrechtlichen Identität der Bundesrepublik Deutschland, die auch in europäischen und internationalen Zusammenhängen zu wahren ist. Die Konferenz fordert deshalb die Bundesregierung auf, sich für eine Aufhebung der Europäischen Richtlinie 2006/24/EG einzusetzen.

Darüber hinaus betont das Bundesverfassungsgericht, dass die Freiheitswahrnehmung der Bürgerinnen und Bürger nicht total erfasst und registriert werden darf. Daher strahlt die Entscheidung über den eigentlichen Entscheidungsgegenstand hinaus und muss auch in anderen Bereichen, etwa bei der diskutierten Speicherung der Daten von Flugpassagieren oder bei der Konzeption von Mautsystemen beachtet werden. Auch die zentrale ELENA-Datenbank muss jetzt auf den Prüfstand. Der Gesetzgeber ist bei der Erwägung neuer Speicherungspflichten oder -berechtigungen im Hinblick auf die Gesamtheit der verschiedenen Datensammlungen zu größerer Zurückhaltung aufgerufen.

Anlage 17:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Ein modernes Datenschutzrecht für das 21. Jahrhundert

Zusammenfassung

Jeder Mensch soll selbst bestimmen können, wer was wann über ihn weiß. Doch wie soll dieses Recht auf informationelle Selbstbestimmung im Zeitalter der allgegenwärtigen, oftmals unbemerkten Datenverarbeitung gewährleistet werden? Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat Eckpunkte formuliert, die Grundlage einer Diskussion über eine Reform des Datenschutzrechts sein sollen.

1. Konkrete Schutzziele und Grundsätze verankern

Das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze sollten als allgemeingültige datenschutzrechtliche Grundregelungen einen verbindlichen Mindeststandard festlegen. Sie sollten allgemeine Vorgaben enthalten, die als Grundlage aller datenschutzrechtlichen Regelungen und Maßnahmen für öffentliche und nicht-öffentliche Stellen dienen. Ausgehend von den Schutzzielen sollten sanktionsbewehrte Grundsatznormen formuliert werden, die für alle Formen der Datenverarbeitung gleichermaßen gelten. Dies betrifft etwa den Grundsatz der Zweckbindung, also das Prinzip, dass personenbezogene Daten ausschließlich für den Zweck verwendet werden dürfen, für den sie erhoben worden sind. Neu eingeführt werden sollte zudem ein grundsätzliches Verbot der Profilbildung. Die Vorgaben des allgemeinen Datenschutzrechts können - soweit erforderlich - in Bezug auf bestimmte Anwendungsgebiete weiter konkretisiert werden.

2. Technikneutralen Ansatz schaffen

Den aus der technologischen Entwicklung resultierenden Gefährdungen sollte durch technikneutrale Vorgaben begegnet werden, die auf konkrete Systeme und Anwendungsfelder durch Auslegung und Normierung konkretisiert werden können. Anhand festgelegter Schutzziele können so einfache, flexible, und praxistaugliche gesetzliche Bedingungen geschaffen werden, die das Grundrecht auf informationelle Selbstbestimmung und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme durch technischen und organisatorischen Datenschutz sichern.

3. Betroffenenrechte stärken

Dreh- und Angelpunkt zur Durchsetzung des Datenschutzes ist der aufmerksame und kritische Betroffene. Die Datenverarbeitung muss für die Betroffenen transparenter werden, etwa indem die Wahrnehmung des Auskunftsanspruchs erleichtert wird. Die Freiwilligkeit der Einwilligung in eine Datenverarbeitung muss gestärkt werden.

4. Datenschutzrecht internetfähig machen

Ein modernes Datenschutzrecht muss internetfähig sein. Grundsätzlich muss eine unbeobachtete Kommunikation und Nutzung des Internets gewährleistet werden. Auch sind besondere Schutzmechanismen zur Gewährleistung und Durchsetzung der Datenschutzrechte der Betroffenen im Netz zu schaffen. Nationale Regelungen sollten durch internationale Vereinbarungen flankiert werden.

5. Mehr Eigenkontrolle statt Zwang

Datenschutz muss von den verantwortlichen Stellen als eigenes Anliegen begriffen werden. Dies kann etwa durch Einführung eines freiwilligen Auditverfahrens befördert werden. Daneben müssen die verantwortlichen Stellen dazu verpflichtet werden, durch interne Mechanismen die Einhaltung des Datenschutzes sicherzustellen, etwa durch verbindliche Datenschutzkonzepte.

6. Stärkung der unabhängigen Datenschutzaufsicht

Die Unabhängigkeit der Datenschutzaufsicht muss rechtlich, organisatorisch und finanziell abgesichert werden. Eine Fach- und Rechtsaufsicht oder die organisatorische Eingliederung in andere Verwaltungseinheiten

ist mit der EG-Datenschutzrichtlinie nicht vereinbar. Erforderlich sind auch verstärkte Mitwirkungspflichten der kontrollierten Stellen bei Datenschutzkontrollen.

7. Wirksamere Sanktionen
Die immer noch vorhandenen Lücken im datenschutzrechtlichen Sanktionssystem müssen endlich geschlossen werden. Sie sollten ergänzt werden um für die Betroffenen einfach zu handhabende Haftungsansprüche, etwa einen pauschalierten Schadenersatzanspruch. Die Zuständigkeiten für die Verfolgung von Ordnungswidrigkeiten sollten bei den jeweiligen Datenschutzbehörden liegen. Auch der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit braucht insoweit wirksame Sanktionsbefugnisse.

8. Gesetz einfacher und besser lesbar machen
Das Datenschutzrecht ist durch wiederholte Änderungen und Ergänzungen selbst für Fachleute nur noch schwer verständlich und bedarf auch insoweit der Überarbeitung. Erforderlich sind etwa Änderungen in der Struktur und bei den Definitionen, die zusätzliche Spezialvorschriften entbehrlich machen.

Anlage 18:
Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 17./18.03.2010
Effektiver Datenschutz braucht unabhängige Datenschutzkontrolle!

Um das Grundrecht der Bürgerinnen und Bürger auf Datenschutz zu gewährleisten, bedarf es einer unabhängigen Datenschutzkontrolle. Der Europäische Gerichtshof hat festgestellt, dass die Datenschutzaufsichtsbehörden für den nichtöffentlichen Bereich in Deutschland nicht völlig unabhängig sind und die Bundesrepublik Deutschland damit gegen die Verpflichtung aus Art. 28 der Datenschutzrichtlinie (Richtlinie 95/46/EG) verstößt (Urteil vom 09.03.2010, C-518/07). Europarechtswidrig ist nicht nur die organisatorische Einbindung zahlreicher Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich in die jeweiligen Innenministerien, sondern auch die Aufsicht der Regierungen über die Datenschutzbehörden. Darüber hinaus ist eine grundsätzliche Neuordnung der Datenschutzaufsicht in Deutschland geboten. Die Grundsätze dieser Entscheidung zur Unabhängigkeit sind auf die Datenschutzkontrolle der öffentlichen Stellen anzuwenden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Gesetzgeber in Bund und Ländern auf, die Datenschutzaufsicht schnellstmöglich den Vorgaben der Richtlinie entsprechend umzugestalten.

