IX. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz

Landesbeauftragter für den Datenschutz - Postfach 1947 - 39009 Magdeburg

Telefon	(0391) 8 18 03 - 0
Bürgertelefon	(0800) 9 15 31 90
Fax	(0391) 8 18 03 33
Internet	http://www.datenschutz. sachsen-anhalt.de
E-Mail	poststelle@lfd.sachsen-anhalt.de

Dienstgebäude: Berliner Chaussee 9 - 39114 Magdeburg
ab 26. August 2009: Leiterstraße 9 - 39104 Magdeburg

Vorwort

25 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts hat der Datenschutz wieder Konjunktur: Die rechtlich wie politisch brisanten Themen der Vorratsdatenspeicherung sowie der heimlichen Online-Durchsuchung - diese erfuhr ihre Brisanz auch aufgrund der technischen Details - brachten den Datenschutz aus seiner Defensivrolle. Dazu tragen auch Datenskandale in der Wirtschaft zu Lasten von Verbrauchern, Kunden und Arbeitnehmern bei. Hinsichtlich einer durchgreifenden Datenschutzrenaissance besteht aber Anlass zu Skepsis. Die Überwachungsgesellschaft, bewirkt durch Staat und Wirtschaft, angestoßen auch durch das ambivalente, oft sorglos-naive, fahrlässige Verhalten der Privaten selbst, schreitet weiter voran. Dies, und wie dieser Entwicklung entgegengewirkt werden kann, analysiert dieser Tätigkeitsbericht.

Um Vertrauen in die Datenverarbeitungspraxis von Wirtschaft und Staat wiederherzustellen, bedarf es vertrauensbildender Maßnahmen insbesondere auch des Staates. Das ist eine Parallele zur Finanzkrise. Zur Vertrauensbildung gehört mindestens folgendes: Der Staat selbst trägt vorbildlich nur dann zum Grundrechtsschutz bei, wenn er sich bei seiner eigenen Datenverarbeitung zurücknimmt. Der Staat nimmt die Grundrechte ernst und reduziert seine Eingriffe und schützt zudem vor übermäßiger Datenverarbeitung der Wirtschaft. Dazu verpflichtet ihn auch das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Der IX. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2007 bis zum 31. März 2009. Bei einzelnen Beiträgen konnten noch darüber hinaus reichende aktuelle Sachstände einbezogen (Redaktionsschluss: 29. Mai 2009), Entwicklungen in der Gesetzgebung bis Anfang Juli berücksichtigt werden.

Mein besonderer Dank gilt wieder meinen Mitarbeiterinnen und Mitarbeitern in der Geschäftsstelle.

Magdeburg, den 15. Juli 2009

Dr. Harald von Bose
Landesbeauftragter für den Datenschutz Sachsen-Anhalt

Inhaltsverzeichnis

Vorwort

1. Entwicklung und Situation des Datenschutzes 1
1.1. Freiheit und Sicherheit 4
1.2. Nicht-öffentlicher Bereich 6
1.3. eGovernment und Technik 7
1.4. Zusammenfassung und Ausblick 10

2. Der Landesbeauftragte 12
2.1. Tätigkeit im Berichtszeitraum 12
2.2. Schwerpunkte – Empfehlungen 15
2.3. Zusammenarbeit mit anderen Institutionen 16
2.4. Informationszugangsgesetz Sachsen-Anhalt 17
2.5. Internet-Homepage des Landesbeauftragten und Internetkontakt 18

3. Allgemeines Datenschutzrecht 20
3.1. Novellierung des Datenschutzrechts 20
3.2. Effektive und unabhängige Datenschutzaufsicht 23
3.3. Europäischer Datenschutztag 24

4. Entwicklung der automatisierten Datenverarbeitung – eGovernment 25
4.1. Die neue IT-Strategie des Landes Sachsen-Anhalt 25
4.2. Aufbau eines neuen zentralen IT-Dienstleisters - Landesrechenzentrum 28
4.3. Grundkonzept IT-Architektur der Landesverwaltung 33
4.4. Landesleitlinie IT-Sicherheit 36
4.5. eGovernment-Maßnahmenplan 2008-2009 38
4.6. Masterplan Landesportal Sachsen-Anhalt 2007-2011 39
4.7. Umsetzung der EU-Dienstleistungsrichtlinie in Sachsen-Anhalt 40
4.8. Umsetzung des Binnenmarktinformationssystems IMI 42
4.9. Geodateninfrastrukturgesetzgebung in Sachsen-Anhalt 43
4.10. Mehr Befugnisse für das BSI 46
4.11. Bürgerportale und De-Mail 47

5. Archivwesen 48
5.1. Akten ehemaliger politischer Häftlinge in einer Gedenkstätte 48
5.2. Ausstellung in der Gedenkstätte „Roter Ochse“ 49

6. Ausländerangelegenheiten 51
6.1. Gesetzentwurf zur Errichtung einer Visa-Einlader- und Warndatei 51
6.2. Unzulässig gespeicherte Daten im Ausländerzentralregister 52

7. Ausweis- und Melderecht, Personenstandsrecht 52
7.1. Elektronischer Reisepass (ePass) 52
7.2. Elektronischer Personalausweis (ePA) 54
7.3. Zentrales Bundesmelderegister 56
7.4. Melderegisterauskünfte nach Landesrecht 57

7.5. Sorgloser Umgang mit Meldedaten bei Online-Abrufen 58
7.6. Ausführung des Personenstandsgesetzes 58

8. Europäischer und Internationaler Datenschutz 59
8.1. Regelungen zum Datenschutz beim Austausch von Informationen zwischen Strafverfolgungsbehörden der EU sowie zwischen Deutschland und den USA 59
8.2. Terrorlisten der Vereinten Nationen – Rechtsschutz jetzt möglich? 60
8.3. Übermittlung von Fluggastdaten zwischen der EU und den USA 60
8.4. Keine Vorratsdatenspeicherung von Flugpassagierdaten 61
8.5. Überführung des Vertrages von Prüm in EU-Recht 62
8.6. Europäische Datenschutzkonferenzen 62
8.7. Internationale Konferenzen der Beauftragten für den Datenschutz und den Schutz der Privatsphäre 63

9. Finanzwesen 64
9.1. Auskunftsrecht für Betroffene im Steuerverfahren 64
9.2. Kontenabrufverfahren 65
9.3. Einführung der Steuer-Identifikationsnummer zum 1. Juli 2007 66
9.4. Ablösung der Lohnsteuerkarten 68
9.5. Protokollauswertung bei LUNA 68
9.6. Koordinierte neue Softwareentwicklung der Steuerverwaltung 69
9.7. Unsichere Authentifizierung bei der ElsterOnline-Anmeldung 70
9.8. Einführung der Kraftfahrzeugsteuer-Rückständeprüfung in Sachsen-Anhalt 72

10. Forschung 75
10.1. Allgemeines 75
10.2. Forschung mit anonymen Daten 75
10.3. Forschung mit Sozialdaten 76

11. Gefahrenabwehr 77
11.1. Gesetz zur Vorsorge gegen die von Hunden ausgehenden Gefahren 77
11.2. Entwurf eines Versammlungsgesetzes 80
11.3. Änderung des Spielbankgesetzes 82
11.4. Abrufverfahren bei der Waffenbehörde 86

12. Gesundheitswesen 87
12.1. Elektronische Gesundheitskarte 87
12.2. Elektronischer Heilberufsausweis 87
12.3. Novellierung des Maßregelvollzugsgesetzes 88
12.4. Mammographie-Screening 88
12.5. Gendiagnostikgesetz 90
12.6. Einschulungsuntersuchungen/schulärztliche Untersuchungen 90
12.7. Amtsärztliche Stellungnahme zu Eingliederungshilfeleistungen 92
12.8. Herausgabe von Rettungsdienstprotokollen zu Abrechnungszwecken 93
12.9. Archivierung von Patientenunterlagen 94
12.10. Datenübermittlung per Telefax 95

13. Gewerbe und Wirtschaft 95
13.1. Neufassung des Ingenieurgesetzes Sachsen-Anhalt 95
13.2. Änderung der Gewerbeordnung 96

14. Hinweise zum technischen und organisatorischen Datenschutz 97
14.1. Sicherung von Sozialdaten auf Laptops 97
14.2. Fernwartung einer Firewall 98
14.3. Überarbeitung der Sicherheitsleitlinie der Verwaltungs-PKI des BSI 99
14.4. Sichere E-Mails mittels X.509-Zertifikat der PKI Sachsen-Anhalt 99
14.5. Die elektronische Signatur in der Verwaltung 100
14.6. Online Services Computer Interface 2.0 (OSCI 2.0) 102
14.7. Sicherheit des Windows Encrypted File Systems (EFS) 103
14.8. Datenschutzgerechte Webserver-Logs 104
14.9. Webserver-Logs bei externen Dienstleistern 105
14.10. BlackBerry - Einsatz sicher gestaltbar 106
14.11. Offene Verteilerlisten in Rundschreiben per E-Mail 108
14.12. Hinweise zur Absicherung von Wireless-LAN 108
14.13. Kontrolle von Wireless-LAN bei öffentlichen Stellen 109
14.14. Telearbeit 110

15. Hochschulen 111
15.1. Studierendendaten im Internet 111
15.2. Nachwirkungen des Hochschulmedizingesetzes 114

16. Kommunalverwaltung 115
16.1. Grundstückseigentümerangaben unklarer Herkunft 115
16.2. Übermittlung der Namen der Gemeinderäte an private Dritte 116
16.3. Bezüge einzelner Geschäftsführer im Beteiligungsbericht 116

17. Personalwesen 118
17.1. Gesetz zur Neuordnung des Landesbeamtenrechts 118
17.2. Personalmanagementsystem 119
17.3. Fortbildungsmanagement 120
17.4. Durchsuchung der Zentralablage 122
17.5. Daten bei der Personalvertretung 125
17.6. Personaldaten im Internet 126
17.7. Einstellungstests 126
17.8. Polizeiliche Auskunftssysteme und Zentralregisterauskunft für Bewerbungsverfahren 127
17.9. Personalservicecenter 129
17.10. Eingliederungsmanagement und Personalvertretung 130

18. Polizei 131
18.1. Änderung des SOG LSA 131
18.2. Datenschutz bei der Polizei 132
18.3. Änderung des Bundeskriminalamtgesetzes 133
18.4. Bundespolizeigesetz 136
18.5. Videoüberwachung öffentlicher Plätze 136
18.6. Videoüberwachung am Hasselbachplatz in Magdeburg 137
18.7. Kopien von Videoaufzeichnungen für künstlerische Zwecke 139
18.8. Beschwerdestelle Polizei 140

18.9. Datenübermittlung an nichtöffentliche Stellen 141
18.10. Schutz vor haftentlassenen Sexualstraftätern 142
18.11. Archivierungssysteme der Polizei 142
18.12. Automatisierte Kfz-Kennzeichenerfassung durch die Polizei 143
18.13. Protokollierung von Datenabfragen beim Technischen Polizeiamt 145
18.14. Ermittlungsgruppe Schulweg 146
18.15. Zuverlässigkeitsüberprüfungen bei der Deutschen Bundesbank 147
18.16. Speicherung im polizeilichen Informationssystem INPOL 148

19. Rechtspflege 148
19.1. Allgemeines 148
19.2. Telekommunikationsüberwachung überarbeitet - Vorratsdaten-speicherung eingeführt 149
19.3. Verfolgung der Absicht der Vorbereitung von Terrordelikten 151
19.4. Videotechnik in der Justiz 152
19.5. Namen von Verfahrensbeteiligten auf Monitoren im Eingangs-bereich eines Justizzentrums 155
19.6. Schülergremien 156
19.7. Zustellungen durch Gerichtsvollzieher 157
19.8. Justizaktenaufbewahrung 157
19.9. Abfrage von Kreditkartendaten in einem Ermittlungsverfahren 158
19.10. Zwangsversteigerung und Internet 159

20. Schulen 160
20.1. Prüfung in Schulen 160
20.2. Umstellung der Schulstatistik auf Individualdaten (Kerndatensatz) 161
20.3. Schulverwaltungssoftware 162
20.4. Medienkompetenz und Datenschutzbewusstsein von Schülern 163
20.5. Soziale Netzwerke 165
20.6. Bewertungsportale 165
20.7. Gesamtbeurteilungsbogen 166
20.8. Hospitation 166
20.9. Ersatzschulverordnung 167

21. Sozialwesen 169
21.1. Arbeitslosengeld II 169
21.2. Kontroll- und Beratungsbesuche in Arbeitsgemeinschaften (ARGEn) 170
21.3. Anforderung von Kontoauszügen 170
21.4. Erhebung von Sozialdaten des Ehepartners 172
21.5. Löschung der Telefonnummer 173
21.6. Grundsicherung für Selbständige 174
21.7. Angaben zum Leistungsbezug im Adressfeld von Briefsendungen 175
21.8. Netzwerk bei Projekt „Zukunftswerkstatt 50plus“ 176
21.9. Elektronischer Entgeltnachweis 177
21.10. Steuerungsprogramme der gesetzlichen Krankenversicherung 177
21.11. Beeinflussung von Patienten 178
21.12. Landesrechnungshof und Landesprüfungsamt 179
21.13. Private Abrechnungsstellen 180
21.14. Feuerwehr-Unfallkasse-Mitte 181
21.15. Kinder- und Jugendhilfe 181
21.16. Kinderschutzgesetz des Landes 182

21.17. Projekt „Frühwarnsystem Pädiatrie“ 184
21.18. Klientenverwaltungssystem für Integrationsfachdienste 185
21.19. Bundeselterngeld- und Elternzeitgesetz 185
21.20. Antragsformular für die Gewährung der besonderen Zuwendung für Haftopfer 187

22. Statistik 188
22.1. EU-weiter Zensus 2011 188
22.2. Trennung von Erhebungs- und Hilfsmerkmalen 190

23. Strafvollzug 192
23.1. PPP-Projekt Justizvollzugsanstalt Burg 192
23.1.1. Vorgeschichte 192
23.1.2. Nichthoheitliche und hoheitliche Tätigkeit im hoheitlichen Strafvollzug? 192
23.1.3. Absicherung des Datenschutzes durch Vertragsgestaltung? 193
23.1.4. Datenverarbeitung im Ausland? 193
23.1.5. Die Beteiligung des Landesbeauftragten im Übrigen 194
23.1.6. Handflächenvenenerkennung und Berechtigungskonzeption 194
23.1.7. Personalaktenbearbeitung durch private Dritte? 196
23.2. Kontrolle in Justizvollzugsanstalt: Licht und Schatten 197
23.3. Jugendstrafvollzugsgesetz 199
23.4. Mobilfunkblocker im Justizvollzug 202
23.5. Nicht anonymisierte Speicherung von Entscheidungen nach Verkündung/Rechtskraft 203

24. Telekommunikations- und Medienrecht 203
24.1. Vorratsdatenspeicherung 203
24.2. Zehnter Rundfunkänderungsstaatsvertrag 206
24.3. Änderungen im Urheberrecht 207
24.4. Änderungen im Telemediengesetz 208
24.5. Sperrung von Internetseiten zur Bekämpfung von Kinderpornographie 209
24.6. Musterdienstanweisung zur Nutzung von E-Mail und Internet am Arbeitsplatz 210
24.7. SPAM-Filterung von E-Mails 212

25. Verfassungsschutz 213
25.1. Änderung des Verfassungsschutzgesetzes 213
25.2. Dokumentenmanagement beim Verfassungsschutz 216
25.3. GIAZ - Teil II 217

26. Verkehr 219
26.1. Online-Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt 219
26.2. Verkehrsüberwachung mittels Videoaufzeichnung 222
26.3. Datenschutz im Verkehrsordnungswidrigkeitenverfahren 223
26.4. Datenschutz im Kfz-Zulassungsrecht 224
26.5. Videoüberwachung in Straßenbahnen 225

Anlagenverzeichnis

Anlage 1
Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007 **Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln** 227

Anlage 2
Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 **Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert** 229

Anlage 3
Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 **Zentrale Steuerdatei droht zum Datenmoloch zu werden** 231

Anlage 4
Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 **Nein zur Online-Durchsuchung** 233

Anlage 5
Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007 **Zuverlässigkeitsüberprüfungen bei Großveranstaltungen** 235

Anlage 6
75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts** 236

Anlage 7
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“** 238

Anlage 8
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Vorgaben des Bundes-verfassungsgerichts bei der Online-Durchsuchung beachten** 239

Anlage 9
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Mehr Augenmaß bei der Novellierung des BKA-Gesetzes** 241

Anlage 10
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Keine Vorratsspeicherung von Flugpassagierdaten** 243

Anlage 11
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden** 245

Anlage 12
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern** 246

Anlage 13
Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen** 247

Anlage 14
Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin **Informationssystem „IMI“** 249

Anlage 15
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008 **Entschlossenes Handeln ist das Gebot der Stunde** 250

Anlage 16
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Adress- und Datenhandel nur mit Einwilligung der Betroffenen** 252

Anlage 17
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Mehr Transparenz durch Informationspflichten bei Datenschutzpannen** 253

Anlage 18
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren** 254

Anlage 19
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Datenschutzgerechter Zugang zu Geoinformationen** 256

Anlage 20
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Elektronische Steuererklärung sicher und datenschutzgerecht gestalten** 257

Anlage 21
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten** 258

Anlage 22
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen** 259

Anlage 23
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich** 261

Anlage 24
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten** 264

Anlage 25
Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn **Gegen Blankettbefugnisse für die Software-Industrie** 266

Anlage 26
Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. Februar 2009 **Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes!** 267

Anlage 27
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin **Defizite beim Datenschutz jetzt beseitigen!** 269

Anlage 28
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin **Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz** 270

Anlage 29
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin **Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten!** 272

Anlage 30
Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin **Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage** 273

Anlage 31
Entschließung der Konferenz der Datenschutzschutzbeauftragten des Bundes und der Länder vom 16. April 2009 **Datenschutz beim vorgesehenen Bürgerportal unzureichend** 274

Anlage 32
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 08./09. November 2007 in Hamburg
Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte 276

Anlage 33
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 08./09. November 2007 in Hamburg
Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring 277

Anlage 34
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden **Keine fortlaufenden Bonitätsauskünfte an den Versandhandel** 278

Anlage 35
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden **Internet-Portale zur Bewertung von Einzelpersonen** 279

Anlage 36
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden
Datenschutzkonforme Gestaltung sozialer Netzwerke 280

Anlage 37
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden
Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit 282

Anlage 38
Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden
Datenschutzrechtliche Bewertung von digitalen Straßenansichten insbesondere im Internet 283

Anlage 39
ERKLÄRUNG der Europäischen Datenschutzkonferenz über die Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung vom 11. Mai 2007 284

Anlage 40
Erklärung der Europäischen Datenschutzkonferenz von Zypern, angenommen am 11. Mai 2007 299

Anlage 41
Europäische Datenschutzkonferenz vom 17. –18. April in Rom **Erklärung** 303

Anlage 42
29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre - Montreal (Kanada), 26.-28. September 2007 -
Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden 305

Anlage 43
29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre - Montreal (Kanada), 26.-28. September 2007 -
Resolution über die Entwicklung internationaler Standards 309

Anlage 44
29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre - Montreal (Kanada), 26.-28. September 2007 -
Resolution über internationale Zusammenarbeit 311

Anlage 45
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007
Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Erarbeitung einer gemeinsamen Entschließung zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten 313

Anlage 46
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007
Entschließung zum Datenschutz in Sozialen Netzwerkdiensten 318

Anlage 47
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007
Entschließung zum Schutz der Privatsphäre von Kindern im Internet 323

Anlage 48
30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007
Entschließung zur Prüfung der Einrichtung eines Internationalen Tages oder einer Woche für den Schutz der Privatsphäre/Datenschutz 326

Anlage 49
Organigramm **329**

Abkürzungsverzeichnis

3DES	Triple DES (dreifach angewendetes DES)
A	
ABl. EU	Amtsblatt der Europäischen Union
AD	Active Directory
AES	Advanced Encryption Standard (ein Verschlüsselungsalgorithmus)
a. F.	alte Fassung
AnwBl.	Anwaltsblatt
AO	Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
ARGE	Arbeitsgemeinschaft
AZR	Ausländerzentralregister
B	
BCC	Blind Carbon Copy
BDSG	Bundesdatenschutzgesetz
BEEG	Bundeselterngeld- und Elternzeitgesetz
BES	BlackBerry Enterprise Server
BG LSA	Beamtengesetz des Landes Sachsen-Anhalt
BGBl.	Bundesgesetzblatt
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz)
BPolG	Bundespolizeigesetz
BR-Drs.	Bundesratsdrucksache
BSG	Bundessozialgericht
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungssammlung des Bundesverfassungsgerichts
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BZRG	Bundeszentralregistergesetz
C	
CC	Carbon Copy
CERT	Computer Emergency Response Team
D	
DES	Data Encryption Standard (ein Verschlüsselungs-Algorithmus)
DNS	Domain Name System
DOL	Deutschland Online Initiative
DRA	Data Recovery Agent (Datenwiederherstellungs-Bevollmächtigter)
DSG-LSA	Gesetz zum Schutz personenbezogener Daten der Bürger
DVBl	Deutsches Verwaltungsblatt

E

EA	Einheitlicher Ansprechpartner
EAG LSA	Gesetz über den einheitlichen Ansprechpartner in Sachsen-Anhalt
EFS	Encrypted File System (verschlüsseltes Dateisystem)
EG	Europäische Gemeinschaft
eGBR	Elektronisches Beruferegister der Gesundheitsberufe
EGVP	Elektronisches Gerichts- und Verwaltungspostfach
ELENA	Elektronischer Entgeltnachweis
ELSTER	Elektronische Steuererklärung
EMSA	Elektronisches Mahnverfahren Sachsen-Anhalt
EOSS	Evolutionär Orientierte Steuersoftware
ePA	Elektronischer Personalausweis
ESch-VO	Ersatzschulverordnung
EU	Europäische Union
EU-DLR	EU-Dienstleistungsrichtlinie
EuGH	Europäischer Gerichtshof

F

FISCUS	Föderales Integriertes Standardisiertes Computer-Unterstütztes Steuersystem
FEB	Fahrerlaubnisbehörden
FeV	Fahrerlaubnis-Verordnung
FRZ	Finanzrechenzentrum

G

GDG LSA	Gesundheitsdienstgesetz des Landes Sachsen-Anhalt
GDIG LSA	Geodateninfrastrukturgesetz für das Land Sachsen-Anhalt
GenDG	Gesetz über genetische Untersuchungen bei Menschen - Gendiagnostikgesetz
GeoZG	Gesetz über den Zugang zu digitalen Geodaten - Geodatenzugangsgesetz
GewO	Gewerbeordnung
GEZ	Gebühreneinzugszentrale
GG	Grundgesetz für die Bundesrepublik Deutschland
GIAZ	Gemeinsames Informations- und Auswertungszentrum islamistischer Terrorismus
GO LSA	Gemeindeordnung Sachsen-Anhalt

H

HAMISSA	Haushalts-Aufstellung, -Management- und Informations-System Sachsen-Anhalt
HMG	Hochschulmedizingesetz
HSG LSA	Hochschulgesetz des Landes Sachsen-Anhalt
HGB	
Hundegesetz	Gesetz zur Vorsorge gegen die von Hunden ausgehenden Gefahren

I

IAM	Identity and Access Management
ICAO	International Civil Aviation Organization (Internationale Zivilluftfahrt-Organisation)

IMI	Internal Market Information System (Binnenmarktinformationssystem)
INPOL	polizeiliches Informationssystem
INSPIRE	Infrastructure for Spatial Information in the European Community
INVEKOS	Integriertes Verwaltungs- und Kontrollsystem (zur Durchsetzung einer einheitlichen Agrarpolitik in der EU)
IP-Adresse	Internetprotokoll-Adresse
IT	Informationstechnik
IT-KA	Koordinierungsausschuss Informationstechnik
ITN-LSA	Informationstechnisches Netz des Landes Sachsen-Anhalt
IuK	Informations- und Kommunikationstechnik
IZG LSA	Informationszugangsgesetz Sachsen-Anhalt

J

JSchrG LSA	Gesetz zur Aufbewahrung von Schriftgut der Justiz im Land Sachsen-Anhalt
JStVollzG LSA	Jugendstrafvollzugsgesetz
JZ	Juristenzeitung

K

KBA	Kraftfahrtbundesamt
KMK	Kultusministerkonferenz
KomStat	Kommission für Statistik der Kultusministerkonferenz
KONSENS	KOrdinierte Neue Software ENtwicklung der Steuerverwaltung
KraftStG	Kraftfahrzeugsteuergesetz
KV	Kassenärztliche Vereinigung

L

LAN	Local Area Network
LHO	Landeshaushaltsordnung
LIS	Landesleitstelle IT-Strategie (in der Staatskanzlei)
LISA	Landesinstitut für Schulqualität und Lehrerbildung
LIT	Leitstelle für Informationstechnik (ehemals Ministerium des Innern)
LIZ	Landesinformations-Zentrum
LKA	Landeskriminalamt
LPSA	Landesportal Sachsen-Anhalt
LRZ	Landesrechenzentrum
LT-Drs.	Landtagsdrucksache
LUNA	Länderumfassende Namensabfrage
LVermGeo	Landesamt für Vermessung und Geoinformation

M

MAC	Media Access Control
MMR	Multimedia und Recht
MZuKraftStG	Gesetz über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer Sachsen-Anhalt

N

n. F.	neue Fassung
NJW	Neue Juristische Wochenschrift
NTLM	NT LAN Manager (Authentifizierungsprotokoll in Verbindung mit SMB)

NVwZ	Neue Zeitschrift für Verwaltungsrecht
NZS	Neue Zeitschrift für Sozialrecht

O

OFD	Oberfinanzdirektion Magdeburg
OSCI	Online Services Computer Interface

P

PC	Personalcomputer
PD Nord	Polizeidirektion Sachsen-Anhalt Nord
PD Süd	Polizeidirektion Sachsen-Anhalt Süd
PDA	Personal Digital Assistant (persönlicher digitaler Assistent)
PersAuswG	Gesetz über Personalausweise
PGP	Pretty Good Privacy (Name einer Verschlüsselungssoftware)
PIN	persönliche Identifikationsnummer
PKD	Public Key Directory (Verzeichnisdienst für öffentliche Schlüssel)
PKI LSA	Public Key Infrastruktur Land Sachsen-Anhalt (Infrastruktur für öffentliche Schlüssel)
PMS	Personalmanagementsystem
PNR	Passenger Name Record
PPP	Public-Private Partnership
PSC	Personalservicecenter
PStG-AG LSA	Gesetz zur Ausführung des Personenstandsgesetzes in Sachsen-Anhalt
PStVO LSA	Verordnung über das Personenstandswesen des Landes Sachsen-Anhalt

R

RADIUS	Remote Authentication Dial-In User Service (Authentifizierungsdienst für sich einwählende Benutzer)
RDV	Recht der Datenverarbeitung
RGebStV	Rundfunkgebührenstaatsvertrag
RIM	Research In Motion (Hersteller von BlackBerry)

S

SALSA	Secure Access Land Sachsen-Anhalt
SAM	Security Account Manager (Sicherheits- und Benutzer-Verwaltung)
SchulG LSA	Schulgesetz des Landes Sachsen-Anhalt
Schüler-ID	Schüler-Identifikationsnummer
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SMB	Server Message Block (Kommunikationsprotokoll u. a. für Datei- und Druckdienste)
SMS	Short Message Service)
SOAP	Simple Object Access Protocol
SOG LSA	Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt
SPAM	SPiced hAM (unerwünschte Werbe-E-Mails)
SpielO-VO	Verordnung über die Spielordnung in öffentlichen Spielbanken

SSID	Service Set Identifier (Netzwerkname)
Steuer-ID	Steuer-Identifikationsnummer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StRehaG	Strafrechtliches Rehabilitierungsgesetz
SÜG	Sicherheitsüberprüfungs- und Geheimschutzgesetz
StVG	Straßenverkehrsgesetz

T

TESTA	Trans-European Services for Telematics between Administrations (Internes Netzwerk von europäischen Verwaltungen)
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
TMG	Telemediengesetz
TPA	Technisches Polizeiamt

U

UHD	User Help Desk (zentrale Nutzerbetreuung)
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USB	Universal Serial Bus

V

VerfSchG-LSA	Gesetz über den Verfassungsschutz im Land Sachsen-Anhalt
VersG	Versammlungsgesetz des Bundes
VKS	Verkehrs-Kontroll-System
VPN	Virtual Private Network (virtuelles privates Netz)
VS - NfD	Verschlusssache - Nur für den Dienstgebrauch

W

WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network (drahtloses Netzwerk, Funknetz)
WPA	Wi-Fi Protected Access

X

X.509	Internationaler Standard für Zertifikate
XML	Extensible Markup Language

Z

ZVG	Gesetz über die Zwangsversteigerung und die Zwangsverwaltung
ZFER	Zentrales Fahrerlaubnisregister

1. Entwicklung und Situation des Datenschutzes

Der Datenschutz ist durch staatliche Überwachungsmaßnahmen und Skandale beim Adresshandel und der Arbeitnehmerüberwachung, die im Berichtszeitraum 2007 - 2009 festzustellen waren, wieder ein Thema in der Gesellschaft. Die Medienberichterstattung unterstützt die Forderung nach einem besseren Datenschutz. Datenmissbräuche und Datenschutzverstöße haben einen Bewusstseinswandel bewirkt und den Wert des Datenschutzes deutlich werden lassen. Jedoch fehlen noch Taten in Gesetzgebung und Vollzug.

Im Berichtszeitraum wurde das **Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983** 25 Jahre alt. Die Bilanz nach 25 Jahren sieht nicht gut aus: Regelungs- und Vollzugsdefizite, unbegrenzte technische Möglichkeiten, insbesondere die Revolution durch das Internet, gerade auch im Berichtszeitraum Datenskandale im privatwirtschaftlichen und öffentlichen Bereich, lückenhaftes Datenschutzbewusstsein, staatliche Überwachungskataloge.

Doch die verfassungsrechtlichen Mahnungen und Warnungen gelten nach wie vor und strikter:
„*Das Recht auf informationelle Selbstbestimmung trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen, insbesondere unter den Bedingungen moderner Datenverarbeitung, aus informationstechnischen Maßnahmen ergeben. Dieses Recht flankiert und erweitert den grundrechtlichen Schutz von Verhaltensfreiheit und Privatheit; es lässt ihn schon auf der Stufe der Persönlichkeitsgefährdung beginnen.*

Eine derartige Gefährdungslage kann bereits im Vorfeld konkreter Bedrohungen von Rechtsgütern entstehen. Mittels elektronischer Datenverarbeitung sind Einzelangaben über persönliche und sachliche Verhältnisse einer Person unbegrenzt speicherbar und jederzeit und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Sie können darüber hinaus mit anderen Datensammlungen zusammengefügt werden, wodurch vielfältige Nutzungs- und Verknüpfungsmöglichkeiten entstehen. Dadurch können weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können. Eine weitere Besonderheit des Eingriffspotentials von Maßnahmen der elektronischen Datenverarbeitung liegt in der Menge der verarbeitbaren Daten, die auf konventionellem Wege gar nicht bewältigt werden könnte. Der mit solchen technischen Möglichkeiten einhergehenden gesteigerten Gefährdungslage entspricht der hierauf bezogene Grundrechtsschutz.

Der Schutzumfang des Rechts auf informationelle Selbstbestimmung beschränkt sich nicht auf Informationen, die bereits ihrer Art nach sensibel sind und schon deshalb grundrechtlich geschützt werden. Auch der Umgang mit personenbezogenen Daten, die für sich genommen nur geringen Informationsgehalt haben, kann, je nach seinem Ziel und den bestehenden Verarbeitungs- und Verknüpfungsmöglichkeiten, grundrechtserhebliche Auswirkungen auf die Privatheit und Verhaltensfreiheit des Betroffenen haben. Insofern

gibt es unter den Bedingungen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum mehr.

Auch entfällt der grundrechtliche Schutz nicht schon deshalb, weil die betroffene Information öffentlich zugänglich ist. Auch wenn der Einzelne sich in die Öffentlichkeit begibt, schützt das Recht der informationellen Selbstbestimmung dessen Interesse, dass die damit verbundenen personenbezogenen Informationen nicht im Zuge automatisierter Informationserhebung zur Speicherung mit der Möglichkeit der Weiterverwertung erfasst werden."

(Urteil des Bundesverfassungsgerichts vom 11. März 2008, BVerfGE 120, 378 (397ff.) im Anschluss an das Volkszählungsurteil vom 15. Dezember 1983, BVerfGE 65, 1(42ff.))

Das Verständnis von Privatheit hat sich nicht erst seit dem Volkszählungsurteil des Bundesverfassungsgerichts von 1983 grundlegend verändert. Privates wurde schon zuvor öffentlich, angestoßen insbesondere durch das Fernsehen, das Tabubrüche unterstützt hat.
Das Verhalten der Verbraucher und Kunden (Kundenkarten) und die Nutzung von Mobilfunktelefonen und des Internets durch die „Online-Generation" (soziale Netzwerke, Bewertungsportale, Suchmaschinen) belegt darüber hinaus einen Wandel bei der Wahrnehmung der informationellen Selbstbestimmung. Der Soziologe Sennett sprach schon 1974 von der „Tyrannei der Intimität". Im Zuge des digitalen Lebensstils verkommt die alte Kultur der Privatheit zu einer unermüdlichen Selbstpräsentation. Das Gespür für die Bedeutung von Privatheit verfällt. Zur Entblößung kommt die Bloßstellung hinzu. Dem passt sich vieles an, bis hin zum Recht. Der Verbraucher will es, der Bürger hat nichts zu verbergen - angeblich. Doch die Beiträge von Wirtschaft und Staat zur „Überwachungsgesellschaft" sind ungleich umfangreicher und maßgeblicher. Öffentlicher und privater Bereich verschwimmen.
Transparenz und Informationsfreiheit tragen im Übrigen zu einer offenen Gesellschaft bei; dabei kommt es auch zu Widersprüchen zwischen Informationsfreiheit und Datenschutz.

Die gesellschaftspolitischen Auswirkungen der modernen Informations- und Kommunikationsgesellschaft einschließlich des sich daran beteiligenden Staates auf die Bedeutung der Privatsphäre und letztlich auf das Gemeinwesen insgesamt sind noch nicht absehbar. Dies gilt zumal für die digitale Revolution des Internets, das nichts mehr vergisst. Was wir gewinnen, was wir verlieren, das ist noch offen.

Dass die Privatsphäre auch in der digitalen Welt ein wertvolles, zu achtendes Rechtsgut ist, hat das Bundesverfassungsgericht mit seinem grundlegenden Urteil vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07, NJW 2008, 822) hervorgehoben. Danach umfasst das allgemeine Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG auch das **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**. Die seit dem Volkszählungsurteil veränderte Lage und Entwicklung zu dezentralen Computern und globalen vernetzten Systemen (vgl. zur RFID-Technik schon VIII. Tätigkeitsbericht, Ziff. 4.4) bewirkt neue Grundrechtsge-

fährdungen. Über den Schutz der Persönlichkeit, rechtlich wie technisch-organisatorisch, bei einzelnen Datenerhebungen und -verarbeitungen hinaus ist der Schutz des eigengenutzten Systems selbst, dessen integre Funktionsweise geboten. So ist die Technik nicht mehr nur Regelungsinstrument („Datenschutz durch Technik“), sondern Regelungsgegenstand. Es geht um Schutz vor Infiltration oder Manipulation ohne Kenntnis des Nutzers (vgl. zum „Cloud Computing“ Ziff. 1.3) und damit um Vertrauen in das System selbst (Systemdatenschutz). Der Selbstschutz, etwa durch Verschlüsselungstechnik, greift hier zu kurz. Die Grundrechte auf informationelle Selbstbestimmung, Schutz des Telekommunikationsgeheimnisses (Art. 10 GG) und der Unverletzlichkeit der Wohnung (Art. 13 GG) erfassen die neue Gefährdungsdimension nicht. Dieser neue Grundrechtsschutz verhindert weitreichende Persönlichkeitsprofile.
Das neue Grundrecht ist Abwehrrecht gegen den Staat (siehe zur heimlichen Online-Durchsuchung Ziff. 18.3) und Schutzrecht gegen Private, z. B. im Bereich der Wirtschaft, und den Staat (vgl. Ziff. 1.3). Eine ausführliche Kommentierung „seines“ Urteils gibt Hoffmann-Riem in JZ 2008, 1009.
Die nähere Ausgestaltung - rechtlich, organisatorisch, verfahrensbezogen - dieses Gewährleistungsanspruchs in der elektronisch vermittelten Informations- und Kommunikationsgesellschaft steht aus. Die Verhinderung von Datenmissbrauch im Rahmen moderner Kommunikation wird nicht mittels Selbstverpflichtungen und Transparenz allein, wie dies EU-Kommission und Bundesregierung einstweilen etwa für die RFID-Anwendung im Internet der Dinge empfehlen, durchzusetzen sein. Die Schaffung zusätzlicher Regelwerke wird mit einer Überprüfung und Modernisierung vorhandener Vorschriften unter Berücksichtigung der Entwicklungen einhergehen.

Die Tätigkeit des Landesbeauftragten hat - bedingt durch die Aufgabenstellungen, Anforderungen und Anfragen - weiter an Intensität und Umfang zugenommen. Die Maßstäbe des Bundesverfassungsgerichts bzw. der Grundrechte sind Richtschnur.

Zu erinnern ist insbesondere an einen Grundsatz aus dem Urteil von 1983, den das Gericht immer wieder wiederholt hat: **Selbstbestimmung ist eine elementare Funktionsbedingung des freiheitlichen demokratischen Gemeinwesens.** Selbstbestimmung und Privatheit werden nicht um ihrer selbst willen geschützt.
Anlasslose Maßnahmen des Staates gegen jedermann und heimliche Maßnahmen sind daher von besonderer Brisanz im Hinblick auf allgemeine Einschüchterungseffekte bei der Ausübung von Grundrechten. Aber auch das Handeln der Wirtschaft hat Einfluss auf die Wahrnehmung der Grundrechte. Die gesellschaftliche Ordnung und die sie ermöglichende Rechtsordnung bedürfen des Vertrauens ihrer Bürger, ein verlässlicher Datenschutz trägt aufgrund seines gemeinwohlfördernden Charakters dazu bei. Um es mit einer Aussage aus dem VIII. Tätigkeitsbericht zu beschreiben: **Datenschutz ist Maßstab der Freiheitlichkeit des Gemeinwesens.** Denn wenn der Bürger oder Verbraucher nicht mehr wissen kann, wer was wann bei welcher Gelegenheit über ihn weiß, wäre dies eine grundrechtswidrige Rechts- und Gesellschaftsordnung. Diese kommt nicht ohne Daten aus, und der Mensch ist als sozialgemeinschaftsgebundenes Individuum auf Kommunikation angewiesen, trotzdem gibt es aber kein unbegrenztes Recht auf Verarbeitung

fremder Daten. Die Balance zu finden, heißt generell, dem Freiheitscharakter der Selbstbestimmung Rechnung zu tragen und dort, wo diese verloren geht oder gegangen ist, wiederherzustellen. **Datenschutz schützt die Menschenwürde.** Daran ist auch vor dem Hintergrund des 60. Jahrestages der Verkündung des Grundgesetzes am 23. Mai nachdrücklich zu erinnern.

Der IX. Tätigkeitsbericht umfasst den Zeitraum vom 1. April 2007 bis zum 31. März 2009.
Der Bericht enthält wiederum grundsätzliche datenschutzpolitische und rechtliche wie technische Feststellungen und Beschreibungen und zudem ausgewählte Materialien und Hinweise aus der Beratungs- und Kontrollpraxis. Der Bericht dient damit:

- der Unterrichtung des Landtages, zusammen mit der zum Bericht abzugebenden Stellungnahme der Landesregierung (§ 22 Abs. 4a Satz 1 und 2 DSG-LSA),
- der Öffentlichkeitsarbeit (§ 22 Abs. 4a Satz 3 DSG-LSA),
- der Information der Behörden und behördlichen Datenschutzbeauftragten und interessierter Bürgerinnen und Bürger.

Wie schon bei den beiden vorangegangenen Berichten empfiehlt sich neben der Beratung in den Ausschüssen des Landtages auch in dessen Plenum eine öffentliche Debatte.

1.1. Freiheit und Sicherheit

Die Sicherheitsgesetzgebung und die Entwicklung zum Präventionsstaat waren bereits im VIII. Tätigkeitsbericht ausführlich beschrieben worden (Ziff. 1.1), insbesondere die Gefahren aus einer Missachtung der Balance zwischen Sicherheit und Freiheit.
BKA-Gesetz-Novelle, heimliche Online-Überwachung, Anti-Terror-Datei, Kfz-Kennzeichen-Scanning, biometrische Ausweise, Vorratsdatenspeicherung, Fluggastdatenspeicherungen sind Themenstellungen des Berichtszeitraums. Etwa bei der BKA-Gesetz-Novelle oder der Anti-Terror-Datei sind auch Landesbelange betroffen. Ohnehin gilt dies für das durch den Landesbeauftragten ebenfalls begleitete und kommentierte Vorhaben einer Änderung des Verfassungsschutzgesetzes (Ziff. 25.1). Daneben war die Zunahme der Videoüberwachungsmaßnahmen auffällig (Ziff. 18.4, 18.5, 18.6, 18.7, 19.4, 26.5).

Der von der Landesregierung in ihrer Stellungnahme zum VIII. Tätigkeitsbericht zitierte Bundesverfassungsrichter Di Fabio (LT-Drs. 5/1097, zu 1.1.) beschreibt die Entwicklung allgemein als „präventionstechnischen Überbietungswettbewerb“ (Di Fabio, Sicherheit in Freiheit, NJW 2008, 421).

Dass der Staat Eingriffe in den status negativus der Grundrechte rechtfertigen muss und insofern der **Abwehrcharakter der Grundrechte** einen Primat der Freiheit auch bei der Verhältnismäßigkeitsprüfung vorgibt, hat der Landesbeauftragte bereits im Vorgängerbericht ausführlich dargestellt (VIII. Tätigkeitsbericht, Ziff. 1.1). Niemand muss sich dafür rechtfertigen, dass er seine Privatsphäre verbergen will.

Zu den rechtsstaatlichen Essentials zählt auch die Beachtung rechtsstaatlicher Kompetenzgrenzen. Das bedingt auch, den Gegner des Rechtsstaats nicht unter ein eigenes Feindstrafrecht zu stellen, im Inneren und auch nicht im Äußeren im Rahmen der internationalen Zusammenarbeit in einer globalisierten Welt (so auch Di Fabio, a. a. O.). Asymmetrische Konflikte gehen nicht mit asymmetrischen Mitteln einher. *„Daran, dass der Rechtsstaat auch den Umgang mit seinen Gegnern den allgemein geltenden Grundsätzen unterwirft, zeigt sich gerade die Kraft dieses Rechtsstaats“* (Bundesverfassungsgericht im Beschluss zur polizeilichen Rasterfahndung vom 4. April 2006, BVerfGE 115, 320 (358)). Wer also den Rechtsstaat schützen will, sollte nicht seine Wurzeln angreifen. Insofern gibt es weit mehr Tabus als das Folterverbot.