Die Ausgestaltung der Unabhängigkeit der Datenschutzkontrollinstanzen muss insbesondere folgenden Kriterien entsprechen:

- Die Datenschutzkontrollstellen müssen ihre Aufgaben ohne jegliche unmittelbare und mittelbare Einflussnahme Dritter wahrnehmen können.
- Es darf keine Fach- und Rechtsaufsicht geben.

- Auch eine mögliche Dienstaufsicht darf nicht zu einer unmittelbaren oder mittelbaren Einflussnahme auf Entscheidungen der Datenschutzkontrollstellen führen.
- Eine Einflussnahme seitens der kontrollierten Stellen ist auszuschließen.
- Zu einer unabhängigen Amtsführung gehören ausreichende Eingriffs- und Durchsetzungsbefugnisse.
- Um eine unabhängige Wahrnehmung der Tätigkeit der Datenschutzkontrollstellen zu gewährleisten, muss ihnen die notwendige Entscheidungshoheit bei Personal, Haushalt und Organisation zustehen.

Anlage 19:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22.06.2010
Beschäftigtendatenschutz stärken statt abbauen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass die Bundesregierung nach nahezu 30-jähriger Diskussion den Bereich Beschäftigtendatenschutz gesetzlich regeln will. Angesichts der Bedeutung des Beschäftigtendatenschutzes für Arbeitgeber und Arbeitnehmer sollte im Gesetzgebungsverfahren der Grundsatz "Qualität vor übereilten Regelungen" gelten. Im Hinblick darauf wäre es verfehlt, den Gesetzentwurf in einem Schnellverfahren ohne gründliche Diskussion durchzupauken. Ein solches Verfahren würde unweigerlich zu handwerklichen Fehlern und zu einer nicht akzeptablen inhaltlichen Unausgewogenheit der Bestimmungen führen. Beides gilt es zu vermeiden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bedauert daher, dass der vom Bundesminister des Innern vorgelegte Entwurf das angestrebte Ziel eines zeitgemäßen und verbesserten Schutzes der Beschäftigten vor Überwachung und übermäßiger Kontrolle in wesentlichen Punkten und Zusammenhängen verfehlt. Zudem bleibt eine ganze Reihe von Fragen und Problemen ungeklärt. Im Ergebnis würden die vorgesehenen Änderungen in zentralen Bereichen des Arbeitslebens eine Verschlechterung des Datenschutzes für die Beschäftigten zur Folge haben. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an den Bundesgesetzgeber, den vorliegenden Gesetzentwurf grundlegend zu überarbeiten, jedenfalls aber deutlich zu Gunsten des Persönlichkeitsrechts der Beschäftigten zu ändern. Ein Gesetz zur Regelung des Beschäftigtendatenschutzes sollte einen angemessenen Ausgleich zwischen den berechtigten Informationsinteressen des Arbeitgebers und dem verfassungsrechtlich geschützten Persönlichkeitsrecht des Beschäftigten schaffen. An diesem Anspruch muss sich ein Beschäftigtendatenschutzgesetz messen lassen, das diesen Namen verdient.

Substantielle Verbesserungen an dem Entwurf eines Beschäftigtendatenschutzgesetzes sind insbesondere in den folgenden Punkten geboten:

- Die im Gesetzentwurf vorgesehene Erlaubnis zur Datenverarbeitung bei Verhaltens- und Leistungskontrollen ist zu weit gefasst und lädt zur Ausweitung der Kontrolle und Überwachung der Beschäftigten geradezu ein. Sie muss deshalb präzise gefasst werden und ist an strenge Voraussetzungen zu knüpfen, damit die durch höchstrichterliche Rechtsprechung

gefestigte Auslegung des derzeitigen Datenschutzrechts im Sinne des Schutzes der Beschäftigten vor übermäßiger Überwachung bestehen bleibt.

- Auch die im Entwurf vorgesehene allgemeine Erlaubnis zur Verarbeitung und Nutzung von Beschäftigtendaten zur "Verhinderung und Aufdeckung von Vertragsverletzungen zu Lasten des Arbeitgebers, Ordnungswidrigkeiten und Straftaten" würde den Arbeitgebern sehr weitgehende zusätzliche Befugnisse zur Auswertung und Verknüpfung unterschiedlichster Datensammlungen in die Hand geben. Der Gesetzgeber muss vielmehr klarstellen, dass Maßnahmen, die zu einer ständigen Kontrolle der Beschäftigten führen oder den Betroffenen den Eindruck einer umfassenden Überwachung am Arbeitsplatz vermitteln - etwa durch ständige Videoüberwachung oder regelmäßige Aufzeichnung, Mitschnitte oder Mithören von Ferngesprächen -, weiterhin zu unterbleiben haben.
- Die Intention des Gesetzentwurfs, den Umfang der in Bewerbungsverfahren und während des Beschäftigungsverhältnisses verwendeten Daten zu begrenzen, wird auch verfehlt, wenn - wie im Entwurf vorgesehen - Arbeitgeber im Internet verfügbare Informationen generell nutzen dürfen, und zwar sogar dann, wenn diese durch Dritte ohne Kenntnis der Betroffenen und somit häufig rechtswidrig eingestellt wurden. Damit wird vom datenschutzrechtlichen Grundsatz der Direkterhebung beim Betroffenen abgewichen und Arbeitgeber werden geradezu dazu eingeladen, im Internet und in sozialen Netzwerken systematisch nach dort vorhandenen Informationen über Bewerber und Beschäftigte zu recherchieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet vom Gesetzgeber, dass er die Nutzung derartiger Daten untersagt oder zumindest wirksam begrenzt und die Arbeitgeber dazu verpflichtet, die Betroffenen aktiv - und nicht erst auf Nachfrage - darüber aufzuklären, woher die verwendeten Daten stammen.
- Der Schutz der Beschäftigten vor unangemessener Kontrolle und Überwachung ist gerade bei der zunehmenden Nutzung elektronischer Medien am Arbeitsplatz von besonderer Bedeutung. Es ist eine normenklare, strikte Begrenzung der Einsichtnahme der Arbeitgeber in die elektronische Kommunikation von Beschäftigten unter Berücksichtigung von deren schützenswerten Belangen erforderlich.
- Die im Gesetzentwurf an mehreren Stellen vorgesehene "Einwilligung" der Beschäftigten führt zu einer erheblichen Erweiterung der (Kontroll-) Befugnisse der Arbeitgeber. Diese wären jedoch rechtlich höchst zweifelhaft, weil Einwilligungen im Arbeitsverhältnis in den meisten Fällen mangels Freiwilligkeit nicht rechtswirksam erteilt werden können. Hinzu kommt, dass im Gesetzentwurf an keiner Stelle definiert ist, welche Anforderungen an die Rechtswirksamkeit von Einwilligungen im Arbeitsverhältnis zu stellen sind.

Anlage 20:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24.06.2010
Erweiterung der Steuerdatenbank enthält große Risiken

Bundesrat und Bundestag beraten in Kürze über die im Jahressteuergesetz 2010 vorgesehenen ergänzenden Regelungen zur Erweiterung der zentralen Steuerdatenbank. Die Datenbank soll um elektronische Lohnsteuerabzugsmerkmale

(ELStAM), wie z.B. sensible Angaben zu Religionszugehörigkeit und Familienangehörigen, ergänzt werden. Die Datenschutzbeauftragten des Bundes und der Länder halten es für erforderlich, diese Regelungen kritisch daraufhin zu prüfen, ob sie datenschutzrechtlichen Belangen genügen und die Rechte der betroffenen Arbeitnehmer hinreichend wahren. Folgende Punkte müssen besondere Beachtung finden:

- Vorherige Information der Arbeitnehmer
  Mit der Bildung der elektronischen Lohnsteuerabzugsmerkmale ist die Ablösung der Papierlohnsteuerkarte verbunden. Um eine transparente Verfahrensumstellung zu gewährleisten, müssen die betroffenen Arbeitnehmer vor der erstmaligen Anwendung über die sie jeweils konkret betreffenden neuen Merkmale informiert werden. Dies ermöglicht den Arbeitnehmern, etwaige Fehler in der Datenerfassung beim Bundeszentralamt für Steuern vor dem Datenabruf durch den Arbeitgeber zu korrigieren.

- Keine Speicherung auf Vorrat
  In der zentralen Datenbank sollen auch Datensätze zu Personen erfasst werden, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Die Speicherung von Datensätzen auf Vorrat ist verfassungsrechtlich höchst fragwürdig. Im Rahmen eines anlassbezogenen Vorgehens sollten Datensätze nur zu solchen Personen gespeichert werden, die tatsächlich lohnsteuerpflichtig sind.

- Verhindern des unzulässigen Datenabrufs
  Die gespeicherten Datensätze werden bundesweit ca. vier Millionen Arbeitgebern zur Verfügung stehen. Ein Abruf der elektronischen Lohnsteuerabzugsmerkmale soll nur möglich sein, wenn sich der Arbeitgeber oder ein von ihm beauftragter Dritter authentifiziert und seine Steuernummer mitteilt. Das vorgesehene Verfahren muss jedoch gewährleisten, dass nur befugte Arbeitgeber die Datensätze abrufen können. Ob dies tatsächlich erreicht wird, bleibt klärungsbedürftig. Ist ein unzulässiger Datenabruf nicht auszuschließen, sollte der Abruf generell nur unter Mitwirkung des betroffenen Arbeitnehmers möglich sein.

- Kein Start ohne verfahrensspezifisches IT-Sicherheitskonzept
  Die erweiterte zentrale Datenbank wird sehr sensible steuerliche Daten von mehr als 40 Millionen Arbeitnehmern enthalten. Ein hoher Standard hinsichtlich der Datensicherheit muss daher spätestens mit Inbetriebnahme gewährleistet sein. Dies setzt voraus, dass ein umfassendes und vollständiges verfahrensspezifisches IT-Sicherheitskonzept vorliegt. Die Erfahrung zeigt, dass die Entwicklung von IT-Sicherheitskonzepten für Datenbanken dieses Umfangs in zeitlicher Hinsicht einen längeren Vorlauf benötigt. Die notwendigen Arbeiten an einem IT-Sicherheitskonzept müssen unbedingt vor dem Aufbau der Datenbank abgeschlossen sein.

Anlage 21:
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11.10.2010
Rundfunkfinanzierung: Systemwechsel nutzen für mehr statt weniger Datenschutz!

Die Staatskanzleien der Länder bereiten zurzeit den auch von den Datenschutzbeauftragten des Bundes und der Länder seit langem geforderten Systemwechsel bei der Finanzierung des öffentlich-rechtlichen Rundfunks vor. Ab 2013 soll diese nicht mehr durch eine gerätebezogene Abgabe erfolgen, sondern durch einen wohnungs- bzw. betriebsbezogenen Beitrag, der für jede Wohnung nur einmal, unabhängig von der Art und Anzahl der betriebenen Empfangsgeräte, zu entrichten ist und den Betriebe gestaffelt nach ihrer Größe bezahlen sollen. Der Modellwechsel eröffnet die Möglichkeit, sowohl Finanzierungssicherheit für den öffentlich-rechtlichen Rundfunk zu schaffen, als auch endlich die datenschutzrechtlich relevanten Befugnisse beim Gebühreneinzug auf das erforderliche Maß zu begrenzen und den Grundsatz der Datensparsamkeit und -vermeidung bei der Beitragserhebung umzusetzen.

Der Staat ist gehalten, gesetzlich dafür zu sorgen, dass die Datenverarbeitung auf ein Maß beschränkt wird, das für den Zweck der Rundfunkfinanzierung unerlässlich ist. Der zur Anhörung zu dem Modellwechsel vorgelegte Entwurf des 15. Rundfunkänderungsstaatsvertrages (Rundfunkbeitragsstaatsvertrages - RBStV-E) entspricht dem nicht, sondern schafft statt dessen eine Vielzahl von Datenerhebungsbefugnissen für die Beitragserhebungsstelle, die diese nach dem Modellwechsel von der Gebühr zur Wohnungsabgabe nicht mehr benötigt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Staatskanzleien daher auf, den vorgelegten Entwurf noch einmal unter Beachtung der Grundsätze der Erforderlichkeit, Verhältnismäßigkeit, Normenklarheit und Datensparsamkeit nachzubessern und dabei insbesondere

- die Datenerhebungsbefugnisse beim Beitragseinzug von Wohnungsinhabern auf das erforderliche Maß zu beschränken, den Direkterhebungsgrundsatz zu beachten und vor allem auf Datenerhebung beim Adresshandel zu verzichten,
- bei Befreiungsanträgen von Wohnungsinhabern aus sozialen Gründen wie Armut oder Behinderung nur die Vorlage einer Bestätigung des Leistungsträgers zuzulassen, auf die Vorlage der vollständigen Leistungsbescheide aber zu verzichten und
- auf die beabsichtigten Übermittlungen der Adressdaten aller gemeldeten Volljährigen durch die Meldestellen als Einstieg in das neue Beitragsmodell über einen Zeitraum von zwei Jahren zu verzichten, stattdessen die Datenübermittlung auf zeitnahe Übermittlungsbefugnisse nach dem Melderecht zu beschränken.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist in diesem Zusammenhang auch auf die Stellungnahme hin, die sie zur Anhörung zum 15. Rundfunkänderungsstaatsvertrag abgegeben hat.