Kritik - auch von Gerichten oder Medien - an staatlichen Vorhaben und Maßnahmen seines Gewaltmonopols dient, da sie nicht diffamiert, dem Rechtsstaat. Die Kontrolle der Datenschützer ergänzt das Vertrauen, das der Rechtsstaat erwarten darf. Letztlich stärkt es seine Verantwortung und Akzeptanz. Wer Datenschutz so denkt, kann ihn auch nicht mehr als Hindernis disqualifizieren. Grundrechte gelten nicht nur dann, wenn sie nicht stören.

Das Gemeinwesen wird nicht zuletzt dadurch gestärkt, dass der Staat Menschen anderer Kulturen von den Freiheitswerten überzeugt, mindestens eine aktive Integrationspolitik betreibt und so im Sinne eines erweiterten Sicherheitsbegriffs auch Ursachen von Gewalt und Terrorismus beseitigen hilft.

Die Akzeptanz staatlicher Tätigkeit wird darüber hinaus durch das Verhalten der öffentlichen Stellen, die faktisch und in der Wahrnehmung der Bevölkerung Inhaber des Gewaltmonopols sind, gefördert, wenn sich diese insbesondere transparent und an der Verfassung ausgerichtet verhalten. In besonderer Weise ist die Handhabung des vielleicht noch „kleinen“, aber als Ausfluss des allgemeinen Persönlichkeitsrechts nicht hoch genug zu schätzenden „Jedermannsrechts“, des Rechts auf Auskunft der von Datenverarbeitung Betroffenen gesondert hervorzuheben. Zwar mag es sein, dass das **Recht auf Auskunft** im Zusammenhang mit den verstärkt wahrgenommenen Informationsfreiheitsgesetzen im Empfinden der Öffentlichkeit „größer“ wird. Es unterscheidet sich jedoch, nicht nur hinsichtlich seiner grundsätzlichen Kostenfreiheit, vielfach vom Anspruch nach den Informationsfreiheitsgesetzen des Bundes und der Länder.
Das Auskunftsrecht über die eigenen personenbezogenen Daten ist die wesentliche organisatorische und verfahrensrechtliche Vorkehrung zur Sicherung des Datenschutzgrundrechts. Es darf nur dann zurückgestellt werden, wenn „*ein gegenläufiges Geheimhaltungsinteresse ...erheblich überwiegt*“ (BVerfG NJW 2008, 2099, siehe dazu Ziff. 9.1). Es bezieht sich selbstredend auf Akten wie auf Dateien (vgl. BVerwG NVwZ 2008, 580). Gerade im Hinblick auf die durch heimliche Datenerhebungen der Polizei, der Geheimdienste oder der Finanzbehörden (vgl. Ziff. 9.1) deutlich erhöhte Schwere des Grundrechtseingriffs erlangt es eine besondere Bedeutung. Wenn Betroffene nicht wissen, was über sie gespeichert wird, haben sie keine Möglichkeit, die Rechtmäßigkeit dieser Datenverwendung ggf. auch gerichtlich überprüfen zu lassen. Die Datenschutzbeauftragten sahen sich immer wieder mit Sachverhalten konfrontiert, die sie nötigten, deutlich auf die Grundrechts-

bedeutsamkeit der Auskunftserteilung hinzuweisen. So werden Auskunftsbegehren häufig verweigert oder hinsichtlich des Umfangs der Antwort sehr begrenzt. Aber selbst anzuerkennende Erwägungen wie das Bestehen einer Ausforschungsgefahr der Datenhaltung oder Quellenschutz können nur nach einer Einzelfallprüfung eine Auskunftsverweigerung rechtfertigen. Selbst eine Negativauskunft darf nur verweigert werden, wenn der „*Möglichkeit des Rückschlusses auf vorhandene Datenspeicherungen überwiegende staatliche Belange entgegenstehen*“ (BVerfG NVwZ 2001, 185; vgl. VIII. Tätigkeitsbericht Ziff. 18.4).

1.2. Nicht-öffentlicher Bereich

Dass aus dem objektiven Wertgehalt der Grundrechte Schutzansprüche des Einzelnen gegen andere Private erwachsen und dass der Staat diese Schutzansprüche umzusetzen hat, ist seit langem in Rechtsprechung und Wissenschaft anerkannt. Das Bundesverfassungsgericht hat zu dieser Schutzkonstellation näher ausgeführt, dass das allgemeine Persönlichkeitsrecht und mithin das Recht auf informationelle Selbstbestimmung als Norm des objektiven Rechts seinen Rechtsgehalt auch im Privatrecht entfalte. Dieses Recht als Schutznorm gewährleistet dem Einzelnen dabei einen informationellen Selbstschutz im Rahmen der Teilnahme an den gesellschaftlichen Kommunikationsprozessen, der - im Falle unzureichender selbstbestimmter Kommunikationsteilhabe - vom Staat mittels der Schaffung wirkungsvoller rechtlicher Voraussetzungen umzusetzen ist (BVerfG, Beschluss vom 23. Oktober 2006, 1 BvR 2027/02, MMR 2007, 93).

Der Staat beruft sich bei seiner Tätigkeit schnell auf die Notwendigkeit des Schutzes der Grundrechte der Bürger auf Leben, Gesundheit und Eigentum vor Kriminalität und Terrorismus (siehe oben Ziff. 1.1) - und überzieht in seinen Maßnahmen bis hin zur Behauptung eines vermeintlichen „Rechts auf Sicherheit“.
Doch gilt der Schutzanspruch auch für andere Grundrechte und Schutzkonstellationen. So gibt es grundrechtlichen Schutz auch für das Recht auf informationelle Selbstbestimmung, das Recht auf Privatsphäre, das Recht auf Gewährleistung der Vertraulichkeit sowie Sicherheit informationstechnischer Systeme. So wird der Einzelne vor unlauteren Datenverarbeitungen der Wirtschaft geschützt. Die zahlreichen Datenskandale belegen Handlungsbedarf. Der Präsident des Bundesverfassungsgerichts Prof. Hans-Jürgen Papier warnte bei einer von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum 25. Geburtstag des Volkszählungsurteils am 15. Dezember 2008 in Karlsruhe durchgeführten Veranstaltung vor einem **„Super-Gau des Datenschutzes“** angesichts der Datenmissbräuche der Privatwirtschaft in einer globalen Welt mit internetgestützter moderner Technik. Es geht darum, dem Verbraucher und Kunden seine Selbstbestimmungsrechte zurückzugeben. Die aktuellen - im Ergebnis noch unzureichenden - Entscheidungen zur Änderung des BDSG zielen in diese Richtung (siehe Ziff. 3.1).

Auch das neue Recht auf Systemdatenschutz wirkt im privaten Rechtsverkehr und verpflichtet den Staat zur Gewährleistung eines differenzierten Schutzregimes.

Die Forderung nach einem Beschäftigtendatenschutzgesetz ist ein ebenfalls hochaktuelles Thema (siehe Ziff. 3.1).

1.3. eGovernment und Technik

eGovernment ist mittlerweile nicht nur der Weg, sondern vielmehr zum Motor der Verwaltungsmodernisierung bei Bund, Ländern und Kommunen geworden. Unterstützt und beschleunigt wird dieser Modernisierungsprozess in der öffentlichen Verwaltung durch ein weiteres Wachstum bei Speicherkapazitäten und verfügbaren Rechenleistungen vom Personalcomputer bis zum Großrechner sowie durch weiter ansteigende Nutzerzahlen im Internet sowie der fast inflationsartigen Entstehung neuer Web-Services, aber auch der Weiterentwicklung des Web 2.0, in dem die Internetnutzer selbst zu Gestaltern werden (Soziale Netzwerke, Blogs, Bewertungsportale, Chatrooms, Wikipedia, usw.).

Im zurückliegenden Berichtszeitraum ist bei den Systemen und Netzen eine Entwicklung weg vom Client-Server-System hin zum Terminal-Server-System sowie ein bis jetzt bereits seit ca. drei Jahren anhaltender Trend zur Virtualisierung von Hard- und Software zu beobachten gewesen. Virtualisierung ist heute fast schon Standard in Rechenzentren auch in Sachsen-Anhalt. Sie hält verbunden mit einer Zentralisierung und Konsolidierung der Informationstechnik von bisher dezentralen IT-Strukturen und IT-Insellösungen unvermindert an. Es findet quasi eine Rückbesinnung auf die Wurzeln der **zentralen** Datenverarbeitung statt, natürlich aber auf einem anderen, höheren Niveau. Hierzu gehören **serviceorientierte Architekturen** (SOA) wie auch das in letzter Zeit immer häufiger als Begriff genannte „Cloud Computing“. Dabei werden Dienste im Netz bereitgestellt, ohne dass sich diese auf einem bestimmbaren Server befinden müssen. Die zugrunde liegende Plattform tritt in den Hintergrund. Der Dienst wird aus einer „Rechnerwolke“ (Cloud) erbracht. Er begegnet schon deshalb wesentlichen datenschutzrechtlichen Bedenken, hat aber gegenwärtig auf die öffentliche Verwaltung noch keine unmittelbaren Auswirkungen.
eGovernment benötigt aber weit mehr als nur den Einsatz modernster Informations- und Kommunikationstechnologie. Der Berichtszeitraum zeichnet sich durch Bemühungen aus, insbesondere **elektronische Identifizierung** und **Kommunikation** im Internet **sicherer** und **rechtsverbindlicher** zu gestalten (ePass, Bürgerportale, De-Mail).

Diese neuen technischen und technologischen Entwicklungen und Möglichkeiten der Informations- und Kommunikationstechnologie bringen erhöhte Anforderungen besonders an die Sicherheit kritischer Geschäftsprozesse in der Wirtschaft und in der öffentlichen Verwaltung mit sich. Zu einem Schwerpunktthema hat sich dabei die vertrauliche Verarbeitung von Unternehmensdaten sowie Mitarbeiterdaten, aber vor allem auch die vertrauliche Verarbeitung personenbezogener Daten der Bürgerinnen und Bürger durch die öffentliche Verwaltung in Bund, Ländern und Kommunen entwickelt. eGovernment benötigt vor allem Nutzer, und das wiederum setzt **Vertrauen** in die vom Staat angebotenen Online-Dienstleistungen voraus. Denn im Zeitalter der Informationsgesellschaft nimmt die Angst der Bürgerinnen und Bürger, bei der

Nutzung des Internets, bei der Nutzung von Online-Diensten der Wirtschaft und von eGovernment-Diensten der öffentlichen Verwaltung zum „Gläsernen Bürger“ zu werden, immer mehr zu.

Besonderes Augenmerk legt deshalb die Bundesregierung auf den Schutz **kritischer Infrastrukturen** zur Sicherheit der IT. Mit dem hierzu im Jahr 2005 verabschiedeten Konzept „Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI)“ und dem insbesondere mit und für die Wirtschaft erarbeiteten Umsetzungsplan „KRITIS“ sowie dem 2007 verabschiedeten „Umsetzungsplan Bund“ und deren Realisierung soll dieser Bedrohungslage für IT begegnet werden. Die Bürgerinnen und Bürger können sich seit einigen Jahren über das beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eingerichtete „Bürger-CERT“ aktuell über die Gefährdungslage im Internet informieren und erhalten dort auch wichtige Verhaltenshinweise zum Selbstschutz.
Auch der nunmehr dritte vom BSI seit 2005 alle zwei Jahre veröffentlichte **Lagebericht 2009** zur IT-Sicherheit in Deutschland schätzt die Bedrohungslage der IT-Sicherheit bei Verwaltungen, Unternehmen und den Privatanwendern auf einem anhaltend hohen Niveau ein. Das zeigt sich sowohl bei der voranschreitenden Qualität und Professionalität der Internetkriminalität (Drive-by-Downloads, Trojanische Pferde mit Backdoor- und Spyware-Funktionen, Bildung von Bot-Netzen) als auch bei der quantitativen Anzahl der Angriffe (Denial-of-Service-Angriffe, weitere Erhöhung des Spam-Anteils am E-Mail-Verkehr).

Standen am Anfang des eGovernment-Prozesses in Deutschland das Bereitstellen von Informationsangeboten der öffentlichen Verwaltung für die Bürgerinnen und Bürger und die Erledigung von Verwaltungsangelegenheiten und -prozessen über das Internet im Mittelpunkt der Bemühungen und Aktivitäten der öffentlichen Verwaltung, ist nunmehr das sog. „**One-Stop-Government**“ das Ziel der Bemühungen auf Bundes- und Landesebene im Rahmen einer neuen eGovernment-Gesamtstrategie für Deutschland. Im Idealfall sollen die Bürgerinnen und Bürger aber auch die Wirtschaft alle in einer bestimmten Situation anfallenden Verwaltungsangelegenheiten im Kontakt mit nur einer Stelle über das Internet erledigen können. Aktuelles Beispiel dieser strategischen Ausrichtung und dieses Paradigmenwechsels im Verwaltungshandeln in Deutschland stellt die Umsetzung der Europäischen Dienstleistungsrichtlinie (EU-DLR) bis zum 31. Dezember 2009 dar. Der „Einheitliche Ansprechpartner“ nach Vorgabe der EU-DLR, über oder durch den zukünftig Verwaltungsprozesse abgewickelt werden sollen, widerspiegelt diese Ausrichtung auf den neuen Dienstleistungscharakter der öffentlichen Verwaltung.

Treibende Kräfte dieses Modernisierungsprozesses sind die Initiative „**Deutschland Online**“ (DOL), d. h. die gemeinsame nationale eGovernment-Strategie von Bund, Ländern und Kommunen, und der „**Nationale IT-Gipfel**“ (-Prozess) auf Initiative der Bundesregierung in enger Zusammenarbeit mit der Wissenschaft und Wirtschaft, mit dem Ziel Deutschland zu einem der führenden IKT-Standorte in Europa und der Welt zu entwickeln. Seit dem 1. Nationalen IT-Gipfel am 18. Dezember 2006 (Potsdam) wird nunmehr im Sprachgebrauch seitens der Bundesregierung und der Wissenschaft für den

Begriff „Informations- und Kommunikationstechnologie“ die Abkürzung **IKT** verwendet.

Allerdings ergeben bzw. stellen sich damit neue Fragen gerade für die öffentliche Verwaltung auf allen Ebenen:
Wie wird zukünftig die **digitale Identität** der Bürgerinnen und Bürger im Internet geschützt? Welchen Beitrag kann hier der Staat leisten?
Wer trägt die Verantwortung für die **öffentlichen IT-Infrastrukturen** (Bundes- und Landesnetze), insbesondere auch im Hinblick auf die Rechtsprechung des Bundesverfassungsgerichts und das neue Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme?
Wie erlangt man das Vertrauen der Bürgerinnen und Bürger zu neuen eGovernment-Angeboten? Wie werden effiziente Datenflüsse mit dem Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung in Übereinstimmung gebracht?

Einige Aktivitäten zur Lösung dieser grundsätzlichen Probleme sind mittlerweile auf den Weg gebracht worden.
So hat sich die Föderalismuskommission II in ihrer abschließenden Sitzung im März 2009 neben den Regelungen zur Schuldenbegrenzung auch auf wichtige Maßnahmen zur Modernisierung der Verwaltung verständigt. An erster Stelle ist hier die Schaffung einer **verfassungsrechtlichen Grundlage (Art. 91c GG)** für die Zusammenarbeit von Bund und Ländern in der Informationstechnologie (IT) der öffentlichen Verwaltungen zu erwähnen. Die Verantwortung für die Sicherheit der länderübergreifenden IT-Netzinfrastruktur soll künftig beim Bund liegen. Der Bund soll eine Kompetenz für die Errichtung und den Betrieb eines sicheren Verbindungsnetzes erhalten, das die informationstechnischen Netze des Bundes und der Länder miteinander verbindet (BT-Drs. 16/12410). Das Nähere soll ein Bundesgesetz mit Zustimmung des Bundesrates regeln (BT-Drs. 16/12400). Der Bundesrat stimmte beiden Vorhaben am 12. Juni 2009 zu.
Auffällig und erstaunlich ist die Tatsache, dass die Datenschutzgrundrechte nach wie vor nicht ausdrücklich in das Grundgesetz aufgenommen worden sind – eine Forderung nicht nur der Datenschutzbeauftragten.

Neben dem bereits seit Januar 2008 berufenen Beauftragten der Bundesregierung für Informationstechnik (sog. „Bundes-CIO“ - Chief Information Officer) soll darüber hinaus ein **neues System der IT-Steuerung** von Bund und Ländern eingerichtet werden, das insbesondere einen **IT-Planungsrat** von Bund und Ländern vorsieht, der wichtige Koordinierungsaufgaben in Fragen der Informationstechnik von Bund und Ländern, wie etwa die Festlegung von IT-Sicherheitsstandards, erhalten soll. Über die Einzelheiten besteht weitgehend Einvernehmen. Sie sollen durch Staatsvertrag und Verwaltungsabkommen verbindlich festgelegt werden.
Gleichzeitig sollen die bisherigen Gremien wie der Arbeitskreis der Staatssekretäre für eGovernment in Bund und Ländern und der Kooperationsausschuss von Bund, Land und Kommunen für automatisierte Datenverarbeitung (KoopA ADV) mit allen ihren Untergremien sowie einzelne Vorhaben aus der Initiative „Deutschland Online“ damit auf- und abgelöst bzw. aufgegeben werden.

Das sind nur einige Themen, die von datenschutzrechtlicher Relevanz sind und im zurückliegenden Berichtszeitraum den Landesbeauftragten und seine Kolleginnen und Kollegen im Bund und den Ländern intensiv beschäftigt haben. Allerdings sind sie und insbesondere der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, im Gegensatz zum eGovernment-Prozess in Bund und Ländern, in den „IT-Gipfel-Prozess“ der Bundesregierung nicht unmittelbar eingebunden. Der Landesbeauftragte hatte in seinem VIII. Tätigkeitsbericht (Ziff. 4.2) diesen Umstand bereits kritisch angemerkt. Nach dem 2. Nationalen IT-Gipfel in Hannover am 10. Dezember 2007 und dem 3. Nationalen IT-Gipfel am 20. Dezember 2008 in Darmstadt wird man für den 4. Nationalen IT-Gipfel Ende 2009 abwarten müssen, in wieweit angesichts der o. a. Rechtsprechung des Bundesverfassungsgerichts Antworten von Politik, Wirtschaft und Wissenschaft gegeben werden, die die Belange des Datenschutzes in dieser sich schnell fortentwickelnden Informationsgesellschaft ausreichend berücksichtigen.

Die Entwicklung in Sachsen-Anhalt und die Anstrengungen der Landesregierung in diesem Modernisierungsprozess für die öffentliche Verwaltung hat der Landesbeauftragte im Kapitel 4 dieses Berichts in den entsprechenden Schwerpunkten dargestellt.

1.4. Zusammenfassung und Ausblick

Die **verfassungsrechtliche Vorgabe, eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger zu unterlassen** (BVerfGE 65, 1, 53 - Volkszählungsurteil im Anschluss an BVerfGE 27, 1, 6 - Mikrozensus), wird durch die zunehmenden Datenverarbeitungen von Staat und Wirtschaft in Frage gestellt. Der Mensch wird dadurch mehr und mehr als Sache behandelt, nicht als Subjekt mit Anspruch auf Persönlichkeitsschutz. Die unbegrenzte und ausufernde Datenverarbeitung und Datenvernetzung ist Zeichen der „Überwachungsgesellschaft“ (vgl. VIII. Tätigkeitsbericht, Ziff. 1.4). Die Problematik erwächst aus der bedenklichen Einzelmaßnahme, aber auch aus deren Summe, aus einer Gesamtschau der Überwachung infolge additiver Grundrechtseingriffe (vgl. auch BVerfG, Urteil vom 12. April 2005, 2 BvR 581/01, BVerfGE 112, 304), zumal angesichts zunehmender präventiver Überwachung (diese greift im Übrigen nicht nur im Bereich der inneren Sicherheit, sondern auch im sozialen Bereich). Ein gläserner Mensch wird niemals mit der Menschenwürde zu vereinbaren sein. Noch befinden wir uns nicht in einem „Überwachungsstaat“, doch ist die bisherige Entwicklung besorgniserregend. Dazu tragen auch Projekte zu Identity Cards und Ordnungskennzeichen bei, wie die neue Steuer-ID (vgl. Ziff. 9.3), aber auch Data Mining, Scoring und andere Bewertungsverfahren der Privatwirtschaft.

Auch in diesem IX. Berichtszeitraum gab es für den Datenschutz einige wichtige, herausragende Entscheidungen des Bundesverfassungsgerichts:

- Beschluss vom 13. Juni 2007 (1 BvR 1550/03 u. a.) - Automatisierte Abfrage von Kontodaten (vgl. Ziff. 9.2),

- Urteil vom 27. Februar 2008 (1 BvR 370/07, 1 BvR 595/07) - Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, u. a. gegen heimliche Online-Durchsuchung (vgl. Ziff. 18.3),
- Beschluss vom 10. März 2008 (1 BvR 2388/03) - Auskunftsrecht über Daten als Teil des Grundrechts auf informationelle Selbstbestimmung (vgl. Ziff. 9.1),
- Urteil vom 11. März 2008 (1 BvR 2074/05, 1 BvR 1254/07) - automatisierte Erfassung von Kraftfahrzeugkennzeichen (vgl. Ziff. 18.12),
- Beschluss vom 17. Februar 2009 (1 BvR 2492/08) - einstweilige Außerkraftsetzung von Teilen des Bayerischen Versammlungsgesetzes (vgl. Ziff. 11.2).

Darüber hinaus bleibt der Beschluss vom 23. Februar 2007 (1 BvR 2368/06; NVwZ 2007, 688) maßgeblich, in dem es um eine Videoüberwachung im öffentlichen Raum ging (vgl. Ziff. 18.5).

Bei der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 3. bis 4. April 2008 in Berlin wurde der Blick in Vergangenheit und Gegenwart des Datenschutzes mit einem Ausblick verbunden:

Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts
Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung

und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

Das Datenschutzrecht bedarf einer grundlegenden Modernisierung. Datenschutz und Privatsphäre gehören zum Bildungsauftrag von Schule und sind Bestandteil der politischen Bildung in der Demokratie.

2. Der Landesbeauftragte

2.1. Tätigkeit im Berichtszeitraum

Die Zahl der Eingänge und Anfragen ist erneut gewachsen.
2007 gab es 3.350 schriftliche Eingänge, im Jahre 2008 3.730 (zum Vergleich: 2005 = 3.120, 2006 = 3.412).

Insgesamt wurden im 2007/2008 2.300 schriftliche Äußerungen (Stellungnahmen, Antworten etc.) verfasst (zum Vergleich: 2005/2006 = 1.570), darunter befanden sich 111 Petentenfälle (zum Vergleich: 2005/2006 = 115).

Die Feststellung, dass dann, wenn keine Datenschutzverletzungen festgestellt worden seien, dies ein Zeichen für einen funktionierenden Datenschutz „auf hohem Niveau“ sei - so die Landesregierung - trifft kaum zu. Der Landesbeauftragte hat bei verschiedenen Kontrollen und Vorgängen nicht selten ein unzureichendes Bewusstsein für Datenschutzbelange bei Behörden, deren Leitungen und Datenschutzbeauftragten feststellen müssen.

Anlassunabhängige Kontrollen fanden u. a. in der Verfassungsschutzabteilung des Innenministeriums und im Landesverwaltungsamt zu Akten der Sicherheitsüberprüfung statt. Geprüft wurden auch Vollzugspolizeidienststel-

len, Ausländerbehörden, eine Einbürgerungsbehörde, eine Kfz-Zulassungsbehörde, die Tätigkeit eines Verkehrsamtes in Bezug auf den sogenannten ruhenden Straßenverkehr, ein Finanzamt, im Bereich der Justiz der Soziale Dienst, ein Sozial-, Arbeits- und Amtsgericht, eine Justizvollzugsanstalt und ein Auftragsdatenverarbeiter, der für Justizdienststellen tätig ist. Desweiteren wurden datenschutzrelevante Vorgänge mehrerer kommunaler Personalämter und eines Universitätsklinikums begutachtet. Im Bereich der Schulen wurden Gymnasien und Sekundarschulen hinsichtlich deren Umgangs mit Schüler- und Elterndaten untersucht. Ebenso war ein Jobcenter, auch ARGE genannt, Gegenstand besonderer Aufmerksamkeit. Zusätzliche technisch-organisatorische Prüfungsschwerpunkte waren ein kreisinternes Richtfunknetz, Videoüberwachungseinrichtungen in öffentlichen Verkehrsmitteln, die Lesegeräte für den ePass, das mobile Bürgerbüro einer Stadt sowie das Wireless-LAN in einer Universität.
Informationsbesuche erfolgten u. a. im Zentralen Mahngericht der Länder Sachsen-Anhalt, Sachsen und Thüringen beim Amtsgericht Aschersleben, im zentralen Registergericht des Landes beim Amtsgericht Stendal und im „Gemeinsamen Informations- und Auswertungszentrum islamistischer Terrorismus“ (GIAZ).

Der Landesbeauftragte hat nach der zum 1. Juli 2007 in Kraft getretenen Kreisgebietsreform begonnen, die neuen **Landkreise** zu besuchen und in Gesprächen mit den Landräten und behördlichen Datenschutzbeauftragten für eine Sensibilisierung in Datenschutzbelangen geworben. Mit dem letzteren Adressatenkreis wurden in 2007 und 2008 zusätzliche Erfahrungsaustausche durchgeführt.

Im Herbst 2007 hatte der Landesbeauftragte die behördlichen Beauftragten für den Datenschutz der Landkreise und kreisfreien Städte zu einem Erfahrungsaustausch eingeladen. Dabei konnten Aufgaben, Befugnisse und Position der Beauftragten und Themen zu Technik und Organisation des Datenschutzes ausführlich erörtert werden. Die Beauftragten hatten Gelegenheit, die Rahmenbedingungen ihrer Tätigkeit in ihrem Kreis darzustellen.
Hierbei zeichnete sich ein nicht einheitliches Bild mit der deutlichen Tendenz ab, dass zumeist nur Zeit zur Reaktion, nicht jedoch zur aktiven Bearbeitung datenschutzrechtlicher Anliegen besteht. Die faktische Situation in den Landkreisen wird daher oftmals den steigenden Anforderungen an den Selbstdatenschutz nicht hinreichend gerecht. Schon im Volkszählungsurteil vom Dezember 1983 hat das Bundesverfassungsgericht die Verpflichtung des Staates zur auch verfahrensmäßigen Absicherung des Grundrechts auf informationelle Selbstbestimmung durch rechtzeitige Vorkehrungen unter Beteiligung unabhängiger Datenschutzbeauftragter formuliert. § 14a DSG-LSA macht hierzu klare Vorgaben, die angesichts der aktuellen Entwicklungen eine angemessene Ausstattung der Position des behördlichen Datenschutzbeauftragten verlangen.

Die Möglichkeit der gemeinsamen Erörterung auch einzelner Probleme in den Landkreisen fand so viel Resonanz, dass auch im Herbst 2008 ein Erfahrungsaustausch durchgeführt wurde. Dabei wurde als ein Schwerpunktthema das Informationszugangsgesetz des Landes behandelt. Inhalt und Auswirkung für die Bearbeitung vor Ort wurden durch den Landesbeauftrag-

ten dargestellt. Die Berichte der behördlichen Datenschutzbeauftragten zeigten, dass sie vielfach in die Vorgänge einbezogen werden. Ein weiteres Schwerpunktthema in technisch-organisatorischer Hinsicht war die Revisionssicherheit unter Microsoft Windows.

Infolge des breiten Interesses wird der Landesbeauftragte auch für 2009 einen Erfahrungsaustausch mit den behördlichen Datenschutzbeauftragten der Kreisebene vorsehen.

Der Landesbeauftragte macht in diesem Zusammenhang erneut auf die auf seiner Homepage eingestellten Hinweise zu Aufgaben und Befugnissen **behördlicher Datenschutzbeauftragter** (§ 14a DSG-LSA) aufmerksam (siehe auch Anlage 20 zum VI. Tätigkeitsbericht). Verantwortlich für den Datenschutz ist aber die jeweilige öffentliche Stelle (§ 14 Abs. 1 Satz 1 DSG-LSA).

In mehreren Fällen gab es **erhebliche Rechtsverstöße**, bei denen nur aufgrund der getroffenen Abhilfen von einer förmlichen Beanstandung abgesehen werden konnte (Ziff. 15.1, 18.6 und 19.4).

Das **Datenschutzbewusstsein** allgemein zu wecken, zu befördern und zu stärken, ist eine der Daueraufgaben des Landesbeauftragten.
Dazu dient auch die **Öffentlichkeitsarbeit**, die im Berichtszeitraum ausgedehnt wurde.

Durch den Landesbeauftragten und Mitarbeiter der Geschäftsstelle wurden Vorträge gehalten und Fortbildungen durchgeführt.

Einen besonderen neuen Schwerpunkt setzte der Landesbeauftragte mit Überlegungen und Maßnahmen zu einer **Verbesserung des Datenschutzbewusstseins bei der jungen Online-Generation**, also der Zielgruppe der Schüler, und dabei auch mit Fortbildungskonzepten für Lehrer (vgl. Ziff. 20.4). Datenschutz und das Recht auf Privatsphäre wurden im Schulunterricht bislang vernachlässigt. Das Kultusministerium hat Initiativen und Vorschläge des Landesbeauftragten zwar allgemein begrüßt, bei der konkreten Umsetzung bestehen aber Defizite. Dagegen gestaltet sich die Zusammenarbeit mit dem Landesinstitut für Schulqualität und Lehrerbildung erfreulich. Allenthalben ist bei Schülern, Eltern und Lehrern eine große Aufgeschlossenheit für die Themen des Web 2.0 zu spüren, aber auch für die damit zusammenhängenden Wertefragen.

Die Verstärkung der Geschäftsstelle durch einen IT-Referenten (besetzt zum 1. August 2007) - leider vom Landtag bislang nur befristet bis Ende 2011 zugewiesen - erlaubte zusätzliche **Beratungen und Prüfungen in technisch-organisatorischen Belangen des Datenschutzes**, auf die früher verzichtet werden musste. Angesichts der fortschreitenden technischen Entwicklungen sind moderne technische Systeme und Anwendungen zugunsten des Datenschutzes frühzeitig zu implementieren. Um den Gefährdungen des Grundrechts auf informationelle Selbstbestimmung gerade durch automatisierte Datenverarbeitungen zu begegnen, sind rechtzeitige Beteiligungen und entsprechende Beratungen seitens des Landesbeauftragten sinnvoll. Der Lan-

desbeauftragte hat bei einer Vielzahl von grundsätzlichen Vorhaben und Einzelprojekten sowie in mehreren Gremien mitwirken können (vgl. Kapitel 4).

Im Übrigen wurde mit der dem Landesbeauftragten zum 1. Oktober 2008 übertragenen Aufgabe des Landesbeauftragten für die Informationsfreiheit die Stelle eines juristischen Referenten bewilligt (siehe Ziff. 2.4).

Im Tätigkeitszeitraum setzten sich auch Bemühungen des Landesbeauftragten um eine neue dauerhafte Unterbringung der Behörde fort. Angesichts von erheblichen Schäden im derzeitigen Dienstgebäude wurde eine Zwischenlösung auf Mietbasis vor einer anderweitigen angemessenen Unterbringung in einem Landesobjekt angestrebt.

Das aktuelle Organigramm der Geschäftsstelle ist diesem Bericht beigefügt **(Anlage 49).**

2.2. Schwerpunkte - Empfehlungen

Schwerpunktthemen bei Beratung, Prüfung und Kontrolle in 2007 und 2008 betrafen:

- IT-Strategie für das Land Sachsen-Anhalt
- zentraler IT-Dienstleister für die Landesverwaltung
- Personalmanagementsystem für die Landesverwaltung
- Namensnennung in Gedenkstättenausstellung des „Roten Ochsen“ in Halle (Saale)
- Studierendendaten der Universität Magdeburg im Internet
- Suchlauf auf der Zentralablage des Ministeriums für Landwirtschaft und Umwelt
- Videoüberwachung im öffentlichen Raum, insbesondere Justizzentrum Magdeburg
- Justizvollzugsanstalt Burg-Madel - PPP-Projekt
- Medienkompetenz und Datenschutzbewusstsein von Schülern und Lehrern
- Kinderschutzgesetz Sachsen-Anhalt
- Gendiagnostikgesetz des Bundes
- Entwicklung des Datenschutzes im nicht-öffentlichen Bereich
- Informationsfreiheit

<u>Empfehlungen</u>

Was hilft angesichts der Entwicklungen und Probleme, angesichts der Diskrepanzen zwischen Grundrechtsansprüchen und Wirklichkeit?
Generell und beim einzelnen Vorhaben:

- Verfahrensrechte und technischer Datenschutz helfen, Eingriffe in die informationelle Selbstbestimmung abzumildern. Diese begleitenden Maßnahmen ersetzen aber nicht die Beachtung der materiellen Anforderungen. Besser ist also:
- Normenklarheit und Normenbestimmtheit,
- Datensparsamkeit,
- strenge Zweckbindung bei Datenerhebung und - verarbeitung,
- Befristung und Evaluation von Eingriffsmaßnahmen,

- Förderung des Datenschutzbewusstseins, auch für mehr Selbstdatenschutz,
- Verstärkung der Schulbildung und politischen Bildung zu Themen der Privatheit und Selbstbestimmung als Werte und Bedingung von Demokratie und Rechtsstaat,
- Transparenz bei der Datenverarbeitung,
- stärkere Beteiligung behördlicher Datenschutzbeauftragter als Teil eines umfassenden Datenschutzmanagements,
- effektive unabhängige Datenschutzaufsicht.

Die Richterin des Bundesverfassungsgerichts Christine Hohmann-Dennhardt fasste die Situation des Datenschutzes prägnant zusammen und gibt entsprechende allgemeine Empfehlungen im folgenden Aufsatz:

- Hohmann-Dennhardt, Informationeller Selbstschutz als Bestandteil des Persönlichkeitsrechts, RDV 2008, 1.

2.3. Zusammenarbeit mit anderen Institutionen

Die **Zusammenarbeit mit dem Landtag** insbesondere im Zusammenhang mit der Beratungsaufgabe des Landesbeauftragten gemäß § 22 Abs. 4 DSG-LSA bei verschiedenen Gesetzgebungsvorhaben (siehe z. B. Ziff. 11.1, 11.2, 11.3), aber auch bei anderen Vorgängen, war erneut intensiv. Die Aufgeschlossenheit dem Datenschutz gegenüber wächst und ist spürbar.

Die Zusammenarbeit mit dem **Landtagspräsidenten** Dieter Steinecke und seiner Verwaltung - für deren Mitwirkung bei der Durchführung haushaltsmäßiger und personalrechtlicher Vorgänge - war weiterhin vertrauensvoll und durch eine unkomplizierte Kooperation geprägt. Der Landesbeauftragte sieht das Modell einer Anbindung der Geschäftsstelle an den Landtagspräsidenten als gelungen an; ohne dass der unabhängige Landesbeauftragte, wie es die Landesregierung in ihrer Stellungnahme zum VIII. Tätigkeitsbericht behauptet (LT-Drs. 5/1097, zu 3.3), damit zu einer parlamentsnahen Institution wird (vgl. auch Ziff. 3.2).
Angestoßen durch die Überprüfung der Videoüberwachungspraxis im Justizzentrum in Magdeburg (siehe Ziff. 19.4) wurde auch das Videoüberwachungssystem im Landtagsgebäude näher untersucht. Die Landtagsverwaltung räumte dabei ein, dass nicht nur eine bloße Videobeobachtung, sondern eine Videoaufzeichnung erfolgt, allerdings in noch maßvollem Umfang. Der Landesbeauftragte gab technische und praktische Hinweise.

Das Verhältnis zur **Exekutive** war sachlich-konstruktiv, ungeachtet oftmals bestehender Meinungsverschiedenheiten. Das Beratungsangebot des Landesbeauftragten wird allgemein angenommen, wenn auch in manchen Fällen zu spät. Es gab aber auch Fälle, wo nach zunächst erfolgter Annahme des Beratungsangebots dieses in der Folge trotz der Bedeutung des Vorgangs vernachlässigt wurde (Ziff. 23.1). Auch in der Umsetzung der Empfehlungen gibt es Defizite.

Der Finanzminister stellte für die Landesregierung anlässlich der Beratung des VIII. Tätigkeitsberichts im Landtag u. a. fest:

„Besser eine Unterrichtung zu viel als eine zu wenig. ...Die rechtzeitige und umfassende Unterrichtung des Landesbeauftragten ist ein zentrales Anliegen aller Mitglieder der Landesregierung."
Dem ist nichts hinzuzufügen, außer dass der Wunsch besteht, dass in der Alltagspraxis diesem Anliegen Rechnung getragen wird.

Mit den **Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich** (vgl. § 38 BDSG), dem für Datenschutz zuständigen Referat im Ministerium des Innern und dem entsprechenden Referat im Landesverwaltungsamt, gab es wiederum auf Initiative des Landesbeauftragten konstruktive Erfahrungsaustausche (siehe auch § 22 Abs. 7 Satz 1 DSG-LSA), zumal die Fragestellungen der Datenverarbeitung im nicht-öffentlichen Bereich zunahmen (vgl. Ziff. 1.2, 3.1).
Der Landesbeauftragte thematisierte auch in diesem Zusammenhang weiterhin die Notwendigkeit einer effektiven unabhängigen Datenschutzkontrolle (vgl. Ziff. 3.2). Mehr und mehr wird der Landesbeauftragte mit Anfragen aus dem nicht-öffentlichen Bereich befasst.

Die Zusammenarbeit mit den Kolleginnen und Kollegen in der **Konferenz der Datenschutzbeauftragten des Bundes und der Länder** und deren Arbeitskreisen hat sich im Berichtszeitraum weiter verstärkt. Dass dabei im Rahmen der Beurteilung der Entwicklungen zur Überwachungsgesellschaft und der Zusammenarbeit von Bund und Ländern auf vielen Feldern, z. B. im Bereich der inneren Sicherheit, auch Kommentierungen von Bundesgesetzen erfolgen müssen und dürfen, wurde von der Landesregierung akzeptiert (Rede des Finanzministers in der 37. Sitzung des Landtages am 17. April 2008, TOP 7, anders noch die Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht, LT-Drs. 5/1097, zu 1.1).
Der Landesbeauftragte unterrichtet Landtagsausschüsse und Ministerien aktuell über die Entschließungen der Datenschutzkonferenz.

Dass **europäische und internationale Datenschutzthemen** die Diskussionen mitprägen, war und ist Alltagspraxis (vgl. Kap. 8, Ziff. 4.7, 4.8, 19.2, 24.1). Der Landesbeauftragte nahm an der 30. Internationalen Datenschutzkonferenz in Straßburg im Herbst 2008 teil (vgl. Ziff. 8.7, **Anlagen 45 - 48**).

2.4. Informationszugangsgesetz Sachsen-Anhalt

Am 1. Oktober 2008 sind das Informationszugangsgesetz Sachsen-Anhalt (IZG LSA) und die dazugehörige Kostenverordnung in Kraft getreten (GVBl. LSA 2008 S. 242 bzw. S. 302). Sachsen-Anhalt ist damit das zehnte Land, das ein Informationsfreiheitsgesetz eingeführt hat. Der Landesbeauftragte hat das Gesetzgebungsverfahren von Anfang an begleitet und sich für einen interessensgerechten Ausgleich zwischen Informationsfreiheit und Datenschutz eingesetzt (vgl. VIII. Tätigkeitsbericht, Ziff. 3.5).

Das neue Gesetz ermöglicht erstmals den freien, an keine weiteren Voraussetzungen gebundenen Zugang zu amtlichen Informationen aller öffentlichen Stellen des Landes. Der Informationsanspruch darf nur dann abgelehnt werden, wenn im Einzelfall ein gesetzlich geregelter Versagungsgrund greift. Damit wurde der Grundsatz der Amtsverschwiegenheit durch das Prinzip der

Aktenöffentlichkeit ersetzt. Die Verwaltung muss darlegen, warum der Informationsanspruch ausnahmsweise nicht besteht.
Besondere öffentliche Belange, Betriebs- und Geschäftsgeheimnisse sowie personenbezogene Daten bleiben im Rahmen der Auskunftsversagungsgründe grundsätzlich geschützt. Die Auskunft erfolgt allerdings nicht unentgeltlich. Für Handlungen nach dem IZG LSA werden Gebühren und Auslagen erhoben, sofern es sich nicht um einfache Auskünfte handelt. Die Höhe richtet sich nach dem Verwaltungsaufwand.

Dem Landesbeauftragten für den Datenschutz überträgt das Informationszugangsgesetz Sachsen-Anhalt die Aufgaben des **Landesbeauftragten für die Informationsfreiheit.** Zu seinen wesentlichen Aufgaben gehört die Vermittlung bei Streitfällen zwischen Bürgerinnen und Bürgern und Behörden, die Beratung der Verwaltung und die Kontrolle der Anwendung des Informationszugangsgesetzes. Alle Personen, die sich in ihren Rechten nach dem Informationszugangsgesetz verletzt sehen, können sich an ihn wenden. Er kann Akten einsehen, die Behörden zu einer Stellungnahme auffordern, vermitteln, bei Verstößen gegen das Informationszugangsgesetz auf ein ordnungsgemäßes Verfahren hinwirken und im Fall der Nichtabhilfe Verstöße beanstanden.

Damit der Landesbeauftragte seine neuen Aufgaben erfüllen kann, wurde ihm ab dem 1. Juli 2008 eine weitere Stelle zugewiesen. Um eine möglichst nahtlose Umsetzung des IZG LSA zu gewährleisten, hat der Landesbeauftragte zum 1. Oktober 2008 Anwendungshinweise, ein Prüfschema, Antworten auf häufig gestellte Fragen sowie einen Flyer zum IZG LSA herausgegeben. Diese Unterlagen stehen auf seiner Homepage zum Abruf bereit. Zusätzlich hält der Landesbeauftragte Seminare zum IZG LSA. Die Nachfrage nach Schulungen ist groß, da die Verwaltungen sich kurzfristig auf eine neue Aufgabe einstellen müssen.

Für das erste Halbjahr 2009 hat der Landesbeauftragte den Vorsitz über die Konferenz der Informationsfreiheitsbeauftragten in Deutschland übernommen und damit die Gastgeberfunktion für den Arbeitskreis und die Konferenz der Informationsfreiheitsbeauftragten. Ab dem Jahr 2010 wird der Landesbeauftragte für die Informationsfreiheit dem Landtag alle zwei Jahre einen Tätigkeitsbericht zum IZG LSA vorlegen.

2.5. Internet-Homepage des Landesbeauftragten und Internetkontakt

Der Landesbeauftragte berichtet regelmäßig über die Weiterentwicklung seiner Internetpräsenz www.datenschutz.sachsen-anhalt.de (zuletzt im VIII. Tätigkeitsbericht, Ziff. 2.4.1).
Im Berichtszeitraum ist das Angebot wieder erweitert und ergänzt worden. Die stetig wachsenden Zugriffszahlen (im Berichtszeitraum wurden - natürlich anonym - über 1,5 Millionen Seitenaufrufe registriert) zeigen, dass das Angebot als aktuelle umfassende Informations- und Wissensquelle bekannt ist. Es richtet sich nach wie vor nicht nur an die der Kontrolle durch den Landesbeauftragten unterliegenden öffentlichen Stellen des Landes, sondern allgemein an die interessierte Fachöffentlichkeit sowie Bürgerinnen und Bürger,

die so auch erfahren können, wie ihr Landesbeauftragter für die Verbesserung des Datenschutzes in Sachsen-Anhalt wirkt.

Wie in Ziff. 2.4 berichtet, wurden dem Landesbeauftragten durch das Informationszugangsgesetz Sachsen-Anhalt auch die Aufgaben des Landesbeauftragten für die Informationsfreiheit übertragen. Dem Rechnung tragend wurde seine Internetpräsenz durch einen eigenen umfangreichen Fachbereich Informationsfreiheit ergänzt:
www.informationsfreiheit.sachsen-anhalt.de

Seit der Inbetriebnahme des überarbeiteten und völlig neu gestalteten Landesportals unter www.sachsen-anhalt.de vor einigen Jahren haben Nutzerinnen und Nutzer von fast jeder Unterseite aus die Möglichkeit, durch Anklicken eines Briefumschlagsymbols eine E-Mail an die Portalredaktion zu senden, z. B. um über Änderungsbedarf einzelner Seiten zu informieren oder um nähere Informationen zu Seiteninhalten zu bitten. Das gilt auch für das Fachportal des Landesbeauftragten, das, wie im VIII. Tätigkeitsbericht (Ziff. 2.4.1) berichtet, seit Mitte Januar 2007 Teil des Landesportals ist und im gleichen Design dargestellt wird. Allerdings bereitete dies im Berichtszeitraum zunehmend datenschutzrechtliche Probleme.
Beim Anklicken des genannten Briefumschlages öffnete sich nämlich ein Kontaktformular, in dem es schlicht „Mail an die Online-Redaktion“ hieß. Eine zunehmende Zahl von Nutzerinnen und Nutzern glaubte, in Kontakt mit der Online-Redaktion z. B. eines Finanzamtes, einer anderen Behörde oder auch des Landesbeauftragten zu treten. Jedoch gibt es solche Stellen bisher nicht. Gemeint war die Online-Redaktion des Landesportals in der Staatskanzlei. Die Nutzer offenbarten der Staatskanzlei also ihre höchstpersönlichen Anliegen, z. B. steuerliche Sachverhalte oder auch, eigentlich für den Landesbeauftragten bestimmt, ihre datenschutzrechtlichen Anliegen. Zwar wurden die eingegangenen Nachrichten von der Online-Redaktion an die zuständigen Behörden, so auch den Landesbeauftragten, weitergeleitet, gleichwohl fand fortwährend eine von den Nutzern nicht gewollte und vor allem für diese nicht erkennbare Datenübermittlung an eine unzuständige Stelle statt.
Der Landesbeauftragte teilte dem Presse- und Informationsamt der Landesregierung in der Staatskanzlei mit, dass das Verfahren der Änderung bedürfe. Er übermittelte eine Reihe von Vorschlägen zur Abhilfe. Insbesondere regte er an, den Text „Mail an die Online-Redaktion“ durch wesentlich deutlichere Hinweise auf den Adressaten der E-Mail zu ersetzen. Außerdem wurde geraten, Seiten-, Service- und Kontextmenü bei Aufruf des Kontaktformulars auszublenden, um den Nutzern auch dadurch deutlich zu machen, dass bei Nutzung des Formulars kein Zusammenhang mehr mit der Behörde, deren Seiten zuvor besucht wurden, besteht.
Die durch die Staatskanzlei rasch erarbeitete Lösung bestand nun darin, dem Kontaktformular folgenden Hinweistext voranzustellen: „Mit dem nachfolgenden Kontaktformular kann eine E-Mail an die Online-Redaktion der Staatskanzlei des Landes Sachsen-Anhalt gesandt werden. Die Nachricht wird - sofern diese in die Zuständigkeit eines anderen Fachressorts fällt - weitergeleitet. Sie erhalten von dort schnellstmöglich eine Antwort.“
Der Landesbeauftragte erkennt die Bemühungen der Staatskanzlei zur Problemlösung an, würde jedoch begrüßen, wenn sich die Kontaktformularseite entsprechend seinen o. g. Vorschlägen deutlicher von den bisher besuchten

Fachportalseiten abheben würde. Optimal wäre natürlich, wenn die Nachricht direkt an die Behörde gelangen würde, von deren Internetseiten aus das Kontaktformular aufgerufen worden war.

3. Allgemeines Datenschutzrecht

3.1. Novellierung des Datenschutzrechts

Im VIII. Tätigkeitsbericht (Ziff. 3.1) hatte der Landesbeauftragte auf die vielfältigen Ansätze, Meinungen und Forderungen hingewiesen, die sich mit der Notwendigkeit der Novellierung des Datenschutzrechts befassten. Dies umfasste nicht nur das BDSG und die Regelung eines Audits, sondern auch die Forderung nach differenzierten datenschutzrechtlichen Regelungen für das Arbeitsverhältnis.

Die fortschreitende technologische Entwicklung schafft durch Vernetzung und branchenübergreifende zentrale Dateien Auswertungsmöglichkeiten, die zu undurchsichtigen Bewertungen der betroffenen Bürgerinnen und Bürger führen können. Daher begrüßten die Datenschutzbeauftragten grundsätzlich einen Gesetzentwurf der Bundesregierung (BT-Drs. 16/10529), der Übermittlungen an Auskunfteien strenger reguliert und durch Informations- und Auskunftsansprüche ein transparenteres **Scoringverfahren** regelt. Die im Entwurf vorgesehene Möglichkeit der Erweiterung der Auskunfteitätigkeit auf jegliche Form rechtlichen und wirtschaftlichen Risikos verlagerte aber einseitig die vertraglichen Risiken. Die Auskunfteitätigkeit sollte auf kreditorische Risiken beschränkt bleiben. Scoringverfahren sollten noch offener werden. Hierzu erging die Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2007 „Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteiregelungen gefordert“ **(Anlage 2).**

In der am 29. Mai 2009 im Bundestag verabschiedeten Fassung der Änderung des BDSG wurde jedoch lediglich die „ausschließliche“ Nutzung von Anschriftendaten zur Berechnung des Wahrscheinlichkeitswertes ausgeschlossen. Die wünschenswerte Benennung der für die Berechnung verwandten Datenarten wurde ebenfalls nicht aufgenommen. Allerdings sind dem Betroffenen bei ungünstigen automatisierten Entscheidungen die wesentlichen Gründe mitzuteilen und zu erläutern (BT-Drs. 16/13219).

Insbesondere Ereignisse seit dem Jahr 2008 haben den Bedarf datenschutzrechtlicher Neuregelung in den Medien zum regelmäßigen Tagesthema werden lassen. Eine Vielzahl von „Datenskandalen“ lässt auch weniger interessierte Bürgerinnen und Bürger aufhorchen. Denn einmal kann jeder als Beschäftigter betroffen sein, wenn es um die Ausforschung durch den Arbeitgeber geht, wie die Fälle vom Lebensmittel- über den Telekommunikations- bis zum Logistikkonzern zeigen. Zum anderen geht es um die teilweise sensiblen Datensätze (Adressen, Telefonnummern, Kontoverbindungen, inhaltliche Informationen) von Kunden der Telekommunikations- und Medienkonzerne oder auch Landesbanken, die „im Handel erhältlich“ sind.

Demgemäß drängen die Datenschutzbeauftragten des Bundes und der Länder auf eine **grundlegende Modernisierung des Datenschutzrechts**, u. a. auf bessere Auskunftsrechte, eine Informationspflicht bei Datenpannen und missbräuchlicher Datennutzung, eine Gewinnabschöpfung bei unbefugtem Datenhandel, ein gesetzliches Datenschutzaudit und die Stärkung der Datenschutzbeauftragten. Hierzu fasste die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im September 2008 die Entschließung „Entschlossenes Handeln ist das Gebot der Stunde“ **(Anlage 15).**

Die informationelle Selbstbestimmung im Bereich des Adress- und Datenhandels setzt eine wirkliche Wahlfreiheit der Verbraucherinnen und Verbraucher voraus. Daher forderte die Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom November 2008 „Adress- und Datenhandel nur mit Einwilligung der Betroffenen“, trotz des Widerstands aus der Wirtschaft nicht vom Vorhaben einer Einwilligungslösung abzuweichen **(Anlage 16).**

Viele aktuell bekannt gewordene Datenschutzverstöße lagen lange zurück, ohne dass sie bis dahin von den Betroffenen oder den Datenschutzbehörden wahrgenommen werden konnten. Die Notwendigkeit der Schaffung von Informationspflichten - grundsätzlich auch für öffentliche Stellen - wurde durch die Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Mehr Transparenz durch Informationspflichten bei Datenschutzpannen“ **(Anlage 17)** betont.

Im Dezember 2008 legte die Bundesregierung einen Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften vor (BT-Drs. 16/12011). Danach ist für Unternehmen die Möglichkeit vorgesehen, sich einem Datenschutzaudit zu unterziehen, um für Datenschutzkonzepte und technische Einrichtungen ein Datenschutzsiegel zu erhalten.
Weiterhin soll die Verwendung von personenbezogenen Daten für Zwecke der Markt- und Meinungsforschung ohne Einwilligung der Betroffenen grundsätzlich beschränkt werden. Die Verwendung von Daten für Zwecke des Adresshandels sowie für fremde Markt- oder Meinungsforschung soll nur mit Einwilligung des Betroffenen möglich sein. Marktbeherrschende Unternehmen sollen zudem die Einwilligung nicht durch Koppelung mit dem Vertragsschluss erzwingen dürfen.

Der Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nichtöffentlichen Bereich „Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit“ vom November 2008 **(Anlage 37)** nahm positiv zur Kenntnis, dass nach dem Gesetzentwurf unter anderem eine wirksame Einwilligung in die Werbenutzung von Daten vorliegen muss, da somit die Transparenz und die Freiwilligkeit verbessert werden.
In Folge des Datenschutzgipfels beim Bundesministerium des Innern am 4. September 2008 waren jedoch weitergehende Vorschläge zu Verbesserung des Datenschutzrechts gemacht worden (z. B. Kennzeichnungspflicht für die Herkunft der Daten, bessere Kontroll- und Sanktionsmöglichkeiten), worauf auch die obersten Aufsichtsbehörden hinwiesen.

Im März 2009 erinnerten die Datenschutzbeauftragten an den dringenden Bedarf nach gesetzgeberischem Handeln. Der Deutsche Bundestag wurde aufgefordert, noch in der laufenden Legislaturperiode die vorliegenden Gesetzentwürfe zu ersten Korrekturen zu verabschieden. Die grundlegende Modernisierung des Datenschutzrechts müsse in der neuen Legislaturperiode umgehend angegangen werden, auch der Einsatz datenschutzfreundlicher Technik müsse geregelt werden (vgl. dazu die Entschließung 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2009 „Defizite beim Datenschutz jetzt beseitigen!“, **Anlage 27**).

Nach bis zuletzt kontroversen Erörterungen zwischen Interessenvertretern des Daten- und Verbraucherschutzes und der Werbewirtschaft beschloss der Bundestag den Kompromissvorschlag seines Innenausschusses vom 1. Juli 2009 (BT-Drs. 16/13657). Dieser umfasst im Wesentlichen: Weiterhin nur ein Widerspruchsrecht gegen die Verwendung von listenmäßig erfassten personenbezogenen Daten zu Werbezwecken, aber stärkere Transparenz mittels eines Anspruchs auf Information über die Herkunft der Daten und mittels Dokumentationspflicht; mehr Datensicherheit durch mehr Anonymisierung; Kündigungsschutz für betriebliche Datenschutzbeauftragte; materielle Eingriffsbefugnisse der Aufsichtsbehörden im nicht-öffentlichen Bereich. Diese Verbesserungen gehen in die richtige Richtung, bleiben aber noch hinter den Empfehlungen des o. a. Datenschutzgipfels zurück. Das Datenschutzaudit wurde im Übrigen einstweilen nicht geregelt.

Zum Ende der 16. Legislaturperiode des Bundestages liegen darüber hinaus sowohl vom Bundestag als auch vom Bundesrat allgemeine positive Voten zu einer Novellierung des Datenschutzrechts vor. Dies müsse modern (also die technologischen Entwicklungen aufnehmend und die Technologien als Regelungsinstrument einbeziehend), leicht verständlich und übersichtlich (als Beitrag auch zur Entbürokratisierung) sein. Dazu gehört auch eine Systematisierung zwischen allgemeinem Datenschutzrecht und bereichsspezifischen Regelungen.

Ein Entwurf zu klaren Regelungen zum **Beschäftigtendatenschutz** steht dagegen seit vielen Jahren aus. Bereits in mehreren Legislaturperioden stand das Thema auf der politischen Agenda. In der Antwort auf eine Kleine Anfrage (BT-Drs. 16/9178) verwies die Bundesregierung darauf, dass sie in der Vergangenheit die Notwendigkeit moderner bereichsspezifischer Datenschutzregelungen im Arbeitsverhältnis anerkannt hat. In letzter Zeit hatte u. a. der Bundesrat mit dem Beschluss vom 7. November 2008 (BR-Drs. 665/08B) die Bundesregierung gebeten, entsprechende Regelungen vorzulegen. Bisher ist jedoch keine Umsetzung erfolgt. Dabei standen Entwürfe als Diskussionsgrundlagen zur Verfügung (u. a. ein Entwurf eines Arbeitsvertragsgesetzes durch Hochschullehrer oder ein Vorschlag für Arbeitnehmerdatenschutzregelungen eines Berufsverbandes von Datenschützern).

Die Entschließung „Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz“ der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder **(Anlage 28)** fordert die Bundesregierung auf, nach jahrelanger Untätigkeit jetzt unverzüglich einen entsprechenden Gesetzentwurf vorzulegen. Unter anderem werden die Einbeziehung auch der Beschäftigten im öffentlichen

Dienst, der Umfang der Datenerhebungen und ihre Nutzung, der Datenabgleich, die Informations- und Kommunikationstechnologien und die Auswertung ihrer Nutzung, der Einsatz von Überwachungssystemen, die Rechte der Beschäftigten und eine effektive Kontrolle als regelungsbedürftig genannt.

In die o. g. Gesetzesänderung des BDSG (BT-Drs. 16/13657) ist nur eine allgemeine Zusammenfassung der Rechtsprechung zum Datenschutz in Beschäftigungsverhältnissen aufgenommen worden; ein umfassendes Arbeitnehmerdatenschutzgesetz steht danach aus.

3.2. Effektive und unabhängige Datenschutzaufsicht

Im VIII. Tätigkeitsbericht (Ziff. 3.3) hatte der Landesbeauftragte ausführlich zur Frage der Unabhängigkeit der Datenschutzaufsicht berichtet. Insbesondere wurde auf das Vertragsverletzungsverfahren der Kommission der Europäischen Gemeinschaften hingewiesen. Hierzu steht nunmehr die Entscheidung des Europäischen Gerichtshofs über die Klage der Kommission gegen den Mitgliedsstaat Deutschland vom 29. November 2007 aus. Die Klage begehrt die Feststellung, dass in allen 16 Ländern in jeweils unterschiedlicher Ausprägung gegen das Gebot der **„völligen Unabhängigkeit“** aus Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG verstoßen wird. In den Ländern, in denen die Zuständigkeit für den Datenschutz im nicht-öffentlichen Bereich zwar bereits bei den Landesbeauftragten für den Datenschutz liegt, ermangelt es nach Auffassung der Kommission auch dort der umfassenden Unabhängigkeit wegen des Vorhandenseins von Einflussmöglichkeiten der sonstigen öffentlichen Verwaltung. Es läge eher eine relative Unabhängigkeit vor, die der noch bestehenden Aufsicht geschuldet ist.

In der öffentlichen Diskussion steht die Frage, welche Stelle als Aufsichtsbehörde nach § 38 BDSG für den nicht-öffentlichen Bereich zuständig sein soll, häufig im Zusammenhang mit der Problematik der völligen Unabhängigkeit der Aufsichtsbehörden. Betont werden regelmäßig zu erwartende Synergieeffekte bei einer gemeinsamen Wahrnehmung der Aufgaben von Datenschutzaufsicht und -kontrolle im öffentlichen und nicht-öffentlichen Bereich. In neun Ländern besteht bereits eine gemeinsame Aufgabenwahrnehmung. Erfahrungsgemäß ist es ratsuchenden Bürgerinnen und Bürgern oft schwer zu vermitteln, dass sie sich an die falsche (unzuständige) Datenschutzbehörde gewandt haben. Die Anfragen an den Landesbeauftragten aus dem nicht-öffentlichen Bereich haben im Berichtszeitraum erheblich zugenommen. Auch das Medieninteresse unterscheidet oft nicht zwischen öffentlicher und nicht-öffentlicher Datenschutzaufsicht. Der Bedarf nach Zusammenführung zur Erzielung von mehr Effektivität ist offenbar. Die Landesregierung will vor weiteren Schritten die Entscheidung des Europäischen Gerichtshofs abwarten.

Auch im Landtag von Sachsen-Anhalt ist die Lage des Datenschutzes und auch die Problematik der Aufsichtsstrukturen mehrfach intensiv erörtert worden. Der Landesbeauftragte nimmt die Gelegenheit, sich an den Beratungen zu beteiligen, im Interesse der Förderung des Datenschutzes gern wahr und stößt dabei auf Aufgeschlossenheit und Unterstützung.

3.3. Europäischer Datenschutztag

Der Europarat hat den 28. Januar als jährlich zu begehenden Datenschutztag ausgerufen, um das Bewusstsein für den Datenschutz in Europa zu stärken. Der Termin erinnert daran, dass im Jahr 1981 die Unterzeichnung der Europaratskonvention 108 begonnen wurde. Damit verpflichteten sich die unterzeichnenden Staaten, für die Achtung der Rechte und Grundfreiheiten, insbesondere des Persönlichkeitsrechts, bei der automatisierten Datenverarbeitung Sorge zu tragen.

Anlässlich des Ersten Europäischen Datenschutztages fand im Januar 2007, wie im VIII. Tätigkeitsbericht (Ziff. 7.4) dargestellt, eine zentrale Veranstaltung der Datenschutzbeauftragten des Bundes und der Länder statt. An der Vorbereitung für den Zweiten Europäischen Datenschutztag hat sich der Landesbeauftragte beteiligt. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder favorisierte im Ergebnis die Erprobung von dezentralen Veranstaltungen.

Anlässlich des Zweiten Europäischen Datenschutztages am 28. Januar 2008 besuchte der Landesbeauftragte zusammen mit dem Landtagspräsidenten ein Gymnasium, um vor Ort mit Schülerinnen und Schülern aktuelle Fragen mit Bezug zum Datenschutz zu erörtern. Die Veranstaltung diente der Vitalisierung des Datenschutzbewusstseins. Neben den rechtlichen Grundlagen wurde die Bedeutung des Datenschutzes und der Datensicherheit im Alltag für Jugendliche verdeutlicht. Dabei erfolgte vor allem eine kritische Wertediskussion, insbesondere zum Zielkonflikt von Freiheit und Sicherheit. Nach einem einführenden Referat und weiteren theoretischen Erläuterungen wurden die Schülerinnen und Schüler zur Diskussion und Mitwirkung an einem Rollenspiel aufgefordert. Die Erörterung von Fragen, die die Persönlichkeitsrechte betrafen, sollten für den Unterricht fruchtbar gemacht und die Medienkompetenz gestärkt werden.
Diese sowie eine weitere parallele Veranstaltung von Mitarbeitern des Landesbeauftragten in einer Sekundarschule verstand der Landesbeauftragte als Auftakt, dem weitere Veranstaltungen im Schulbereich folgen sollen (siehe Ziff. 20.4).

Anlässlich des Dritten Europäischen Datenschutztages am 28. Januar 2009 haben die Datenschutzbeauftragten des Bundes und der Länder neben einzelnen Vorhaben wieder eine gemeinsame, zentrale Veranstaltung in Berlin durchgeführt. Unter dem Titel „Die ideale Angestellte, der genormte Arbeitnehmer. Wie viel darf mein Arbeitgeber über mich wissen?“ diskutierten Vertreter der Bundesregierung, der Gewerkschaften, der Wissenschaft und des Datenschutzes.

Wie mehrere Überwachungsvorgänge in großen Unternehmen in der letzten Zeit belegen, sind Persönlichkeitsrechte und Datenschutz im Arbeitsverhältnis vielfältig bedroht. Der Schutz des Persönlichkeitsrechts und die Achtung des Grundrechts auf informationelle Selbstbestimmung zählen jedoch ebenso zu den fairen Arbeitsbedingungen, wie Chancengleichheit und gerechte Bezahlung, ohne dass legitime Arbeitgeberinteressen außer Acht gelassen werden.

Auch auf internationaler Ebene ist weiter beabsichtigt, durch entsprechende Maßnahmen auf die Privatsphäre und den Datenschutz aufmerksam zu machen. Auf der 30. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre 2008 wurde die „Entschließung zur Prüfung der Einrichtung eines internationalen Tages oder einer Woche für den Schutz der Privatsphäre/Datenschutz“ gefasst **(Anlage 48).**

4. Entwicklung der automatisierten Datenverarbeitung – eGovernment

4.1. Die neue IT-Strategie des Landes Sachsen-Anhalt

Der Landesbeauftragte hatte zuletzt in seinem VIII. Tätigkeitsbericht (Ziff. 4.1) ausführlich über die Aktivitäten und Bemühungen der Landesregierung berichtet, grundlegend neue Wege bei der konzeptionellen Fortentwicklung des Einsatzes der Informationstechnologie (IT) in der Landesverwaltung zu beschreiten.

Das damals im November 2005 vom Ministerium des Innern vorgelegte und vom Kabinett zustimmend zur Kenntnis genommene „IT-Konzept - Fortschreibung 2005“, an dessen Erarbeitung in einer interministeriellen Arbeitsgruppe unter Federführung des Ministeriums des Innern auch der Landesbeauftragte beteiligt war, hatte zur Berücksichtigung wesentlicher datenschutzrechtlicher Belange bei den Zielen und Leitlinien in diesem IT-Konzept geführt.
Eine vorgesehene jährliche Anpassung, spätestens im November 2006, an aktuelle Entwicklungen und die Fortschreibung dieses IT-Konzepts, wie im damaligen Kabinettsbeschluss vom 15. November 2005 festgelegt, erfolgte allerdings nicht mehr. Der wesentliche Grund hierfür war ein von der Staatskanzlei in Auftrag gegebenes externes Gutachten „Zusammenführung aller zentralisierbaren Rechenzentrumsdienstleistungen in eine übergreifende Organisationsstruktur in der Landesverwaltung Sachsen-Anhalt“ vom 6. Februar 2006 (dessen Erstellung bereits am 28. Februar 2005 durch den Ständigen Staatssekretärsausschuss „Informationstechnologie“ beschlossen worden war).
Erst auf seine Nachfrage in der Staatskanzlei und der Bitte um Zusendung hin wurde dem Landesbeauftragten das besagte Gutachten am 16. Januar 2007 zugeleitet.

Die Landesregierung hat weitreichende Beschlüsse zur Umsetzung der im Gutachten aufgezeigten notwendigen Veränderungen und Handlungsvorschläge gefasst.
Zu nennen ist hier in erster Linie der Kabinettsbeschluss vom 14. November 2006, der die Neuausrichtung der IT-Organisation und eine neue Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei, dem Ministerium des Innern und dem Ministerium der Finanzen einleitete.
Die Zuständigkeit für die IT-Strategie liegt damit seit dem 1. Dezember 2006 bei der Staatskanzlei (Landesleitstelle IT-Strategie - LIS). Weiterhin ist die Staatskanzlei für das Landesportal Sachsen-Anhalt (www.sachsen-anhalt.de), in Abstimmung mit dem Ministerium des Innern, verantwortlich.

Die Koordinierung und Umsetzung des eGovernment-Aktionsplanes 2004-2010 erfolgt in der Verantwortung des Ministeriums des Innern durch den derzeit geltenden eGovernment-Maßnahmenplan 2008-2009.
Das Ministerium der Finanzen ist seit diesem Zeitpunkt für die IT-Konsolidierung und - als wichtigste Aufgabe - für den Aufbau eines zentralen IT-Dienstleisters für die Landesverwaltung Sachsen-Anhalt verantwortlich.

Mittlerweile hat sich, beginnend ab dem Frühjahr 2007, die Unterrichtung und Einbeziehung des Landesbeauftragten bei grundlegenden Planungen des Landes, die eine datenschutzrechtliche Relevanz haben - auch wenn von manchem nicht sofort erkannt oder für nicht notwendig gehalten - doch spürbar verbessert.
Zu nennen sind hier in diesem Zusammenhang in erster Linie nachfolgende Ressorts und Themen:

- Die Landesleitstelle IT-Strategie (LIS) der Staatskanzlei zum Thema IT-Strategie des Landes,
- das Ministerium des Innern zur Umsetzung des eGovernment-Maßnahmeplans 2008-2009 und insbesondere auch zur IT-Umsetzung der EU-Dienstleistungsrichtlinie,
- das Ministerium der Justiz zum IT-Ressortplan sowie zum PPP-Projekt JVA Burg,
- das Ministerium für Wirtschaft und Arbeit zur Umsetzung des Binnenmarktinformationssystems (IMI) und der Umsetzung der EU-Dienstleistungsrichtlinie,
- das Ministerium der Finanzen zur Thematik KONSENS und nach anfänglichen Verständigungsschwierigkeiten auch die Stabsstelle „Konsolidierung des IT-Betriebes“ zum Thema Aufbau eines zentralen IT-Dienstleisters (Landesrechenzentrum) in Sachsen-Anhalt.

Diese Aufzählung ist nicht abschließend, zeigt aber zugleich, dass der Landesbeauftragte im zurückliegenden Berichtszeitraum umfangreich im Rahmen seines Beratungsauftrages nach § 22 Abs. 4 DSG-LSA in Anspruch genommen wurde. Diese auch starke personelle Belastung der Geschäftsstelle wurde durch die Bereitstellung einer IT-Referentenstelle (ab dem 1. August 2007) gemildert, so dass trotz der ausgeweiteten Beratungstätigkeit die Kontrollen im technisch-organisatorischen Bereich durchgeführt werden konnten. Es ist zu hoffen, dass diese bis Ende 2011 befristete IT-Referentenstelle in ein unbefristetes Beschäftigungsverhältnis umgewandelt werden kann, denn die Entwicklung der Informations- und Kommunikationstechnologie in Sachsen-Anhalt macht im Jahr 2012 sicher nicht Halt.

Die Staatskanzlei hat, federführend durch die LIS, nach einer Ist-Analyse der vom Ministerium des Innern übernommenen Aufgaben den Prozess der grundlegenden Überarbeitung und Fortschreibung des IT-Konzeptes aus dem Jahre 2005 als IT-Strategie des Landes, wie dem Landesbeauftragten Anfang des Jahres 2007 avisiert, eingeleitet.

Den Auftakt für die Erarbeitung dieser neuen IT-Strategie für das Land bildete ein Workshop am 10./11. Oktober 2007, an dem auch der Landesbeauftragte beteiligt wurde.

Im Ergebnis dieses Workshops wurden acht Themenfelder ermittelt, für die zur Weiterführung der Verwaltungsmodernisierung unabdingbar Handlungsbedarf besteht und für die Festlegungen von zielorientierten Maßnahmen unbedingt erforderlich sind. Zu diesen Themenfeldern gehören:

- Ziele der IT-Strategie,
- Rahmenbedingungen für die IT,
- IT-Organisation,
- IT-Standards,
- IT-Architektur,
- IT-Management,
- IT-Services,
- IT-Controlling.

An drei von insgesamt acht Arbeitsgruppen, die entsprechend den Themenfeldern gebildet wurden, beteiligte sich der Landesbeauftragte aktiv (AG Rahmenbedingungen, AG IT-Architektur, AG IT-Management). Als Grundlage der Erarbeitung einer ganzheitlichen IT-Strategie für das Land in diesen Arbeitsgruppen verabschiedete der Koordinierungsausschuss Informationstechnik (IT-KA) mit Beschluss 06/2007 am 4. Dezember 2007 „Thesen und Ansätze zur Erarbeitung der IT-Strategie der Landesverwaltung“.
Durch diese intensive Arbeit, an der alle Ressorts teilnahmen, wurde es der Landesregierung letztendlich möglich, das von der Staatskanzlei vorgelegte Konzept für eine ressortübergreifende Strategie zur Modernisierung und Konsolidierung der Informations- und Kommunikationstechnologie der Landesverwaltung zu verabschieden.

Mit dem **Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008** (MBl. LSA S. 619) liegt damit erstmals ein umfassendes strategisches Dokument vor, welches auch die Belange des Datenschutzes und der Datensicherheit berücksichtigt. Die Modernisierung der Verwaltung wird demnach unter Beachtung des informationellen Selbstbestimmungsrechts und des durch die aktuelle Rechtsprechung des Bundesverfassungsgerichts zum Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme fortgesetzt.
Diese IT-Strategie erfordert, dass das Thema IT-Sicherheit in den Führungsebenen verankert wird. Gleiches sollte auch für das Thema Datenschutz und Datensicherheit gelten.
In einer Landesleitlinie IT-Sicherheit sollen die wesentlichen Ziele festgelegt und damit die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in den Ressorts geschaffen werden. Der Datenschutz wird als fester Bestandteil des IT-Managements beschrieben; es ist vorgesehen, ihn in die Landesleitlinie IT-Sicherheit zu integrieren. Der Landesbeauftragte regt in diesem Zusammenhang an, die behördlichen Datenschutzbeauftragten (§ 14a DSG-LSA) der Ressorts und auch der übrigen Landesbehörden stärker in diesen Prozess einzubeziehen, um hier einen ganzheitlichen Ansatz für IT- und Datensicherheitsmaßnahmen (§ 6 Abs. 2 DSG-LSA) zu erreichen, wenn es um die automatisierte Verarbeitung personenbezogener Daten geht.

Dieser Erlass zur IT-Strategie legt die Ziele sowie mittel- und längerfristige Maßnahmen für die nächsten fünf Jahre fest, eine Fortschreibung ist unter Beachtung der sich schnell verändernden Gegebenheiten und Entwicklungen der Informations- und Kommunikationstechnologie vorgesehen. Es bleibt zu

hoffen, dass dieser Beschluss zur IT-Strategie des Landes nicht nur eine Absichtserklärung darstellt, sondern dass gerade die darin verankerten Ziele für den Datenschutz und die Datensicherheit aktiv von der Landesregierung verfolgt und umgesetzt werden. Der Landesbeauftragte sieht in der Umsetzung der IT-Strategie, insbesondere in der Schaffung eines umfassenden Sicherheitsmanagements mit der Implementierung entsprechender Sicherheitsstandards, eine grundlegende Voraussetzung, auch das Vertrauen der Bürgerinnen und Bürger in die rechtsstaatliche, sichere und datenschutzkonforme automatisierte Verarbeitung ihrer Daten zu stärken.

Abschließend sei noch angemerkt, dass mit dem Beschluss der Landesregierung vom 29. Juli 2008 und der gleichzeitigen Aufhebung des Gemeinsamen Runderlasses des MI, der StK und der übrigen Ministerien vom 1. Juni 1992 – IT-Grundsätze (MBl. LSA S. 805) endlich ein vom Landesbeauftragten seit Jahren kritisierter Zustand beendet wurde (vgl. IV. Tätigkeitsbericht Ziff. 8.1, V. Tätigkeitsbericht Ziff. 6.2, VI. Tätigkeitsbericht Ziff. 7.3, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3).

4.2. Aufbau eines neuen zentralen IT-Dienstleisters - Landesrechenzentrum

Neben der Entscheidung der Landesregierung zur Neuausrichtung der IT-Organisation und der damit verbundenen Veränderung der Aufgabenverteilung und -abgrenzung zwischen der Staatskanzlei und dem Ministerium des Innern entsprechend des Kabinettsbeschlusses vom 14. November 2006 war die zweite, fast noch wesentlichere Entscheidung der Auftrag an das Ministerium der Finanzen zur IT-Konsolidierung der Landesverwaltung und zum gleichzeitigen Aufbau des zentralen IT-Dienstleisters, des neuen **Landesrechenzentrums** (LRZ). Dieser Auftrag ist integraler Bestandteil der am 29. Juli 2008 vom Kabinett verabschiedeten IT-Strategie des Landes (siehe Ziff. 4.1).

Das Konzept zur IT-Konsolidierung der Landesverwaltung sah vor, innerhalb eines noch zu gründenden IT-Betriebsstättenverbundes ein LRZ als teilrechtsfähige Anstalt des öffentlichen Rechts zu errichten. Kern des zukünftigen LRZ bildet das Finanzrechenzentrum (FRZ) der Oberfinanzdirektion Magdeburg (OFD), welches dazu mit dem Landesinformations-Zentrum (LIZ) in Halle zusammengeführt wurde. Mit Kabinettsbeschluss vom 3. Juni 2008 (MBl. LSA S. 404) wurde das LIZ dem Geschäftsbereich des Ministeriums der Finanzen zugeordnet.
Neben dem zukünftigen LRZ sollten das Justizrechenzentrum Barby und Teile des Rechenzentrums des Landesamtes für Vermessung und Geoinformation (LVermGeo) in einem IT-Betriebsstättenverbund zusammengefasst werden.

Zur Bewältigung dieses umfangreichen und komplexen Auftrags der Landesregierung hat das Ministerium der Finanzen hierzu eine temporäre Stabsstelle „Konsolidierung des IT-Betriebes“ (KIT) gebildet. Dieser sog. „**Aufbaustab**“ soll solange bestehen bleiben, bis das LRZ seine Arbeit aufgenommen hat.

Zu Beginn der Arbeitsaufnahme der Stabsstelle KIT erfuhr der Landesbeauftragte über den E-Mail-Verteiler des IT-Koordinierungsausschusses von der Ausarbeitung zweier Kabinettvorlagen durch diese Stabsstelle des Ministeriums der Finanzen. Eine Kabinettvorlage betraf die Einrichtung der sog. „Kompetenzteams“ und die zweite Kabinettvorlage betraf die Errichtung des Aufbaustabes und dessen weiteres konzeptionelles Vorgehen bei der Konsolidierung des IT-Betriebes.
Beide Kabinettvorlagen betrafen auch datenschutzrechtliche Belange. Der Landesbeauftragte hätte also gem. § 14 Abs. 1 Satz 2 DSG-LSA informiert werden müssen. Erst nach Aufforderung zur Information stellte der Aufbaustab dem Landesbeauftragten dann beide Kabinettvorlagen zur Verfügung.
Allerdings verwunderte den Landesbeauftragten die damalige Begründung des Aufbaustabes zu seiner Nichtbeteiligung wegen „Nichterwähnung“ im Kabinettsbeschluss vom 14. November 2006. Damit verkannte der Aufbaustab die Gesetzeslage und die sich daraus ergebende Verpflichtung **jeder** öffentlichen Stelle des Landes. Die rechtzeitige Beteiligung des Landesbeauftragten über grundlegende Planungen des Landes zum Aufbau oder zur Änderung von automatisierten Verfahren zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten bedarf keiner ausdrücklichen Erwähnung in einem Kabinettsbeschluss, sie gilt für **alle** Normadressaten des DSG-LSA, so auch für den Aufbaustab.

Leider kommt der Landesbeauftragte nicht umhin, auch an dieser Stelle zum wiederholten Mal (vgl. VI. Tätigkeitsbericht, Ziff. 7.1, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3) auf diese so wichtige gesetzliche Verpflichtung hinzuweisen. Bei Beachtung durch die öffentlichen Stellen des Landes ist so mit Unterstützung des Landesbeauftragten ein vorgezogener Grundrechtsschutz möglich.
Die **Unterrichtung** an den Landesbeauftragten ist an keine Form gebunden. Im einfachsten Fall reicht also zur Erfüllung dieser Pflicht eine Übersendung von Planungsunterlagen, u. a. auch Kabinettvorlagen, mit Hinweis auf eine Unterrichtung nach § 14 Abs. 1 Satz 2 DSG-LSA aus. Sie verursacht damit, im Gegensatz zu der dem Landesbeauftragten gegenüber oft geäußerten Meinung eines damit verbundenen „erheblichen zusätzlichen Aufwandes“, diesen eben nicht.
Daneben müssen in einem noch viel stärkerem Maße die behördlichen Datenschutzbeauftragten (§ 14a DSG-LSA) ebenfalls bereits in der Planungsphase von IT-Projekten und -Verfahren der Ressorts beteiligt und einbezogen werden.

Diese „Meinungsverschiedenheiten“ zwischen dem Aufbaustab und dem Landesbeauftragten sind aber mittlerweile ausgeräumt. Im Übrigen ist der Landesbeauftragte Mitglied des **Projektbeirates** des Aufbaustabs. Dieser hat allerdings nur eine beratende Funktion. Die Mitarbeit im Projektbeirat beeinträchtigt die Unabhängigkeit des Landesbeauftragten nicht, er ist bei seiner Aufgabenerfüllung nur dem DSG-LSA (§ 21 Abs. 1 Satz 1) unterworfen. Sie bietet ihm vielmehr eine weitere Möglichkeit zur Information und Erörterung, aber auch ansatzweise zur Beratung bei datenschutzrechtlichen Problemstellungen im Rahmen dieses anspruchsvollen und komplexen Projekts zur IT-Konsolidierung der Landesverwaltung.

Für die Abarbeitung der ressortübergreifenden Aufgaben wurden entsprechend des Kabinettsbeschlusses vom 28. August 2007 neun **Kompetenzteams** (K-Teams) in der Projektorganisation des Aufbaustabes gebildet (siehe VIII. Tätigkeitsbericht, Ziff. 4.1). Dieser Prozess der IT-Konsolidierung auf Landesebene wird zeitgleich durch ressortinterne Projektteams unterstützt.
Die Projektorganisation des Aufbaustabs und dessen weiteres konzeptionelles Vorgehen wurden mit Kabinettsbeschluss vom 25. September 2007 bestätigt. Damit wurden die für den Aufbaustab notwendigen Regelungen zur Strukturierung und Steuerung des Projekts der IT-Konsolidierung getroffen.

Die weiteren Planungen bis Ende 2007 sahen vor, mit Unterstützung der Kompetenzteams zu den einzelnen zukünftig zentral durch das LRZ bereitzustellenden **IT-Querschnittsdiensten** wie Datenhaltung und -archivierung, E-Mail-, Intranet- und Internet-Dienst, zentraler Verzeichnisdienst, zentrale Softwareverteilung, Benutzerbetreuung (zentraler User Help Desk) zunächst Grobkonzepte zu entwickeln und nach deren Bestätigung durch den Ständigen Staatssekretärsausschuss „Informationstechnologie“ (StS-Ausschuss IT) als Lenkungsausschuss für das Gesamtprojekt IT-Konsolidierung entsprechende Fein- und Umsetzungskonzepte zu erstellen.
Die dem Landesbeauftragten im Laufe des Oktobers 2007 zugeleiteten ersten drei Entwürfe von Grobkonzepten der Kompetenzteams zu den Themen Zentralisierung und Virtualisierung von Servertechnik (K-Team „Terminal-Server-Technik“), Server-Konsolidierung (K-Team „Storage/Archivierung“) und Datensicherung (K-Team „Storage/Archivierung“) beinhalteten hinsichtlich der Aussagen zum Datenschutz und zur Datensicherheit nicht viel mehr als eine Kapitelüberschrift „Datenschutz“. Zudem war die vom Aufbaustab gesetzte Frist von ganzen 3 Tagen für Ergänzungs- und Änderungsvorschläge mit Hinblick auf eine damals im IT-KA am 23. Oktober 2007 vorgesehenen Erörterung dieser Grobkonzepte wohl mehr als eine Zumutung anzusehen und scheinbar reine „Formsache“ für den Aufbaustab. Der Landesbeauftragte hat diese Praxis gegenüber dem Aufbaustab kritisiert.
Dem Landesbeauftragten wurde nach dieser Kritik und seinem Beratungsangebot seitens des Aufbaustabs die Gelegenheit gegeben, im Rahmen seiner Besprechung mit den Teamleitern der Kompetenzteams am 15. November 2007, die Anforderungen zum Datenschutz materiell-rechtlich, insbesondere aber aus technisch-organisatorischer Sicht mit Hinblick auf die Erfordernisse bei der automatisierten Verarbeitung personenbezogener Daten (Sicherheitsziele des § 6 Abs. 2 DSG-LSA) zu erörtern. Die genannten drei Grobkonzepte wurden am 9. Juni 2008 vom StS-Ausschuss IT bestätigt. Das vom Aufbaustab erarbeitete Grobkonzept zur zentralen Benutzerbetreuung (User Help Desk, Stand: 25.11.2008) wurde am 2. Dezember 2008 im IT-KA vorgestellt.
Die geplante Umsetzung der technischen und organisatorischen Maßnahmen zur Datensicherheit (Sicherheitsziele) der Kompetenzteams „Software-Verteilung“, „Terminal-Server-Technik“, „SAP“, „Security- und Netzinfrastruktur“, „Solaris“, „Storage/Archivierung“ und „E-Mail/Intranet und Internet“ sind für den Landesbeauftragten von besonderem Interesse. Die hierfür besonders datenschutzrechtlich relevanten Grobkonzepte der Kompetenzteams „Security- und Netzinfrastruktur“ und „E-Mail/Intranet und Internet“ liegen dem Landesbeauftragten bisher nicht vor.

Das **Feinkonzept** zur **Server-Konsolidierung** (Vers. 2.3, Stand: 29. April 2009 des K-Teams „Storage/Archivierung“) liegt dem Landesbeauftragten vor, ebenso das Feinkonzept für **Datensicherung** (K-Team „Storage/Archivierung“). Das 125-seitige Feinkonzept zur Server-Konsolidierung lässt schon eine intensive Auseinandersetzung mit dem Thema IT-Sicherheit erkennen. Der Landesbeauftragte weist aber darauf hin, dass gerade zu den datenschutzspezifischen Sicherheitszielen **Revisionsfähigkeit** und **Transparenz**, die für eine datenschutzrechtliche Kontrolle unabdingbar ist, keine Aussagen getroffen werden. Hier besteht Nachbesserungsbedarf. Zu verweisen ist hier auf den IT-Strategie-Beschluss der Landesregierung vom 29. Juli 2008, Ziff. 3.5 Datenschutz (MBl. LSA S. 404).
Weitere datenschutzrechtliche Fragen bedürfen in diesem Zusammenhang einer Klärung, u. a. zum Thema Auftragsdatenverarbeitung (§ 8 DSG-LSA) sowie zu automatisierten Abrufverfahren (§ 7 DSG-LSA) in Verbindung mit der Vorabkontrolle bei bestimmten automatisierten Verfahren (§ 14 Abs. 2 DSG-LSA), die durch die behördlichen Datenschutzbeauftragten des jeweiligen Ressorts durchzuführen sind (§ 14a Abs. 4 Nr. 2 DSG-LSA).
Gerade zukünftige zentrale, virtuelle Server-Farmen benötigen für einen datenschutzkonformen Betrieb entsprechende Zugriffs- und Berechtigungskonzepte sowie die Sicherstellung der Revisionsfähigkeit im datenschutzrechtlichen Sinn. Umfangreiche personenbezogene Datenbestände bei einem zentralen IT-Dienstleister wie dem zukünftigen LRZ sind hinsichtlich ihrer rechtlichen Zulässigkeit und den getroffenen Maßnahmen zur Datensicherheit zu beurteilen. Zur konzeptionellen Planung dieser IT-Konsolidierungsprozesse gehört nicht zuletzt auch die Beachtung und Berücksichtigung der datenschutzrechtlichen Rahmenbedingungen.