Anlage 22:
Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010
Keine Volltextsuche in Dateien der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung und die Landesregierungen auf, volltextbasierte Dateisysteme nur innerhalb der sehr engen verfassungsrechtlichen Grenzen auszugestalten.

Die Sicherheitsbehörden des Bundes und der Länder (Verfassungsschutz, Polizei) bauen zurzeit ihre elektronischen Dateisysteme aus. Dabei beziehen sie auch Daten mit ein, die bisher nur in Akten vorhanden sind, und streben eine umfassende Volltextverarbeitung mit Suchmöglichkeiten an. Nach jedem in einem Dokument vorkommenden Wort oder Datum kann elektronisch gesucht werden, weil das Dokument als Ganzes erfasst wird.

Dies hat gravierende Folgen: In Akten befinden sich auch Daten von Personen, gegen die sich die behördlichen Maßnahmen nicht als Zielperson richten. Auch wer als unbescholtene Bürgerin oder unbescholtener Bürger unwissentlich Kontakt mit einer Zielperson hatte und beiläufig in den Akten genannt wird, wird nun gezielt elektronisch recherchierbar.

Ein solcher Paradigmenwechsel steht im Widerspruch zum geltenden Recht. Danach dürfen die Sicherheitsbehörden nur unter restriktiven Voraussetzungen ausgewählte personenbezogene Daten in automatisierten Dateien speichern und übermitteln. Heute sind die zu speichernden Datenarten und Datenfelder in spezifischen Datei- und Errichtungsanordnungen genau festzulegen. Die Datenschutzbeauftragten müssen zuvor beteiligt werden.

Durch eine Volltextrecherche würden diese datenschutzrechtlichen Sicherungen aufgehoben. Die Zweckbindung der Datenverarbeitung wäre nicht mehr zu gewährleisten. Die gesetzlichen Begrenzungen sind von verfassungsrechtlichem Gewicht. Der Gesetzgeber hat bewusst engere Voraussetzungen vorgegeben, wenn personenbezogene Daten in IT-Systemen gespeichert werden. Denn elektronisch erfasste Daten können, wie das Bundesverfassungsgericht in ständiger Rechtsprechung betont, in Sekundenschnelle umfassend ausgewertet und ohne Rücksicht auf Entfernungen abgerufen werden. Damit würde in das Grundrecht der Betroffenen auf informationelle Selbstbestimmung besonders intensiv eingegriffen, insbesondere wenn die Daten ohne Wissen der Betroffenen erhoben und verarbeitet werden.

Diese verfassungsrechtlich gebotenen Vorkehrungen zum Schutz des Rechts auf informationelle Selbstbestimmung, insbesondere die informationelle Gewaltenteilung, würden hinfällig, wenn die unbegrenzte elektronische Volltexterfassung sämtlicher Informationen zugelassen würde.

Daran würde sich rechtlich nichts ändern, wenn technische Mechanismen derartige Auswertungen (vorübergehend) erschweren. Denn zum einen sind diese jederzeit technisch änderbar. Zum anderen würde eine vorübergehende Erschwe-

rung der Recherchemöglichkeit weder den Eingriff in das Recht auf informationelle Selbstbestimmung noch den Verstoß gegen die vom Bundesverfassungsgericht vorgegebenen Grenzen einer Vorratsdatenverarbeitung beseitigen.

Bestehen diese Datenschutzrisiken schon bei allgemeinen Verwaltungsbehörden, sind sie bei den Sicherheitsbehörden umso gravierender. Dies gilt besonders für den Bereich der Nachrichtendienste, die auch Informationen zu legalem Verhalten und Erkenntnisse mit noch unklarer Relevanz sammeln dürfen. Für die - ggf. gänzlich unverdächtigen - Betroffenen hätte eine systemweite gezielte Suche möglicherweise gravierende Konsequenzen. Diese Risiken sind bei der Weiterentwicklung der IT-Systeme bereits in der Konzeptplanung zu berücksichtigen und auszuschließen.

Anlage 23:
Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010
Datenschutz bei der digitalen Messung und Steuerung des Energieverbrauchs

Das Energiewirtschaftsgesetz legt fest, dass seit Anfang des Jahres 2010 digitale Zähler in Häuser und Wohnungen eingebaut werden müssen, die den tatsächlichen Energieverbrauch (z.B. Strom und Gas) und die tatsächliche Nutzungszeit messen (Smart Metering). Damit sollen Verbraucher ihren Energieverbrauch künftig besser kontrollieren und steuern können und zur Verbesserung der Energieeffizienz beitragen.

Digitale Zähler ermöglichen die sekundengenaue Erfassung des Verbrauchs. Bei diesen Informationen handelt es sich um personenbezogene Daten, mit denen detaillierte Nutzungsprofile erstellt werden können. Viele Handlungen des täglichen Lebens in der Wohnung führen zumindest mittelbar zum Verbrauch von Energie. In der Nutzung dieser Ressourcen spiegeln sich somit Tagesabläufe wider. Die detaillierte Erfassung des Verbrauchs birgt daher ein hohes Ausforschungspotenzial bezüglich der Lebensgewohnheiten der Betroffenen in sich. Dies gilt in besonderem Maße, wenn neben dem Gesamtverbrauch im häuslichen Bereich auch der Verbrauch einzelner Endgeräte erfasst wird. Zusätzliche Risiken entstehen, wenn die digitalen Zähler zu Steuerungszentralen für im Haushalt betriebene Geräte ausgebaut werden.

Die detaillierte Erfassung des Energieverbrauchs kann zu tiefgreifenden Verletzungen der Persönlichkeitsrechte der Betroffenen führen und sowohl das Recht auf informationelle Selbstbestimmung als auch die verfassungsrechtlich garantierte Unverletzlichkeit der Wohnung beeinträchtigen. Durch die langfristige Aufzeichnung, die Verknüpfungsmöglichkeiten derartiger Verbrauchsprofile mit anderen Daten und ein Auslesen der Daten per Fernzugriff sind weitere Gefährdungen der Privatsphäre der Betroffenen zu befürchten.

Eine effiziente Energiedistribution und -nutzung darf nicht mit datenschutzrechtlichen Beeinträchtigungen einhergehen. Die zur Einführung digitaler Zähler bisher erlassenen Rechtsnormen im Energiewirtschaftsgesetz schützen die Privatsphäre der Betroffenen jedoch nur unzureichend.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine gesetzliche Regelung für die Erhebung, Verarbeitung und Nutzung der durch digitale Zähler erhobenen Verbrauchsinformationen. Eine solche Regelung muss die schutzwürdigen Interessen der Betroffenen berücksichtigen und eine strikte Zweckbindung der erhobenen personenbezogenen Daten vorschreiben. Die Regelung muss zudem sicherstellen, dass die Prinzipien der Transparenz der Datenverarbeitung beachtet und die Betroffenenrechte gewahrt werden.