Zu Beginn des Jahres 2008 erfolgte seitens des Aufbaustabs ein Strategiewechsel, was die Übernahme der IT-Querschnittsdienste durch das zukünftige LRZ betraf. Die bisherige Planung, über die drei Phasen Test-, Probe- und Pilotbetrieb diese Dienste beim LRZ aufzubauen und danach landesweit einzuführen, wurde aufgegeben und statt dessen durch ein Migrationskonzept je Behörde ersetzt, welches eine Ist-Analyse und Konzepterstellung zur Ablösung der IT-Querschnittsdienste und danach die Übernahme dieser IT-Querschnittsdienste von der jeweiligen Behörde durch das LRZ vorsieht. Wesentlicher Vorteil dieser Vorgehensweise ist die jeweils nur einmal notwendige Befassung mit einer Behörde.

Das vom Aufbaustab erarbeitete Konzept zum übergreifenden **IuK-Betriebsmodell** des Landes Sachsen-Anhalt wurde vom Kabinett am 1. Juli 2008 bestätigt. Das IuK-Betriebsmodell bestimmt die vom LRZ und dem Betriebsstättenverbund zukünftig zu erbringenden IT-Dienstleistungen und die allein von diesen zu betreibenden IT-Querschnittsaufgaben. Es trifft Festlegung zum sog. Leistungsschnitt, d. h. der Abgrenzung der Verantwortung zwischen zukünftigen LRZ und den Ressorts und sieht Servicevereinbarungen der Ressorts und der jeweiligen Dienststellen mit dem LRZ vor. Für den operativen Betrieb werden ebenfalls Regelungen für die Zusammenarbeit zwischen den Ressorts und dem LRZ getroffen.

Noch am 18./19. November 2008 wurde den Ressorts und dem Landesbeauftragten in einem Workshop vom Aufbaustab das **Geschäftsmodell** für

den zukünftigen zentralen IT-Dienstleister in Form einer teilrechtsfähigen Anstalt des öffentlichen Rechts (sog. Anstalts-Modell) als Zusammenschluss von FRZ und LIZ vorgestellt. Die Anstalt sollte Bestandteil eines IT-Betriebsstättenverbundes werden, der im Errichtungszeitraum mit dieser Anstalt und dem Rechenzentrum im Technischen Polizeiamt (TPA), dem Justizrechenzentrum Barby und dem Rechenzentrum des LVermGeo gebildet werden sollte. Der künftige zentrale IT-Dienstleister sollte über zwei Standorte in Magdeburg und Halle (Saale) verfügen, mit Hauptsitz in Halle (Saale). Die Bildung der Anstalt sollte durch ein entsprechendes Errichtungsgesetz erfolgen.
Nach einer Grundsatzentscheidung durch das Ministerium der Finanzen im **Januar 2009** wurde das bisherige Geschäftsmodell überraschend geändert. Nunmehr sollen in Form einer Verwaltungslösung, d. h. innerhalb der Oberfinanzdirektion Magdeburg (OFD), das FRZ und das LIZ den Kern des zentralen IT-Dienstleisters bilden. Das LRZ soll nunmehr als **Abteilung 4 der OFD** angegliedert werden.
Dieses neue Geschäftsmodell wurde am 12. Mai 2009 in einem Workshop den Ressorts durch den Präsidenten der Oberfinanzdirektion persönlich erläutert. Ein wesentlicher Vorteil dieser Verwaltungslösung (sog. Behörden-Modell) soll darin bestehen, dass die Fusion von FRZ und LIZ zum LRZ zunächst in den bewährten Strukturen erfolgen kann. Das LRZ soll in den kommenden Jahren sukzessive alle IT-Querschnittsaufgaben für über 300 Behörden des Landes übernehmen.
Eine Entscheidung zum Betreiber für das zukünftige Landesnetz (ITN XT) anstelle des bisherigen Betreibers des Landesnetzes (ITN-LSA), des TPA, steht aber bisher noch aus.
Der Landesbeauftragte hat an dem genannten Workshop ebenfalls teilgenommen. Er hat insbesondere in Bezug auf die vorgesehene Übernahme von über 90 Leistungsvereinbarungen des LIZ in das LRZ an die Beachtung datenschutzrechtlicher Bestimmungen erinnert und gleichzeitig seine Unterstützung für die Begleitung dieses Überführungsprozesses angeboten.

Der Betriebsbeginn des LRZ ist für den 1. Juli 2009 geplant. Zeitgleich soll die Pilotierung im Geschäftsbereich des Ministeriums der Finanzen, als erstem Ressort, zur Migration der IT-Querschnittsdienste beginnen.

Der Landesbeauftragte wird sich im kommenden Berichtszeitraum verstärkt mit dem Aufbau des LRZ beschäftigen und insbesondere sein Augenmerk auf die datenschutzkonforme Einrichtung und Übernahme von IT-Querschnittsdiensten durch das LRZ und die Überführung der Leistungsvereinbarungen des LIZ in das LRZ legen.
Er geht davon aus, dass er weiterhin zeitnah und ausreichend über die weitere Umsetzung des IT-Konsolidierungsprozesses informiert wird und ihm dadurch die Gelegenheit und Möglichkeit gegeben wird, auf eine datenschutzgerechte Realisierung dieses komplexen und ehrgeizigen Vorhabens der Landerregierung zur IT-Konsolidierung der Landesverwaltung Sachsen-Anhalt hinzuwirken und allen dabei Beteiligten beratend zur Verfügung zu stehen.

4.3. Grundkonzept IT-Architektur der Landesverwaltung

Bereits im Dezember 2006 hatte die Staatskanzlei dem Landesbeauftragten den Entwurf „Konzept für IT-Infrastruktur Land Sachsen Anhalt“ mit der Bitte um Stellungnahme zugeleitet. Dieser Konzeptentwurf resultierte aus einem davor bereits Anfang 2006 erteilten Auftrag des damals noch für die IT-Strategie zuständigen Ministeriums des Innern für ein solches Grundkonzept für IT-Infrastrukturdienste an das Landesinformations-Zentrum (LIZ).
Grundsätzlich begegnete dieses Konzept keinen datenschutzrechtlichen Bedenken, schuf es doch die grundlegende Voraussetzung für eine längst überfällige landesweite einheitliche IT-Infrastruktur, die den optimalen Einsatz standardisierter eGovernment-Verfahren der öffentlichen Stellen des Landes erst ermöglicht. Bei einer datenschutzgerechten Umsetzung wird damit der Grundstein für die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität personenbezogener Daten in IT-Infrastrukturdiensten (u. a. Mitarbeitereinträge im zentralen Namens- und Verzeichnisdienst) entsprechend den Sicherheitszielen des § 6 Abs. 2 DSG-LSA gelegt.

Mit Beschluss 02/2007 des Koordinierungsausschusses Informationstechnik (IT-KA) vom 23. Januar 2007 wurden dieses Konzept bestätigt und grundlegende Entscheidungen zur Überarbeitung und Fortentwicklung zu einem Grundkonzept „IT-Architektur der Landesverwaltung Sachsen-Anhalt“ getroffen. Gleichzeitig wurde das LIZ mit der Erarbeitung eines Konzepts für das Identitäts- und Zugriffsmanagement (engl.: Identity and Access Management-System - IAM-System) beauftragt.
Zur Zentralisierung des Namens- und Verzeichnisdienstes wurde die im Konzept vorgeschlagene Architekturvariante III „Zentral - integriert“ auf homogener Microsoft Plattform vom IT-KA mit Beschluss 05/2007 vom 1. Oktober 2007 bestätigt.
Wesentliches Merkmal dieser Architekturvariante ist die Trennung der Administration von **Diensten** und **Daten**. Das bedeutet, dass zukünftig mehr IT-Querschnittsdienste zentral bereitgestellt werden (siehe Ziff. 4.2), zu denen u. a. der Namens- und Verzeichnisdienst zählt, ohne damit die Selbständigkeit der Ressorts und deren Verantwortlichkeit für die eigene Datenverwaltung zu beeinträchtigen. Ein solcher Infrastrukturdienst wird landesweit zur Verfügung stehen und ist von jeder öffentlichen Stelle der Landesverwaltung nutzbar. Dieser Prozess geht einher mit der Vereinheitlichung und Standardisierung von Datenformaten und Schnittstellen. Die Bereitstellung und die Administration erfolgt durch den zentralen IT-Dienstleister. Die Ressorts werden Nutzer dieses Infrastrukturdienstes sein, betreiben diesen aber nicht.

Zur Begleitung der Weiterentwicklung des IT-Architektur-Konzepts LSA wurde eine ressortübergreifende Arbeitsgruppe **IT-Architektur** unter Federführung der Staatskanzlei (LIS) gebildet.
Mit IT-KA-Beschluss 07/2007 vom 4. Dezember 2007 wurde das in der AG IT-Architektur erarbeitete **Namenskonzept** für diesen einheitlichen Namens- und Verzeichnisdienst des Landes für verbindlich erklärt und durch den Ständigen Staatssekretärsausschuss „Informationstechnologie“ bestätigt. Dieses umfassende Namenskonzept ist als Anlage 2 Bestandteil des Beschlusses der Landesregierung über die IT-Strategie des Landes Sachsen-

Anhalt vom 29. Juli 2008 (MBl. LSA S. 619). Es ist damit verbindlich für die gesamte Landesverwaltung die Migration zu einem zentralen Namens- und Verzeichnisdienst festgeschrieben.
Der Landesbeauftragte ist Mitglied dieser Arbeitsgruppe, die ihre Tätigkeit über den jetzigen Berichtszeitraum hinaus auch in den nächsten Jahren noch fortsetzen wird.

Die erste Bewährungsprobe für diesen integrierten IT-Infrastrukturdienst und dessen zentrale Verwaltung stellt die zum 1. Juli 2009 geplante Betriebsaufnahme des zentralen IT-Dienstleisters in Sachsen-Anhalt dar. Eine funktionsfähige einheitliche IT-Infrastruktur mit zentralem Management und der Aufbau eines IAM-Systems bilden die Grundlage für eine optimale standardisierte eGovernment-Infrastruktur und die weitere Umsetzung der im eGovernment-Maßnahmenplan 2008-2009 vorgesehenen Leitprojekte und Basiskomponenten (siehe Ziff. 4.5).

Die Konzepte zum Namens- und Verzeichnisdienst und zum Aufbau eines IAM-Systems, die von der AG IT-Architektur mit externer Unterstützung eines Beratungsunternehmens erarbeitet und durch den IT-KA bestätigt wurden, sowie der Beschluss der Landesregierung zur IT-Strategie bilden zugleich die Grundlage für die konzeptionelle Arbeit des Kompetenzteams „E-Mail/Intranet und Internet“ (siehe Ziff. 4.2).
Die dem Landesbeauftragten seit dem 22. Mai 2009 vorliegende Endfassung des Grobkonzepts „Verzeichnisdienste/Identity und Access Management“ (Stand: 19. Mai 2009) dieses Kompetenzteams berücksichtigt seine Empfehlungen zur Absicherung und Veröffentlichung personenbezogener Daten. Hierzu gehören geplante Regelungen zu abgestuften Zugriffsrechten und zur Revisionsfähigkeit der Administration sowie für die Absicherung der Systeme des Namens- und Verzeichnisdienstes durch den Einsatz geeigneter IT-Sicherheitstechnologien wie Firewall und Proxy-Server.

Zum Schutz der Accounts des zentralen Namens- und Verzeichnisdienstes folgt das Kompetenzteam in seinem Grobkonzept ebenfalls der Empfehlung des Landesbeauftragten zum Einsatz eines chipkartenbasierten Anmeldeverfahrens. Die Sicherheitsinfrastruktur hat das Land bereits im Jahr 2006 geschaffen (siehe VIII. Tätigkeitsbericht, Ziff. 4.3). Der Landesbeauftragte begrüßt ausdrücklich den Einsatz der Signaturkarte Sachsen-Anhalt mit Zertifikaten der Public Key Infrastruktur Land Sachsen-Anhalt (PKI LSA) für eine vertrauliche und sichere Anmeldung an den zentralen Namens- und Verzeichnisdienst.

Für die Veröffentlichung der Daten, insbesondere der personenbezogenen Mitarbeiterdaten, ist im Grobkonzept vorgesehen, die bereits mit dem Landesbeauftragten für das Zentrale Adressverzeichnis abgestimmte abgestufte Veröffentlichungsregelung anzuwenden (siehe VI. Tätigkeitsbericht, Ziff. 7.4).

Der Landesbeauftragte geht davon aus, dass mit der Erstellung des Feinkonzepts „Verzeichnisdienste/Identity und Access Management“ diese vorgesehenen Regelungen zum Datenschutz und der Datensicherheit mit konkreten Maßnahmen untersetzt werden und er hiervon rechtzeitig unterrichtet wird. Besonderes Augenmerk wird er auf die Erarbeitung des IT-

Sicherheitskonzepts für diesen zentralen Namens- und Verzeichnisdienst richten, welches die datenschutzrechtlichen Anforderungen berücksichtigen muss.

Ziel eines Identitäts- und Zugriffsmanagement-Systems ist es, personenbezogene Daten konsistent, sicher und ständig verfügbar für das IT-Management bereitzuhalten. Die Vielzahl von Services, deren Daten untereinander abzugleichen sind, stellt an die Administration hohe Anforderungen. Veränderungen der Daten der Mitarbeiter und Mitarbeiterinnen, bei Neueinstellungen oder Dienstbeendigung sowie aufgrund von Funktions- oder Behördenwechsel, müssen in allen beteiligten Systemen dann sicher und automatisch erfolgen können.
Die datenschutzrechtlichen Anforderungen hinsichtlich der Einrichtung von Accounts (Benutzerkonten), deren Benutzerrechte und Vergabe für eine natürliche Person in einem Identitäts- und Zugriffsmanagement-System sind aus den Arbeitsaufgaben (Dienstposten/Arbeitsplatzbeschreibung) der Mitarbeiter und Mitarbeiterinnen abzuleiten.

In diesem Zusammenhang kommt der durch die Landesregierung beabsichtigten Schaffung eines IT-gestützten **Personalmanagementsystems** (PMS) für die gesamte Landesverwaltung (siehe Ziff. 17.2) eine besondere Bedeutung zu. Für eine natürliche Person muss zukünftig eine **digitale Identität** durch das PMS erzeugt werden können.
Historisch bedingt existiert für die Landesverwaltung kein zentrales Identitäts- und Zugriffsmanagement-System. Dadurch sind in den Ressorts unterschiedliche Identitätsspeicher im Einsatz. Die Informationen über diese digitalen Identitäten werden in einem zentralen Verzeichnis aus Identitätsspeichern der Ressorts über Schnittstellen zusammengeführt werden. Zukünftig wird der überwiegende Teil der Behörden der Landesverwaltung einen Active Directory (AD) als primären einheitlichen Identitätsspeicher nutzen. Das AD dient als standardisierter und zentraler Verzeichnisdienst und primärer (führender) Identitätsspeicher. Es bildet die Voraussetzung für eine effektive und sichere Identitäts- und Zugriffsverwaltung.
Nach der Einführung eines PMS kann die Zuordnung einer Person zu einer bestimmten Stelle (Verwaltungsrolle) und zu ihrer Rolle im IT-System (IT-Rolle) durch die Personalabteilung vorgenommen werden. Deshalb besteht auch aus datenschutzrechtlicher Sicht das Erfordernis, zukünftig das PMS hinsichtlich der Zuordnung einer Person zur Verwaltungsrolle als führendes System einzuführen. Über eine Datenschnittstelle des PMS können dann die Daten für das IAM-System bereitgestellt werden. Digitale Identitäten (Benutzer, Gruppen, Geräte, Dienste) werden zentral mit Hilfe des IAM-Systems verwaltet. Diesen Identitäten werden die im IAM-System abgebildeten IT-Rollen und Rechte für Applikationsrollen (z. B. für Anwendungen im Landesportal, E-Mail, HAMISSA, SALSA usw.) zugeordnet: Dieses Konzept zur Verbindung von PMS mit einem IAM-System setzt aber für seine optimale Umsetzung die Umstellung auf **ein** PMS für alle Landesbehörden voraus.

Der Landesbeauftragte ist bereit, das Kompetenzteam „E-Mail/Intranet und Internet“ bei dieser schwierigen Aufgabe beratend zu unterstützen. Als Mitglied in der AG IT-Architektur wird er die Konzepterarbeitung und Einführung

eines auf dem zentralen integrierten Namens- und Verzeichnisdienst aufbauenden IAM-Systems für das Land weiter begleiten.

4.4. Landesleitlinie IT-Sicherheit

In den zurückliegenden Jahren wurde seitens der Landesregierung mehrfach versucht, durch entsprechende Beschlüsse den Prozess zur Etablierung einer IT-Sicherheitsplattform für die Landesverwaltung voran zu bringen.
Im damaligen Kabinettsbeschluss vom 15. Juli 2003 wurde das der Kabinettvorlage des Ministeriums des Innern beigefügte „Landeseinheitliches Konzept Informationstechnologie, IT-Investitionen 2003“ vom 10. Juli 2003 als verbindliche Grundlage der informationstechnischen Basisversorgung der Landesverwaltung bestätigt.
In diesem Konzept wurde hinsichtlich der IT-Infrastruktur und deren Sicherheit Handlungsbedarf festgestellt.
Eine entsprechende Konzeption zu einem IT-Sicherheitsmanagement auf Landesebene sollte durch das Technische Polizeiamt (TPA) und das Landesinformations-Zentrum (LIZ) erarbeitet werden. Darin sollten auch die Grundlagen und Bedingungen zum kurzfristigen Einrichten eines sog. CERT-LSA (Computer Emergency Response Team) definiert werden. Nach einem Beschluss des IT-KA am 28. Oktober 2003 wurde das TPA durch das Ministerium des Innern mit der Leitung der hierzu gebildeten Projektgruppe beauftragt. Dabei sollen die Erfahrungen des CERT-Bund und der in den Ländern vorhandener CERTs einfließen.
Die von der Projektgruppe erarbeiteten Vorschläge wurden aber nicht aufgegriffen und weiterverfolgt.

Ein Jahr später, im November 2004, leitete die damalige Landesleitstelle IT/eGovernment (LIT) des Ministeriums des Innern in Vorbereitung einer Kabinettsbefassung zum Thema IT-Sicherheit in der Landesverwaltung dem Landesbeauftragten den Entwurf eines geplanten Gem. RdErl. „Kommunikations- und Infrastrukturerlass Sachsen-Anhalt (KommIn-LSA)“ zu. Die LIT erarbeitete gleichzeitig unter Mitwirkung des TPA und des Landesbeauftragten den Entwurf einer Sicherheitsrichtlinie für das Informationstechnische Netz des Landes Sachsen-Anhalt (ITN-LSA), welche als Anlage Bestandteil des KommIn-LSA werden sollte. Dazu kam es jedoch nicht.
Im November 2005 wurde dem Landesbeauftragten per E-Mail durch das Ministerium der Innern (LIT) die „IT-Sicherheitsrichtlinie des ITN-Betreibers für das Informationstechnische Netz des Landes Sachsen-Anhalt (ITN-LSA)“ als ab sofort anzuwendende Richtlinie bekannt gegeben.
Eine Fortschreibung dieser IT-Sicherheitsrichtlinie des ITN-Betreibers (dem TPA) soll gemäß Ziff. 6 nach regelmäßiger Prüfung erfolgen und dem neuesten Stand der Technik angepasst sowie der LIT/eGovernment des Ministeriums des Innern (die es aber seit dem 1. Dezember 2006 nicht mehr gibt) zur Genehmigung vorgelegt werden. Die Bekanntgabe der jeweils aktuellen Fassung soll in geeigneter Weise erfolgen.
Die im Informationsportal der Staatskanzlei veröffentlichte Fassung trägt das Datum 18. Juli 2007. Das sich innerhalb von fast zwei Jahren kein Anpassungsbedarf dieser IT-Sicherheitsrichtlinie ergeben hat, darf bezweifelt werden.

Nach der Übernahme der Zuständigkeit für die IT-Strategie durch die Staatskanzlei hatte deshalb die Leitstelle für IT-Strategie (LIS) die Initiative ergriffen und zu einem 1. Erfahrungsaustausch zum Thema IT-Sicherheit im November 2007 eingeladen. Auch der Landesbeauftragte ist dieser Einladung gefolgt. Das Ministerium der Finanzen hatte sich nicht an diesem Erfahrungsaustausch beteiligt. Das Ergebnis der Bestandsaufnahme war für alle am Erfahrungsaustausch Beteiligten ernüchternd. Bis auf den Bereich der Landespolizei (IT-Sicherheitsleitlinie; RdErl. des Ministeriums des Innern vom 29. Januar 2004), dem LIZ, und dem Ministerium für Landwirtschaft und Umwelt für den INVEKOS-Verbund war kein IT-Sicherheitsmanagement in den übrigen Ressorts etabliert.

Das Thema „**IT-Sicherheitsmanagement**“ rückt aber mit dem Beschluss der Landesregierung über die IT-Strategie des Landes Sachsen-Anhalt vom 29. Juli 2008 (MBl. LSA S. 619) wieder mehr in den Fokus der Aufmerksamkeit der Ressorts. Als mittelfristige Maßnahme im Rahmen der IT-Strategie des Landes soll nunmehr die IT-Sicherheit institutionalisiert werden. In einer neuen **Landesleitlinie IT-Sicherheit** werden zukünftig wesentliche Ziele sowie deren Umsetzung für die Landesverwaltung verbindlich festgelegt. Diese soll dann die Grundlage für die Etablierung einer IT-Sicherheitsorganisation in der Verantwortung der Ressorts bilden.
Und auch das etwas in Vergessenheit geratene CERT-LSA soll wieder zum Leben erweckt werden und zur Lösung akuter Sicherheitsvorfälle im Land beitragen.

Im Rahmen der IT-Konsolidierung der Landesverwaltung befasst sich auch das Kompetenzteam „Security/Netzinfrastruktur“ unter Federführung des TPA mit dieser Thematik. Dem Landesbeauftragten liegt aber bisher kein Grobkonzept des Kompetenzteams hierzu vor.
In diesem Zusammenhang erinnert der Landesbeauftragte auch an seine Kritik aus zurückliegenden Berichtszeiträumen zum Thema IT-Sicherheitskonzept für das ITN-LSA und dem damit in Zusammenhang stehenden sog. „Netz-Erlass“, dem Gem. RdErl. des Ministeriums des Innern, der Staatskanzlei und der übrigen Ministerien vom 7. Februar 1994 (MBl. LSA S. 1251) (siehe IV. Tätigkeitsbericht, Ziff. 8.2.2, V. Tätigkeitsbericht, Ziff.6.3, VI. Tätigkeitsbericht, Ziff. 7.3, zuletzt VIII. Tätigkeitsbericht, Ziff. 1.3). Dieser sollte im Zuge der Erarbeitung einer Landesleitlinie IT-Sicherheit entweder aufgehoben oder grundsätzlich überarbeitet und den aktuellen Gegebenheiten des ITN-LSA angepasst werden.

Abschließend sei noch auf das zentrale IT-Sicherheitsmanagement des Landes Mecklenburg-Vorpommern durch Nutzung des „GSTOOL“ (einem kostenfreien BSI Software-Tool zum IT-Grundschutz) durch den dortigen zentralen IT-Dienstleister hingewiesen. Damit wurde eine effiziente und praktikable Verfahrensweise gefunden, die Ressorts bei Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz zu unterstützen. Zugleich ist damit die Möglichkeit verbunden, diesen IT-Sicherheitsprozess zu planen, Maßnahmen umzusetzen und auch den Umsetzungsstand bei der IT-Sicherheit im Land darzustellen und abzurechnen.

4.5. eGovernment-Maßnahmenplan 2008-2009

Über die Umsetzung des von der Landesregierung am 29. April 2003 beschlossenen „Grundkonzept eGovernment in Sachsen-Anhalt“, dem daraus durch das Ministerium des Innern erarbeiteten und vom Kabinett am 17. August 2004 verabschiedeten Aktionsplan für den Zeitraum 2004 bis 2010 und zu dessen Umsetzung unter Federführung des Ministeriums des Innern in daraus abgeleiteten eGovernment-Maßnahmenplänen für die Jahre 2005/2006, 2007 berichtet der Landesbeauftragte in seinen Tätigkeitsberichten regelmäßig (siehe VII. Tätigkeitsbericht, Ziff. 7.1, VIII. Tätigkeitsbericht, Ziff. 4.2). Die Informationen und Beurteilungen des Landesbeauftragten erfolgen dabei aus datenschutzrechtlicher Sicht und stellen damit keine grundsätzliche Kritik an dieser Form der Verwaltungsmodernisierung dar. Gleichwohl sind bei allen diesen Leitprojekten die bereichsspezifischen und die allgemeinen Regelungen zum Datenschutz und der Datensicherheit zu berücksichtigen und einzuhalten. Anfragen zu Beratung bzw. Unterrichtung der Ressorts zeugen zumindest von einer stärkeren Beachtung datenschutzrechtlicher Belange.

Das Ministerium des Innern hat gegenüber dem Landesbeauftragten, wie in der Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht des Landesbeauftragten vom 23. Januar 2008 (LT-Drs. 5/1097) angekündigt, seine Informationspolitik verbessert. Dem Landesbeauftragten wurde der aktuelle eGovernment-Maßnahmenplan 2008-2009, wenn auch sehr kurzfristig, doch noch vor der Beschlussfassung des Kabinetts am 4. März 2008 zugeleitet.
Auch beide Sachstandsberichte zum Umsetzungsstand des derzeitigen eGovernment-Maßnahmenplans zur Information des Kabinetts (vom 16. Oktober 2008 und 20. Februar 2009) hat das Ministerium des Innern dem Landesbeauftragten zeitnah zur Verfügung gestellt.
Der aktuelle eGovernment-Maßnahmenplan 2008-2009 umfasst mittlerweile 23 Leitprojekte und 6 Basiskomponenten. Sowohl bei der Bereitstellung von eGovernment-Basiskomponenten als auch bei der Umsetzung von Leitprojekten sind Fortschritte zu verzeichnen. So hat sich das Landesportal (www.sachsen-anhalt.de) zu einem Dienstleistungsportal entwickelt. Besondere Anstrengungen sind bei der weiteren IT-Umsetzung der EU-Dienstleistungsrichtlinie und des Binnenmarktinformationssystem IMI (Internal Market Information System) erforderlich. Auch die Umsetzung der Vorhaben zur Deutschland Online Initiative (DOL), als der nationalen eGovernment-Strategie von Bund, Ländern und Kommunen in Sachsen-Anhalt, erfordert erhebliche Anstrengungen. Das Land beteiligt sich hier aktiv an solchen DOL-Projekten. Beispielhaft sind hier das DOL-Projekt „IT-Umsetzung der EU-DLR“, die Mitarbeit im Verbund der Länder zum „Zuständigkeitsfinder“ und den Arbeitsgruppen der „D115-Initiative“, der einheitlichen Behördenrufnummer für Deutschland, zu nennen.

Mit dem Ministerium des Innern wurde im o. a. Sinne eine grundsätzliche Verfahrensweise in Bezug auf Unterrichtungen des Landesbeauftragten zu eingesetzten automatisierten Verfahren im Geschäftsbereich des Ministeriums des Innern im beiderseitigen Einvernehmen erörtert und abgestimmt.
Positiv ist auch die Berichterstattung des Ministeriums der Justiz hinsichtlich der Unterrichtung des Landesbeauftragten zur Planung und Umsetzung sei-

nes IT-Ressortplans zu erwähnen. Der Landesbeauftragte informierte sich in diesem Zusammenhang bei Besuchen im September 2008 über das beim Amtsgericht Stendal geführte EDV-Handels-, Genossenschafts-, Partnerschafts- und Vereinsregister (Regis STAR) sowie im Dezember 2008 beim Amtsgericht Aschersleben über das in der Zweigstelle Staßfurt geführte Elektronischen Mahnverfahren Sachsen-Anhalt (EMSA), welches gemeinsam mit den Freistaaten Sachsen und Thüringen betrieben wird.

Hinsichtlich der zukünftigen Aufstellung der IT-Ressortpläne wurde der Landesbeauftragte im Februar 2009 von der Landesleitstelle IT-Strategie (LIS) der Staatskanzlei darüber informiert, dass ein sog. **„IT-Kataster“** geplant wird. Im Rahmen einer Ausschreibung und externen Vergabe dieser Dienstleistung soll mit diesem IT-Kataster eine Datenbanklösung zur Erfassung, Darstellung und anwenderübergreifenden Nutzung von Informationen über alle relevanten IT-Verfahren der Landesverwaltung entwickelt werden. Diese Datenbanklösung soll mandantenfähig gestaltet werden.
Auf Anregung des Landesbeauftragten sind in dem an die LIS einzureichenden IT-Ressortplan bzw. -konzept auch die jeweiligen Maßnahmen zum Datenschutz und Datensicherheit darzustellen. Diese Informationen wären für den Landesbeauftragten natürlich von besonderem Interesse und ständen ihm zeitnah und aktuell zur Verfügung, ohne den Ressorts zusätzlichen Aufwand zu bereiten. Voraussetzung bildet natürlich die Umsetzung der geplanten anwenderübergreifenden Nutzung.
Der Landesbeauftragte bittet deshalb die Staatskanzlei, bei der Entwicklung dieses IT-Katasters eine solche Nutzungsmöglichkeit für ihn zu berücksichtigen.
Natürlich entbindet dies die Ressorts nicht von ihrer gesetzlichen Unterrichtungspflicht gemäß § 14 Abs. 1 Satz 2 DSG-LSA. Es würde aber unnötige Nachfragen vermeiden helfen und zusätzliche Berichterstattungen an den Landesbeauftragten auf ein Minimum beschränken, wenn ihm mittels des Zugangs zum IT-Kataster diese Informationen aktuell zur Verfügung stehen würden.

4.6. Masterplan Landesportal Sachsen-Anhalt 2007-2011

Aufbauend auf dem „Grundkonzept eGovernment in Sachsen-Anhalt“ wurde ein eGovernment-Aktionsplan für die Landesverwaltung für die Jahre 2004-2010 erarbeitet. Nach der Systematik dieses Aktionsplans wurde das Landesportal Sachsen-Anhalt (LPSA) als Basiskomponente (Nr. 1) eingestuft, da es den Anforderungen eines Dienstleistungsportals bereits in beachtlichen Ansätzen gerecht wurde. Im Leitprojekt Internetportal wurden zahlreiche Online-Dienstleistungen zusammengefasst, die unter Federführung der Staatskanzlei umgesetzt und in das Landesportal eingebunden werden sollen (vgl. Beschluss der Landesregierung vom 26. September 2006 zum Masterplan Landesportal Sachsen-Anhalt). Der Landesbeauftragte hatte bereits in seinem VIII. Tätigkeitsbericht unter Ziff. 4.2 ausführlich dazu berichtet.

Die Landesregierung beabsichtigt, das Landesportal zum zentralen Einstiegspunkt zu allen Dienstleistungen des Landes auszubauen. Es wird weit über eine reine Informationsplattform hinaus verstärkt transaktionsorientierte

Dienstleistungen gebündelt anbieten. Mit diesem Ziel kommuniziert eng die Bereitstellung der Basiskomponenten

- Geodatenserver
- Zahlungsverkehrsplattform
- Formularserver
- elektronische Signatur/virtuelle Poststelle.

Dass diese Basiskomponenten erhebliche datenschutzrechtliche Relevanz besitzen und bei ihrer weiteren Gestaltung der Landesbeauftragte gem. § 14 Abs. 1 Satz 2 DSG-LSA zur Wahrnehmung seines gesetzlichen Beratungs- und auch Kontrollauftrages rechtzeitig zu beteiligen ist, versteht sich von selbst. Der Landesbeauftragte hatte in diesem Zusammenhang mehrfach, auch im VIII. Tätigkeitsbericht in Ziff. 4.2, entsprechende Appelle an die Landesregierung und an die für die einzelnen Basiskomponenten verantwortlichen Fachministerien gesandt.

Gleiches gilt im Übrigen auch für die zahlreichen im Rahmen der eGovernment-Initiative umzusetzenden Leitprojekte, die für den Masterplan Landesportal von Relevanz sind. Das sind, neben dem o. g. Internetportal www.sachsen-anhalt.de, die Leitprojekte

- elektronische Steuererklärung/ELSTER
- Geoinformationsdienste
- elektronisches Grundbuch
- elektronisches Mahnverfahren
- elektronische Vergabe- und Beschaffung
- Internetgestützte Einsicht in die Handels-, Genossenschaft- und Partnerschaftsregister
- zentrale Stellenbörse
- Bürgerinformationssystem der Landesverwaltung
- IBA-Stadt-Monitor
- sowie das nachträglich als Leitprojekt qualifizierte Sperrinformationssystem

mit sehr unterschiedlichem Realisierungsstand, die je nach Entwicklungsfortschritt in das Landesportal eingebunden werden. Der Landesbeauftragte hat bei vielen Projekten im Rahmen seiner Zuständigkeit mitgearbeitet und wertvolle Hinweise zu datenschutzrechtlichen Verbesserungen geben können.

4.7. Umsetzung der EU-Dienstleistungsrichtlinie in Sachsen-Anhalt

In Sachsen-Anhalt koordiniert das Ministerium für Wirtschaft und Arbeit die inhaltliche Umsetzung der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über die Dienstleistungen im Binnenmarkt (ABl. EU Nr. L 76 S. 36) (**EU-Dienstleistungsrichtlinie** - EU-DLR). Für die IT-Umsetzung der EU-DLR ist das Ministerium des Innern verantwortlich. Nach einer Abstimmung des Ministeriums für Wirtschaft mit dem Ministerium des Innern wurde auf der Grundlage einer vom Ministerium für Wirtschaft und Arbeit abgegebenen Empfehlung durch Kabinettsbeschluss am 23. September 2008 als **Einheitlicher Ansprechpartner** (EA) nach Art. 6 der EU-DLR das Landesverwaltungsamt bestimmt.

Der Landesbeauftragte hatte zuvor das Ministerium für Wirtschaft und Arbeit bereits im April 2008 über den Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Umsetzung des Binnenmarktinformationssystems IMI (Internal Market Information System) vom 3. und 4. April 2008 **(Anlage 14)** in Kenntnis gesetzt und sich gleichzeitig für die seit August 2007 erfolgten, regelmäßigen Informationen zum IMI bedankt. Der Wirtschaftsminister hatte im Mai 2008 positiv auf das Angebot des Landesbeauftragten zur Mitarbeit in der Projektgruppe zur Umsetzung der EU-DLR reagiert und den Landesbeauftragten über die weitere Vorgehensweise zur Umsetzung der EU-DLR und zugleich über den Sachstand bei der Umsetzung des IMI informiert.

Sowohl die Umsetzung der EU-DLR als auch des IMI waren Gegenstand intensiver Beratungen des Arbeitskreises „Grundsatzfragen der Verwaltungsmodernisierung“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder. Datenschutzrechtliche Grundanforderungen bei der Umsetzung der EU-DLR und insbesondere für den EA wurden von diesem Arbeitskreis erarbeitet und von der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 zustimmend zur Kenntnis genommen. Diese Ausarbeitung zu datenschutzrechtlichen Anforderungen hat der Landesbeauftragte ebenfalls dem Ministerium für Wirtschaft und Arbeit zur Verfügung gestellt.

Eine erste Beratung der Unterarbeitsgruppe „Einheitlicher Ansprechpartner“ (UAG EA) unter Beteiligung des Landesbeauftragten hat am 12. März 2009 stattgefunden. Schwerpunkt der Beratung des Ministeriums für Wirtschaft über diese Sitzung hinaus bildet zum gegenwärtigen Zeitpunkt der vom Ministerium erarbeitete Entwurf des Gesetzes über den einheitlichen Ansprechpartner in Sachsen-Anhalt (EAG LSA).
Die Überprüfung der datenschutzrechtlichen Ausgangssituation unter Berücksichtigung der Verortung des EA beim Landesverwaltungsamt in Halle lässt eine spezifische normative Regelung zum Datenschutz im Entwurf des EAG LSA als nicht unbedingt notwendig erscheinen. Die Aufgaben des EA sind bereits im Verwaltungsverfahrensrecht geregelt. Zu beachten ist insofern der § 3 Abs. 4 DSG-LSA. Danach gehen die Bestimmungen des DSG-LSA denen des Verwaltungsverfahrensgesetzes des Landes vor, wenn bei der Ermittlung des Sachverhaltes personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Der EA unterliegt als öffentliche Stelle des Landes (§ 2 Abs. 8 DSG-LSA) ohnehin den Bestimmungen des DSG-LSA. Inwieweit darüber hinaus spezielle Regelungen zur Ausgestaltung der Rolle des EA in seiner Vermittler- bzw. Koordinierungsfunktion erforderlich sind, kann durch den Landesbeauftragten zum gegenwärtigen Zeitpunkt nicht beurteilt werden.

Das dem Landesbeauftragten zur Stellungnahme im Januar 2009 vorgelegte „Konzept zur Einführung des elektronischen Binnenmarktinformationssystems (Internal Market Information System - IMI) nach der Europäischen Dienstleistungsrichtlinie“ mit der Vorzugsvariante „Kombinationsmodell“ wurde in Version 1.3 (Stand: 9. April 2009) um eine weitere Variante, dem „Koordinierungsmodell“ als neue Vorzugsvariante, erweitert. Mit Kabinettsbeschluss vom 12. Mai 2009 wurde die Umsetzung dieses Konzepts mit der

Vorzugsvariante „**Koordinierungsmodell**“ verbindlich für das IMI-Basismodul EU-DLR festgelegt. Als IMI-Behörden werden nach diesem Modellvariante die Landkreise und kreisfreien Städte registriert, soweit sie fachlich oder fachaufsichtlich zuständig sind. Andere Zuständigkeiten werden ebenfalls berücksichtigt, so dass ergänzend auch Kammern und Gerichte registriert werden. Gegenüber dem vorher favorisierten Kombinationsmodell entfällt hier beim Koordinierungsmodell der zentrale Eingang von Anfragen bei einer registrierten zentralen Behörde.

Auch das Ministerium des Innern hat den Landesbeauftragten bei der IT-Umsetzung der EU-DLR rechtzeitig durch die Übergabe eines Grobkonzepts (Stand: 27. Oktober 2008) informiert. Am 23./24. Februar 2009 hat hierzu ein Workshop zum Kommunikationskonzept der IT-Umsetzung der EU-DLR unter Beteiligung des Landesbeauftragten stattgefunden. Der Ständige Staatssekretärsausschuss „Informationstechnologie“ hat dem nunmehr vorgelegten IT-Umsetzungskonzept zur EU-DLR des Ministeriums des Innern (Stand: 8. April 2009) zugestimmt.
Für diese Lösung werden sowohl Basiskomponenten gemäß Rahmenvereinbarung zwischen dem Land Sachsen-Anhalt und den Kommunen genutzt, aber auch in anderen Ländern bereits bestehende Lösungen wie z. B. das Elektronische Gerichts- und Verwaltungspostfach (EGVP). Neu beschafft werden müssen für das Service-Portal das Registrierungs- und das Authentifizierungsmodul sowie das Fallmanagement für den EA und die zuständige Stelle (jeweilige entscheidungsbefugte Fachbehörde).
Damit ist die IT-Umsetzung der EU-DLR bis zur Umsetzungsfrist (31. Dezember 2009) möglich.

Der Landesbeauftragte ist gerne bereit, zu gegebener Zeit weiterhin das Ministerium für Wirtschaft und Arbeit und den interministeriellen Arbeitskreis Umsetzung der EU-DLR und dessen UAG EA sowie und das Ministerium des Innern bei der IT-Umsetzung der EU-DLR beratend zu unterstützen, insbesondere im Hinblick auf die technische Umsetzung (Datensicherheitsziele gemäß § 6 Abs. 2 DSG-LSA).

4.8. Umsetzung des Binnenmarktinformationssystems IMI

Das Binnenmarktinformationssystem IMI (Internal Market Information System) stellt ein mehrsprachiges System (Datenbank) zum Austausch von Informationen zwischen den EU-Mitgliedsstaaten untereinander sowie mit der Europäischen Kommission dar. Die Europäische Kommission betreibt dieses System und stellt es den EU-Mitgliedsstaaten kostenlos zur Verfügung. Zur Umsetzung der Richtlinie 2005/36/EG des Europäischen Parlaments und des Rates vom 7. September 2005 über die Anerkennung von Berufsqualifikationen (ABl. EU Nr. L 255 S. 22) - Berufsanerkennungsrichtlinie - wurde dieses System auch in Sachsen-Anhalt mit vier Pilotberufen getestet. Im Zeitraum März bis August 2008 wurden insgesamt 150 Anfragen über das IMI-System verschickt. Nach einer erfolgreichen Testphase sollen sämtliche Berufe, die unter die Berufsanerkennungsrichtlinie fallen, in das IMI integriert werden, so das Ministerium für Wirtschaft und Arbeit in seiner Information.
Die Landesregierung traf am 18. September 2007 in einem Kabinettsbeschluss Regelungen zur Einführung des IMI im Rahmen der Umsetzung der

Berufsanerkennungsrichtlinie. Dem Landesinformations-Zentrum (LIZ) wurde die Aufgabe des IMI-Koordinators für technische Fragen übertragen. IMI-Koordinatoren für fachliche Fragen sind die Ministerien im Rahmen ihrer Zuständigkeit für die von der Berufsanerkennungsrichtlinie erfassten Berufsgruppen.

Bereits im Februar 2008 informierte das Ministerium für Wirtschaft und Arbeit den Landesbeauftragten über das IMI.
Der Landesbeauftragte seinerseits unterrichtete das Ministerium für Wirtschaft und Arbeit im April 2008 über den Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2009 in Berlin zur Umsetzung des Binnenmarktinformationssystems IMI **(Anlage 14).** Die Forderung, das IMI-System auf eine tragfähige Rechtsgrundlage zu stellen, besteht auf europäischer Ebene nach wie vor. Der Landesbeauftragte verweist hierzu nochmals auf die Stellungnahme des Europäischen Datenschutzbeauftragten zur Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarkinformationssystems (IMI) (2008/49/EG) (ABl. EU Nr. C 270/1 vom 25. Oktober 2008).

Nach der Stellungnahme des Europäischen Datenschutzbeauftragten und Gesprächen mit Datenschutzbeauftragten und der Art. 29 Arbeitsgruppe hat man sich jetzt auf einen Kompromiss geeinigt.
Mit Hilfe des Europäischen Datenschutzbeauftragten hat die Europäische Kommission Datenschutzleitlinien für das Binnenmarktinformationssystem IMI entwickelt. Diese Datenschutzleitlinien sind von der Europäischen Kommission am 26. März 2009 angenommen worden. Spätestens nach neun Monaten (bis zum 26. Dezember 2009) sollen alle EU-Mitgliedsstaaten aufgrund der im Rahmen der Pilotphase gesammelten Erfahrungen Rückmeldungen zu den Datenschutzleitlinien und zu deren praktischer Anwendbarkeit geben. Die Europäische Kommission wird danach in einem zweiten Schritt einen Bericht zu den bisherigen Erfahrungen erstatten, welcher im 1. Quartal 2010 angenommen werden soll. Der Inhalt des Berichts wird eine datenschutzrechtliche Bewertung beinhalten, nach der dann entschieden werden soll, ob noch verbindliche EU-Rechtsvorschriften zum IMI-System erlassen werden müssen.

Der Landesbeauftragte hat daraufhin die Situation mit dem Ministerium für Wirtschaft und Arbeit im April 2009 erörtert und als datenschutzrechtliche Grundlage für die Erhebung und Verarbeitung personenbezogener Daten im IMI-System eine modifizierte informierte Einwilligung gemäß § 4 Abs. 2 DSG-LSA empfohlen. Dieser Empfehlung ist das Ministerium für Wirtschaft und Arbeit gefolgt und hat alle beteiligten IMI-Behören des Landes entsprechend informiert.

4.9. Geodateninfrastrukturgesetzgebung in Sachsen-Anhalt

Bereits Ende April 2003 hatte die Landesregierung das „Grundkonzept eGovernment in Sachsen-Anhalt“ beschlossen. Ziel des vorgesehenen 7-Jahre-Aktionplans, der bis zum Jahr 2010 gilt, ist das Bereitstellen verschiedener Basiskomponenten, zu denen auch ein Geo- und Metadatenserver gehört.

Die Basiskomponenten dienen der Umsetzung der 23 eGovernment-Leitprojekte. Eines dieser Leitprojekte, das Leitprojekt Nr. 9, ist die Bereitstellung von Geoinformationsdiensten, zu denen u. a. die Bereitstellung von Geobasisinformationen zählt (vgl. VII. Tätigkeitsbericht, Ziff. 7.1). Verantwortlich für die Bereitstellung von Geobasisinformationen ist das Landesamt für Vermessung und Geoinformation als Vermessungs- und Geoinformationsbehörde des Landes nach dem Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt.
Mit der Richtlinie 2007/2/EG des Europäischen Parlamentes und des Rates vom 14. März 2007 (ABl. L 108/1 vom 25.4.2007) zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE – Infrastructure for Spatial Information in the European Community) war den Mitgliedsstaaten aufgegeben worden, bis zum 14. Mai 2009 Vorschriften in Kraft zu setzen, die die Schaffung und den Betrieb eines Netzes für Geodatensätze und -dienste rechtlich regeln.
Zunächst begann der Bund, dem durch Erarbeitung des Entwurfes eines Geodatenzugangsgesetzes (GeoZG) nachzukommen. Unbeeindruckt von jeglicher Kritik schränkt das im Februar 2009 in Kraft getretene GeoZG zur Umsetzung der INSPIRE-Richtlinie den Schutz personenbezogener Daten stärker ein, als dies durch die INSPIRE-Richtlinie gefordert war. Während die INSPIRE-Richtlinie die Vertraulichkeit personenbezogener Daten bereits vor jeder **nachteiligen Auswirkung** durch den Zugang der Öffentlichkeit zu Geodatensätzen und -diensten schützt (Art. 13 Abs. 1 INSPIRE-Richtlinie), greift der Schutz des Einzelnen nach § 12 Abs. 2 GeoZG (BGBl. I S. 278) i. V. m. §§ 8, 9 Umweltinformationsgesetz erst bei einer **erheblichen Beeinträchtigung** seiner personenbezogenen Daten. Dies ist vor allem vor folgendem Hintergrund kritisch zu sehen: Geodaten sind Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet. Entsprechend georeferenzierte Angaben beliebiger Art können aufgrund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten schnell zu sensiblen personenbezogenen Daten werden. Dies kann entsprechende Schutz- und Abwehransprüche Betroffener auslösen.
Leider wurde der Aufforderung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in der Entschließung „Datenschutzgerechter Zugang zu Geoinformationen“ vom 6./7. November 2008 **(Anlage 19)** im Zuge des Gesetzgebungsverfahrens einen angemessenen Ausgleich zwischen den Informations- und den Schutzinteressen zu schaffen und wenigstens die „mageren“ Mindestvorgaben der INSPIRE-Richtlinie zu beachten, nicht Rechnung getragen.

Wesentlich datenschutzfreundlicher war dagegen der dem Landesbeauftragten im Berichtszeitraum vorgelegte **Entwurf eines Geodateninfrastrukturgesetzes für das Land Sachsen-Anhalt** (GDIG LSA). Dieser Gesetzentwurf beruht auf den unter Beteiligung von Sachsen-Anhalt erarbeiteten Musterempfehlungen für die Geodateninfrastrukturgesetzgebungen in den Ländern. Das Gesetz soll den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten grundsätzlich zwar erlauben. Es beschränkt ihn aber, datenschutzrechtlich viel wirkungsvoller als das GeoZG, u. a. genau dann, wenn durch den Zugang zu Geodaten personenbezogene Daten offenbart und damit schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Der Landesbeauftragte wurde bei der Erarbeitung des Gesetzentwurfs frühzeitig

durch das federführende Innenministerium beteiligt und konnte Änderungsempfehlungen abgeben (LT-Drs. 5/1786).
So hatte sich der Landesbeauftragte gegenüber dem Ministerium des Innern beispielsweise dafür eingesetzt, den Geltungsbereich des § 10 GDIG LSA auszudehnen. § 10 GDIG LSA regelt den Schutz öffentlicher und sonstiger Belange, darunter auch die Belange des Datenschutzes. Im ersten Entwurf des GDIG LSA sollten diese Vorschriften zum Schutz öffentlicher und sonstiger Belange in Anlehnung an die INSPIRE-Richtlinie nach § 4 Abs. 2 GDIG LSA ausschließlich auf die sog. Referenzversionen von Geodaten beschränkt werden, also auf die Ursprungsversion eines Datenbestandes. Da aber auch von bei anderen Behörden gespeicherten Kopien dieser Daten Beeinträchtigungen öffentlicher und sonstiger Belange ausgehen könnten, hatte der Landesbeauftragte dringend dazu geraten, den Geltungsbereich des § 10 GDIG LSA auch auf diese Daten auszudehnen.

Leider zunächst nicht durchsetzen konnte er sich in Bezug auf die Ausdehnung des Geltungsbereichs des GDIG LSA auf Geodaten der Kommunen, deren elektronische Erfassung und Bereitstellung gesetzlich nicht explizit vorgeschrieben ist, sondern auf freiwilliger Basis erfolgt. Er teilte dem Innenausschuss des Landtags im Rahmen der Anhörung zum GDIG LSA mit, dass er es begrüßen würde, wenn eine Formulierung des § 4 Abs. 4 GDIG LSA gewählt würde, die einerseits der Intention des Ministeriums des Innern entspräche, eine neue Kostenerstattungspflicht des Landes gegenüber den Kommunen zu verhindern, andererseits aber den Geltungsbereich des GDIG LSA - insbesondere des § 10 GDIG LSA - auch auf die genannten Daten erstreckte. Dadurch wäre der Schutz öffentlicher und sonstiger Belange, für alle Fälle geregelt in § 10 GDIG LSA, aus einem Guss. Der Datenschutz ist, darauf wies der Landesbeauftragte das Innenministerium und später den Innenausschuss hin, z. B. neben dem Schutz von Betriebs- und Geschäftsgeheimnissen nur eine der denkbaren Beeinträchtigungen öffentlicher und sonstiger Belange durch den Zugang der Öffentlichkeit zu Geodaten und Geodatendiensten.
Das Ministerium des Innern unterstützt jedoch in diesem Zusammenhang den Vorschlag des Landesbeauftragten, Art und Umfang der von Kommunen außerhalb des Anwendungsbereiches des GDIG LSA gespeicherten Geodaten feststellen zu lassen. So könnte ermittelt werden, wie dringlich eine eigenständige Regelung für diesen Datenbestand wäre.

Auch im nicht-öffentlichen Bereich entsteht weitergehender Schutzbedarf bei der Veröffentlichung georeferenzierter Dienste im Internet durch digitale Bildaufnahmen von Straßenpanoramen. Zunächst haben hierzu die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im November 2008 den Beschluss „Datenschutzrechtliche Bewertung von digitalisierten Straßenansichten, insbesondere im Internet“ gefasst **(Anlage 38).** Auch im Rahmen solcher **Street-View-Projekte** ist die Wahrung der Persönlichkeitsrechte der Betroffenen sicherzustellen (Information, Widerspruchsrecht, Datenlöschung auch der Rohdaten). Gegenüber Google wurden durch den zuständigen Hamburgischen Datenschutzbeauftragten entsprechende Maßnahmen erwirkt.

4.10. Mehr Befugnisse für das BSI

Durch den am 14. Januar 2009 vom Bundeskabinett beschlossenen Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BT-Drs. 16/11967) wird das Bundesamt für Sicherheit in der Informationstechnik (BSI) in die Lage versetzt, Angriffe auf Bundesbehörden abwehren zu können. Dem BSI wird damit ermöglicht, die Datenströme der Bundesbehörden zu scannen, aufzuzeichnen und gesammelte Daten an Verfassungsschutz sowie die Polizei weiterzureichen. Parallel dazu werden Änderungen des Telemediengesetzes und des Telekommunikationsgesetzes vorgenommen (vgl. Ziff. 24.4).

Der Entwurf des BSI-Gesetzes enthielt keine datenschutzgerechten Regelungen. Wenn es z. B. erlaubt werden soll, ein- und ausgehende Daten des Bundes auf Viren zu untersuchen, dann hätte dies auch im Gesetz formuliert werden müssen. Die Regelung, dass das BSI im Rahmen der Schadsoftwarebekämpfung *„die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten“ darf,* ist zu allgemein formuliert, und so ist es nicht verwunderlich, dass dieses Gesetz weiterhin aus den Reihen der Internetgemeinschaft, von Datenschutzbeauftragten und auch Berufsverbänden kritisiert wird.
Auch die im Gesetzgebungsverfahren durch Berücksichtigung der Empfehlungen des Innenausschusses des Bundestages (BT-Drs. 16/13259 vom 29. Mai 2009) eingeflossenen leichten Verbesserungen u. a. wie:

- Möglichkeit der Pseudonymisierung erfasster Daten (§ 5 Abs. 2),
- Regelungen zur Benachrichtigung der von einer Datenübermittlung Betroffenen sowie Dokumentation bei Nichtbenachrichtigung (§ 5 Abs. 4),
- Einschränkung der Übermittlungsbefugnisse des BSI auf die Katalogstraftaten (§§ 202a, 202b, 303a, 303b StGB),
- Richtervorbehalt bei der Übermittlung von Daten zu sonstigen Zwecken (§ 5 Abs. 6) bei der Strafverfolgung und der Gefahrenabwehr,
- Beweisverwertungsverbot für zeugnisverweigerungsberechtigte Berufsgruppen sowie verbesserter Schutz des Kernbereichs privater Lebensgestaltung (§ 5 Abs. 7),
- Kalenderjährliche Benachrichtigungspflichten des BSI an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Innenausschuss des Bundestages (§ 5 Abs. 9) und
- Rechtzeitige Information zu Sicherheitslücken an Hersteller (§ 7 Abs. 1)

ändern nichts an der grundsätzlichen Kritik an diesem Gesetz.

Mögliche Eingriffe in die Grundrechte von Bürgerinnen und Bürgern durch zu umfangreiche Befugnisse für eine Behörde stellen eine Gefahr für Demokratie und Rechtsstaat dar. Die Datenschutzbeauftragten des Bundes und der Länder forderten deshalb in der Entschließung vom 18. Februar 2009 „Stärkung der IT-Sicherheit - Aber nicht zu Lasten des Datenschutzes!“ **(Anlage 26)** konkrete Nachbesserungen für den damaligen Entwurf des BSI-Gesetzes.
Im Gesetz wurden leider nicht alle Forderungen dieser Entschließung umgesetzt, um bei Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und den Datenschutz der Nutzerinnen und Nutzer umfassend zu gewährleisten.

Der Bundesrat hat mit seinem Beschluss vom 10. Juli 2009 (BR-Drs. 578/09) den Gesetzentwurf gebilligt. Er will das Gesetzgebungsvorhaben nicht verzögern, gleichzeitig die Interessen der Länder wahren und erwartet eine Beteiligung in wichtigen Bereichen.

4.11. Bürgerportale und De-Mail

Die Bundesregierung plant, durch die Errichtung von Bürgerportalen eine zur herkömmlichen E-Mail-Kommunikation alternative Methode der Kommunikation zu schaffen. Vorteil soll die sichere Zustellung nach dem Vorbild der herkömmlichen Papierpost sein. Es sollen also bspw. Einschreiben und Einschreiben mit Rückschein auf elektronischem Wege möglich werden. Nutzer eines Bürgerportals sollen eine De-Mail-Adresse erhalten, über welche mit anderen De-Mail-Nutzern kommuniziert werden kann. Übertragungen sollen verschlüsselt erfolgen, so dass das Manko der normalen E-Mail-Übertragungen - die grundsätzliche Unsicherheit, sofern alle beteiligten Nutzer nicht durch Verschlüsselungsmaßnahmen gemeinsam Vorkehrung treffen - behoben wird. Schnittstellen zum Internet, sogenannte Gateways, soll es nach aktueller Planung nicht geben, so dass auch kein SPAM von außen ins De-Mail-Netz gelangen können soll. Sinn der De-Mails ist die Schaffung eines medienbruchfreien und kostengünstigen Kommunikationsweges zwischen Verwaltung und Bürger (BT-Drs. 16/12598).

Die Intention, die Schaffung einer sicheren Kommunikationsmöglichkeit per E-Mail, ist sinnvoll und wird begrüßt. Über Stellungnahmen zu Gesetzentwürfen, z. B. dem des Bundesmeldegesetzes, wurde versucht, an Verbesserungen mitzuarbeiten. Dabei traten immer mehr Kritikpunkte zu Tage. Die Realisierung als Webportal ist zwar einfach möglich, erlaubt jedoch nur mit unverhältnismäßig hohem Aufwand oder unter Komforteinbußen eine Ende-zu-Ende-Verschlüsselung. Es ist unverständlich, warum nicht herkömmliche Standards weiterentwickelt werden. Solche existieren bereits und deren Nutzung würde sogar eine Ende-zu-Ende-Verschlüsselung erlauben. Stattdessen soll eine neue E-Mail-Form geschaffen werden. Eine De-Mail-Adresse muss genauso wie normale E-Mails mit einem E-Mail-Client abrufbar sein. Dies ist derzeit nicht vorgesehen. Der Zwang, sich täglich in Erwartung neuer Post zusätzlich an einem Web-Mail-Portal anzumelden, könnte dafür sorgen, dass De-Mails nicht akzeptiert werden.

Für die sichere und authentische elektronische Kommunikation mit Einwilligung des Betroffenen wird die elektronische Bürgeradresse, die De-Mail, erfasst. Mit Hilfe des elektronischen Personalausweises soll eine sichere Kommunikation in Bürgerportalen ermöglichen werden. Das bedeutet jedoch nicht, dass der Bürger dadurch erreichbar ist und die De-Mails auch aktiv liest. Viele Nutzer werden De-Mails nur für gelegentliche Behördenkommunikation verwenden, jedoch nicht regelmäßig die Nachrichten abfragen, da dazu keine automatisierbaren Abfrageprotokolle geplant sind und nur Bürgerportale den Zugang gewähren werden.

Die Konferenz der Datenschutzschutzbeauftragten des Bundes und der Länder wies in einer Entschließung vom 16. April 2009 „Datenschutz beim vor-

gesehenen Bürgerportal unzureichend“ **(Anlage 31)** darauf hin, dass der Gesetzentwurf noch Mängel aufwies, welche zu korrigieren sind. Forderungen wie eine verschlüsselte Ende-zu-Ende-Kommunikation nach dem Stand der Technik sind darin ebenso enthalten wie die nach optionaler Pseudonymnutzung oder grundsätzlich sicherer Anmeldung am Portal, ohne ausschließlich auf Passwörter zu setzen. Die Umsetzung dieser Forderungen hat direkte Auswirkungen auf die Sicherheit und Akzeptanz von Bürgerportalen und darf deshalb nicht ignoriert werden.

Der Bundestag vertagte die Initiative; im Rahmen einer Gesamtstrategie zu Datenschutz und Sicherheit in eGovernment und eBusiness soll auch das Projekt De-Mail fortgesetzt werden.

Ob Web-Portale wirklich eine Alternative zu normalen E-Mails werden können, ist noch völlig offen, da hier eine Technologie genutzt wird, welche nicht nur Vor-, sondern auch Nachteile bei der Nutzung bietet. Nutzer müssen ein Web-Portal nutzen, um auf De-Mails zugreifen zu können. Ein Nutzen des Zugangs mit einem E-Mail-Programm unter Verwendung von Standard-Protokollen ist somit nicht möglich. Warum werden nicht herkömmliche Methoden für sichere Mail-Kommunikation wie PKI-basierte Zertifikate in Verbindung mit standardisierten E-Mail-Übertragungsprotokollen eingesetzt? Das würde die Akzeptanz deutlich verbessern und die Verbreitung von Zertifikat-basierten Sicherheitsfunktionen erhöhen.

5. Archivwesen

5.1. Akten ehemaliger politischer Häftlinge in einer Gedenkstätte

Seit Januar 2007 werden Gedenkstätten durch die Gedenkstättenstiftung des Landes verwaltet. Die Vertreter der Stiftung und einer Gedenkstätte baten den Landesbeauftragten um Beratung hinsichtlich solcher Unterlagen, die ihnen ehemalige Häftlinge für die Gedenkstättenarbeit zur Verfügung gestellt hatten. Es handelte sich dabei um Unterlagen zur Inhaftierung der Betroffenen, insbesondere Vorgänge, die den Betroffenen von der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik überlassen wurden. Die Unterlagen wurden der Gedenkstätte für ihre Arbeit auf der Grundlage einer besonderen Vertrauensbeziehung zur Verfügung gestellt. Konkrete schriftliche Vereinbarungen mit ehemaligen Häftlingen zur Verwendung gab es nicht. Jedoch sei stets mündlich vereinbarte Voraussetzung gewesen, dass den Unterlagen größtmöglicher Schutz nach bestem Gewissen zukommen solle. Die Unterlagen durften nur für die interne Arbeit der Gedenkstätte verwendet werden. Gegebenenfalls war auch eine Weitergabe an andere Personen zugestanden worden, jedoch nur nach schriftlicher Rückfrage und schriftlicher Erklärung der Betroffenen.

Nunmehr sollte über die Frage der weiteren sicheren Aufbewahrung nachgedacht werden. Dabei war u. a. an die Einbeziehung eines privaten Wachdienstes gedacht worden.

Seitens des Landesbeauftragten wurde darauf hingewiesen, dass nach der Darstellung von einer Depositalvereinbarung im Sinne des § 5 des Archivgesetzes als Geschäftsgrundlage der zur Verfügungstellung der Akten ausgegangen werden kann. Die Vorgaben und der gewünschte Vertrauensschutz sind auch dann zu berücksichtigen, wenn keine konkrete schriftliche Vereinbarung vorliegt. Dies war bisher so geschehen. Demgemäß hätte bei einer gravierenden Abweichung im Umgang mit den Unterlagen eine Information an die auf die Einhaltung der Geschäftsgrundlage vertrauenden Depositalgeber erfolgen müssen.

Eine im Hinblick auf die besondere Sensibilität der Unterlagen kritische Veränderung wäre der mögliche Zugang von Dritten zu den Akten gewesen. Während der Beratung konnten Hinweise zum technisch-organisatorischen Datenschutz, insbesondere zur Einrichtung und Ausstattung des Gebäudekomplexes der Gedenkstätte gegeben werden. Die Einschaltung eines privaten Wachdienstes mit Zugang zu den Vorgängen wurde verworfen.

5.2. Ausstellung in der Gedenkstätte „Roter Ochse“

Die Dauerausstellungen Politische Justiz | 1933-1945 | 1945-1989 in der Gedenkstätte „Roter Ochse“ in Halle/Saale fanden besondere Beachtung in der Öffentlichkeit. Einige ehemalige hauptamtliche Mitarbeiter des Ministeriums für Staatssicherheit (MfS), die in der Ausstellung namentlich und auch mit Bild aufgeführt waren, hatten den Landesbeauftragten um datenschutzrechtliche Prüfung gebeten.

In die Bewertung wurden Erkenntnisse aus Stellungnahmen der Gedenkstätte „Roter Ochse“, der Stiftung Gedenkstätten Sachsen-Anhalt und des Landesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (LStU) sowie eines Besuches vor Ort einbezogen. Zudem erfolgte eine Beratung mit dem Justitiariat der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (BStU).

Die Ausstellung von ausgewählten personenbezogenen Informationen zu hauptamtlichen Mitarbeitern der Untersuchungsabteilung IX des MfS in der Gedenkstätte „Roter Ochse“ war aus datenschutzrechtlicher Sicht vertretbar und nicht unzulässig.

Die Bewertung war durch den gesetzlichen Rahmen auf eine rein datenschutzrechtliche Betrachtung begrenzt. Aspekte der historischen Aufarbeitung, der politischen Bildung oder der Didaktik wurden daher nur in diesem Zusammenhang einbezogen.

Die Veröffentlichung personenbezogener Daten stellt zwar grundsätzlich einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung und damit das Persönlichkeitsrecht dar. Dieser war jedoch verfassungsrechtlich gerechtfertigt.

Als Rechtsgrundlage der Verwendung der personenbezogenen Daten griff die Regelung des § 32 Abs. 3 Nr. 2 des Gesetzes über die Unterlagen des

Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (StUG). Diese Auffassung wurde vom LStU und von der BStU geteilt.

Danach dürfen Unterlagen des Staatssicherheitsdienstes für Zwecke der politischen und historischen Aufarbeitung und für Zwecke der politischen Bildung (§ 32 Abs. 1 StUG) von der BStU zur Verfügung gestellt und nach § 32 Abs. 3 StUG veröffentlicht werden, soweit es sich um Mitarbeiter - auch inoffizielle - des Staatssicherheitsdienstes handelt. Nach der gesetzlichen Vorgabe war es daher zunächst nicht erforderlich, sich bei der Verwendung auf Informationen zu hochrangigem Führungspersonal zu beschränken. Die Ausstellung beschränkte sich allerdings auf einige ehemals hauptamtlich Tätige, die in den 50er bis 80er Jahren als Vernehmer tätig waren.

Nach § 32 Abs. 3 S. 2 StUG dürfen durch die Veröffentlichung aber keine überwiegenden schutzwürdigen Interessen der genannten Personen beeinträchtigt werden. Dafür lagen in den geprüften Fällen keine hinreichenden Anhaltspunkte vor. Bei der Auslegung und Anwendung dieser Bestimmung hatten die verantwortlichen Stellen die grundrechtliche Position der Petenten nicht verkannt.

Zwar konnte das Bekanntwerden der Tätigkeit in der Untersuchungsabteilung IX einen gewissen Einfluss auf Ansehen und Wertschätzung in der Öffentlichkeit haben. Zudem wurde im erläuternden Begleittext in der Ausstellung allgemein auf Unrecht hingewiesen, das von der Dienststelle ausging.

An der möglichst präzisen Darstellung der Vergangenheit bestand aber ein öffentliches Interesse von erheblichem Gewicht. Dies gibt zudem § 2 Abs. 1 des Gedenkstättenstiftungsgesetzes des Landes Sachsen-Anhalt vor. Auch das Bundesverfassungsgericht hatte die Bedeutung der Aufarbeitung der Tätigkeit des MfS besonders betont (BVerfG Beschluss vom 23. Februar 2000, 1 BvR 1582/94). Auch hier gab aus dokumentarischer Sicht erst die Benennung und die Möglichkeit bildlicher Vorstellung nachhaltigen Einblick in die Einbindung Einzelner in die Funktionen und verlor sich nicht in der Abstraktheit bloßer Zahlen. So wurde das Ziel der politischen Bildung verdeutlicht, dass die Herrschaftsausübung und das Funktionieren eines Verfolgungs- und Repressionsapparates erst durch Individuen gewährleistet werden.

Dem erheblichen öffentlichen Aufklärungsinteresse kam die Ausstellung unter Verwendung nur weniger und verhältnismäßig wenig beeinträchtigender Informationen in einer die Persönlichkeitsinteressen der ehemaligen Mitarbeiter schonenden Weise nach.

Schon die BStU hatte, bevor sie die Informationen zur Verfügung stellte, selbst nach § 32 Abs. 1 StUG zu prüfen, ob überwiegende schutzwürdige Interessen beeinträchtigt würden.
Zudem waren nicht alle Daten veröffentlicht, die von der BStU nach § 32 Abs. 1 StUG zur Verfügung gestellt wurden.
Die Ausstellung verwendete nur dienstliche Tatsachen des beruflichen Werdegangs, Daten der Privat- oder Intimsphäre sind dagegen nicht betroffen.
Steckbriefartige Diffamierungen konnten nicht festgestellt werden. Die abstrakte Tätigkeit für die Untersuchungsabteilung war nicht strafrechtsrelevant;

konkrete, individualisierte Vorwürfe wurden insoweit nicht erhoben. Ausgrenzungen oder Stigmatisierungen waren nicht erkennbar. Der Gefahr einer Gleichsetzung mit nationalsozialistischem Unrecht begegneten die räumliche Trennung und die sachliche, unterschiedliche Darstellung. Damit war dem Gebot Rechnung getragen, nicht nur inhaltlich, sondern auch der Form nach Verletzungen des Persönlichkeitsrechts zu vermeiden.

Mangels einer diffamierenden Darstellung und einer besonderen sozialen Ausgrenzung lagen die Beeinträchtigungen des Persönlichkeitsrechts somit im hinzunehmenden Rahmen.

6. Ausländerangelegenheiten

6.1. Gesetzentwurf zur Errichtung einer Visa-Einlader- und Warndatei

Im Februar 2009 erhielten die Datenschutzbeauftragten des Bundes und der Länder Kenntnis von einem Referentenentwurf des Bundesministeriums des Innern, welcher sich mit der beabsichtigten Errichtung einer Visa-Einlader- und Warndatei befasste.

In der Begründung zum Gesetzentwurf wurde dargelegt, dass Sicherheitsbehörden bei der Auswertung von Ermittlungsverfahren wegen des Verdachts der gewerbs- und bandenmäßigen Schleusung festgestellt hätten, dass sich Netzwerke und Scheinfirmen gebildet hätten, welche im Verdacht stünden, in den vergangenen Jahren Schengen-Visa in einer nicht unerheblichen Zahl erschlichen zu haben. Für die Behörden, welche am Visaverfahren beteiligt sind, sei die Visaerschleichung die am schwierigsten erkennbare Form der Einschleusung von Ausländern.

Zu diesem Zweck sollte eine zentrale Datei aufgebaut werden, welche unter anderem die Daten der Einladenden enthält. Eine weitere Datei sollte Daten zu Personen beinhalten, welche mit rechtswidrigen Handlungen und Verurteilungen im Zusammenhang mit Visaverfahren, Terrorismus, schweren Straftaten oder anderen Delikten mit Auslandsbezug in Beziehung zu bringen seien.

Die Datenschutzbeauftragten des Bundes und der Länder sehen insbesondere in der Einlader-Datei einen unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung, da die Betroffenen ohne jeden Anhaltspunkt auf ein konkretes rechtswidriges Verfahren erfasst würden und auf lange Zeit gespeichert blieben. Damit würde eine weit in das Vorfeld der Abwehr konkreter Gefahren verlagerte verdachtsunabhängige Datenspeicherung entstehen. Mehrfacheinladungen sollen zu Warnhinweisen führen und stellen die Gastfreundschaft so unter Verdacht.

Da insbesondere auch aus dem Bereich der Betroffenen, vor allem den Kirchen und sozialen Organisationen, massive Kritik gegen den Gesetzesentwurf geäußert wurde, zog die Bundesjustizministerin ihre Zustimmung zu dem Gesetzesentwurf kurzfristig zurück.
Damit wurde die Einführung der Visa-Einlader- und Warndatei zumindest in dieser Legislaturperiode unwahrscheinlich.

6.2. Unzulässig gespeicherte Daten im Ausländerzentralregister

Das Bundesamt für Migration und Flüchtlinge, eine dem Bundesministerium des Innern nachgeordnete Bundesbehörde, führt das Ausländerzentralregister (AZR), in welchem personenbezogene Daten derjenigen Ausländerinnen und Ausländer zusammengefasst werden, welche sich nicht nur vorübergehend in der Bundesrepublik Deutschland aufhalten. Ein österreichischer Staatsangehöriger, der bereits seit mehreren Jahren in Deutschland lebt, hatte beantragt, dass seine Daten aus dem AZR gelöscht werden. Dies wurde vom Oberverwaltungsgericht für das Land Nordrhein-Westfalen abgelehnt.

Am 16. Dezember 2008 entschied der Europäische Gerichtshof in einer Vorabentscheidung der Rechtssache C-524/06 (DVBl 2009, 171), dass ein zentrales Ausländerregister nur solche Daten enthalten darf, welche zur Anwendung ausländerrechtlicher Vorschriften unbedingt erforderlich sind. Eine Speicherung und Verarbeitung personenbezogener Daten von Unionsbürgern, die keine Staatsangehörigen des jeweiligen Mitgliedsstaates sind, zu rein statistischen Zwecken entspricht nicht der Erforderlichkeit im Sinn der europäischen Richtlinie zum Schutz der personenbezogenen Daten.
Gleichfalls würde es gegen das Diskriminierungsverbot verstoßen, wenn ein solches Register zur Bekämpfung der Kriminalität geschaffen würde. Die Kriminalitätsbekämpfung bezieht sich zwingend auf die Verfolgung von Verbrechen und Vergehen unabhängig von der Staatsangehörigkeit der Täter. Ein System zur Verarbeitung personenbezogener Daten zum Zweck der Kriminalitätsbekämpfung zu errichten, das nur Unionsbürger erfasst, die keine Staatsangehörigen des jeweiligen Mitgliedsstaates sind, wäre somit unzulässig.

Welche Folgerungen aus der Entscheidung zu ziehen sind - gesetzliche Änderung; Löschung von Daten -, wird noch in Bund und Ländern geprüft.

7. Ausweis- und Melderecht, Personenstandsrecht

7.1. Elektronischer Reisepass (ePass)

Für Reisen ins Ausland werden durch die Bundesrepublik Deutschland Reisepässe, sogenannte Europapässe, ausgegeben. Mit dem Begriff ePass wird ein maschinenlesbares Ausweisdokument bezeichnet. Im Bestreben, den Reisepass sicherer zu gestalten, wurde bereits 2001 das Identigram (holografische und kinegrafische Strukturen) als zusätzliches Sicherheitsmerkmal aufgenommen. Die Sicherheit der ePass-Daten ist unter anderem von der Nutzung der zugrunde liegenden, globalen Public-Key-Infrastruktur (PKI) und des zugehörigen Public-Key-Verzeichnisses (Public Key Directory - PKD) abhängig. Eine solche PKI muss von allen Ländern der Welt genutzt werden, um die maschinenlesbaren Elemente des ePasses international verifizieren zu können. Andernfalls müssten zwischen den einzelnen Ländern bilaterale Abkommen zur elektronischen Ausweisüberprüfung getroffen werden, was ggf. nicht umfassend möglich ist. Das PKD befindet sich noch im Aufbau. Für den britischen ePass ist bereits eine, durch das von der International Civil Aviation Organization empfohlene Prüfgerät unbemerkte Modifikation der auf dem Mikrochip enthaltenen Daten bekannt, welche durch PKI-

Nutzung erkannt worden wäre. Eine Duplizierung ist beim deutschen ePass möglich, wird jedoch als nicht missbrauchsfähig angesehen, so dass auf entsprechende Gegenmaßnahmen (z. B. „Active Authentication“) bewusst verzichtet wurde. Ein unbemerktes Auslesen des ePasses ohne Vorzeigen durch den Inhaber soll aufgrund des „Basic Access Control“-Verfahrens unmöglich sein, da zuvor die maschinenlesbare Zone des Ausweises optisch gelesen wird und daraus Zugriffsdaten für den Chip abgeleitet werden. Jedoch wurde auch dieses Verfahren mit Hilfe von vorab bekannten Informationen zum Inhaber bereits erfolgreich ausgehebelt.

Seit November 2007 werden auf Grundlage eines neuen Passgesetzes (BGBl. I S. 1566) im ePass zusätzlich zum 2 Jahre zuvor eingeführten digitalen Passfoto mit den Abdrücken zweier Finger des Passinhabers weitere biometrische Daten gespeichert. Diese werden (im Gegensatz zum Lichtbild) in den Einwohnermeldeämtern nicht dauerhaft vorgehalten, sondern nur zur Erstellung des Passes verschlüsselt übertragen. In einem TV-Beitrag wurde über eine Unsicherheit des Fingerabdruck-Erfassungssystems in Meldebehörden berichtet und sogar eine auf dem PC installierte Software zur Fälschung dieser Daten gezeigt. Aus diesem Grund wird darauf hingewiesen, dass eine Anbindung der Fingerabdruck-Scanner bzw. zugehöriger PCs an das Internet ein Sicherheitsrisiko darstellt. Die Datenübertragung der Geräte zum PC ist aufgrund der Anzeige- und Kontrollmöglichkeiten auf diesem nicht sinnvoll verschlüsselt realisierbar. Gleichwohl muss ein solcher Rechner auf sichere Art und Weise ins Netzwerk integriert werden. Der Landesbeauftragte rät aufgrund möglicher Hackerangriffe von einer Internetanbindung dieser Rechner ab und wird die Absicherungsmaßnahmen einzelner Meldebehörden näher untersuchen.

Der Landesbeauftragte informierte sich 2008 über die Erfassung der biometrischen Daten in einer Stadtverwaltung. Zur Passantragsbearbeitung wird DIGANT (digitales Antragsverfahren), herausgegeben von der Bundesdruckerei, verwendet. Mittels Scanner werden die Anträge erfasst und zusammen mit Fingerabdrücken und Unterschrift verschlüsselt per E-Mail an die Bundesdruckerei versandt. Zu Verschlüsselungsparametern wurden keine Informationen gegeben. Ein Sicherheitskonzept existierte nicht. Die Einstellungen erfolgten auf Basis von Empfehlungen der Bundesdruckerei und des Herstellers der Software. Rechtevergaben erfolgten nach eigenem Ermessen. Da dieses Verfahren durch Verwendung des XML-basierten Datenaustauschformates XPass auf der Grundlage des Übermittlungsprotokolls OSCI-Transport abgelöst werden sollte, wurde eine nähere Untersuchung des Datenübermittlungsverfahrens vertagt. Die Umstellung erfolgte Ende 2008. Es wurden mehrere hundert Passfotos und Unterschriften in Dateiform teilweise aus dem Juni 2007 vorgefunden. Eine dauerhafte Lagerung nicht mehr erforderlicher, personenbezogener Daten ist aktiv zu unterbinden. Das im Bürgerbüro vorhandene Lesegerät für ePässe war in der Lage, die Besitzerdaten (Name, Vorname, Geburtsdatum usw.), das Passbild und, nach Einstecken einer Signaturkarte der Bundesdruckerei, die Fingerabdrücke (diese ca. im Maßstab 1:1) anzuzeigen. Die Unterschrift wurde nicht angezeigt. Auch fehlte eine Möglichkeit, die digital gespeicherten Fingerabdrücke mit den Fingerabdrücken des Passbesitzers zu vergleichen. Damit lag ein Verstoß gegen § 16 Abs. 6 PassG vor. Die Prüfung der Korrektheit der im ePass enthalte-

nen Daten war nur teilweise möglich. Das Gerät war u. a. nicht mit § 16 Abs. 4 DSG-LSA vereinbar.

Insgesamt macht der ePass keinen sehr sicheren Eindruck. Wünschenswert wäre es, wenn generell der Stand der Technik bei der Realisierung der Anforderungen Anwendung finden und gefundene Sicherheitslücken in einem Nachfolge-ePass sofort geschlossen werden würden.

7.2. Elektronischer Personalausweis (ePA)

Ab November 2010 soll der bisherige Personalausweis durch einen elektronischen Personalausweis im Scheckkartenformat abgelöst werden. Bundestag und Bundesrat ebneten den Weg für ein entsprechendes Gesetz (BT-Drs. 16/10489), das auch aus Sicht der Datenschutzbeauftragten brisant ist. Der ePA soll als hoheitliches Reisedokument dienen, daneben wird er standardmäßig mit einer elektronischen Authentisierungsfunktion ausgestattet sein (freiwillige Anwendung) und schließlich kann er optional ein qualifiziertes elektronisches Signaturzertifikat erhalten (Gesetz vom 18. Juni 2009, BGBl. I S. 1346).

Die bisher nur optisch lesbaren Daten werden elektronisch auslesbar sein, der enthaltene Datenumfang wurde erweitert. Das Lichtbild wird in digitaler Form enthalten sein, um die Identitätsfeststellung bei behördlichen Kontrollen im Inland und an den Grenzen zu unterstützen. Kritisiert wird die optionale, freiwillige und überflüssige Speicherung von zwei Fingerabdrücken im Ausweis. Diese soll der engeren Bindung des Ausweises an den Besitzer dienen. Das biometrische Gesichtsbild und die Daten der zwei Fingerabdrücke sollen drahtlos, ohne autorisierende PIN-Abfrage, auslesbar sein.

Der ePA realisiert die elektronische Authentifizierung im Internet mit Hilfe des sogenannten elektronischen Identitätsnachweises. Ein im ePA enthaltener, fortgeschrittener, elektronischer Signaturschlüssel ohne eigenes Zertifikat ermöglicht die digitale Ausweisfunktion, welche sowohl im eGovernment gegenüber Behörden als auch im Umgang mit privatwirtschaftlichen Dienstleistern eingesetzt werden kann. Der Ausweisinhaber wird sich gegenüber seinem Kommunikationspartner verbindlich ausweisen können (elektronischer Identitätsnachweis). Es wird möglich sein, gezielt nur einzelne, elektronische Identitätsmerkmale zu übermitteln. Der Diensteanbieter muss seinerseits durch Vorlage eines gültigen Zertifikates seine Berechtigung zur Datenerhebung im gewünschten Umfang nachweisen. So kann beispielsweise im Internet oder an Automaten das Alter überprüft werden, ohne dass unnötige Daten (Name, Anschrift, etc.) offenbart werden müssen. Gleichzeitig wird dem Ausweisinhaber garantiert, dass keine unbemerkten Datenabfragen erfolgen können, indem jede Datenweitergabe per Geheimnummer freigegeben werden muss.

Es ist geplant, die technischen und rechtlichen Voraussetzungen zum Aufbringen einer qualifizierten, elektronischen Signatur nach § 2 Nr. 3 Signaturgesetz zu schaffen. Um die drahtlose Nutzung (im Lesegerät) dieser Signatur zu erlauben, soll das Signaturgesetz geändert werden. Leider wird aus Kostengründen auf das generelle zusätzliche Aufbringen und Verwenden eines

qualifizierten, elektronischen Signaturzertifikats verzichtet. Dieses kann lediglich optional und verbunden mit Kosten nachgerüstet werden. Der Bürger wird zur Nutzung der Identitätsfunktion des ePA im Internet aufgefordert. Nur mit einer Authentisierungsfunktion können jedoch weder Signatur noch Verschlüsselung sicher realisiert werden. Mit dem zusätzlichen Aufbringen eines qualifizierten Signaturzertifikats hätte der Staat die Möglichkeit, ein für alle Mal die elektronische Kommunikation in Netzwerken auf eine sichere Grundlage zu stellen. Die Kosten für das Chipkarten-Lesegerät und den neuen Ausweis müssen in beiden Fällen getragen werden. Elektronische Personalausweise mit elektronischem Identitätsnachweis könnten mit nur minimalem Mehraufwand um eine qualifizierte elektronische Signatur ergänzt werden. Durch Umleiten von Finanzmitteln aus unsicheren Projekten, wie z. B. der Authentifizierung am ElsterOnline-Portal, könnte ein Ausweis mit qualifizierter elektronischer Signatur vielleicht sogar ohne größere Mehrkosten möglich sein.

Eine fortgeschrittene, elektronische Signatur ist nicht für rechtsverbindliche, der händischen Unterschrift gleichgestellte, Signaturen im Internet zu gebrauchen. Gleichwohl ist sie eine Unterschrift, welche durchaus genutzt werden kann. Insbesondere mit Blick auf die Wirtschaft, welche z. B. an Automaten ein qualifiziertes elektronisches Zertifikat oft gar nicht prüfen könnte, ist diese Signatur sinnvoll. Sie dient damit insbesondere Unternehmen der freien Wirtschaft, da die Prüfung solcher Signaturen vereinfacht erfolgen kann und mit dem Einsatz geringere Anforderungen und Rechtsfolgen verknüpft sind.

Fortgeschrittene elektronische Zertifikate sind für viele Anforderungen nur bedingt einsetzbar, während qualifizierte Zertifikate zwar der händischen Unterschrift gleichgestellt sind, aber aufgrund zu hoher Anforderungen oft nicht genutzt werden können. Mit dem ePA hält ein neues Zertifikat (derzeit nur ein Schlüssel und kein Zertifikat) Einzug: ein fortgeschrittenes elektronisches Zertifikat mit Zusatzfunktionen (z. B. Nachweise über einzelne Datenfelder – Alter, Wohnort, etc.). Die Bundesregierung will mit der Authentisierungsfunktion des ePA eine Alternative für bestehende, unsichere Verfahren (Benutzernamen und Passwort) etablieren. Da der ePA mehr ist, als beispielsweise ein bloßes Softwarezertifikat, da er ja auch eines Kartenlesers bedarf und z. B. die Identifizierung des Inhabers vertrauenswürdig erfolgt, könnte ein ePA-Zertifikat eine neue Klasse von Zertifikaten begründen. Dies würde auch die Forderung stützen, dass die Papierwelt (nur aufgrund von § 126a BGB) nicht 1 zu 1 in die elektronische Welt abgebildet werden braucht. Die qualifizierte elektronische Signatur sollte Dokumenten entsprechender Wichtigkeit vorbehalten bleiben. Für die elektronische Kommunikation des Bürgers mit Behörden und Unternehmen wurde der ePA geschaffen und dafür sollte er auch genutzt werden. Des Weiteren auch für Signaturen im täglichen Leben. Sonst könnten in Zukunft eventuell an jeder Supermarktkasse qualifizierte elektronische Unterschriften benötigt werden, selbst wenn der Warenwert minimal ist. Es braucht für solche Fälle - auch um Missbrauch der qualifizierten Unterschrift zu vermeiden - (abgestufte) Signaturen. Hier sollte sich der Gesetzgeber Gedanken machen und ggf. das Signaturgesetz ergänzen. Der digitale Schlüssel des ePA könnte zu einem solchen neuen Zertifikatstyp ausgebaut werden.

Die rechtliche „Unsicherheit“ der Nutzung eines nur fortgeschrittenen elektronischen Schlüssels könnte bei entsprechenden Rahmenbedingungen aus technischer Sicht tragbar sein, da identische technische Grundlagen genutzt werden. Die Rahmenbedingungen müssten definiert werden und die Realisierung der Anwendungen muss sehr genau kontrolliert werden. Zum derzeitigen Zeitpunkt stellt der ePA eine deutliche Verbesserung zu den herkömmlichen Authentifizierungsmethoden im Internet dar. Behörden werden damit erstmalig sichere Dienstleistungen ohne explizite Nutzung einer qualifizierten elektronischen Signatur anbieten können. Dass die Sicherheit des ePA nicht mit der eines qualifizierten Zertifikates vergleichbar ist, ist klar. Die Aufgabe der Datenschutzbeauftragten ist es, den hohen Sicherheitslevel der qualifizierten elektronischen Zertifikate dort zu verlangen, wo dieser erforderlich ist, und zu verhindern, dass der ePA diese nachweisbar sicheren Methoden auf breiter Front mit seiner eigenen ersetzt.