Die Gewährleistung des Datenschutzes muss dabei bereits bei der Konzeption und Gestaltung der Infrastruktur zur Energiemessung und der technischen Einrichtungen erfolgen. Dies gilt insbesondere für den Grundsatz der Datenvermeidung und für die Datensouveränität der Betroffenen. So ist sicherzustellen, dass detaillierte Verbrauchswerte von Endgeräten unter ausschließlicher Kontrolle der Betroffenen verarbeitet und nicht mit direktem oder indirektem Personenbezug an Dritte übermittelt werden. Die Inanspruchnahme von umweltschonenden und kostengünstigen Tarifen darf nicht davon abhängig gemacht werden, dass Betroffene personenbezogene Nutzungsprofile offenbaren.

Für digitale Zähler und intelligente Verteil- bzw. Verarbeitungsnetze (Smart Grids) sind technische und organisatorische Maßnahmen nach dem jeweils aktuellen Stand der Technik zu schaffen, die insbesondere die Vertraulichkeit, Integrität, Verfügbarkeit und Transparenz bei der Verarbeitung aller Energieverbrauchs-, Steuerungs- und sonstigen Daten sicherstellen. Hierzu gehört auch die Verschlüsselung personenbezogener Verbrauchsdaten. Die Anforderungen an den technischen Datenschutz und die IT-Sicherheit sind durch verbindliche Standards festzuschreiben, die der Sensitivität der Daten und den zu erwartenden Missbrauchsrisiken Rechnung tragen. Für die Datenverarbeitungssysteme ist zudem ein integriertes Datenschutz- und Sicherheitsmanagementsystem aufzubauen.

Anlage 24:
Entschließung der 80. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 03./04.11.2010
Förderung des Datenschutzes durch Bundesstiftung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nimmt zur Kenntnis, dass die Bundesregierung mit Hilfe einer Stiftung den Datenschutz stärken will. Ungeachtet der noch zu klärenden verfassungsrechtlichen Vorfragen wird dieses Ziel von den Datenschutzbeauftragten nachdrücklich unterstützt. Dieses Vorhaben setzt voraus, dass

- die Stiftung ihre Aufgaben unabhängig von den Daten verarbeitenden Stellen und der IT-Wirtschaft wahrnimmt,
- die größtmögliche Transparenz der Tätigkeit garantiert ist und
- die Stiftung eng mit den Datenschutzbehörden des Bundes und der Länder kooperiert.

Die Stiftung kann nur solche Aufgaben übernehmen, die nicht ausschließlich den Datenschutzbehörden zugewiesen sind. Dies gilt insbesondere für die Kontrolle, ob gesetzliche Anforderungen eingehalten werden.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für angezeigt, möglichst frühzeitig in die Überlegungen zur Stellung und zu den Aufgaben der Stiftung einbezogen zu werden. Insoweit bieten sie der Bundesregierung ihre Unterstützung und Mitarbeit an.

Abkürzungsverzeichnis

a.a.O.	am angegebenen Ort
Abl.	Amtsblatt
a.F.	alte Fassung
Abs.	Abs.
ACUSTIG	Arbeitsplatz-Computer-Unterstützung in der Geschäftsstelle
AD	Active Directory
AGO	Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern
AKDB	Anstalt für Kommunale Datenverarbeitung in Bayern
ÄLRD	Ärztlicher Leiter Rettungsdienst
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft nach § 44 b SGB II
Art.	Artikel
AVBayEAG	Ausführungsverordnung Einheitlicher Ansprechpartner
Az.	Aktenzeichen
BauGB	Baugesetzbuch
BayArchivG	Bayerisches Archivgesetz
BayBeamtVG	Bayerisches Beamtenversorgungsgesetz
BayBG	Bayerisches Beamtengesetz
BayDSG	Bayerisches Datenschutzgesetz
BayEAG	Gesetz über die Zuständigkeit für die Aufgaben des Einheitlichen Ansprechpartners im Freistaat Bayern
BayEUG	Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen
BayFwG	Bayerisches Feuerwehrgesetz
BayHSchG	Bayerisches Hochschulgesetz
BayKOM 2010	Bayerisches Kommunikationsnetz 2010
BayKRG	Bayerisches Krebsregistergesetz
BayPrG	Bayerisches Pressegesetz
BayPVG	Bayerisches Personalvertretungsgesetz
BayRMS	Bayerisches Reisekostenmanagementsystem
BayStatG	Bayerisches Statistikgesetz
BayStVollzG	Bayerisches Strafvollzugsgesetz
BayUIG	Bayerisches Umweltinformationsgesetz
BayVBl	Bayerische Verwaltungsblätter
BayVersG	Bayerisches Versammlungsgesetz
BayVGH	Bayerischer Verwaltungsgerichtshof
BayVSG	Bayerisches Verfassungsschutzgesetz
BayVwVfG	Bayerisches Verwaltungsverfahrensgesetz
BayZeit	Basiskomponente Integriertes Zeitmanagement
BDSG	Bundesdatenschutzgesetz
BGBl	Bundesgesetzblatt
BKAG	Bundeskriminalamtgesetz
BMF	Bundesministerium der Finanzen
BR-Drs.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts (zitiert nach Band und Seite)
BYBN	Bayerisches Behördennetz

bzgl.	bezüglich
bzw.	beziehungsweise
ca.	circa
CD	Compact Disc
CIO	Chief Information Officer
d.h.	das heißt
DIN	Deutsche Industrie Norm
DNA	Desoxyribonuclein Acid, Träger der Erbinformation
DNA-Analyse	Molekulargenetische Untersuchung
DOMEA	.Dokumentenmanagementsystem
DVD	Digital Versatile Disc, Digital Video Disc
EC-Karte	electronic cash-Karte
ED-DI	Erkennungsdienst Digital
EDV	Elektronische Datenverarbeitung
eFA	elektronische Fallakte
EG	Europäische Gemeinschaft
EG-Datenschutzrichtlinie	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
eID	Elektronischer Identitätsnachweis
ELENA	Elektronischer Entgeltnachweis
ELStAM	Elektronische LohnSteuerAbzugsMerkmale
ELSTER.	Elektronische Steuererklärung
E-Mail	Elektronische Post
emDoc	Notarzteinsatz-Dokumentation
EnWG	Energiewirtschaftsgesetz
EStG	Einkommensteuergesetz
etc.	et cetera
EU	Europäische Union
evtl.	eventuell
f.	folgende
ff.	fortfolgende
FIFA	Féderation Internationale de Football Association
FMG	Flughafen München GmbH
GDVG	Gesundheitsdienst- und Verbraucherschutzgesetz
gem.	gemäß
GenDG	Gendiagnostikgesetz
GewO	Gewerbeordnung
GewV	Gewerbeverordnung
GG	Grundgesetz
ggf.	gegebenenfalls
GmbH	Gesellschaft mit beschränkter Haftung
GO	Gemeindeordnung
GOBS	Grundsätze ordnungsgemäßer Buchführung
GVBl	Gesetz- und Verordnungsblatt
GVG	Gerichtsverfassungsgesetz
HGB	Handelsgesetzbuch
https.	Hyper Text Transfer Protocol Secure
i.S.d.	im Sinne des
i.V.m.	in Verbindung mit
IfSG	Infektionsschutzgesetz
IGVP	Integrationsverfahren der Bayerischen Polizei
INPOL	Informationssystem der Polizei (bundesweit)