7.3. Zentrales Bundesmelderegister

Wie bereits im vorherigen Tätigkeitsbericht (vgl. VIII. Tätigkeitsbericht, Ziff. 6.2) geschildert, plant die Bundesregierung das Melderecht zu ändern. Bereits im Vorfeld von Gesetzesänderungen beschlossen die Datenschutzbeauftragten des Bundes und der Länder hierzu im Oktober 2007 ein gemeinsames Eckpunktepapier, in welchem die datenschutzrechtlichen Kritikpunkte gegen ein zentrales Bundesmelderegister zusammengestellt wurden.
Dabei wurde herausgestellt, dass für eine mehrfache Datenhaltung durch ein zentrales Melderegister und die örtlichen Melderegister keine Notwendigkeit besteht. Die vorhandene Vernetzung und ein standardisierter Datenaustausch zwischen den Melderegistern, wie er bereits seit 2002 praktiziert wird, sind ausreichende Voraussetzungen für eine effektive Nutzung.
Weiterhin darf ein Bundesmeldegesetz nicht zur Schaffung eines verfassungsrechtlich unzulässigen verwaltungsübergreifenden Identifikationsmerkmals führen.
Auch die Speicherung weiterer Daten, welche im Widerspruch zum originären Zweck des Melderegisters, der Feststellung der Identität und des Wohnsitzes der Einwohner, stehen, so z. B. Waffenerlaubnisse, Sprengstofferlaubnisse und die steuerliche Identifikationsnummer, müssten einer kritischen Prüfung unterzogen werden.
Bei Datenabrufen aus dem Melderegister muss sichergestellt sein, dass jede Behörde nur die Daten erhält, die sie zu ihrer Aufgabenerfüllung benötigt.
Die Änderung des Melderechts sollte auch zum Anlass genommen werden, die Rechte der Meldepflichtigen zu stärken. So sollten bestehende Widerspruchslösungen z. B. bei Gruppenauskünften an Parteien zur Wahlwerbung durch Einwilligungslösungen ersetzt werden.

Dieses Eckpunktepapier wurde auch an die zuständigen Ministerien weitergeleitet, mit der Bitte die Datenschutzbeauftragten in ihren Forderungen bei der Erarbeitung eines Gesetzentwurfes zu unterstützen.

Im August 2008 legte das Bundesinnenministerium einen ersten Entwurf zum Bundesmeldegesetz vor. So ist geplant, zusätzlich zu den bestehenden örtlichen Melderegistern ein zentrales Bundesmelderegister zu schaffen, wel-

ches die gleichen Daten enthält wie die örtlichen Melderegister. Auf die Forderung der Datenschutzbeauftragten, den Datenkatalog auf den originären Zweck des Melderegisters zu reduzieren, wurde nicht eingegangen.

Auch hierzu nahm der Landesbeauftragte gegenüber dem Ministerium des Innern Stellung und bat um Berücksichtigung der datenschutzrechtlichen Bedenken anlässlich dessen Stellungnahme gegenüber dem Bundesministerium des Innern. Dabei verwies er nochmals auf die Grundanforderungen aus dem Eckpunktepapier sowie auf einige andere kritische Aspekte des Gesetzesentwurfs, wie z. B. die Schaffung eines gemeinsamen Ordnungsmerkmals. Durch Zusammenführen von Ordnungsmerkmalen und Speicherungen bei anderen auch nicht staatlichen Stellen könnte ein sogenanntes Personenkennzeichen entstehen, welches vom Bundesverfassungsgericht bereits 1983 im sogenannten „Volkszählungsurteil“ als verfassungsrechtlich unzulässig erklärt wurde.
Im Weiteren wäre u. a. zu klären, wie elektronische Verfahren ausgestaltet sein müssen, um sichere Auskünfte und Übermittlungen über das Internet erhalten zu können. Auch der Umfang der zu speichernden Daten ist noch unklar.
Es erscheint dem Landesbeauftragten notwendig, dass über die Erforderlichkeit eines so tief in die Grundrechte aller Bürgerinnen und Bürger eingreifenden Vorhabens nochmals gründlich nachgedacht wird. Der Bund besitzt für die Thematik keine Verwaltungskompetenz.

7.4. Melderegisterauskünfte nach Landesrecht

Durch Presseberichte in 2008 wurden in einigen Ländern Fälle von Missbrauch der von Meldebehörden übermittelten personenbezogenen Daten bekannt. Danach hatten Adresshändler, die im Auftrag von Unternehmen Kundendaten bei den Meldeämtern überprüfen, die Datensätze verbotenerweise in eigenen Datenbanken gespeichert und anschließend weiterverkauft.

In diesem Zusammenhang haben die Datenschutzbeauftragten auch den Verkauf von Melderegisterauskünften durch die Kommunen kritisiert. So könne jedermann gegen eine Gebühr bei den Meldebehörden Adressdaten erfragen, sofern ihm der Name und das Geburtsdatum bekannt sind. Nur wenn Betroffene im Vorfeld solchen Auskünften widersprechen, ist eine Melderegisterauskunft nicht möglich. Eine ausdrückliche Zustimmung der Betroffenen zur Weitergabe von Daten für Werbezwecke ist gesetzlich nicht geregelt.

Eine Nachfrage beim Ministerium des Innern in Sachsen-Anhalt ergab keine Erkenntnisse, dass in Sachsen-Anhalt ähnliche Missbräuche stattgefunden haben.

Gleichwohl wurden die Meldebehörden in Sachsen-Anhalt durch das Ministerium des Innern über die Erteilung von Melderegisterauskünften und der einhergehenden Abforderung personenbezogenen Daten informiert und sensibilisiert sowie auf die rechtliche Verfahrensweise, insbesondere zur zweckentsprechenden Verwendung, hingewiesen.

7.5. Sorgloser Umgang mit Meldedaten bei Online-Abrufen

Im Sommer des Jahres 2008 erhielt der Landesbeauftragte durch die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht des Landes Brandenburg die Information, dass es zu unberechtigten Online-Melderegisterauskünften gekommen ist.

Einer der führenden Anbieter von Meldesoftware, welche auch in Sachsen-Anhalt häufig Einsatz findet, hatte im Internet eine Demonstrationsseite mit unbeschränktem Lesezugriff auf Meldedaten eingerichtet und zu Testzwecken eine Benutzerkennung und ein Passwort veröffentlicht.
Die gleiche Benutzerkennung und das Passwort verwendete die Firma als Standardeinstellung bei der Installation der Programme in den jeweiligen Behörden. Da in den bekanntgewordenen Fällen die zuständigen Bearbeiter bei der Anmeldung verabsäumten, das Passwort zu ändern, wie es in den Sicherheitskonzepten der Firma vorgesehen gewesen sein soll, war ein unberechtigter Zugriff möglich geworden.

In Sachsen-Anhalt kam es nach bisherigen Ermittlungen nicht zu diesen unberechtigten Online-Abrufen. Trotzdem wurden alle Meldebehörden, sofern die Online-Melderregisterauskunft angeboten wurde, durch das Ministerium des Innern aufgefordert, diese sofort zu sperren. Erst nach Prüfung und gegebenenfalls nach Überarbeitung der Sicherheitskonzepte bzw. nach Neuinstallation sollte eine Öffnung der Portale ermöglicht werden.

7.6. Ausführung des Personenstandsgesetzes

Im Mittelpunkt der Reform des Personenstandsrechts zum 1. Januar 2009 (BGBl. 2007 I S. 122) steht die Einführung elektronischer Personenstandsregister anstelle der bisherigen Personenstandsbücher.

Die dem Landesbeauftragten vorgelegten Entwürfe zum Gesetz zur Ausführung des Personenstandsgesetzes im Land Sachsen-Anhalt (PStG-AG LSA) und zur Verordnung über das Personenstandswesen des Landes Sachsen-Anhalt (PStVO LSA) sollen die Grundlage zur Umsetzung der Personenstandsrechtsreform im Land darstellen. Datenschutzrechtliche Bedenken hatte der Landesbeauftragte nicht erhoben. Das PStG-AG LSA (GVBl. LSA 2008 S. 406) und die PStVO LSA (GVBl. LSA 2008 S. 294) sind zum 1. Januar 2009 in Kraft getreten.

Zu den technischen Aspekten der elektronischen Personenstandsregisterführung hat das Ministerium des Innern die Landkreise, kreisfreien Städte und die Verwaltungsgemeinschaften entsprechend informiert. Dieses Register ist verbindlich ab dem 1. Januar 2014 vorzusehen. Für die Übergangszeit dürfen die Standesämter die Personenstandsfälle noch in einem Papierregister beurkunden.

Die Einrichtung des elektronischen Personenstandsregisters und deren Führung befinden sich zur Zeit in der Umsetzungsphase.

8. Europäischer und Internationaler Datenschutz

8.1. Regelungen zum Datenschutz beim Austausch von Informationen zwischen Strafverfolgungsbehörden der EU sowie zwischen Deutschland und den USA

Die Europäische Union (EU) hat sich zum Ziel gesetzt, den Bürgern ihrer Mitgliedsstaaten auf dem Gebiet der EU ein hohes Maß an Sicherheit zu bieten. Mit dem Wegfall der Kontrollen an den Binnengrenzen sei es notwendig geworden, durch die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden eine bessere Verhütung und Bekämpfung der Kriminalität zu erreichen.
Die Grundsätze und Regeln bezüglich der Menschenrechte, der Grundfreiheiten und der Rechtsstaatlichkeit, auf denen die Union beruht und die den Mitgliedsstaaten gemeinsam sind, sollen dabei beachtet werden. Hierzu hat die EU am 18. Dezember 2006 einen Rahmenbeschluss, die sogenannte „Schwedische Initiative“, verabschiedet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in ihrer Entschließung „Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedsstaaten geboten“ **(Anlage 24)** auf der 76. Konferenz im November 2008 in Berlin darauf hin, dass eine wesentliche Vorraussetzung zur Umsetzung dieses Beschlusses ein möglichst gleichwertiger Datenschutz in allen Mitgliedsstaaten auf hohem Niveau ist. In den EU-Mitgliedsstaaten bestehen nach wie vor unterschiedliche Datenschutzregelungen hinsichtlich der Verwendung von Daten, es herrschen keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Daten für die Betroffenen.

In diesem Zusammenhang fordern die Datenschutzbeauftragten den Gesetzgeber auf, „den verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedsstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln“ (**Anlage 24**, vgl. auch Ziff. 8.6).

Während hinsichtlich dieses Rechtsetzungsakts immerhin der Rahmenbeschluss 2008/977/JI vom 27. November 2008 (über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit verarbeitet werden) grundrechtliche Mindeststandards gewährleisten kann, ist eine vergleichbare Sicherung von Grundrechten Betroffener im zwischen der Bundesrepublik und den Vereinigten Staaten von Amerika getroffenen Abkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität nicht vorgesehen. Die nachdrückliche Kritik der Konferenz der Datenschutzbeauftragten an den grundrechtlichen Defiziten dieses Abkommens **(vgl. Anlage 11)** hat der Bundesrat in seinem Beschluss vom 15. Mai 2009 (Drs. 331/09) zum Entwurf des entsprechenden Bundesgesetzes inhaltlich aufgegriffen. Es bestehen indessen erhebliche Zweifel, dass dem vom Bundesrat erbetenen Hinwirken der Bundesregierung auf hohe Datenschutzstandards im Zuge der Durchführung des Abkommens großer Erfolg beschieden sein wird. Daher erscheint die

weitere Aufforderung des Bundesrates wichtiger, nämlich Datenschutzaspekte bei künftigen Verhandlungen zu berücksichtigen.

8.2. Terrorlisten der Vereinten Nationen – Rechtsschutz jetzt möglich?

In seinem VIII. Tätigkeitsbericht (Ziff. 7.7) hatte der Landesbeauftragte auf die Problematik des fehlenden Rechtsschutzes gegen die Aufnahme einer Person oder Organisation in eine Terrorliste der Vereinten Nationen hingewiesen.

Vom Europäischen Gerichtshof (EuGH) wurde nunmehr mit Urteil vom 3. September 2008 (C-402/05P; C-415/05P, DVBl 2009, 175) Rechtsschutz gewährt. Dabei stellte der EuGH fest, dass die Kontrolle einer Verordnung der Europäischen Gemeinschaft wegen des Verstoßes gegen Grundrechte als „Ausdruck einer Verfassungsgarantie in einer Rechtsgemeinschaft zu betrachten“ sei, die „durch völkerrechtliche Abkommen wie die UN-Charta nicht beeinträchtigt werden“ könne.
Die Tatsache, dass eine Person oder Organisation in eine Terrorliste aufgenommen wurde, muss dem Betroffenen schnellstmöglich mitgeteilt und begründet werden. Nur wenn den Betroffenen die Umstände bekannt sind, besteht eine Möglichkeit zu entscheiden, ob gerichtlicher Rechtsschutz in Anspruch genommen wird. Eine Begründung ist ebenfalls notwendig, um eine richterliche Überprüfung der Aufnahme in die Terrorliste veranlassen zu können.

Die Europäische Kommission will die vom EuGH geforderten Verfahrensanforderungen erfüllen.

8.3. Übermittlung von Fluggastdaten zwischen der EU und den USA

Die Artikel 29-Datenschutzgruppe kam im Zusammenhang mit dem neuen Langzeitabkommen zwischen der EU und den USA zur Übermittlung von Passagierdaten an die USA im Sommer 2007 zu dem Schluss, dass das Datenschutzniveau des neuen Abkommens erheblich niedriger ist als in den vorherigen Abkommen (vgl. VIII. Tätigkeitsbericht, Ziff. 7.5).

In der Stellungnahme wird insbesondere kritisiert, dass die Anzahl der zu übermittelnden Datenelemente erhöht wurde und Angaben zu Dritten eingeschlossen werden. Aber auch, dass die Zwecke, für die die Daten übermittelt werden, unzureichend bestimmt und umfangreicher sind, als die bisher geltenden Datenschutzstandards. Weiterhin dürfen sensible Daten in besonderen Fällen von US-Behörden genutzt werden. Sensible Daten sind hier z. B. Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie Daten über Gesundheit und Sexualleben. Nach EU-Recht ist ihre Nutzung grundsätzlich verboten.
Als weiterer Punkt wurde kritisiert, dass die Speicherfrist von dreieinhalb auf 15 Jahre erweitert wurde und selbst diese Frist noch verlängert werden könnte. Eine Weiterleitung an einheimische und ausländische Stellen ist einfacher geworden und unterliegt nicht länger strengen Datenschutzvorschriften. Eine

gemeinsame Überprüfung des Abkommens schließt nicht länger die Mitwirkung unabhängiger Aufsichtsbehörden ein.

Ebenfalls als Besorgnis erregend wird angesehen, dass das Abkommen den Betroffenen keinerlei Rechte gewährt und jede Änderung in der US-Gesetzgebung das Datenschutzniveau betreffen kann.

8.4. Keine Vorratsdatenspeicherung von Flugpassagierdaten

Im November 2007 wurde der Bundesrat durch die Kommission der Europäischen Gemeinschaften zu einem Vorschlag für einen Rahmenbeschluss des Rates über die Verwendung von Fluggastdatensätzen (PNR-Daten – Passenger Name Record) zu Strafverfolgungszwecken beteiligt.
Die Kommission verfolgt das Ziel, durch Harmonisierung der Vorschriften der Mitgliedsstaaten über die Erhebung und Weitergabe von Fluggastdaten einen Beitrag zur Verhütung und Bekämpfung des Terrorismus und der organisierten Kriminalität zu leisten. Dabei sollte der Fluggastdatensatz über die bisher übermittelten Daten hinaus erweitert werden. Auch eine Verlängerung der Speicherfristen bis zu 13 Jahren wird vorgesehen.
Der Bundesrat fasste im Februar 2008 einen Beschluss (BR-Drs. 826/07), in welchem er feststellte, dass er grundsätzlich das verfolgte Anliegen der EU teile. Jedoch habe er erhebliche rechtliche Bedenken. So stelle die Verarbeitung der PNR-Daten einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Weiterhin besteht nach Rechtsprechung des Bundesverfassungsgerichts (vgl. BVerfGE 65, 1, 47) außerhalb statistischer Zwecke ein *„striktes Verbot der Sammlung personenbezogener Daten auf Vorrat“.* Eine Sammlung von Daten, die zur Erfüllung einer konkreten Aufgabe nicht benötigt werden, jedoch zu einem unbestimmten Zeitpunkt eventuell gebraucht werden könnten, ist demnach unzulässig. Weiterhin überschreitet eine Speicherfirst von 13 Jahren die übliche Speicherfrist für polizeiliche Sammlungen.

Die Datenschutzbeauftragten des Bundes und der Länder setzten sich mit dieser Problematik auf der Konferenz der Datenschutzbeauftragten im April 2008 in Berlin auseinander. Hierzu fassten sie die Entschließung „Keine Vorratsspeicherung von Flugpassagierdaten“ **(Anlage 10)** in welcher sie die Bundesregierung aufforderten, den Entwurf des Rahmenbeschlusses abzulehnen. Sie bestätigten die im Bundesrat geäußerten verfassungsrechtlichen Bedenken. Weiterhin kritisierten sie, dass kaum datenschutzrechtliche Regelungen in dem Vorschlag enthalten sind. Dies sei besonders bedenklich, da ein angemessenes Datenschutzniveau nicht in allen Ländern der EU einheitlich vorhanden ist.

Bei einer Debatte im Bundestag im April 2008 wurde festgestellt, dass der Diskussionsprozess erst begonnen habe, die Bundesregierung werde sich jedoch für einen Beschluss einsetzen, *„der das Gleichgewicht zwischen Sicherheits- und Datenschutzinteressen wahrt“.*
Eine Stellungnahme der Bundesregierung zu diesem Rahmenbeschluss soll nach Angaben der Bundesjustizministerin nicht vor der Bundestagswahl im September 2009 erfolgen. Außerdem wolle man vor Einführung einer weiteren Form der Vorratsdatenspeicherung zunächst das Urteil des Bundesver-

fassungsgerichts im Streit um die verdachtsunabhängige Protokollierung von Verbindungs- und Standortdaten abwarten (vgl. Ziff. 24.1).

8.5. Überführung des Vertrages von Prüm in EU-Recht

Wie bereits im VIII. Tätigkeitsbericht (Ziff. 7.1) erläutert, ist der Vertrag von Prüm ein zwischenstaatliches Abkommen über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration.
Vertragsparteien sind derzeit zehn EU-Mitgliedsstaaten. Er wurde am 27. Mai 2005 zwischen den Ländern Belgien, Deutschland, Spanien, Frankreich, Luxemburg, den Niederlanden und Österreich geschlossen. Mittlerweile sind noch andere EU- Mitgliedsländer dem Vertrag beigetreten, so Finnland, Slowenien und Ungarn. Andere EU-Staaten haben die Absicht, dem Vertrag beizutreten.

Die Innenminister der Mitgliedsländer der EU haben beschlossen, den Vertrag von Prüm in EU-Recht zu überführen.
Das bedeutet, dass den Behörden aller EU-Staaten ein automatisierter Zugriff auf DNA-Daten, Fingerabdrücke und Daten des Zentralen Fahrzeugregisters ermöglicht wird.

Weiterhin stimmten die EU-Innenminister auch einer zentralen Erfassung der biometrischen Daten aller Visumantragsteller aus Drittstaaten im europäischen Schengen Raum zu. Das Visum-Informationssystem soll bis zum Ende des Jahres 2009 eingeführt werden. Neben Europol sollen auch andere staatliche Stellen Zugang zu diesem System erhalten.

Am 23. Juni 2008 wurde vom Rat der Europäischen Union ein Beschluss (Ratsbeschluss Prüm) angenommen, welcher nun in nationales Recht umzusetzen ist.

In diesem Zusammenhang hat die 76. Konferenz der Datenschutzbeauftragten die Entschließung „Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich“ **(Anlage 23)** verabschiedet.

Ein erster Gesetzentwurf der Bundesregierung, in welchem die rechtlichen Voraussetzungen zur Umsetzung des Beschlusses des Rates vom 23. Juni 2008 geschaffen werden, liegt dem Deutschen Bundestag seit April 2009 vor (BT-Drs. 16/12585). Der Entwurf sieht hauptsächlich die Anpassung des Bundespolizeigesetzes und des Straßenverkehrsgesetzes vor. Der Gesetzentwurf wurde am 19. Juni 2009 vom Bundestag angenommen.

8.6. Europäische Datenschutzkonferenzen

Zur Europäischen Konferenz der Datenschutzbehörden der EU-Mitgliedsstaaten trafen sich die Datenschutzbeauftragten vom 10. bis 11. Mai 2007 in Larnaka (Zypern). Wichtige Themen waren hier u. a. „Datenschutz in der Dritten Säule“, „Die Zukunft der Arbeitsgruppe Polizei“ sowie „Die Elektronische Gesundheitskarte“. Zum Thema „Anwendung des Verfügbarkeitsprin-

zips bei der Strafverfolgung“ hat sich die Europäische Konferenz einen gemeinsamen Standpunkt gebildet (**Anlage 39**, vgl. auch Entschließung der Konferenz des Bundes und der Länder „Besserer Datenschutz bei der Umsetzung der „schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedsstaaten geboten“, **Anlage 24**).
Eine Erklärung zum „Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“ **(Anlage 40)** wurde verabschiedet.
Dabei forderten die Europäischen Datenschutzbeauftragten, sich mehr Zeit für die Erarbeitung einer solchen Richtlinie zu lassen, um einen harmonisierten und hohen Standard des Datenschutzes zu gewährleisten. Insbesondere wurde darauf verwiesen, dass Regelungen zur Zweckbegrenzung der Verarbeitung personenbezogener Daten, angemessene Sicherheitsvorkehrungen für die Verarbeitung biometrischer und genetischer Daten, sowie differenzierte Regelungen für die Verarbeitung personenbezogener Daten bei unterschiedlichen Betroffenenkategorien zu treffen sind.
Weiterhin muss ein Verfahren definiert werden, um den Datenschutzstandard in einem Drittland oder einer internationalen Einrichtung einschätzen zu können, bevor personenbezogene Daten übertragen werden.
Regelungen zur Benachrichtigung der Betroffenen, einschließlich der Identität der für die Verarbeitung verantwortlichen Stelle, der möglichen Empfänger und der Rechtsgrundlage für die Verarbeitung, sowie zum Auskunftsrecht sollen umfassend sein und im Einklang mit den Anforderungen der Europäischen Menschenrechtskonvention und der Rechtsprechung stehen.
Eine Gemeinsame Kontrollbehörde soll als unabhängige Kontrollinstanz konzipiert sein und für die Vorabkontrolle der Verarbeitung personenbezogener Daten zuständig sein.

Die Europäische Datenschutzkonferenz in Rom (Italien) vom 17. bis 18. April 2008 befasste sich hauptsächlich mit der Kontrolle von Reisenden in die Europäische Union und aus der Europäischen Union und verabschiedete hierzu eine Erklärung **(Anlage 41).**

8.7. Internationale Konferenzen der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Eines der wichtigsten Themen auf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Montreal vom 25. bis 28. September 2007 betraf den Schutz von Passagierdaten.
Auf Antrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde, unterstützt von einer Reihe anderer Teilnehmer der Konferenz, eine „Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden“, verabschiedet **(Anlage 42).**
Hierbei ruft die Konferenz dazu auf, dass internationale Organisationen und Regierungsstellen mit den Beauftragten für den Datenschutz zusammenarbeiten, um verbindliche globale Lösungen zur Sicherung eines angemessenen Datenschutzniveaus einzuführen.

Weitere Resolutionen betreffen die Festlegung internationaler Standards, wie die Forderung nach stärkerer Einbeziehung in ISO-Mechanismen, und die internationale Zusammenarbeit u. a. bei der grenzüberschreitenden Durchsetzung und den Initiativen zur Schärfung des Bewusstseins für Datenschutzaspekte.

Vom 15. bis 17. Oktober 2008 fand die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Straßburg statt. Hier forderten die Teilnehmer vor allem eine stärkere internationale Zusammenarbeit zwischen den Datenschutzbehörden, um verbindliche Datenschutzregeln zu erarbeiten **(Anlage 45).**

9. Finanzwesen

9.1. Auskunftsrecht für Betroffene im Steuerverfahren

Das Bundesverfassungsgericht hat am 10. März 2008 in einem Beschluss (1 BvR 2388/03, NJW 2008, 2099) die umfangreiche Speicherung von Informationen über steuerliche Auslandsbeziehungen durch das Bundeszentralamt für Steuern als mit dem Grundgesetz vereinbar erklärt. In diesem Zusammenhang wurde auch über den Auskunftsanspruch eines Betroffenen im Steuerverfahren entschieden.

Das Bundesverfassungsgericht lehnte diesen zwar im vorliegenden Sachverhalt ab, stellte aber als selbstverständlich das grundsätzliche, grundrechtsgeschützte Interesse Betroffener fest, Kenntnis von den sie betreffenden Datensammlungen zu erlangen. Dieses Interesse diene der Verwirklichung des Grundrechts auf informationelle Selbstbestimmung.
„Der auf das Grundrecht auf informationelle Selbstbestimmung vermittelte Grundrechtsschutz erschöpft sich nicht in einem Abwehrrecht gegen staatliche Datenerhebung und Datenverarbeitung. Dieses Grundrecht schützt auch das Interesse des Einzelnen, von staatlichen informationsbezogenen Maßnahmen zu erfahren, die ihn in seinen Grundrechten betreffen.
Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen und zu entscheiden (vgl. BVerfGE 65, 1 <43>). Nur wenn der Einzelne, der möglicherweise von einem Eingriff in das Recht auf informationelle Selbstbestimmung betroffen ist, eine Möglichkeit hat, von diesem Eingriff zu erfahren, kann er die für die freie Entfaltung seiner Persönlichkeit wichtige Orientierung und Erwartungssicherheit erlangen.
Eine Informationsmöglichkeit für den von einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung Betroffenen ist ferner Voraussetzung dafür, dass er die Rechtswidrigkeit der Informationsgewinnung oder etwaige Rechte auf Löschung oder Berichtigung geltend machen kann. Insoweit ist der Anspruch auf die Kenntniserlangung ein Erfordernis effektiven Grundrechtsschutzes im Bereich sowohl des behördlichen als auch des gerichtlichen Verfahrens (vgl. BVerfGE 100, 313 <361>; 109, 279 <363 f.>).

Das Informationsinteresse des Beschwerdeführers wird nach diesen Maßgaben von Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG geschützt. ...
Der von der Rechtsschutzgarantie des Art. 19 Abs. 4 GG vermittelte Anspruch auf eine wirksame gerichtliche Kontrolle in Fällen, in denen eine Verletzung subjektiver Rechte durch die öffentliche Gewalt möglich erscheint, beschränkt sich nicht auf die Durchführung der gerichtlichen Kontrolle und das gerichtliche Verfahren. Zur Gewährleistung eines tatsächlich effektiven Rechtsschutzes gehört auch, dass der von einem Eingriff in das Grundrecht auf informationelle Selbstbestimmung Betroffene von diesem Eingriff Kenntnis erhalten kann (vgl. BVerfGE 65, 1 <70>). In derartigen Fällen kann auch Art. 19 Abs. 4 GG einen Informationsanspruch begründen.
Das Informationsinteresse des Beschwerdeführers wird unter diesen Voraussetzungen nicht nur durch das Grundrecht auf Schutz der Persönlichkeit, sondern auch durch Art. 19 Abs. 4 GG geschützt."

Jedoch ist daraus kein Anspruch auf eine bestimmte Art der Informationserlangung abzuleiten. Der Gesetzgeber muss bei der Ausgestaltung des Zugangs zu Informationen vielmehr berücksichtigen, welche Bedeutung dem Grundrechtsschutz des Betroffenen zukommt. § 19 Bundesdatenschutzgesetz (BDSG) - entsprechend § 15 Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) - sehe grundsätzlich *„einen weit reichenden Anspruch des Betroffenen auf Auskunft vor",* so das Bundesverfassungsgericht. Jedoch stellt die in § 19 BDSG ebenfalls enthaltene Abwägungsklausel zugleich sicher, dass eine Auskunft unterbleiben dürfe, *„wenn das Interesse an der ordnungsgemäßen Aufgabenerfüllung dem Informationsinteresse des Betroffenen vorgeht"*.

Im krassen Widerspruch zu diesem Beschluss des Bundesverfassungsgerichts steht hingegen eine Verwaltungsanweisung des Bundesministeriums der Finanzen vom 17. Dezember 2008, in welcher der Auskunftsanspruch der Bürgerinnen und Bürger im Besteuerungsverfahren von einem „berechtigten Interesse" abhängig gemacht wird.

Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Erstaunen fest, dass wohl keine Beamtin, kein Beamter gegen diese verfassungswidrigen Verwaltungsvorgaben remonstriert hat. Anlässlich der 77. Konferenz am 26. und 27. März 2009 haben sie in einer Entschließung **(Anlage 29)** gefordert, unverzüglich die Verwaltungsanweisung aufzuheben und die Finanzbehörden des Bundes und der Länder zu verpflichten, entsprechende Auskunftsansprüche nach geltendem Recht zu erfüllen.
Seitens des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde dieser Erlass förmlich beanstandet.

9.2. Kontenabrufverfahren

Bereits im VIII. Tätigkeitsbericht (Ziff. 8.2) hatte der Landesbeauftragte darauf verwiesen, dass das Bundesverfassungsgericht mit einer Entscheidung über die Rechtmäßigkeit der Kontenabrufverfahren befasst ist. In der Abgabenordnung (AO) wurde durch Art. 2 des Gesetzes zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I S 2928, 2931) in § 93 Abs. 7 und Abs. 8 die Möglichkeit des automatisierten Abrufes von Kontoinformatio-

nen durch Finanzbehörden sowie für Behörden und Gerichte eröffnet, die für die Anwendung solcher Gesetze zuständig sind, welche an Begriffe des Einkommensteuergesetzes anknüpfen.
In seiner Entscheidung vom 13. Juni 2007 (1 BvR 1550/03, 1 BvR 2357/04, 1 BvR 603/05, NJW 2007, 2464) hat das Bundesverfassungsgericht festgestellt: *„§ 93 Absatz 8 der Abgabenordnung vom 23. Dezember 2003 (Bundesgesetzblatt I Seite 2928), zuletzt geändert durch das Gesetz zur Neuorganisation der Bundesfinanzverwaltung und zur Schaffung eines Refinanzierungsregisters vom 22. September 2005 (Bundesgesetzblatt I Seite 2809), ist mit dem Grundgesetz unvereinbar."*
In der Begründung wird dazu vom Bundesverfassungsgericht unter anderem ausgeführt, dass das Gesetz gegen das Gebot der Normenklarheit verstößt. Es sei nicht hinreichend bestimmt festgelegt, welche Behörden ein Ersuchen zum Abruf der Kontostammdaten stellen können, sowie welchen Aufgaben ein solches Ersuchen dienen könne.

§ 93 Abs. 7 AO ist dagegen noch hinreichend normenklar - und bestimmt; routinemäßige Kontendatenabfragen „ins Blaue hinein" ohne konkrete Anhaltspunkte sind danach ausgeschlossen. Ein bundeseinheitlich abgestimmter Vordruck der Finanzämter dient als Hilfsmittel zur Dokumentation der Ermessensentscheidung bei der Durchführung eines Kontenabrufverfahrens (Erforderlichkeit, Anhörung des Betroffenen, Mitteilung nach erfolgter Abfrage).

Der Bundesgesetzgeber hat eine Neuregelung des **§ 93 Abs. 8 AO** beschlossen, nach der die Verwaltungsbehörden, welche zuständig sind für:
1. die Grundsicherung für Arbeitssuchende nach dem Zweiten Buch Sozialgesetzbuch,
2. Sozialhilfe nach dem Zwölften Buch Sozialgesetzbuch,
3. Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz,
4. Aufstiegsfortbildungsförderung nach dem Aufstiegsfortbildungsförderungsgesetz und
5. Wohngeld nach dem Wohngeldgesetz

die Möglichkeit eines automatisierten Kontenabrufes beim Bundeszentralamt für Steuern nutzen können (BGBl. I 2007 S. 1912).
Für andere Zwecke sind Abrufersuchen nur zulässig, soweit sie durch ein Bundesgesetz ausdrücklich zugelassen werden.

Der Landesbeauftragte für den Datenschutz informiert sich mit Hilfe einer Übersicht monatlich, in welchem Umfang Behörden des Landes Sachsen-Anhalt von der Möglichkeit des Kontoabrufes nach § 93 Abs. 8 AO Gebrauch machen. Dabei ist erkennbar, dass Abfragen bisher nur in wenigen Einzelfällen erfolgten.

9.3. Einführung der Steuer-Identifikationsnummer zum 1. Juli 2007

Mit der Einführung der persönlichen Steuer-Identifikationsnummer (Steuer-ID) soll ein Steuerbetrug vor allem durch einen Steuerabgleich erheblich erschwert werden. Bereits im vergangenen Berichtszeitraum (vgl. VIII. Tätigkeitsbericht, Ziff. 8.1) verwies der Landesbeauftragte darauf, dass die Einführung der Steuer-ID trotz zahlreicher Bedenken der Datenschutzbeauftragten

des Bundes und der Länder nicht mehr aufzuhalten war (vgl. Ziff. 7.3). Jedoch wurde eine Reduzierung des Datenkataloges erreicht, welcher im Bundeszentralamt für Steuern über die Steuerpflichtigen gespeichert wird. Denn ursprünglich plante die Bundesregierung zu den Daten eines jeden Steuerpflichtigen auch Daten wie die Religionszugehörigkeit, den Ehepartner, die Kinder und deren Steuer-ID sowie Angaben zu den Steuerklassen im Register zu speichern.

Letztlich wurde seit Sommer 2007 eine Datenbank im Bundeszentralamt für Steuern aufgebaut, welche die Daten aller rund 82 Millionen in Deutschland gemeldeten Personen vereint. Die Identifikationsnummer wird künftig u. a. an jede Bürgerin und jeden Bürger bereits mit der Geburt vergeben und bleibt bis 20 Jahre über den Tod hinaus gespeichert.

Im Sommer 2008 begann das Bundeszentralamt für Steuern die Mitteilungsschreiben zur Steuer-ID zu versenden. Seither verging kaum ein Tag, an welchem dieser Umstand nicht für Schlagzeilen in der Tagespresse sorgte. So untertitelte die Frankfurter Allgemeine am 19. August 2008 ihren Artikel „Verdruss über die neue Steuernummer“ mit: „In Halle sind 1000 Briefe unzustellbar, in Stade wird der Stadtrat zum Libanesen gemacht“. Zu klären war, wie es zu diesen Fehlern kam und wie weitere zu verhindern wären.

Bei der Übermittlung der Datensätze führte die Nutzung unterschiedlicher Programme zu technischen Problemen bei der Lesbarkeit der Daten. Aus diesem Anlass versandte das Bundeszentralamt für Steuern Fehlermeldungen an das Meldeamt, welche vom jeweiligen Meldeamt geprüft werden mussten. Danach wurden die korrigierten Daten erneut übermittelt. Insbesondere musste darauf geachtet werden, dass kein Datensatz doppelt angelegt wurde, was z. B. durch eine leichte Veränderung der Schreibweise des Namens passieren konnte. Auch Umzüge mussten von den Meldeämtern umgehend an das Bundeszentralamt für Steuern gemeldet werden, damit dort der Datensatz zeitnah aktualisiert werden konnte. Sonst wäre das Mitteilungsschreiben an die alte Adresse gesandt worden, wo es nicht ordnungsgemäß hätte zugestellt werden können. Auch in den Fällen, in denen sich ein Einwohner einer Stadt bei einem Umzug nicht ordnungsgemäß an seinem neuen Wohnort angemeldet hatte, gab es Zustellungsprobleme. Hier mussten die Meldeämter den Verbleib der Einwohner klären und es erfolgte eine erneute Übersendung des korrigierten Datensatzes an das Bundeszentralamt für Steuern.

Ein weiterer Problemfall war die Mitteilung des Geburtslandes. Bei der Öffnung des Mitteilungsschreibens zur Erteilung der bundeseinheitlichen Steuer-ID staunten einige Bürgerinnen und Bürger nicht schlecht, als sie erfuhren, dass sie in „Polen“ oder der „Tschechischen Republik“ geboren waren. Die Betroffenen gingen bisher davon aus, in Deutschland geboren zu sein, nämlich in den ehemaligen deutschen Ostgebieten.
Das Problem ergab sich aus der vorgesehenen Speicherung des Merkmals „Geburtsland“ im Register des Bundeszentralamts für Steuern.

Zur Verschlüsselung des Geburtslandes wird von den Meldebehörden ein Staatsangehörigkeits- und Gebietsschlüssel verwendet, welcher auf dem

Länderverzeichnis für den amtlichen Gebrauch in der Bundesrepublik Deutschland beruht. Dieses Länderverzeichnis wird ständig überarbeitet und entspricht dem jeweils aktuellen Gebietsstand. Bei einer gegenwärtigen Anmeldung kann es somit passieren, dass nicht der Geburtsstaat eingetragen werden kann, zu dem der Geburtsort zum Zeitpunkt der Geburt gehörte (z. B. nicht „Tschechoslowakei“, sondern „Tschechien“ oder „Slowakei“).
Vor allem bei der älteren Generation unserer Bevölkerung entstanden hierdurch Verwirrungen. Der Landesbeauftragte für den Datenschutz konnte nur darauf verweisen, dass die betroffenen Personen sich an ihr Meldeamt wenden müssen, um diesen Eintrag korrigieren zu lassen.

Auf Nachfrage teilte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit mit, dass der Datensatz auch beim Bundeszentralamt für Steuern korrigiert wird, wenn die betroffene Person es beantragt.

9.4. Ablösung der Lohnsteuerkarten

Mit der Neuregelung des § 39e Einkommenssteuergesetz im Zusammenhang mit der Änderung des Jahressteuergesetzes 2008 sieht die Bundesregierung vor, die Lohnsteuerkarte kurzfristig bis 2011 durch ein elektronisches Abrufverfahren (ElsterLohn II) zu ersetzen (BGBl. I 2007 S. 3150).
Zu diesem Zweck sollen die Datensätze, welche beim Bundeszentralamt für Steuern für die Steuer-Identifizierungsnummer gespeichert sind, nun doch um lohnsteuerrechtlich bedeutsame Merkmale wie Religionszugehörigkeit, Ehepartner und Angaben zu den Steuerklassen erweitert werden.
Hier entstehende Datensammlungen wecken Begehrlichkeiten auch aus anderen Bereichen. Beispiele aus der Vergangenheit, wie die Erhebung der Mautdaten, haben gezeigt, dass Daten, welche zunächst nur für einen engen Zweck gespeichert werden, später auch für andere Zwecke zugänglich gemacht werden sollen.
Auf der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2007 war noch gefordert worden, die geplante Umstellung auf ein elektronisches Abrufverfahren nicht mit dem Jahressteuergesetz 2008 zu beschließen **(Anlage 3).**
Bei der abschließenden Beratung des Finanzausschusses des Deutschen Bundestages wurden die datenschutzrechtlichen Bedenken zwar erwähnt, der Gesetzentwurf aber ohne weitere datenschutzrechtliche Feststellungen beschlossen.

9.5. Protokollauswertung bei LUNA

Zur effektiveren Bekämpfung des Umsatzsteuerbetrugs wurde das Verfahren einer sogenannten „länderumfassenden Namensabfrage“ (LUNA) entwickelt. Durch bundesweite Nutzung des Systems LUNA sollen mehrfache umsatzsteuerliche Registrierungen in verschiedenen Ländern vermieden und somit Umsatzsteuerhinterziehungen vorgebeugt werden.

Dieses Verfahren wurde im Berichtszeitraum wesentlich erweitert. Mit der Version 2.0 sind zum bisherigen Datenkatalog weitere zahlreiche Datenbereiche, insbesondere aus dem Grundinformationsdienst, den Veranlagungs-

und Kraftfahrzeugsteuer-Konten sowie Daten des Umsatzsteuer-Voranmeldungsverfahren bereitgestellt worden.

Die Datenschutzbeauftragten des Bundes und der Länder waren sich einig, dass einer regelmäßigen Kontrolle der LUNA-Abfrageprotokolle, gerade auch durch die behördlichen Datenschutzbeauftragten, eine große Bedeutung zukommt. Da es bei den Eingaben des Abfragegrundes trotz Vorgaben zu unterschiedlichen Eingabeformen (z. B. Nutzung von Abkürzungen, Groß-Kleinschreibung) kommen kann, sowie eine individuelle Eingabe von Gründen möglich ist, ist eine automatisierte Prüfung der Protokolldateien kaum möglich. Eine wirksame datenschutzrechtliche Kontrolle der LUNA-Abfragen kann letztlich nur durch eine häufige konkrete Überprüfung einzelner Abfragen erfolgen.

9.6. Koordinierte neue Softwareentwicklung der Steuerverwaltung

Im zurückliegenden Berichtszeitraum wurde unter dem Projektnamen „Koordinierte neue Softwareentwicklung der Steuerverwaltung“ (KONSENS) die Vereinheitlichung der Verwaltungssoftware der deutschen Finanzämter, in einem Nachfolgeprojekt zu FISCUS, vorangetrieben. Die von der abgewickelten fiscus GmbH entwickelten Projekte wurden, soweit es wirtschaftlich sinnvoll erschien, in das neue Vorhaben KONSENS übernommen. Laut Beschluss der Finanzministerkonferenz vom 9. Mai 2008, im Einvernehmen mit dem Bundesfinanzministerium, soll die Vereinheitlichung der Steuersoftware in Deutschland schneller erfolgen als bisher geplant.
Im KONSENS-Projekt soll eine einheitliche Steuersoftware geschaffen werden, deren Entwicklung und Einsatz gemeinsam in allen Ländern erfolgt. Das Bundesland Bayern, das mit EOSS (Evolutionär orientierte Steuersoftware) eine eigene Software-Lösung entwickelte und nutzte, soll wieder ins FISCUS-Projekt zurückgeholt werden. Gemeinsame Basis der KONSENS-Vorhaben sind die Programme, welche in den einzelnen Bundesländern eingesetzt werden. Diese sollen, zusammen mit der Software des EOSS-Verbunds und einer durch das Land Nordrhein-Westfalen entwickelten Software, eine einheitliche Anwendung bilden. Federführend in der Entwicklung sind die Bundesländer Bayern, Nordrhein-Westfalen, Niedersachsen, Baden-Württemberg und Hessen. Ein weithin bekanntes KONSENS-Verfahren ist ELSTER (Elektronische Steuererklärung); vgl. dazu Ziff. 9.7.

Im Arbeitskreis Steuerverwaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder war KONSENS natürlich Thema. Unter anderem wurden Fragen der rechtlichen Stellung der Clearingstellen und zur Datensammelwut der Steuerverwaltung - insbesondere im Rahmen des neuen Verfahrens DAME - thematisiert. DAME (Data-Warehouse-Auswertungen und Business-Intelligence-Methoden) soll die Finanzverwaltung im Vorhaben KONSENS bei Auswertungsmöglichkeiten durch die Nutzung einheitlich strukturierter Daten unterstützen.

Das Ministerium der Finanzen hat den Landesbeauftragten zu Beginn des Jahres 2009 über das weitere Vorgehen beim Vorhaben KONSENS (Vorhabenplan 2009) informiert. Dieser Vorhabenplan konsolidiert die Planungen für

den Zeitraum 2009 bis 2013. Der Landesbeauftragte geht davon aus, dass er bei konkreten Umsetzungsvorhaben rechtzeitig informiert und beteiligt wird.

9.7. Unsichere Authentifizierung bei der ElsterOnline-Anmeldung

ELSTER ist das Verfahren zur Elektronischen Steuererklärung, welches als Abkürzung im Rahmen der Einkommensteuererklärung ein Begriff ist. Das ELSTER-Projekt selbst ist in unzählige Unterprojekte zersplittert, von denen eines die Anmeldung am ElsterOnline-Portal betrifft. Diese ist alles andere, nur nicht der Stand der Technik, insbesondere ist es unsicher und nicht vertrauenswürdig implementiert.

Die Nutzung dieser Anmeldeform am Elster-Online-Portal war bisher nicht verbindlich vorgeschrieben. Vielmehr wurde bisher auf die Abgabenordnung (AO) verwiesen, die nähere Details regelte. Nun soll ELSTER scheinbar festgeschrieben werden, um die kostenintensivere, dafür aber sichere Nutzung qualifizierter Signaturen zu vermeiden.

Der Landesbeauftragte befasste sich auch mit dem Entwurf eines Gesetzes zur Modernisierung und Entbürokratisierung des Steuerverfahrens (Steuerbürokratieabbaugesetz). In diesem wurde Ende 2008 über die „Hintertür“ einer Änderung der Abgabenordnung eine vereinfachte (unsichere) Datenübertragung zum Standard für die Finanzverwaltung erhoben (BGBl. I S. 2850, 2856):

„Dem § 150 werden folgende Absätze 7 und 8 angefügt:
(7) Ordnen die Steuergesetze an, dass der Steuerpflichtige die Steuererklärung nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung zu übermitteln hat, ist der Datensatz mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zu versehen. Zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens kann das Bundesministerium der Finanzen durch Rechtsverordnung mit Zustimmung des Bundesrates
1. bis 5. ... bestimmen sowie
6. im Benehmen mit dem Bundesministerium des Innern anstelle der qualifizierten elektronischen Signatur ein anderes sicheres Verfahren, das die Authentizität und die Integrität des übermittelten elektronischen Dokuments sicherstellt, und ...(Ausnahmen) ... zulassen.“

Eine solche Gesetzesänderung ist bedenklich. Anstelle der Formulierung „im Benehmen“ mit dem Bundesministerium des Innern als nicht zuständige Stelle, hätte hier „mit Zustimmung des Bundesamts für Sicherheit in der Informationstechnik“ o. ä. stehen müssen, da das Bundesministerium des Innern über keine Kompetenzen auf diesem Gebiet verfügt. Leider wurde der Gesetzesänderung zugestimmt, so dass die Datenschutzbeauftragten sich nun gegen das „andere sichere Verfahren“ wenden müssen, welches mit ELSTER bereits existiert, jedoch nicht gleichwertig zur qualifizierten elektronischen Signatur ist.

Das Verfahren der qualifizierten elektronischen Signatur ist derzeit alternativlos. Die im Gesetz geschaffene Möglichkeit, anstelle dieser nun ein anderes

sicheres Verfahren beim elektronischen Besteuerungsverfahren zu verwenden oder gar auf beides ganz zu verzichten, wird mit großer Besorgnis gesehen. Es ist unbedingt notwendig, ein solches Verfahren von unabhängigen Gutachtern, beispielsweise dem BSI oder der Bundesnetzagentur, vor der Nutzung evaluieren zu lassen. Des Weiteren muss natürlich auch die qualifizierte elektronische Signatur im Steuerwesen genutzt werden können. Mit der Investition von nicht nur finanziellen Ressourcen in ein unsicheres Projekt werden dringend benötigte Mittel zur Sicherung beispielsweise des ePA fehlgeleitet. Die ELSTER-Authentisierung sollte, wie geplant, den ePA nutzen und zugunsten bspw. dessen Ausstattung mit einer qualifizierten Signatur eigene Entwicklungen stoppen (vgl. Ziff. 7.2).

Das Authentisierungsverfahren am ElsterOnline-Portal ist aus Sicht des Datenschutzes kein zur qualifizierten elektronischen Signatur gleichwertiges Verfahren. Bei einer Authentisierung des Einreichenden ist maximal die Identität dieser Person bekannt. Es wird weder der Steuerpflichtige bzw. der Ersteller der Steuererklärung selbst authentifiziert, noch wird sichergestellt, dass die übermittelten Daten authentisch und unverfälscht sind. Die Schriftformerfordernis kann gem. § 126a BGB nur durch die qualifizierte elektronische Signatur ersetzt werden. Ein Authentisierungsverfahren, zumal in nicht sachgemäßer Art und Weise eingesetzt, kann dies keinesfalls. Damit kann auch keine gleichwertige Sicherheit garantiert werden, zumal die Technik vollkommen falsch angewendet wird. Offensichtlich wird versucht, die hohen Anforderungen, welche zu Recht an eine qualifizierte elektronische Signatur gestellt werden, durch eine Eigenentwicklung abzulösen. Damit könnte das Vertrauen in die staatliche Verwaltung und das sich entwickelnde eGovernment nachhaltig beeinträchtigt werden.

Verbunden mit der Etablierung einer unsicheren Anmeldung am ElsterOnline-Portal wird auch die Übermittlung der Steuerdaten zunehmend unsicherer gestaltet. Mit dem Entwurf zu einem Bürgerentlastungsgesetz (BR-Drs. 168/09) soll die Abgabenordnung erneut weiter verwässert werden. Die eigentlich vorgesehene Pflicht zur Evaluierung des „anderen sicheren Verfahrens“ zur Datenübertragung bis Ende 2011 (§ 87a Abs. 6 Satz 3 AO) will der Bundesrat übergehen und ein solches Verfahren, konkret das Authentisierungsverfahren des ElsterOnline-Portals, für die Fälle, in denen der Steuerpflichtige seine Steuererklärung elektronisch übertragen muss, durch ein nicht evaluiertes Verfahren ersetzen. Durch das Schaffen von vollendeten Tatsachen wird das Ergebnis der Evaluierung vorfristig obsolet. In der Begründung wird im Wesentlichen vorgetragen, dass sich ELSTER bewährt habe. Dem ist nicht so, wie den Kritiken der Datenschutzbeauftragten in den letzten Jahren zu entnehmen war. Damit würde das bewährte Verfahren der qualifizierten elektronischen Signatur aus Kostengründen und unbefristet gegen das unsichere Verfahren ELSTER dauerhaft ausgetauscht.

Diese Entwicklung ist nicht mit den Anforderungen des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme vereinbar. In der Entschließung „Elektronische Steuererklärung sicher und datenschutzgerecht gestalten“ der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 6./7. November 2007 **(Anlage 20)** ist bereits auf diese Fehlentwicklung hingewiesen worden.

Die Bundesregierung will den Vorschlag des Bundesrates noch prüfen; zu einer Gesetzesänderung kam es einstweilen doch nicht.

9.8. Einführung der Kraftfahrzeugsteuer-Rückständeprüfung in Sachsen-Anhalt

Die dem Landesbeauftragten bereits im Frühjahr 2007 vorliegenden Informationen zur geplanten **praktischen** Umsetzung des sich damals noch im Gesetzgebungsverfahren befindlichen Entwurfes eines Gesetzes über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer durch die Oberfinanzdirektion ließen datenschutzrechtliche Bedenken aufkommen.
Gegenstand der datenschutzrechtlichen Bedenken war die geplante tägliche Übermittlung des **gesamten** Datenbestands mit Angabe des jeweiligen Betrags der Steuerschuld jedes Kraftfahrzeugsteuerschuldners des Landes durch die Oberfinanzdirektion an **alle** Zulassungsbehörden mittels der sog. „Rückständedatei".

Die parlamentarische Diskussion über Rückstandsfälle bei der Kraftfahrzeugsteuer verfolgte der Landesbeauftragte bereits seit Juni 2006 (vgl. LT-Drs. 5/71).
Beim damals noch geplanten Verordnungsentwurf des Ministeriums der Finanzen war allerdings für die Zulassungsbehörden von einem Verfahren der „…**Online-Abfrage** zur Einsichtnahme und Prüfung…" die Rede, da die Kraftfahrzeugsteuerrückstände bei den Finanzämtern entstünden und den Zulassungsbehörden nicht bekannt seien.
Die seitens des Ministeriums des Innern vorgetragenen rechtlichen Bedenken hinsichtlich der Umsetzung als „Verordnung" (Art. 80 Abs. 4 GG) führten zu einer Verzögerung des Vorhabens und der Vorlage eines entsprechenden Gesetzentwurfes der Landesregierung.

Nachdem der Gesetzentwurf der Landesregierung vom 2. Oktober 2007 (LT-Drs. 5/894) ohne Debatte in den Ausschuss für Finanzen des Landtages überwiesen wurde, wandte sich der Landesbeauftragte hinsichtlich seiner datenschutzrechtlichen Bedenken zur vorgesehenen praktischen Umsetzung des Gesetzes durch die Oberfinanzdirektion mit Schreiben vom 5. November 2007 direkt an den Ausschuss für Finanzen.
Das Ministerium der Finanzen hatte den Landebeauftragten zwar bei der Erarbeitung des damaligen Verordnungsentwurfes mit Schreiben vom 26. Januar 2007 rechtzeitig beteiligt, dann aber bei der Erarbeitung des Gesetzentwurfes seine Bedenken (Stellungnahme vom 11. Mai 2007) nicht berücksichtigt.

Rechtliche Grundlage für das nunmehr seit 1. April 2008 wirksame Verfahren der Kraftfahrzeugsteuer-Rückständeprüfung ist das Gesetz über die Mitwirkung der Zulassungsbehörden bei der Verwaltung der Kraftfahrzeugsteuer (MZuKraftStG LSA) vom 24. Januar 2008 (GVBl. LSA S. 28).
Danach ist die Zulassung eines Kraftfahrzeugs grundsätzlich nur noch möglich, wenn

1. eine Ermächtigung zum Einzug der Kraftfahrzeugsteuer von einem Konto eines Geldinstituts erteilt wurde und

2. die Person, auf die das Kraftfahrzeug zugelassen werden soll, bei der Finanzverwaltung weder Kraftfahrzeugsteuerrückstände hat noch Nebenleistungen zur Kraftfahrzeugsteuer (Zinsen, Säumniszuschläge) schuldet.

Nach § 3 Abs. 2 des MZuKraftStG LSA erfolgt die Prüfung auf Kraftfahrzeugsteuerrückstände durch die Zulassungsbehörden, die nach dem Gesetzeswortlaut befugt sind, bei den Finanzbehörden des Landes Auskünfte über die Kraftfahrzeugsteuerrückstände einzuholen. Dazu stellen die Finanzbehörden „die für die Prüfung der Kraftfahrzeugsteuerrückstände erforderlichen Daten in elektronischer Form zur Verfügung“.

Der Einzug der Kraftfahrzeugsteuerrückstände wird nach dem MZuKraftStG LSA nicht gleichzeitig den Zulassungsbehörden übertragen, sondern verbleibt in der Zuständigkeit der Finanzämter (§ 3 Abs. 5 MZuKraftStG).
Ein Verfahren der Kraftfahrzeugsteuer-Rückständeprüfung unter Mitwirkung der Zulassungsbehörden musste also unter Beachtung der **Datensparsamkeit** (§ 1 Abs. 2 Satz 1 DSG-LSA) sicherstellen, dass bei einem Abruf oder der Auskunft über den Kraftfahrzeugsteuerrückstand eines Kraftfahrzeughalters den Zulassungsbehörden nur der **Umstand** bekannt wird, ob ein solcher Rückstand besteht oder nicht.
Der Geldbetrag der Kraftfahrzeugsteuerschuld eines Fahrzeughalters unterliegt dem Steuergeheimnis des § 30 AO und darf damit der Zulassungsbehörde, weil für ihre Aufgabenerfüllung **nicht** erforderlich, nicht zur Kenntnis gebracht werden.
Die Fahrzeug-Zulassungsverordnung vom 25. April 2006 (BGBl. I S. 988) erlaubt gem. § 31 Abs. 1 Nr. 21 Buchstabe f der Zulassungsbehörde nur die Speicherung des Hinweises über „Verstöße gegen die Vorschriften über die Kraftfahrzeugsteuer“, nicht aber die Befugnis zur Erhebung und Speicherung des Geldbetrags der bestehenden Kraftfahrzeugsteuerschuld eines Fahrzeughalters.
Dieser Forderung des Landesbeauftragten auf Nichtübertragung des Geldbetrags der Kraftfahrzeugsteuerschuld an die Zulassungsbehörden ist die Oberfinanzdirektion nachgekommen, indem in der sog. Rückständedatei vor Übertragung an die Zulassungsbehörden der Geldbetrag als Datum entfernt wird.

Im April 2008 wurde der Landesbeauftragte durch die Oberfinanzdirektion über die Einrichtung des Verfahrens zur Kraftfahrzeugsteuer-Rückständeprüfung bei den Zulassungsbehörden in Sachsen-Anhalt formell unterrichtet.
Bei weiteren im April 2008, September 2008 und zuletzt im Januar 2009 mit der Oberfinanzdirektion unter Beteiligung des Ministeriums der Finanzen geführten Gesprächen wurden die noch bestehenden Meinungsunterschiede bei der Umsetzung des Verfahrens erörtert, ohne zu einer datenschutzrechtlich letztlich zufriedenstellenden Lösung der Problematik zu gelangen.
Die Oberfinanzdirektion hat sich mit dem Landesbeauftragten darauf verständigt, dass unter der Voraussetzung, dass die Zulassungsbehörde im Rahmen der Rückstandsprüfung als Landesfinanzbehörde tätig wird, kein Abrufverfahren im Sinne des § 7 DSG-LSA vorliegt.
Bei der datenschutzgerechten Auslegung von § 3 Abs. 2 des MZuKraftStG LSA i. V. m. dem § 13 Abs. 1a Satz 4 Kraftfahrzeugsteuergesetz (KraftStG) (Befugnis der Finanzverwaltung zur Auskunftserteilung an die Zulassungsbehörden) und § 13 Abs. 1a Satz 5 KraftStG (Übertragung der Prüfung auf

die Zulassungsbehörde) bestehen immer noch Meinungsverschiedenheiten. Der technische Lösungsansatz zum Verfahren der Rückständeprüfung bei der Kraftfahrzeugsteuer unter Mitwirkung der Zulassungsbehörden wird seitens des Landesbeauftragten weiterhin, insbesondere in Hinblick auf Datensparsamkeit und Datensicherheit, nicht als rechtmäßig angesehen.

Die Mängel bestätigte auch eine im April 2008 in einer Zulassungsbehörde durchgeführte Kontrolle des Landesbeauftragten, denn dort war der ungehinderte Zugriff auf die dem Steuergeheimnis nach § 30 AO unterliegende Rückständedatei möglich. Nach dem Herunterladen der Rückständedatei vom ELSTER-Server der Finanzverwaltung (der sog. Clearingstelle in Düsseldorf) mittels Filetransfer ist die Zulassungsbehörde für die Einhaltung des Steuergeheimnisses verantwortlich, denn sie fungiert hier als Landesfinanzbehörde. Ursächlich für dieses datenschutzrechtliche Defizit bei der kontrollierten Zulassungsbehörde war der Umstand, dass nach Übernahme der Rückständedatei in die Datenbank des Kfz-Zulassungsverfahrens der Behörde die noch vorhandene Rückständedatei nicht sofort automatisch gelöscht wurde. Nur so wäre aber ein unberechtigter Zugriff zu verhindern, denn nach Übernahme in die Kfz-Zulassungsanwendung ist der Zugriff auf eine Information, ob ein Kraftfahrzeugsteuerrückstand besteht, nur noch bei Abruf im Einzelfall durch die Mitarbeiter in der Zulassungsbehörde möglich.
Der Landesbeauftragte hatte sich in diesem Zusammenhang an die Softwarehersteller der Kfz-Zulassungsverfahren gewandt und über diese Sicherheitslücke informiert. Von allen Softwareherstellern wurde bereits mit entsprechenden Softwareupdates dafür gesorgt, dass nach Import der Rückständedatei in die Kfz-Zulassungsdatenbank eine sofortige Löschung dieser Rückständedatei erfolgt.

Der Landesbeauftragte wurde erst im März 2009 seitens der Oberfinanzdirektion über die technische Abwicklung und unterschiedliche Bereitstellung der Rückständedatei für die Finanzämter und die Zulassungsbehörden informiert.
Trotz der dargestellten technischen Zwänge, die sich für die Oberfinanzdirektion bei der Beteiligung an und der Übernahme von länderübergreifend entwickelter und dann gemeinsam genutzter Verfahren des Evolutionär Orientierten Steuersoftware-(EOSS-)Verbundes ergeben, sollte es weiterhin aus datenschutzrechtlicher Sicht beim Ziel bleiben, die Rückständedatei zentral zum Abruf im Einzelfall, wie den Finanzämter, auch den Zulassungsbehörden zur Verfügung zu stellen.

Abzuwarten bleibt zudem, ob der Bundesgesetzgeber die Kraftfahrzeugsteuer, die bisher eine Landessteuer ist, in eine Bundessteuer umwandelt. Dann stellt sich die Frage einer Prüfung von Kraftfahrzeugsteuerrückständen eventuell neu. Aus diesem Grund hat der Landesbeauftragte seine Bedenken zur jetzigen Verfahrensweise der Oberfinanzdirektion zunächst zurückgestellt.

Allerdings rechtfertigen Kostenfragen und praktische Erwägungen bei der Umsetzung eines Landesgesetzes für sich allein keine Eingriffe in die Grundrechte der Bürgerinnen und Bürger.

10. Forschung

10.1. Allgemeines

In diesem Berichtszeitraum wurde der Landesbeauftragte bei 22 neuen und wiederholend bei einigen bereits laufenden Forschungsprojekten beteiligt. Dabei standen Fragen hinsichtlich der Forschung mit anonymen Daten und mit Sozialdaten im Vordergrund.

10.2. Forschung mit anonymen Daten

Bei der Prüfung von Forschungsvorhaben ist bisweilen festzustellen, dass in den Materialien für die Betroffenen und auch in den Einwilligungserklärungen dargestellt wird, dass ausschließlich anonyme Daten an die Forscher übermittelt würden. Anonymisieren ist jedoch eine Veränderung von Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren Person zugeordnet werden können (vgl. § 2 Abs. 7 DSG-LSA).
So war beispielsweise eine „anonyme“ Befragung von Schulkindern kritisch, da aufgrund der kleinen Stichprobe und der Vielzahl der Einzelangaben zur Person eine Identifizierung eines einzelnen Schülers möglich war. Es handelte sich daher um bestimmbare Personen (§ 2 Abs. 1 DSG-LSA), eine anonyme Befragung erfolgte also nicht. Durch eine Änderung des Fragedesigns konnte jedoch eine anonyme Befragung der Schülerinnen und Schüler erreicht werden. Dies hat zur Folge, dass weder das Recht der Betroffenen auf informationelle Selbstbestimmung berührt wird noch es einer Einwilligung als Rechtsgrundlage für die Datenerhebung und -verarbeitung im Rahmen dieser Befragung bedarf. Die Schulkinder und ihre Eltern sollten allerdings rechtzeitig vor der Befragung über das Forschungsvorhaben und die verantwortliche Stelle informiert und ausdrücklich auf die Freiwilligkeit der Befragung hingewiesen werden. Hierzu zählt z. B. auch, darauf hinzuweisen, dass einzelne Fragen unbeantwortet gelassen werden können. Die Beteiligten müssten außerdem nicht nur darüber aufgeklärt werden, dass die Befragung anonym erfolgt, sondern auch darüber, wie Maßnahmen die Anonymität sicherstellen sollen.

Bei einer nach datenschutzrechtlichen Maßstäben anonymen Befragung können auch Fragen über Dritte ohne deren Einwilligung beantwortet werden, beispielsweise Angaben zu den Eltern durch Schüler. Auch hier muss uneingeschränkt sichergestellt sein, dass anhand der Antworten nicht auf einzelne Personen geschlossen werden kann und somit auch für den Dritten kein Identifizierungsrisiko besteht. Eine Einwilligung der Eltern ist nicht erforderlich, sie sollten aber über die Inhalte der Datenerhebung informiert werden.

Auch bei einer pseudonymisierten Datenverarbeitung ist darauf zu achten, dass die Voraussetzungen des § 2 Abs. 7a DSG-LSA tatsächlich erfüllt sind.
So genügt es z. B. nicht, dass, wie in einem Vorhaben vorgesehen, die Patientendaten vom behandelnden Arzt mittels der ersten Buchstaben des Vor- und Nachnamens und des Geburtsdatums „verschlüsselt“ und in dieser Form

an ein Studieninstitut übermittelt werden, wenn in der Einwilligungserklärung dieses Verfahren als Pseudonymisierung bezeichnet wird. Der Landesbeauftragte hat in diesem Fall empfohlen, die einzelnen Verarbeitungs- und Übermittlungsvorgänge detailliert zu beschreiben, ohne jedoch den Begriff „Pseudonymisierung“ zu verwenden.

10.3. Forschung mit Sozialdaten

Oft sind für ein Forschungsvorhaben auch Sozialdaten erforderlich (vgl. auch Ziff. 21.19). Diese unterliegen jedoch einem besonderen Schutz, dem Sozialgeheimnis. Eine Sozialdatenübermittlung für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich ist daher nur zulässig, wenn die engen Voraussetzungen des § 75 SGB X erfüllt sind.
Häufig unterschätzt wird das Erfordernis nach § 75 Abs. 1 Satz 2 SGB X, wonach eine Übermittlung ohne Einwilligung des Betroffenen nicht zulässig ist, soweit es zumutbar ist, die Einwilligung nach § 67b SGB X einzuholen oder den Zweck der Forschung oder Planung auf andere Weise zu erreichen. Die Voraussetzung, dass keine Einwilligungen eingeholt werden können, bedarf einer differenzierten und tragfähigen Begründung. Enge zeitliche Vorgaben oder höhere Kosten vermögen keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung zu rechtfertigen. Der mit der Einholung der Einwilligung verbundene Verwaltungsaufwand reicht für die Begründung der Unzumutbarkeit nicht aus.

Darüber hinaus wird sehr häufig dargestellt, dass Verweigerungen der Einwilligung nicht zufällig verteilt seien, sondern mittels teilnehmerseitiger Selektivität der Einwilligungen zu Verzerrungen führen würden. Die Repräsentativität der Untersuchung erfordere aber eine zufällige Verteilung, beispielsweise sozio-demographischer Merkmale der Population. Es sei seit langem bekannt, dass die Anforderung schriftlicher Einwilligungen die Antwortquoten stark senke und die Ausfälle bei Personen mit geringerem Bildungsgrad systematisch höher seien.
Hinzu käme das Problem trägerproduzierter Selektivität. In einer Untersuchung habe die Einholung der Einwilligung in eine telefonische Befragung durch die Dienststellen, die die Sozialleistungen bewilligten, zu einer Einwilligungsquote zwischen 1% und 63% geführt.

Ungeachtet der bekannten Schwierigkeiten hinsichtlich der Eigenwilligkeit der Betroffenen (Selbstbestimmung) und der organisatorischen (ggf. abstellbaren) Befragungsmängel hat der Gesetzgeber keinen Anlass gesehen, von der Priorität der Einwilligung abzusehen.

Zudem bestehen oft lediglich Vermutungen darüber, welcher Verzerrungseffekt tatsächlich eintritt. In einem bundesweiten Projekt wurde die Frage gestellt, ob nicht die Unzufriedenheit der Befragten auch zu höheren Einwilligungs- und Stellungnahmequoten führen kann. Darauf erging der Hinweis, dass das wissenschaftliche Problem sei, dass man nicht wissen könne, welcher Effekt eintrete bzw. überwiege. Wenn keinerlei Einschätzung möglich sein soll, kann dies nicht zwangsläufig bedeuten, dass die Einholung von Einwilligungen nicht zumutbar wäre. Aus datenschutzrechtlicher Sicht würde dies nämlich bedeuten, dass die Interessen der Betroffenen bereits dann zu-

rückzustehen haben, wenn die Forscher eine Verzerrung lediglich vermuten. Das grundsätzliche Gebot der Einholung einer Einwilligung des § 75 Abs. 1 Satz 2 SGB X würde damit ins Leere laufen.

Die Einholung von Einwilligungen kann jedoch z. B. unzumutbar sein, wenn das zu erwartende Einwilligungsverhalten aus besonderen Gründen notwendig dem Forschungszweck zuwider läuft, unvorhersehbare Entwicklungen eine kurzfristige Erhebung notwendig machen oder der Aufwand der Einholung der Einwilligung aus besonderen Gründen im Einzelfall einen unverhältnismäßigen Aufwand erfordert.

11. Gefahrenabwehr

11.1. Gesetz zur Vorsorge gegen die von Hunden ausgehenden Gefahren

„Dauerstreit beendet: Ab März gilt ein neues Kampfhundegesetz“. So titelte die Magdeburger Volksstimme am 12. Dezember 2008. „Der Landtag von Sachsen-Anhalt hat gestern nach jahrelangen kontroversen Diskussionen mit den Stimmen der Koalitionsfraktionen CDU und SPD ein Kampfhundegesetz beschlossen. Es tritt am 1. März 2009 in Kraft“, war weiter zu lesen. Die kontroversen Diskussionen hier in jeder Einzelheit darzustellen, würde den Rahmen eines Tätigkeitsberichtes sprengen. Deshalb soll es dabei belassen werden, die entscheidenden Entwicklungsstufen aufzuzeigen.

Im Oktober 2006 leitete die Landesregierung ihren Entwurf eines „Gesetzes gegen die von Hunden ausgehenden Gefahren“ (LT-Drs. 5/284) dem Landtag zu. Die öffentliche Anhörung zu diesem Entwurf wurde durch den Ausschuss für Inneres des Landtages im Januar durchgeführt. Den Rest des Jahres 2007 wurde viel über den Entwurf und die Erforderlichkeit eines Hundegesetzes an sich diskutiert. Im Dezember 2007 legten die Fraktionen der CDU und SPD einen eigenen Gesetzentwurf (LT-Drs. 5/1011) vor. Die öffentliche Anhörung zu diesem Entwurf fand im März 2008 statt. Aus Anlass dieser Anhörung wurde der Landesbeauftragte gebeten, eine Stellungnahme insbesondere im Hinblick auf die vorgesehene Regelung zur Meldepflicht von Ärzten und Tierärzten abzugeben.

Dieser Bitte kam der Landesbeauftragte im Mai 2008 nach und stellte zum Gesetzentwurf der Fraktionen fest:
„§ 14 des Gesetzentwurfs [in der Endfassung § 13] verpflichtet sowohl Human- als auch Veterinärmediziner zur Meldung von in Ausübung ihres Berufs erlangten Erkenntnissen zu Beißvorfällen und Verletzungen, die auf Angriffe von Hunden zurückzuführen sind. Die Meldepflicht entfällt nur, wenn der Nachweis einer bereits erfolgten Meldung vorliegt.
Die vorgeschlagene Regelung zur Meldepflicht in § 14 des Entwurfs erscheint rechtsstaatlich unter zwei Gesichtspunkten bedenklich.
So bestehen Zweifel an der Verhältnismäßigkeit. Human- und Veterinärmediziner werden hier ohne jede Möglichkeit zur Differenzierung hinsichtlich Schwere oder Ursache der Verletzungen zur Meldung verpflichtet. ...

§ 14 Abs. 2 des Entwurfs, wonach die Mediziner nicht meldepflichtig sind, wenn dem Arzt ein Nachweis über eine bereits erfolgte Meldung vorliegt, dürfte schon die Geeignetheit, zumindest jedoch die Bestimmtheit fehlen. ...“
„Ich rege an, die medizinischen Fachrichtungen differenziert zu betrachten. Schon in Bezug auf den dem Gesetz zugrundliegende typischen Sachverhalt ergeben sich Unterschiede. Kommt es zu Beißvorfällen mit Verletzungen von Menschen, wird zunächst, wenn nicht sogar ausschließlich, ein Humanmediziner durch die Behandlung Verletzter mit dem Geschehen befasst sein. ...“
„Anders als Humanmedizinern steht zwar Tiermedizinern kein Zeugnisverweigerungsrecht i. S. d. § 53 StPO zu. Aber auch sie unterliegen der Schweigepflicht. Eine gesetzlich fixierte Befugnis zur Weitergabe von Halterinformationen könnte zwar erwogen werden, dürfte aber dem Anliegen des Gesetzentwurfs wohl nicht genügen. ... Tiermediziner einer Meldepflicht zu unterwerfen, erscheint dem Landesbeauftragten daher vom Grundsatz her vertretbar.“ ...
„Darüber hinaus ist der Umfang der Meldung nicht definiert. Welche Angaben bzw. personenbezogenen oder -beziehbaren Daten Mediziner der zuständigen Behörde melden müssen, wird nicht konkretisiert. ...“

Im Juli 2008 legten die Fraktionen der CDU und SPD einen geänderten Gesetzentwurf vor, der auch dem Landesbeauftragten übersandt wurde. Mit der Übersendung war die Bitte verbunden, die beabsichtigten Änderungen hinsichtlich der Schaffung eines **zentralen Registers** datenschutzrechtlich zu prüfen und eine Stellungnahme abzugeben. Nach Auswertung auch der bestehenden Rechtslage in anderen Bundesländern äußerte sich der Landesbeauftragte im August 2008 zu der Fassung des Gesetzentwurfes, die die Errichtung eines Zentralen Registers vorsah.

„Im Vergleich zum bisherigen Gesetzentwurf wurde in § 15 eine Regelung zur Errichtung eines zentralen Registers geschaffen. Erfasst werden sollen hier alle Hunde und nicht nur die gefährlichen.
Die Errichtung eines solchen zentralen Registers begegnet ... derzeit datenschutzrechtlichen Bedenken. Als Zweck definiert der Gesetzentwurf in § 1 die Vorbeugung und Abwehr von Gefahren für die öffentliche Sicherheit, die mit dem Halten und Führen von Hunden verbunden sind. Inwieweit die Errichtung eines zentralen Registers für alle Hunde dazu erforderlich ist, erschließt sich zunächst nicht. ...
Sollte jedoch an der Errichtung eines solchen zentralen Registers festgehalten werden, wäre die Vorschrift für eine datenschutzgerechte Ausgestaltung überarbeitungsbedürftig.
Hinsichtlich des Umfangs der in einem zentralen Register zu erfassenden Daten lehnt sich der Gesetzentwurf an die Regelungen des Hamburgischen Gesetzes über das Halten und Führen von Hunden an. ... Im Gegensatz dazu regelt die Ordnungsbehördliche Verordnung zur Durchführung des Landeshundegesetzes des Landes Nordrhein-Westfalen in § 5 lediglich, dass neben der Nummer des Mikrochips, Neuzugang, Abgang und Wechsel der Behördenzuständigkeit innerhalb des Geltungsbereiches des Gesetzes erfasst werden. Unter datenschutzrechtlichen Gesichtspunkten ist eine Lösung, wie sie in Nordrhein-Westfalen getroffen wurde, zu bevorzugen und für die Aufgabenwahrnehmung auch hinreichend. ...

Die dem Betretensrecht unterfallenden Bereiche wurden ... ausgeweitet. Die derzeitige Entwurfsfassung stellt auf das Grundstück als zu betretender Bereich ab. Der Begriff Grundstück schließt alle sich auf ihm befindenden Gebäude - also auch Wohngebäude und Betriebsräume - ein. Insoweit wurden die vormals bestehenden Einschränkungen für Wohngebäude und Betriebsräume außerhalb der Betriebszeiten aufgehoben. Vor dem Hintergrund des Grundsatzes der Verhältnismäßigkeit erscheint eine derart pauschale Regelung nicht verfassungskonform."

Der Gesetzentwurf in der Fassung vom Juli 2008 wurde insbesondere wegen der Regelungen um die Errichtung eines Zentralen Registers weiter eingehend diskutiert, bis dann im November 2008 die Beschlussempfehlung des Ausschusses für Inneres des Landtages (LT-Drs. 5/1571) erarbeitet war. Dass auch diese dritte Fassung des Gesetzentwurfes nach wie vor datenschutzrechtlich nicht unerheblichen Bedenken begegnete, machte der Landesbeauftragte im November 2008 gegenüber dem Ausschuss für Inneres des Landtages nochmals deutlich.

„Die ... zum Gesetzentwurf getroffenen Feststellungen halte ich, soweit es das Betretensrecht nach § 13 Abs. 2 des Gesetzentwurfes betrifft, aufrecht. Die derzeitige Ausgestaltung des Betretensrechtes erscheint mir vor dem Hintergrund des Grundsatzes der Verhältnismäßigkeit nach wie vor nicht verfassungskonform.

Von besonderer datenschutzrechtlicher Bedeutung ist die Einrichtung eines zentralen Registers, wie es § 15/1 des Gesetzentwurfes vorsieht. Zu den grundsätzlichen Bedenken ... verweise ich auf meine ... dargestellten Bedenken ...
Ich habe u. a. darauf hingewiesen, dass aus dem Entwurf der Vorschrift zum zentralen Register nicht deutlich wird, in welcher Form das zentrale Register durch die zuständigen Behörden genutzt werden kann. Die nunmehr vorliegende Fassung des Gesetzentwurfes beschreibt in § 15/1 Abs. 2 die Zwecke, denen ein zentrales Register dienen soll.
Danach soll das zentrale Register

1. der Durchführung dieses Gesetzes einschließlich der Erstellung der für die Überprüfung der Auswirkungen dieses Gesetzes nach §§ 17 Abs. 4 und 18 erforderlichen Statistiken,
2. der Ermittlung der letzten Halterin oder des letzten Halters eines Fundhundes oder eines herrenlosen Hundes,
3. der Durchführung der nach Maßgabe des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt erforderlichen Maßnahmen, um eine von einem Hund oder der Haltung und Führung eines Hundes ausgehende Gefahr für die öffentliche Sicherheit abzuwehren und
4. bei der Erhebung der Hundesteuer zur Auskunfterteilung über Namen und Anschrift der Hundehalterin oder des Hundehalters an Behörden, soweit dies zur Durchführung dieses Gesetzes, des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt oder des Tierseuchengesetzes erforderlich ist,

dienen.

Bei nicht allen dieser Zwecke erschließt sich der Anwendungsbereich, der mit der jeweiligen Regelung abgedeckt werden soll. ...

Im Übrigen gebe ich ... zu bedenken, dass die Differenzierung bei nicht gefährlichen Hunden, die vor bzw. nach Inkrafttreten des Gesetzes geboren wurden, Fragen nach der Willkürfreiheit eines zentralen Registers aufwirft. ..."

Im Dezember 2008 wurde nach Beratungen im Plenum, im Ausschuss für Inneres und im Ausschuss für Finanzen des Landtages eine Beschlussempfehlung an den Landtag (LT-Drs. 5/1623) abgegeben, die der Landtag in seiner Sitzung am 11. Dezember 2008 beschlossen hat und die am darauffolgenden Tag zu der einführend erwähnten Schlagzeile in der Volksstimme führte. Auch das letztendlich beschlossene Gesetz zur Vorsorge gegen die von Hunden ausgehenden Gefahren begegnet datenschutzrechtlichen Bedenken. Nicht jede Anregung des Landesbeauftragten im Gesetzgebungsverfahren hat sich im Gesetzestext (GVBl. LSA 2009 S. 22) niedergeschlagen. Die Praxis wird nun zeigen, inwieweit die getroffenen Regelungen geeignet sind, den Schutzzweck des Hundegesetzes zu erreichen.

Ende Januar 2009 legte das Ministerium des Innern dem Landesbeauftragten erstmals den Entwurf einer Verordnung zur Durchführung des Gesetzes zur Vorsorge gegen die von Hunden ausgehenden Gefahren vor. Die Prüfung der Unterlagen ergab, dass die Regelungen - insbesondere das Hunderegister betreffend - einer Überarbeitung bedurften. In Abstimmung zwischen dem Ministerium des Innern und dem Landesbeauftragten wurden die entsprechenden Regelungen so angepasst, dass gegen deren Ausgestaltung derzeit keine grundsätzlichen datenschutzrechtlichen Bedenken bestehen (GVBl. LSA 2009 S. 133). Der Landesbeauftragte wird die praktische Umsetzung der Vorschriften begleiten und das Hunderegister auch vor Ort in Augenschein nehmen.
An der Kritik, die der Landesbeauftragte hinsichtlich des Gesetzes an sich äußerte, ändert die Beurteilung der Verordnung allerdings nichts. Die Errichtung eines Hunderegisters in der jetzigen Form betrachtet er nach wie vor als problematisch, da dessen Erforderlichkeit nicht hinreichend belegt ist.

11.2. Entwurf eines Versammlungsgesetzes

Die Landesregierung hat die im Zuge der Föderalismusreform auf die Länder übergegangene Gesetzgebungskompetenz zum Versammlungsrecht wahrgenommen und den Entwurf eines Gesetzes vorgelegt. Mit einem gewissen Erstaunen nahm der Landesbeauftragte zur Kenntnis, dass der Entwurf zunächst im Internetangebot des Landes eingestellt worden war. Ein Hinweis war nicht erfolgt, erst auf Nachfrage wurde dann ein Entwurf übersandt. Dieses Verfahren und die noch verbleibende relativ kurze Frist bis zur zweiten Kabinettsbefassung vermittelten fast den Eindruck, als werde eine Beteiligung des Landesbeauftragten bei diesem Gesetzesvorhaben zumindest für nicht so wesentlich erachtet. Auch erstaunte der Umstand, dass die Anmerkungen des Landesbeauftragten, trotz seiner umgehenden Stellungnahme, keinen Widerhall in der Begründung zum Gesetzentwurf fanden.

In seiner Äußerung wies der Landesbeauftragte zunächst darauf hin, dass vor allem durch Bezugnahme auf das bisher geltende Versammlungsgesetz des Bundes nur auf den ersten Blick der Vorteil von Übersichtlichkeit erreicht wird. Tatsächlich ist diese Regelungsform nicht nur fehleranfällig, sie führt vor allem dazu, dass der durchschnittliche Leser nicht sofort erkennen kann, dass Beschränkungen seiner Grundrechte nicht nur durch den aktuellen Gesetzentwurf vorgenommen werden sollen, sondern dass die auch nach dem bisherigen Recht für die Polizei schon bestehenden Befugnisse zu Grundrechtseingriffen ins Landesrecht eingeführt werden. Verstärkt wurde dies noch dadurch, dass das Zitiergebot hinsichtlich Art. 6 Abs. 1 der Verfassung des Landes Sachsen-Anhalt nicht beachtet worden war. Denn, da das bisherige Bundes-Versammlungsgesetz (VersG) weitgehend als Landesgesetz fortgeführt werden soll, werden auch die dort geregelten Eingriffe in das Grundrecht auf informationelle Selbstbestimmung durch die Bild- und Tonaufnahmebefugnisse nach §§ 12a und 19a VersG überführt.

Nicht nur wegen der Verständlichkeit für Bürgerinnen und Bürger hätte der Landesbeauftragte ein eigenformuliertes Gesetz ohne Verweisnormen - vor allem, da es in einen der wesentlichsten Bereiche aktueller demokratischer Teilhabe eingreift - begrüßt. Die Wahrscheinlichkeit, dass wegen der nun gewählten Regelungstechnik erst durch richterliche Entscheidungen die Rechtslage verklart werden muss, ist hoch. Es ist aber den grundgesetzlichen Rechten ein schlechter Dienst erwiesen, wenn Bürgerinnen und Bürger (und auch Behörden und Polizei) sich zu wesentlichen Einzelheiten erst in Gerichtsurteilen statt durch einen Blick ins Gesetz informieren können.
Durch ein Volltext-Gesetz hätte sich zudem einfacher die Möglichkeit ergeben, in besonderer Weise Rechtsprechung u. a. zu **Bild- und Tonüberwachung** bei Versammlungen zu berücksichtigen. Vor allem dem Erforderlichkeitsgrundsatz, wegen der Einschüchterungswirkungen für die Grundrechtsausübung, hätte Nachdruck verliehen werden können. Der Landesbeauftragte hat angeregt, im Gesetz selbst vorzugeben, dass sich Überwachungsaufnahmen auf Störer zu beziehen haben und andere Personen nur mit aufgezeichnet werden dürfen, wenn dies unvermeidbar ist. Dadurch hätte auch unterstrichen werden können, dass Überblicksaufnahmen als Datenvorratsspeicher ohne zugrunde liegende konkrete tatsächliche Anhaltspunkte für erhebliche Gefahren grundsätzlich nicht zulässig sind, wie es das Bundesverfassungsgericht in seiner Entscheidung zum Bayerischen Versammlungsgesetz vom 17. Februar 2009 (Az.: 1 BvR 2492/08; NVwZ 2009, 441) festgestellt hat. Dies ist notwendig, da bedingt durch die technisch mögliche Auflösungstiefe heutiger Kameras die nachträgliche Identifikation auch von Unbeteiligten/Nichtstörern regelmäßig möglich ist. Wenn es auch bisher keinen Niederschlag im Gesetzentwurf fand, so hat das Ministerium des Innern doch mit Erlass an alle Polizeidienststellen vom 12. März 2009 auf die höchstrichterliche Rechtsprechung aufmerksam gemacht und um Beachtung der Ausführungen des Bundesverfassungsgerichtes zur Anfertigung von Übersichtsaufnahmen gebeten. Der Entwurf eines Vollgesetzes würde zudem die Option für angemessene Datenverarbeitungsregelungen eröffnen, an denen es bisher im Versammlungsrecht fehlt.

Der Landesbeauftragte hat in diesem Zusammenhang erneut darauf hingewiesen, dass das Gesetz über den Verfassungsschutz im Land Sachsen-

Anhalt keine ausreichende Grundlage für insbesondere die optische Erfassung personenbezogener Daten von Demonstrationsteilnehmern durch den Verfassungsschutz bietet. Im Zuge einer Neuregelung des Versammlungsrechts bietet es sich geradezu an, auch Festlegungen zur Video- und Tonüberwachung durch den Verfassungsschutz bei Versammlungen zu treffen. In seinem Antwortschreiben auf eine entsprechende Anfrage des Landesbeauftragten bestätigte das Ministerium des Innern des Landes Sachsen-Anhalt letztlich die Situation eines Grundrechtseingriffs, verneinte aber, insoweit in sich widersprüchlich, dass in die Versammlungsfreiheit eingegriffen wird (VIII. Tätigkeitsbericht, Ziff. 24.5).

Auch angesichts deutlicher Hinweise der Sachverständigen zum Gesetzentwurf (LT-Drs. 5/1301) in der öffentlichen Anhörung des Ausschusses für Inneres des Landtages von Sachsen-Anhalt am 23. Oktober 2008 und des Gesetzgebungs- und Beratungsdienstes wurde in den weiteren Beratungen dessen Volltext-Gesetzentwurf zum Versammlungsgesetz zugrunde gelegt. Die Regelung zu den Bild- und Tonaufzeichnungen orientiert sich an den Vorgaben des Bundesverfassungsgerichts.

11.3. Änderung des Spielbankgesetzes

Im Juli 2008 wurde dem Landesbeauftragten erstmalig Gelegenheit gegeben, zum Gesetzentwurf für ein neues Spielbankgesetz des Landes Sachsen-Anhalt Stellung zu nehmen. Im Stadium eines Referentenentwurfs wurde der Gesetzentwurf dem Landesbeauftragten im Verlauf eines halben Jahres insgesamt dreimal übersandt, bevor er im Februar 2009 von der Landesregierung eingebracht wurde.

In seiner ersten Stellungnahme vom Juli 2008 musste der Landesbeauftragte auf die nicht datenschutzgerechte Ausgestaltung der Regelungen zur Sperrdatei, zur Besucherdatei, zur Videoüberwachung und zur Aufsicht hinweisen.