IP	Internet Protocol
IT	Informationstechnik
IuK	Informations- und Kommunikationstechnik
JGG	Jugendgerichtsgesetz
KAN	Kriminalaktennachweis
KBV	Kassenärztliche Bundesvereinigung
Kfz	Kraftfahrzeug
KIS	Krankenhausinformationssystem
KONSENS	Koordinierte neue Software-Entwicklung der Steuerverwaltung
KVB	Kassenärztliche Vereinigung Bayerns
KWG	Gesetz über das Kreditwesen
kWh	Kilowattstunde
KWMBl	Kultus- und Wissenschaftsministerialblatt
LANR	Lebenslang zugeordnete Arztnummer
LDO	Lehrerdienstordnung
LfV	Landesamt für Verfassungsschutz
LWG	Landeswahlgesetz
LWO	Landeswahlordnung
m.E.	meines Erachtens
m.w.N.	mit weiteren Nachweisen
MDK	Medizinischer Dienst der Krankenkassen
MeldeG	Bayerisches Gesetz über das Meldewesen
Moodle	Modular object-oriented dynamic learning environment
NEPS	National Educational Panel Study - Nationales Bildungspanel
nPA	neuer (elektronischer) Personalausweis
Nr.	Nummer
o.b.	oben bezeichnet
o.g.	oben genannt
PAG	Bayerisches Polizeiaufgabengesetz
PC	Personalcomputer
PIN	Personell Identification Number
PSV	Polizeiliche Sachbearbeitung/ Vorgangsverwaltung-Verbrechensbekämpfung
Rdnr.	Randnummer
RFID	Radio Frequency Identification
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
RMS	Risikomanagementsysteme
S.	Seite
SGB	Sozialgesetzbuch
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrszulassungsordnung
TIZIAN	Gemeinsame EDV für den Gesundheitlichen Verbraucherschutz
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
u.ä.	und ähnliches
u.a	unter anderem

u.U.	unter Umständen
UAG	Unterarbeitsgruppe
USB	Universal Serial Bus
v.a.	vor allem
vgl.	vergleiche
VoIP	Voice over IP
VPN	Virtuelles Privates Netz
WA	Wahlanweisung
z.B.	zum Beispiel
ZAUBER	Zentrale Datenbank zur Speicherung und Auswertung von Umsatzsteuer-Betrugsfällen und Entwicklung von Risikoprofilen
ZIL	Zentrale IuK-Leitstelle

Stichwortverzeichnis

Abgabenordnung
  Auskunftsanspruch ... 151
Ablehnung von Auskünften ... 145
Active Directory ... 28
Adressierung
  Steuerbescheide ... 156
Akkreditierungsverfahren ... 85
  Zuverlässigkeitsüberprüfung ... 5
Akteneinsicht durch Angehörige in Patientenakte eines Verstorbenen ... 124
Alterseinkünftegesetz ... 152
Amtliche Schuldaten ... 161
Amtsträger ... 111
Antragsformular ... 146, 147
Arbeitnehmer
  Drogentests bei der Einstellung ... 187
Arbeitsgemeinschaft ... 141
Archivierung
  Beleg- ... 60
  E-Mail- ... 60
ARGE ... 141, 142, 143, 144, 145, 146, 147
Ärztliche Schweigepflicht ... 126
Ärztlicher Bereitschaftsdienst ... 137
Ärztlicher Hausbesuch ... 137
Arztsuche ... 135
Auftragsdatenverarbeitung
  Cloud Computing ... 31
  Orientierungshilfe ... 24
  Personalverwaltung ... 49
Aufzeichnung von Telefonanrufen ... 138
Auskunft ... 75
  Auskunftsablehnung ... 75
  Auskunftsersuchen ... 75
  Datei Gewalttäter Sport ... 75
Auskunftsanspruch
  Abgabenordnung ... 151
  Steuerverwaltung ... 151
Automatisierte Kontenabfrage ... 155
Automatisiertes Kontenabrufverfahren ... 155
Bayerisches Beamtenversorgungsgesetz ... 178
BayernMoodle ... 165
BayRMS ... 183
BayZeit ... 183
Beanstandung ... 36
Bebauungsplan ... 108
Behandlungsunterlagen
  Weitergabe an Rechtsanwälte ... 125
Behördennetz
  BayKOM 2010 ... 30
  Verschlüsselung ... 30
Behördlicher Datenschutzbeauftragter ... 91
  Bezeichnung im Geschäftsverteilungsplan ... 91

Beiblatt 146, 147
Bekanntgabe
Steuerbescheide 156
Benutzerstatistiken 32
Bereitschaftsdienst 137
Beschäftigte
DNA-Reihentes 191
Drogentests bei der Einstellung 187
Beschäftigtenlaufwerke
Durchsicht 192
Betriebskrankenkasse 142
Bewerber
polizeiliche Daten 189
Bewertung der Lehre an Hochschulen 173
Bibliothek
Benutzerausweis 45
RFID 45
Bildungsverlaufsuntersuchungen 161
Blutentnahmen 95
Anordnung bei Gefahr im Verzug 95
Bluttest
Einstellung neuer Mitarbeiter 187
Briefdienstleistungen 39
Briefpostversand 39
BRN-Moodle 165
Broschüre
Krankenhaus 23
Bundessozialgericht 144
Bürgerentlastungsgesetz Krankenversicherung 153
CIO 27
Cloud Computing 31
Daten Verstorbener 124
Datengeheimnis 35
Datennutzung zu privaten Zwecken 146
Datenschutzbeauftragter
freiberuflich 40
Datenübermittlung
an Arbeitgeber 139
an Betriebskrankenkasse 142
an Dritte 148
an Taxiunternehmen 137
durch Schulen zu Werbezwecken 167
gaststättenrechtliche Gestattungen 51
Dienstunfallunterlagen 178
Dienstvereinbarung
Durchsicht Beschäftigtenlaufwerke 192
Diskretionsräume
Finanzamt 157
DNA-Maßnahme 84
DNA-Reihentest bei Mitarbeitern 191
DOMEA 88
Landesamt für Verfassungsschutz 88
Protokolldatei 88

Drogentest
Einstellung neuer Mitarbeiter ... 187
EDV-Administration
Gemeinde gemeinsam mit Kurbetrieb ... 52
eFA ... 47
eGovernment
Personalbereich ... 183
Eingabeführer ... 109
Einheitliche Ansprechpartner ... 196
Einsichtsrecht von Angehörigen in Patientenakte eines Verstorbenen ... 124
Einstellung
Drogentests ... 187
Einwilligung ... 135, 146
E-Learning
Schule ... 165
Elektronische Dokumentation und Abrechnung von Notarzteinsätzen ... 133
Elektronische Fallakte ... 47
ELStAM ... 149
ELSTER
Elektronische Lohnsteuerabzugsmerkmale ... 149
Elektronische Lohnsteuerkarte ... 149
ELSTERLohn II ... 149
ELSTEROnline ... 149
Neugierabfragen ... 149
Registrierung von Steuerberatern ... 149
Elternbrief
Schulhomepage ... 163
E-Mail
Archivierung ... 60
Zentralisierung ... 28
emDoc ... 48, 133
Erhebungsstellen
Zensus ... 194
Erkennungsdienstliche Behandlung ... 82
Erkennungsdienst Digital ... 82
Täterbildverfahren ... 82
Erlebnistherme ... 103
Anfertigen von Fotografien ... 103
Evaluation der Lehre an Hochschulen ... 173
Fahrerlaubnisentziehung ... 201
Fahrtenbuchauflage ... 200
Fahrzeugregister ... 201
Verfolgung von Rechtsansprüchen ... 201
Fernsehen
Patientendaten ... 126
Fernsehteam filmt Notarzteinsatz ... 126
Finanzamt
ACUSTIG ... 157
Diskretionsräume ... 157
Krankenversicherungsbeiträge ... 153
Neugierabfragen ... 157
Servicezentrum ... 157
ZAUBER ... 157

Fingerabdruckscanner ... 49
Freigabe
Tags ... 50
Fremdpersonal
polizeiliche Daten ... 189
Fundsachen ... 60
Gaststättenrechtliche Gestattung
Datenübermittlung an Polizei ... 51
Gemeinde
gemeinsame EDV-Administration ... 52
Gemeinderatssitzung ... 114
Gesetzgebung ... 90
Dolmetschergesetz ... 90
Maßregelvollzugsgesetz ... 90
Gesundheitsamt ... 121
Gesundheitsdaten
Polizeibeamte ... 190
Übermittlung durch Schule ... 169
Gewerberegister ... 118
Veröffentlichung im Internet ... 118
Google Analytics ... 32
Grundrecht
IT-Grundrecht ... 25
Hausbesuch ... 129
bei Eltern Neugeborener ... 129
Hochschule
Evaluation der Lehre ... 173
Notenkonto ... 175
Hypnose
Einsatz bei der Verfolgung von Straftaten ... 94
Impf-Recall ... 136
Inaktive Kamera ... 122
Informantenschutz ... 112
Integrationsverfahren ... 76
Dokumentation ... 76
Freitextrecherche ... 76
IGVP ... 76
PSV ... 76
Vorgangsverwaltung ... 76
Internet
Google Analytics ... 32
Nutzungsstatistik ... 32
Patientendaten ... 126
Schule ... 163
Internetcafe ... 51
Internetdienst
Arztsuche ... 135
Internetportal ... 147
IT-Grundrecht ... 25
IuK-Organisation
CIO ... 27
Jobcenter ... 141
-Reform ... 141

Jugendamt 129
ärztlicher Untersuchungsbogen für Tagesmutter 130
Hausbesuch 129
Tagesmutter 130
Justizvollzug 98, 99
Abgeordnetenpost 98
Anwesenheit von Vollzugsbeamten bei der ärztlichen Untersuchung von Gefangenen . 99
ärztliche Schweigepflicht 99
unzulässige Öffnung von Briefen an Gefangene 98
Kameraattrappe 122
Kassenbon 143
Kfz-Zulassung
online 56
KIS 62
Klinikregister 120
Kompetenzzentrum Labor 131
KONSENS 149
ELSTER 149
Risikomanagementsysteme RMS 149
Kontenabfrage 155
Kontenabruf 155
Kontoauszug 144
Krankenakte
Weitergabe an Rechtsanwälte 125
Krankenblatt 190
Krankenhaus 23
Broschüre 23
Datenverlust 40
Videoüberwachung 122
Krankenhausinformationssysteme 62
Krankenkassen
Kundenwerbung an Schulen 167
Krankenversicherungsbeiträge
Finanzamt 153
Krebsregister 120
Krebsregistrierung 120
Kriminalaktennachweis 76
Kundenwerbung an Schulen 167
KVB 131, 133, 135, 136, 137
KV-Ident 42
Laborabrechnung 131
LANR 135
Laufwerke
Durchsicht 192
Lebensmittelgutschein 143
Luftbilder 105
Solarpotential 105
Mammographie-Screening 44
Masern-Impferinnerungsservice 136
MDK 138
Melderegisterauskunft in besonderen Fällen 117
Melderegisterdaten 117
Nachwuchswerbung durch die Freiwillige Feuerwehr 117

Mitarbeiter
DNA-Reihentest ... 191
Drogentests bei der Einstellung ... 187
Mitteilungsblatt ... 111
Benachrichtigung von Bürgern ... 111
Nationales Bildungspanel ... 170
NEPS ... 170
Neue Grippe und Datenschutz ... 169
Neues Dienstrecht ... 178
Neugierabfragen
Finanzamt ... 157
Neuorganisation ... 141
Notenkonto
Universität ... 175
Optionskommune ... 141
Ordnungswidrigkeitenrecht ... 99
videogestützte Geschwindigkeits- und Abstandsmessung ... 99
Ordnungswidrigkeitenverfahren ... 100
Lichtbildabgleich im Bußgeldverfahren ... 100
Pandemie und Datenschutz ... 169
Passwortgeschützte Lernplattformen ... 165
Patientenakte Verstorbener
Einsicht durch Angehörige ... 124
Patientendaten
im Fernsehen ... 126
Weitergabe an Rechtsanwälte ... 125
Personal
DNA-Reihentest ... 191
Personal- und Stellenmanagementsystem
VIVA ... 183
Personalakt
Polizei ... 190
Personalausweis
elektronischer ... 53
Personalrat
Durchsicht Beschäftigtenlaufwerke ... 192
Personalverwaltung
Auftragsdatenverarbeitung ... 49
Pflegekasse ... 140
Antrag auf Betreuungsleistungen ... 140
Pflegeservice Bayern ... 138
Planfeststellungsverfahren ... 198
Polizei
ärztlicher Sachbearbeiter ... 190
gaststättenrechtliche Gestattung ... 51
Personalakt ... 190
Polizeiärztlicher Dienst ... 190
Polizeiaufgabengesetz ... 65, 67, 79
Aufbewahrungsfrist ... 67
Benachrichtigungspflicht ... 67
Berufsgeheimnisträger ... 65
Bild- und Tonaufnahmen ... 67
Bundesverfassungsgericht ... 79

Großer Lauschangriff ... 65
heimliche Wohnungsbetretung ... 67
heimliche Wohnungsdurchsuchung ... 67
Online-Durchsuchung ... 67, 79
polizeiliche Beobachtung ... 67
Quellen-Telekommunikationsüberwachung ... 79
Telekommunikationsüberwachung ... 67, 79
Wohnraumüberwachung ... 65, 67
Polizeibeamte
Gesundheitsdaten ... 190
Polizeiliche Daten
Überprüfung von Bewerbern, Praktikanten und Fremdpersonal ... 189
Polizeiliche Pressearbeit ... 77
Bundesverfassungsgericht ... 77
Postdienstleister ... 39
Praktikanten
polizeiliche Daten ... 189
Presse ... 105
Information über kommunale Angelegenheiten ... 105
Reality-TV ... 92
Mitwirkung von Justizbehörden an Reality-Reportagen ... 92
Rechenzentrum
Auftragsdatenverarbeitung ... 28
Reisegewerbe ... 199
Reisekostenmanagementsystem
BayRMS ... 183
Reisezeitmessung ... 46
Rentenbesteuerung ... 152
Rentenbezugsmitteilung ... 152
Rentenversicherungsträger ... 139
RFID
Bibliothek ... 45
Risikomanagementsysteme
Steuerverwaltung ... 149
Schule
BayernMoodle ... 165
BRN-Moodle ... 165
Einwilligungsformular Schulhomepage ... 163
E-Learning ... 165
gelbes Kinderuntersuchungsheft ... 121
Homepage ... 163
Impfausweis ... 121
Impfberatung ... 121
Internet ... 163
Jahresbericht ... 163
Meldungen von Erkrankungen an der Neuen Grippe ... 169
passwortgeschützte Lernplattformen ... 165
Weitergabe von Schülerdaten zu Werbezwecken ... 167
Schuleingangsuntersuchung ... 121
Schülerdaten
Weitergabe zu Werbezwecken ... 167
Schüler-ID ... 161
Schulgesundheitspflege ... 121

Schulhomepage ... 163
Elternbrief ... 163
geschützter Bereich ... 163
Sprechstundenliste ... 163
Vertretungsplan ... 163
Schulstatistik ... 161
Schwärzung ... 144
Schweine-Grippe und Datenschutz ... 169
Servicezentrum
Finanzamt ... 157
Sichtfensterumschläge ... 92
unbeabsichtigte Datenübermittlung ... 92
Smart Meter ... 58
Sozialamt ... 147, 148
Sozialdaten ... 148
Sozialgeheimnis ... 148
Sparkassen
Kundenwerbung an Schulen ... 167
Speicherung ... 74
Versammlungsanmelder ... 74
Versammlungsleiter ... 74
Speicherung von Kindern und Jugendlichen ... 88
Landesamt für Verfassungsschutz ... 88
Verfassungsschutz ... 88
Sprechstundenliste
Schulhomepage ... 163
Staatsanwaltschaft ... 97
Kontenabfrage ... 97
Statistik
Amtliche Schuldaten ... 161
Statistikstellen
Zensus ... 194
Stellungnahme ... 141
Steuerbescheide
Adressierung ... 156
Bekanntgabe ... 156
Steueridentifikationsnummer
Krankenversicherungsbeiträge ... 153
Rentner ... 152
Steuerverwaltung
Auskunftsanspruch ... 151
Strafprozessordnung ... 94
Einsatz von Hypnose bei der Verfolgung von Straftaten ... 94
Stromzähler
intelligent ... 58
Tagesbetreuungsperson ... 130
Tagesmutter ... 130
TIZIAN ... 43, 128
Türöffnungssystem
elektronisch ... 50
Universität
Notenkonto ... 175
Unterhaltspflichtige Angehörige ... 147
Unterstützungspflicht ... 141

Urintest
Einstellung neuer Mitarbeiter ... 187
Verbundverfahren ... 128
Verfassungsschutz ... 86, 89
Auskunftsersuchen ... 89
Auskunftsverpflichtung ... 89
Landesamt für Verfassungsschutz ... 86, 89
Verfassungsschutzgesetz ... 86
automatische Aufzeichnung ... 86
Benachrichtigungspflicht ... 86
Berufsgeheimnisträger ... 86
Großer Lauschangriff ... 86
heimliche Wohnungsbetretung ... 86
heimliche Wohnungsdurchsuchung ... 86
Online-Durchsuchung ... 86
verdeckter Einsatz technischer Mittel. ... 86
Wohnraumüberwachung ... 86
Veröffentlichung von Vornamen ... 147
Verpflichtungsgesetz ... 35
Versammlungsgesetz ... 67, 68, 69
Aufbewahrungspflicht ... 69
Bundesverfassungsgericht ... 68
Dokumentationspflicht ... 69
Erhebung personenbezogener Daten ... 69
heimliche Aufnahmen ... 69
Übersichtsaufnahmen ... 68, 69
Übersichtsaufzeichnungen ... 68, 69
Versammlungsteilnehmer ... 74
Übersichtsaufzeichnung ... 74
Videoüberwachung ... 74
Verschlüsselung
Behördennetz ... 30
Vertretungsplan
Schulhomepage ... 163
Verzeichnisdienste ... 28
Videoaufzeichnung ... 81
erkennungsdienstliche Behandlung ... 81
Videoüberwachung ... 81
Videoüberwachung ... 80, 101, 102
durch Kommunen ... 101
eines Wahllokals ... 102
in Aufzügen im Krankenhaus ... 122
Kameraattrappe ... 122
von Justizgebäuden ... 90
VIVA ... 183
Volkszählung 2011 ... 194
Vorratsdatenspeicherung ... 71
Benachrichtigungspflicht ... 71
Bundesverfassungsgericht ... 71
Richtervorbehalt ... 71
Telekommunikationsverkehrsdaten ... 71
Wahlkreisvorschläge ... 115
Kopien von Unterstützungsunterschriften ... 115

Webserver
Google Analytics 32
Werbung an Schulen 167
Zeitmanagementsystem
BayZeit 183
Zensus
kommunale Erhebungsstellen 194
kommunale Statistikstellen 194
Zensusgesetz 194
Zentralisierung
Active Directory 28
E-Mail 28
Zugangskontrolle
Fingerabdruckscanner 49
Zusatzausführungen 145

Der Bayerische
Landesbeauftragte
für den
Datenschutz

Wagmüllerstraße 18
80538 München
Postfach 22 12 19
80502 München
Telefon 089 21 26 72-0
Telefax 089 21 26 72-50

poststelle@datenschutz-bayern.de
www.datenschutz-bayern.de