Sperrdatei

In die neuen Vorschriften über die Sperrdatei wurden die entsprechenden Regelungen der Verordnung über die Spielordnung in öffentlichen Spielbanken (SpielO-VO) eingebunden. Dabei wurde aber die „Mitwirkungspflicht“ der Besucher vom „Erteilen von Auskünften“ auf das „Beibringen von geeigneten Nachweisen“ ausgedehnt. Die Erforderlichkeit dieser Ausweitung erschloss sich aus dem reinen Gesetzestext – eine Begründung zum Gesetzentwurf lag noch nicht vor – nicht. Sie war insoweit datenschutzrechtlich als nicht zu vertreten anzusehen.

Besucherdatei

Auch für die Besucherdatei wurden die entsprechenden Vorschriften der SpielO-VO in den Gesetzentwurf eingebunden und dabei der Umfang der für die Besucherdatei zu erhebenden personenbezogenen Daten um die Art, Nummer und ausstellende Behörde des amtlichen Ausweises erweitert. Die Erforderlichkeit der Aufnahme dieser Daten erschließt sich aus den vorliegenden Unterlagen nicht und drängt sich auch ansonsten nicht unmittelbar auf. Die Änderung ist in der Folge damit zunächst datenschutzrechtlich abzulehnen.

Videoüberwachung

Die aufgenommene Verpflichtung zum Hinweis auf den Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen war datenschutzrechtlich zu begrüßen. Dennoch sollte unmissverständlich formuliert werden, dass sich die Hinweispflicht auf die Eingangsbereiche für Besucher und Personal erstreckt. Die Mitarbeiter der Spielbanken sind datenschutzrechtlich genauso Betroffene einer Videoüberwachung wie die Besucher. Die Aufnahme einer Informationspflicht des Zulassungsinhabers zu Art und Umfang der Videoüberwachung seinen Beschäftigten gegenüber wurde angeregt.

Aufsicht

Die Vorschrift verpflichtet Spielbanken u. a. dazu, anonymisierte Spielerdaten den Aufsichtsbehörden zur Verfügung zu stellen. Die Form der Anonymisierung ist nicht beschrieben, bedarf aber einer zumindest landeseinheitlichen Festlegung.

Im Oktober 2008 wurde das zweite Mal ein Referentenentwurf - diesmal mit einer ersten Begründung - zur Stellungnahme übersandt. Der überarbeitete Entwurf hatte sich aus datenschutzrechtlicher Sicht in Teilen verbessert, was der Landesbeauftragte auch zum Ausdruck brachte: „Im Vergleich zum Vorgängerentwurf kann ich zunächst feststellen, dass die Regelungen zur Sperrdatei in § 5 und zur Besucherdatei in § 7 nunmehr eine datenschutzrechtlich vertretbare Fassung gefunden haben. Insoweit konnten zwei zentrale Bedenken ausgeräumt werden.“ Auch wenn so ein Teil der Bedenken zerstreut wurden, blieben weitere offen und kamen neue hinzu.

Videoüberwachung

„Zwar wurde meine Anregung, die Hinweispflicht bezüglich der Videoüberwachung ausdrücklich auch für die Eingangsbereiche des Personals aufzunehmen, berücksichtigt. Allerdings wurde der Regelungsumfang gleichzeitig dahingehend verringert, dass entsprechende Hinweise auf den Eintrittskarten nicht mehr vorgesehen sind. In der Begründung wird auf die Präzisierung der Hinweispflicht hinsichtlich des Personals verwiesen, die Einschränkung der Hinweispflicht durch den Verzicht von Hinweisen auf den Eintrittskarten findet keinen Eingang in die Begründung.

Hier ist nicht ersichtlich – und infolge fehlender Begründung auch nicht nachvollziehbar -, aus welchem Grund auf die Hinweispflicht auf Eintrittskarten verzichtet wurde. Die Eintrittskarten bieten dem Besucher viel unmittelbarer die Möglichkeit zur Information als Aushänge. Die Eintrittskarte nimmt der Besucher an sich, was die Wahrscheinlichkeit eines bewussten Wahrnehmens der Hinweise gegenüber Aushängen ungleich höher erscheinen lässt. ...“

Aufsicht

„In der Vorschrift wird die Unterstützung der Aufsichtsbehörde durch das Landeskriminalamt geregelt. Dabei trifft es zu, dass die bisher im Erlasswege ... geregelte Zuständigkeit in das Gesetz übernommen werden soll. Darüber hinaus - und das findet in der Begründung keinen Niederschlag - wird zum einen der Umfang der zu sammelnden und auszuwertenden Daten nicht unerheblich erweitert und zum anderen eine neue Übermittlungsbefugnis begründet.

Nach der bisher geltenden Erlasslage war das Landeskriminalamt berechtigt, Erkenntnisse zu Straftaten und Gefahrenlagen im Zusammenhang mit Spielbanken zu sammeln und auszuwerten. Der vorliegende Gesetzentwurf ermächtigt das Landeskriminalamt nunmehr, Erkenntnisse zu Straftaten und

Gefahrenlagen zu sammeln und auszuwerten. Diese Straftaten und Gefahrenlagen müssen nicht mehr im Zusammenhang mit Spielbanken stehen. ... Die Gesetzesbegründung erläutert die Erforderlichkeit dieser Ausweitung der Befugnisse des Landeskriminalamtes nicht. Mangels Erforderlichkeitsnachweis betrachte ich diese Ausweitung zunächst als unverhältnismäßig und damit unzulässig.
Entsprechend der bestehenden Erlasslage ist das Landeskriminalamt derzeit lediglich berechtigt, die gesammelten und ausgewerteten Erkenntnisse zu Straftaten im Zusammenhang mit Spielbanken an die Spielbankaufsicht im Rahmen der rechtlichen Übermittlungsvoraussetzungen weiterzugeben. ... Mit der vorgesehenen Gesetzesänderung würde allerdings eine spezialgesetzliche Übermittlungsbefugnis für das Landeskriminalamt an die Spielbankaufsicht installiert. Wenn gegen die Einführung einer speziellen Übermittlungsbefugnis in das Spielbankgesetz auch keine grundsätzlichen Bedenken bestehen, so ist deren Ausgestaltung datenschutzrechtlich nicht hinnehmbar. Die Übermittlung von Daten an die Spielbankaufsicht soll lediglich an die Voraussetzung gebunden sein, „... dass deren Kenntnis für die Handhabung der Aufsicht von Bedeutung ist“. Diese Schwelle ist zu niedrig, der Begriff zu unbestimmt. Unter den Begriff „von Bedeutung“ kann so ziemlich jede Information subsumiert werden. Vor allem unter dem Eindruck der vorstehend bereits beschriebenen Erweiterung der Befugnisse des Landeskriminalamtes wären die Zulässigkeitsvoraussetzungen klar zu umreißen, und zwar im Gesetz selbst und nicht im Erlasswege.“

Im Januar 2009 wurde der Gesetzentwurf dem Landesbeauftragten dann zum dritten Mal übersandt. Wenn es vom ersten zum zweiten Entwurf noch deutliche Verbesserungen gab, so musste der Landesbeauftragte dem dritten Entwurf ein schlechteres Zeugnis ausstellen. „Im Vergleich zum Vorgängerentwurf muss festgestellt werden, dass der derzeitige Entwurfsstand weit weniger datenschutzgerecht ist. Die vorgenommenen Veränderungen von datenschutzrechtlicher Relevanz führen ausschließlich zu Verschlechterungen aus Sicht der Betroffenen und sind im Kern lediglich mit einer Arbeitsvereinfachung begründet.“ Im Einzelnen gründet sich diese Einschätzung des Landesbeauftragten auf nachfolgend näher bezeichnete Regelungen im Gesetzentwurf:
<u>Videoüberwachung</u>
„War der Zulassungsinhaber nach ... der bisherigen Regelung zum Einsatz technischer Mittel zur Anfertigung von Bildaufzeichnungen befugt, so ist er nach der Regelung im aktuellen Gesetzentwurf dazu verpflichtet. Worin die Notwendigkeit der Verpflichtung besteht, ist nicht begründet. ... Vor dem Hintergrund dieser neuen Verpflichtung, die eine stärkere Beeinträchtigung der Rechte der Betroffenen bedeutet, erscheint es immer weniger plausibel, dass nach wie vor die Streichung der gesetzlichen Verpflichtung zur Aufnahme von Hinweisen zur Videoüberwachung auf den Eintrittskarten vorgesehen ist. Beide Maßnahmen („Ausbau“ der Videoüberwachung und Verzicht auf Hinweispflicht) gehen einseitig zu Lasten der Betroffenen. ... Die Einschränkung der Hinweispflicht durch den Verzicht von Hinweisen auf den Eintrittskarten findet zudem nach wie vor keinen Eingang in die Begründung.“
„Datenschutzrechtlich gleichfalls eine Verschlechterung der Stellung der Betroffenen stellt die Festsetzung der Speicherfrist für Videoaufzeichnungen auf zwei Wochen dar. Im bisherigen Entwurf waren die Aufzeichnungen „spätes-

tens zwei Wochen nach der Aufzeichnung zu löschen.“ Mit der neuen Regelung wurde die Speicherdauer praktisch erhöht, weil die bisherige Regelung eine frühzeitigere Löschung ermöglichte. ... Die Notwendigkeit der Änderung der Rechtslage ist mangels Begründung nicht nachzuvollziehen.“

Spielangebot

„Es wird ein automatisches Datenerfassungssystem eingeführt, zu dessen Einrichtung und Unterhaltung der Zulassungsinhaber verpflichtet ist. Dienen soll dieses System der Überwachung der Spielsicherheit. Das System muss dabei u. a. als wesentliche Betriebsdaten Anzahl, Betrag, Datum, Uhrzeit von Nachlagen und von Gewinnauszahlungen an Gäste laufend und unterbrechungsfrei erfassen und dokumentieren. In Verbindung mit der Verpflichtung zur Videoüberwachung führt das System zu einer wahrscheinlich lückenlosen Überwachung der Betroffenen. Inwieweit solch ein umfassendes System zur Überwachung des Spielbetriebes in steuerlicher Hinsicht erforderlich ist, erschließt sich nicht. Ob diese Ausgestaltung als angemessen und damit zulässig anzusehen ist, dürfte davon abhängig sein, welche Daten zur Überwachung des Spielbetriebes in steuerlicher Hinsicht tatsächlich erforderlich sind und auf welche andere - ggf. weniger grundrechtsbeeinträchtigende - Art und Weise diese erhoben werden können. Allein personalwirtschaftliche Argumente vermögen einen tieferen als erforderlichen Grundrechtseingriff nicht zu rechtfertigen.“

Aufsicht

„Über die Änderung wurden die Übermittlungsbefugnisse der Finanzbehörden erweitert. Bisher sollten Übermittlungen zulässig sein, „... soweit die Offenbarung der Ausübung der Aufsicht über die Spielbanken dient.“ Nunmehr soll die Zulässigkeit immer dann gegeben sein, „... soweit die Offenbarung der Erreichung der Ziele des § 1 des Glücksspielstaatsvertrages und des § 1 Abs. 1 Satz 2 dient.“ Der Rechtsbegriff „Erreichung der Ziele dient“ dürfte als zu unbestimmt anzusehen sein, zumal die Ziele des Staatsvertrages zum Glücksspielwesen in Deutschland sehr offen und umfassend formuliert sind. Eine Abgrenzung hinsichtlich der Übermittlungsbefugnis wird unter diesen Voraussetzungen schwer vorzunehmen sein, was im Ergebnis dazu führen dürfte, dass im Zweifelsfall alle Informationen übermittelt werden. ... Die vorgesehene Übermittlungsbefugnis erscheint unnötig weit gefasst und für den Anwender ungeeignet, weil keine überschaubaren Voraussetzungen gebildet wurden.“

Zu dem letztendlich im Februar 2009 eingebrachten Gesetzentwurf (LT-Drs. 5/1785) musste der Landesbeauftragte feststellen, dass keine der in seiner Stellungnahme vom Januar 2009 aufgeführten Bedenken Berücksichtigung fanden. Zudem wurde im Rahmen der Gesetzesbegründung auf die vorgetragenen datenschutzrechtlichen Gesichtspunkte kein Bezug genommen. Der Vorlage war lediglich der Satz: „ Der Gesetzentwurf wurde mit dem Landesbeauftragten für den Datenschutz abgestimmt.“ zu entnehmen. Auf nach wie vor bestehende rechtliche Bedenken gegen die Ausgestaltung einzelner Regelungen findet der Leser keinen Hinweis.

Der Landesbeauftragte trug die fortbestehenden Bedenken am 23. April 2009 in einer Anhörung des Innen- und Finanzausschusses des Landtages vor und empfahl zusätzlich mehr Normenklarheit für die Regelungen zu den landes- und bundesweiten Sperrdateien.

11.4. Abrufverfahren bei der Waffenbehörde

Im Oktober 2008 wandte sich der behördliche Datenschutzbeauftragte eines Landkreises an den Landesbeauftragten. Er bat um Unterstützung bei der datenschutzrechtlichen Beurteilung eines Vorhabens des Landkreises. Der Landkreis wollte ein automatisiertes Abrufverfahren für die personenbezogenen Daten der unteren Waffenbehörde einrichten. Damit sollte es dem zuständigen Polizeirevier im Rahmen eines Pilotprojektes möglich sein, außerhalb der Dienstzeiten der Landkreisverwaltung Abfragen aus der Datenbank des Landkreises zu Waffenbesitzern vorzunehmen.

Zulässig sind Anfragen der Polizei an die Waffenbehörden bereits nach geltender Rechtslage. Aus Gründen der Planung des polizeilichen Vorgehens und auch der Eigensicherung der Beamten fragt die Polizei vor Einsätzen an, ob eine der voraussichtlich anzutreffenden Personen im Besitz von Waffen ist und welche Art von Waffen es sind. Diese Abfragen erfolgen während der Dienstzeiten der Landkreisverwaltung telefonisch. Außerhalb der Dienstzeiten wird ein Mitarbeiter des Landkreises angerufen, der sich dann auf den Weg in die Dienststelle macht, die Auskunft erteilt und anschließend wieder den Heimweg antritt. Um so außerhalb der Dienstzeiten eine Auskunft zu erteilen, vergehen bis zu zwei Stunden.

Sowohl der Landkreis als auch die Polizei zeigten ein erhebliches Interesse an der Einrichtung eines solchen automatisierten Verfahrens. Das Interesse des Landkreises richtete sich schwerpunktmäßig auf den verminderten Arbeitsaufwand, den ein automatisiertes Abrufverfahren außerhalb der Dienstzeiten bedeuten würde. Die Polizei versprach sich vor allem zeitnahe Auskünfte. Aber nicht nur diese beiden Beteiligten verfolgten die Angelegenheit mit Nachdruck, sondern auch die durch den Landesbeauftragten um Stellungnahme gebetene Aufsichtsbehörde. Bei so viel positiver Grundeinstellung dem zu errichtenden Verfahren gegenüber kann es für einen behördlichen Datenschutzbeauftragten schwierig werden, die Angelegenheit mit der gebotenen datenschutzrechtlichen Sachlichkeit zu betrachten, Fragen zu stellen und Anforderungen zu formulieren.

Der behördliche Datenschutzbeauftragte des Landkreises hatte sich aus dieser Situation heraus entschieden, sich an den Landesbeauftragten zu wenden. Dabei hat er die Zulässigkeit eines solchen automatischen Abrufverfahrens nicht von vornherein bezweifelt. Auf die Unterstützung des Landesbeauftragten zurückzugreifen, ist dem behördlichen Datenschutzbeauftragten bereits per Gesetz ausdrücklich zugesichert (§ 14a Abs. 2 S. 2 DSG-LSA).

Vor dem Hintergrund dieser Rechtslage muten Äußerungen wie „Insgesamt erscheint mir das Vorgehen Ihres Kollegen aus der Kreisebene ein wenig reichlich überengagiert, zumal er bei sich im Hause anscheinend keinerlei Rückfrage hielt, bevor er sich an Sie wandte.“ befremdlich an. Überengagement kann dem behördlichen Datenschutzbeauftragten des Landkreises hier kaum unterstellt werden. Vielmehr stellt sich die Frage, ob nicht die übrigen Beteiligen, bei allem Einsatz für die Errichtung des automatisierten Abrufver-

fahrens, übersehen haben, dass eine an Recht und Gesetz gebundene Verwaltung erst prüft und dann ggf. handelt.

Die Abstimmungen zwischen dem behördlichen Datenschutzbeauftragten und dem Landesbeauftragten haben letztlich zehn Wochen gedauert, weil sich die Landkreisverwaltung auf der einen Seite und der Landesbeauftragte auf der anderen Seite jeweils die angemessene Zeit für eine datenschutzgerechte Prüfung nahmen. Das automatisierte Abrufverfahren kann nunmehr datenschutzrechtlich zulässig umgesetzt werden. Der Landesbeauftragte wird das Verfahren auch vor Ort in Augenschein nehmen.

12. Gesundheitswesen

12.1. Elektronische Gesundheitskarte

Eigentlich soll sie „ausrollen“, die elektronische Gesundheitskarte (vgl. hierzu VII. Tätigkeitsbericht, Ziff. 10.2, VIII. Tätigkeitsbericht, Ziff. 10.1). Doch trotz jahrelanger Planungen und Tests sind immer wieder Probleme zu lösen.
So musste z. B. während der Tests festgestellt werden, dass die Handhabbarkeit der persönlichen Identifikationsnummer (PIN) für Ärzte und Patienten mehr als fraglich ist. Es handelt sich um eine sechsstellige Patienten-PIN, die innerhalb eines bestimmten Zeitraumes eingegeben werden muss. Vor allem ältere und behinderte Patienten haben Probleme bei der Eingabe. Gerade jedoch mit der PIN-Eingabe verwirklicht der Patient sein informationelles Selbstbestimmungsrecht, da er auf diese Weise seine Einwilligung gibt, dass der Arzt auf seine Daten zugreifen darf.
Nun werden Lösungen diskutiert, um auch für diese betroffenen Patienten die Beteiligung unter Wahrung des Datenschutzes zu gewährleisten. Eine denkbare Variante ist, dass der behandelnde Arzt treuhänderisch für den Patienten dessen PIN am Kartenlesegerät eintippt. Damit bleibt das PIN-Geheimnis durch die ärztliche Schweigepflicht gewahrt. Doch handelt es sich bei einem Arzt um einen am Verfahren Beteiligten, der auch aus eigenem Interesse handelt und dessen Zugriff ermöglicht wird. Daher wird auch vertreten, dass der Treuhänder kein Beteiligter sein sollte.

Gegenstand datenschutzrechtlicher Erörterungen sind u. a. weiterhin Fragen der Zertifizierung von Primärsystemen der Leistungserbringer oder die Ausgestaltung der Anforderungen an das Foto auf der Karte. Da in Sachsen-Anhalt keine Testregion liegt, ist der Landesbeauftragte lediglich über die Beratungen mit den Datenschutzbeauftragten des Bundes und der Länder in die Begleitung einbezogen.

12.2. Elektronischer Heilberufsausweis

Auf der 80. Gesundheitsministerkonferenz im Juli 2007 wurde mehrheitlich beschlossen, ein Gesundheitsberuferegister einzurichten. Eine inhaltliche Beteiligung des Landesbeauftragten vor dieser Beschlussfassung durch das zuständige Ministerium ist leider nicht erfolgt.

Wie bereits im VIII. Tätigkeitsbericht (Ziff. 10.2) dargestellt, war noch offen, welche Stelle die Ausgabe der Heilberufs- und Berufsausweise für die nicht

verkammerten Berufe übernehmen wird. Nach dem Beschluss soll dies durch eine länderübergreifende organisatorische Einheit, dem „Elektronischen Beruferegister der Gesundheitsberufe – eGBR“ erfolgen. Die für die Erteilung der Berufsausübungserlaubnis zuständigen Behörden müssten verpflichtet werden, alle für die Aufgabenerfüllung des eGBR erforderlichen Daten mittels automatisiertem Datenabgleich zur Verfügung zu stellen.

§ 291a Abs. 5a Satz 2 SGB V sieht zwar vor, dass die Länder auch gemeinsame Stellen nach Satz 1 desselben Absatzes bestimmen können. Nach dem im Plural formulierten Gesetzeswortlaut könnte fraglich sein, ob ein einziges nationales Berufsregister geschaffen werden kann. Zudem wird die Notwendigkeit eines bundesweiten Registers nicht hinreichend dargestellt. Da die für die Erteilung der Berufsausübungserlaubnis zuständigen Behörden auch weiterhin sämtliche Daten der Betroffenen erheben und verarbeiten werden, hätten zunächst andere, weniger in das Grundrecht auf informationelle Selbstbestimmung eingreifende Möglichkeiten der Herausgabe der Heilberufs- und Berufsausweise geprüft werden sollen. Eine zentrale Lösung, die lediglich als ökonomisch vorteilhaft begründet wird, vermag einen derartigen Grundrechtseingriff kaum zu rechtfertigen. Zwar mag die Zuverlässigkeit der Gesundheitsdatenverarbeitung eine gewisse Kompetenzbündelung erfordern. Eine bundesweite zentrale Einrichtung korrespondiert jedoch nicht mit der Struktur bei den verkammerten Berufen.

Trotz derartiger Zweifel an einer zentralen Lösung sollte zunächst beobachtet werden, ob die datenschutzkonforme Ausgestaltung des Projektes gelingt.

12.3. Novellierung des Maßregelvollzugsgesetzes

Aufgrund von Änderungen im Strafgesetzbuch und allgemeinem Aktualisierungsbedarf wird eine Novellierung des Maßregelvollzugsgesetzes für das Land Sachsen-Anhalt vorbereitet.
Der Landesbeauftragte wurde bei den Entwurfserarbeitungen beteiligt und beriet das zuständige Ministerium aus datenschutzrechtlicher Sicht.
So wurde u. a. darauf hingewiesen, dass Daten im Krankenhausbetrieb des Maßregelvollzuges zumeist auch der ärztlichen Schweigepflicht unterliegen, so dass für die Verwendung personenbezogener Informationen neben dem allgemeinen Datenschutzrecht auch die Notwendigkeit des Vorliegens einer Offenbarungsbefugnis im Sinne des § 203 StGB zu beachten ist. Außerdem wurden Fragen der Videoüberwachung, der Erhebung und Speicherung von Daten von Besuchern und der Überwachung und Beschränkung des Post- und Telekommunikationsverkehrs erörtert.

12.4. Mammographie-Screening

Seit 1. Oktober 2007 läuft das Mammographie-Screening-Programm in Sachsen-Anhalt. Die Teilnahme ist freiwillig. Die datenschutzrechtliche Prüfung des Programms konnte erfolgreich abgeschlossen werden (siehe auch VII. Tätigkeitsbericht, Ziff. 10.6 und VIII. Tätigkeitsbericht, Ziff. 10.4).

Durch die Regelungen des Gesetzes zur Änderung sozial- und gesundheitsrechtlicher Gesetze vom 10. August 2007 (GVBl. LSA S. 306 ff) wurde u. a.

die öffentliche Stelle zur Durchführung des Mammographie-Screenings errichtet. Die Übernahme der Aufgaben einer Zentralen Stelle für das Land Sachsen-Anhalt wurde mit dem Gesundheitsamt Bremen vertraglich vereinbart und durch das zuständige Ministerium genehmigt. Damit ist die Grundvoraussetzung für die Verwendung von Meldedaten für das Einladewesen durch eine öffentliche Stelle erfüllt.
Darüber hinaus wurde die Änderung des Staatsvertrages zum Gemeinsamen Krebsregister in Sachsen-Anhalt mit Datum vom 20. Februar 2008 ratifiziert, so dass nunmehr auch der vorgesehene Abgleich mit Daten aus dem Krebsregister erfolgen darf (GVBl. LSA S. 68 ff). - Ob und inwieweit infolge der mit dem Begleitgesetz zur Föderalismusreform II beabsichtigten Errichtung eines Bundeskrebsregisters (BR-Drs. 16/12400 - Art. 5) darüber hinaus bestehender Änderungsbedarf gegeben ist, wird im nächsten Tätigkeitszeitraum zu beobachten sein.

In Abstimmung mit dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Bremen konnte festgestellt werden, dass aufgrund der Prüfung des Datenschutzkonzeptes und der Verfahrensbeschreibung der Zentralen Stelle keine datenschutzrechtlichen Bedenken gegen die dortige Datenerhebung und -verarbeitung bestehen.
Um die Anbindung Sachsen-Anhalts an das Gesundheitsamt Bremen, d. h. die Datenübermittlungen zwischen den Meldeämtern und der Zentralen Stelle sowie zwischen den Screening-Einheiten und der Zentralen Stelle prüfen zu können, wurden von der Kassenärztlichen Vereinigung Sachsen-Anhalt ein entsprechendes Datenschutzkonzept und eine Verfahrensbeschreibung angefordert.
Nach Prüfung dieser Unterlagen bestehen zwar auch hier keine grundsätzlichen datenschutzrechtlichen Bedenken, allerdings hat sich der Landesbeauftragte an das Ministerium des Innern gewandt, um von den Meldeämtern eine datenschutzgerechte Verfahrensweise bei der Datenübermittlung an die Zentrale Stelle zu fordern.

Die Meldeämter erstellen auf Anforderung der Zentralen Stelle eine Liste mit Adressdaten aller Frauen im Alter von 50 bis 69 Jahren. In Ballungszentren werden diese Daten vierteljährlich angefordert, in kleineren Gemeinden auch nur alle zwei Jahre. Die Daten werden in der Regel mit WinZip verschlüsselt und per Post mittels CD oder Diskette an die Zentrale Stelle versandt. Das Passwort wird telefonisch mitgeteilt. Es gibt jedoch auch Meldeämter, die die Daten unverschlüsselt versenden.

Da beim Versenden der Datenträger per Post die Gefahr eines Datenverlustes besteht, ist es hier besonders wichtig, dass die Daten verschlüsselt werden und das eingesetzte Verschlüsselungsverfahren die erforderliche Sicherheit bietet, damit im Falle des Abhandenkommens eines Datenträgers die personenbezogenen Daten nicht durch Unbefugte zur Kenntnis genommen werden können. Sorgfalt ist auch bei der Übermittlung des verwendeten Passwortes an die Zentrale Stelle erforderlich, da es zum Entschlüsseln der Daten dort ebenfalls bekannt sein muss.

Nach heutigem Stand der Technik kann die Verschlüsselungsfunktion ab WinZip-Version 9.0 als ausreichend sicher angesehen werden, da sie die

128- und 256-Bit AES-Verschlüsselung unterstützt. Allerdings muss das verwendete Passwort hinsichtlich Länge und verwendeter Zeichen so gestaltet werden, dass es nicht leicht erraten bzw. mit entsprechenden Programmen entschlüsselt werden kann. So sollte es mindestens 8 Zeichen lang sein, in keinem Wörterbuch stehen und Zahlen, Satz- oder Sonderzeichen sowie Groß- und Kleinbuchstaben enthalten.

Das Problem der nicht vorgegebenen Passwortstärke wird mit der aktuellen WinZip-Version 12.0 gelöst, indem benutzerdefinierbare Passwortrichtlinien eingeführt werden, die das Konfigurieren von Komplexitätsanforderungen ermöglichen. Die Parameter für die minimale Passwortlänge sowie die erforderliche Kombination verschiedener Zeichen können bei der Installation vom Systemadministrator festgelegt werden. Die möglichen Zeichentypen sind Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen.

Diese Forderungen hat das Ministerium des Innern in einem Erlass festgeschrieben, der über das Landesverwaltungsamt allen Einwohnermeldeämtern zur Kenntnis gegeben wird, so dass für die Zukunft eine datenschutzgerechte Datenübermittlung an die Zentrale Stelle gewährleistet sein sollte. Der Landesbeauftragte wird dies zu gegebener Zeit überprüfen.

12.5. Gendiagnostikgesetz

Bereits in seinem VI. Tätigkeitsbericht (Ziff. 10.4) hat der Landesbeauftragte die Forderung an den Gesetzgeber formuliert, genetische Untersuchungen am Menschen gesetzlich zu regeln. Auf den Bedarf an einem Gendiagnostikgesetz (GenDG) wurde im VIII. Tätigkeitsbericht (Ziff. 9.5) erneut hingewiesen.
Der Landesbeauftragte begrüßt daher ausdrücklich den Gesetzentwurf über genetische Untersuchungen, der am 27. August 2008 vom Bundeskabinett beschlossen wurde (BT-Drs. 16/10532).
Danach sollen Gentests künftig nur in engen Grenzen möglich sein. Das Gesetz verbietet Versicherungsunternehmen, vor Vertragsabschluss einen Gentest zu verlangen (außer bei hohen Summen). Außerdem werden heimliche Gentests, wie z. B. Abstammungstests, verboten. Auch wird Arbeitgebern verboten, von Beschäftigten einen Gentest oder Auskunft über bereits bekannte Ergebnisse zu verlangen.
Das GenDG soll jedoch ausdrücklich nicht für den Umgang mit genetischen Proben und Daten zu Forschungszwecken gelten. Dadurch gelten für den Forschungsbereich wie bisher die allgemeinen gesetzlichen Regelungen, insbesondere des DSG-LSA bzw. des BDSG. Oftmals genügen diese allgemeinen Bestimmungen jedoch den speziellen Anforderungen, z. B. im Bereich der Biomaterialbanken, nur bedingt (vgl. VIII. Tätigkeitsbericht, Ziff. 9.4). Dies monierte auch der Bundesrat.

12.6. Einschulungsuntersuchungen/schulärztliche Untersuchungen

Um eine landeseinheitliche Datenerhebung und -verarbeitung im Rahmen von Einschulungsuntersuchungen und schulärztlichen Untersuchungen in den Gesundheitsämtern Sachsen-Anhalts zu erreichen, soll zukünftig das be-

reits in einigen Gesundheitsämtern verwendete Programm „Octoware“ um ein zusätzliches Modul ergänzt werden (vgl. VIII. Tätigkeitsbericht, Ziff. 10.5). Darüber hinaus soll vom Programm eine Exportdatei erstellt werden, mit der anonyme Daten an das Landesamt für Verbraucherschutz als Grundlage der Gesundheitsberichterstattung übermittelt werden.
Der Landesbeauftragte wurde frühzeitig vom Gesundheitsministerium und dem Landesamt für Verbraucherschutz in die Planungen einbezogen.

Alle Eltern, deren Kinder eingeschult werden sollen, erhalten eine Einladung und einen Fragebogen, der Fragen zum Schwangerschafts- und Geburtsverlauf, zur Entwicklung des Kindes, zu Erkrankungen und gesundheitlichen Besonderheiten und zum familiären Umfeld enthält. Die Daten des Fragebogens und der Untersuchung werden mit Hilfe des Programms „Octoware“ in den Gesundheitsämtern gespeichert (§§ 9 Abs. 1, 10 Abs. 1 DSG-LSA, § 23 Abs. 1 GDG LSA, § 37 Abs. 2 SchulG LSA) und in anonymisierter Form dem Landesamt für Verbraucherschutz zur Gesundheitsberichterstattung übermittelt (§ 11 GDG LSA).
Hinsichtlich der Datenerhebung hat der Landesbeauftragte darauf hingewiesen, dass es sich bei der Einschulungsuntersuchung nicht um eine umfassende, dem Wohl des Kindes verpflichtete Untersuchung handelt, aus der letztlich das Recht zu einer total erfassenden Datenerhebung abgeleitet werden könnte. Die Einschulungsuntersuchung ist eine staatliche Pflichtuntersuchung, mit der zunächst ausschließlich die Schulreife des Kindes festgestellt werden soll. Die Verfolgung weiterer Zwecke wird von den schulgesetzlichen Grundlagen nicht gedeckt. Sie könnten nur im Rahmen des gesetzlichen Angebotes des öffentlichen Gesundheitsdienstes verfolgt werden, was aber die Freiwilligkeit der Datenangabe voraus setzt.
Deshalb ist nunmehr vorgesehen, dass sämtliche Datenerhebungen freiwillig sein werden.
Der Landesbeauftragte hat darauf hingewiesen, dass die Erhebung aller Daten auf der Basis der Freiwilligkeit kritisch ist. So ist z. B. die Erhebung des Impfstatus bei der Einschulungsuntersuchung pflichtig (§ 34 Abs. 11 Infektionsschutzgesetz). Auch muss mit Totalverweigerung gerechnet werden. Wie dann der gesetzlichen Aufgabe (Feststellung des Entwicklungsstandes des Kindes) nachgekommen werden kann, erscheint fraglich, zumal den Eltern in der Einladung versichert wird, dass bei Nichtangabe keine Nachteile entstehen.
Doch auch wenn die Datenerhebungen nicht aufgrund von § 84a Abs. 3 SchulG LSA i. V. m. § 9 Abs. 1 DSG-LSA, sondern aufgrund von entsprechenden Einwilligungen erfolgen sollen, ist eine Datenerhebung nicht völlig frei, sondern muss sich auch an den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit orientieren.
So konnte z. B. hinsichtlich der vorgesehenen Felder zu Kinderkrankheiten und zum behandelnden Arzt Einigkeit darüber erzielt werden, dass diese Daten nicht erforderlich sind und somit nicht erhoben werden.
Die Angaben zu Schwangerschaft und Geburt (z. B. Normal-, Früh- oder Mehrlingsgeburt) sind laut Landesamt für Verbraucherschutz erforderlich, um Risikofaktoren auszuschließen, die zu Entwicklungsbeeinträchtigungen führen können. Direkte Fragen nach den Risikofaktoren seien aufgrund von Verständnisproblemen bei den Eltern nicht möglich. Auch die Angaben zum familiären Umfeld (z. B. Anzahl und Alter der Geschwister, Erwerbstätigkeit

der Eltern) seien zur Feststellung des seelischen und sozialen Entwicklungsstandes erforderlich.
Ein Zusammenhang dieser Angaben mit der Einordnung und Beurteilung von Befunden und Entwicklungsbesonderheiten des Kindes ist in den intensiven Beratungen letztlich nicht überzeugend belegt worden. Da zu einer Beurteilung spezifische medizinische Fachkenntnis erforderlich ist, wurde abschließend lediglich auf die fortbestehenden Bedenken detailliert hingewiesen und die Beurteilung der Erforderlichkeit den sachkundigen Medizinern im Landesamt für Verbraucherschutz und im zuständigen Ministerium überlassen.

12.7. Amtsärztliche Stellungnahme zu Eingliederungshilfeleistungen

Der Verband der Ärzte im Gesundheitsdienst wies auf Bedenken hin, die sich aus einer Weitergabe von Befundberichten, Gutachten und Informationen anderer Ärzte in Kopie an die jeweils handelnde herangezogene Gebietskörperschaft ergeben, wenn Gutachten für die Eingliederungshilfe erstellt werden. Das Vertrauensverhältnis zu vorbehandelnden Ärzten wird tangiert. Der Landesbeauftragte hat diese Problematik mit dem überörtlichen Träger der Sozialhilfe des Landes Sachsen-Anhalt erörtern können. Danach ist auf Folgendes hinzuweisen:

Im Rahmen der Prüfung der Voraussetzungen für die Eingliederungshilfe nach den §§ 53, 54 Abs. 1 SGB XII i. V. m. § 55 Abs. 1 SGB IX sind vornehmlich die Behinderung im Sinne von § 2 Abs. 1 Satz 1 SGB IX, die Wesentlichkeit der Behinderung im Sinne des § 53 Abs. 1 SGB XII sowie die Aussicht, dass die Aufgabe der Eingliederungshilfe erfüllt werden kann, festzustellen. Die zuletzt verantwortliche Gesamtentscheidung über die beantragte Eingliederungshilfe obliegt dem Sozialamt der herangezogenen Gebietskörperschaft, ggf. im Zusammenwirken mit dem überörtlichen Träger der Sozialhilfe. Die Entscheidung erfolgt zweistufig. Zunächst einmal erfolgt die Feststellung der Zugehörigkeit zum Personenkreis des § 53 Abs. 1 SGB XII, wobei die amtsärztliche Stellungnahme zur Feststellung des Vorliegens der Behinderung zumeist unverzichtbar ist. Darüber hinaus ist unter Berücksichtigung der weiteren Umstände und insbesondere des Bedarfsdeckungsgrundsatzes des SGB XII durch das Sozialamt zu entscheiden, ob und welche Hilfeleistung konkret im Einzelfall angemessen ist.

Nach § 20 Abs. 1 SGB X hat das Sozialamt den erforderlichen Sachverhalt von Amts wegen zu ermitteln. Die Ermittlungshandlungen werden begrenzt durch die Vorschriften des 2. Kapitels des SGB X zum Schutz der Sozialdaten. Dies besagt ausdrücklich die Regelung des § 37 Satz 3 SGB I. Bei der Berufung auf die Ermittlung von Amts wegen wird das leider gelegentlich übersehen. Rechtsgrundlage für die Datenerhebung des Sozialamtes ist demnach § 67a SGB X. Die Datenerhebung ist auf die Daten begrenzt, deren Kenntnis zur Erfüllung der Aufgabe des Sozialamtes unerlässlich ist.

Dazu gehört zunächst die amtsärztliche Stellungnahme mit der medizinisch bewertenden Feststellung der Behinderung. Die konkrete Benennung einer Diagnose nach der Internationale Klassifikation der Krankheiten (ICD) ist dabei zumeist nicht erforderlich. Vielmehr sind die aus einer Erkrankung resultierenden Beschwerden und Einschränkungen deutlich zu beschreiben. Hier

kann ggf. auf die internationale Klassifikation der Funktionsfähigkeit, Behinderung und Gesundheit (ICF) der Weltgesundheitsorganisation Bezug genommen werden. Ein Vordruck für die amtsärztliche Stellungnahme enthielt insoweit sachdienliche Vorgaben.

Auch gegen eine nachvollziehbare Begründung bzw. Dokumentation der ärztlichen Feststellung bestanden aus datenschutzrechtlicher Sicht keine Bedenken. Die tragenden Erwägungen werden Grundlage der vom Sozialamt zu treffenden Entscheidung. Gegebenenfalls ist ein Vertreten vor Gericht erforderlich. Zudem ist es nach Darstellung des überörtlichen Trägers auch erforderlich, die ärztliche Stellungnahme ggf. im Zusammenhang mit anderweitigen Erkenntnissen zu würdigen.

Im Hinblick auf den Grundsatz der Erforderlichkeit darf die Datenerhebung jedoch nicht über den konkreten Zusammenhang mit dem Gutachtenauftrag hinausgehen. Informationen, die nicht mit dem Ergebnis der amtsärztlichen Stellungnahme und ihrer Begründung und Dokumentation zusammenhängen, dürfen nicht an das Sozialamt übermittelt werden. Dies gilt auch für die der Stellungnahme beizufügenden Kopien. Kopien sind nur insoweit beizufügen, als es sich um Unterlagen handelt, die in der amtsärztlichen Stellungnahme verwendet worden sind. Informationen, die nicht für die Klärung zur Voraussetzung der Eingliederungshilfeleistung erforderlich sind und hiermit nicht im Zusammenhang stehen, sollen mit dem vom überörtlichen Träger vorgesehenen Fragebogen nicht erfragt werden.

Auf die Übersendung von Fremdbefunden, Epikrisen und anderen ärztlichen Stellungnahmen in Kopie, die zwar bei der amtsärztlichen Begutachtung vorlagen, aber nicht in die Bewertung eingeflossen sind, ist daher zu verzichten. Soweit einzelne Informationen aus umfänglichen Unterlagen Verwendung gefunden haben, bestehen keine Bedenken, lediglich die Unterlage zu bezeichnen und nur die Seite in Kopie (ggf. unter Schwärzung überschüssiger Informationen) zu übersenden, die die verwendete Information dokumentiert.

Danach sind zwar die für die Entscheidung maßgeblichen Aspekte zu dokumentieren. Trotzdem ist in hinreichendem Maße möglich, das zwischen dem Gesundheitsamt und den vorbehandelnden Ärzten bestehende Vertrauensverhältnis zu berücksichtigen.

12.8. Herausgabe von Rettungsdienstprotokollen zu Abrechnungszwecken

Der Landesbeauftragte hatte sich bereits in der Vergangenheit mit der Thematik der Zulässigkeit der Herausgabe von Rettungsdienstprotokollen (Einsatzprotokollen) zu Abrechnungszwecken befasst (vgl. VIII. Tätigkeitsbericht, Ziff. 10.7). Dennoch kommt es vereinzelt vor, dass Abrechnungsstellen der Krankenkassen über die in § 302 Abs. 1 SGB V erforderlichen Abrechnungsdaten hinaus Informationen von den Leistungserbringern abfordern. Im konkreten Fall hatte sich ein Leistungserbringer bei der Ärztekammer darüber beklagt, dass eine Krankenkasse zu Abrechnungszwecken bei Einsätzen ohne den Transport des Versicherten die Einsatzprotokolle abgefordert hatte.

Nach der Sachverhaltsaufklärung mit der betreffenden Krankenkasse hatte diese die Fehlerhaftigkeit der Abforderung der Einsatzprotokolle zu Abrechnungszwecken erkannt und die Mitarbeiter in der Abrechnungsstelle im Fahrkostenbereich ausdrücklich angewiesen, keine Einsatzprotokolle mehr abzufordern.
Im Ergebnis erhält die Krankenkasse künftig nur die Daten, die sie für Abrechnungszwecke nach § 302 SGB V tatsächlich benötigt.

12.9. Archivierung von Patientenunterlagen

Zur Aufbewahrung von Patientenunterlagen nach Praxisaufgabe hatte sich der Landesbeauftragte bereits im VII. Tätigkeitsbericht (Ziff. 10.4) geäußert. Nunmehr wurde die Frage nach der Möglichkeit externer Archivierung von alten Krankenakten an ihn gerichtet. Der öffentlich-rechtlich organisierten Klinik konnte der Landesbeauftragte folgende Hinweise geben:

Zunächst ist festzustellen, dass in Sachsen-Anhalt keine spezialgesetzliche Rechtsgrundlage gegeben ist, die – wie in anderen Bundesländern – ggf. eine externe Archivierung im Wege der Datenverarbeitung im Auftrag unter bestimmten Voraussetzungen gestatten könnte.
Eine gesetzliche Befugnis für die Aufgabenübertragung im Sinne einer Funktionsübertragung ist ebenfalls nicht ersichtlich.

In datenschutzrechtlicher Hinsicht wären zunächst § 3 Abs. 2 Satz 1 DSG-LSA i. V. m. § 11 BDSG zu berücksichtigen, soweit eine Datenverarbeitung im Auftrag in Betracht käme. Da zudem Gesundheitsdaten als personenbezogene Daten besonderer Art betroffen sind, wären auch § 3 Abs. 2 Nr. 1 DSG-LSA i. V. m. § 28 Abs. 6 BDSG zu berücksichtigen.

Letztlich dürfte aber eine Archivierung von Patientenakten durch Externe auf der Grundlage der vorgenannten Vorschriften kaum in Betracht kommen. Überwiegend sind Daten betroffen, die der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB unterliegen. Hierzu ist auf § 3 Abs. 3 Satz 2 DSG-LSA zu verweisen, wonach Berufsgeheimnisse, die nicht auf gesetzlichen Vorschriften beruhen, unberührt bleiben. Hierzu zählt auch das Arztgeheimnis. Allgemeine datenschutzrechtliche Vorschriften über die Datenverarbeitung im Auftrag sind nicht geeignet, als Offenbarungsbefugnis im Rahmen berufsständischer Schweigepflichten bzw. im Rahmen des § 203 StGB zu fungieren (vgl. Oberlandesgericht Düsseldorf, Urt. vom 20. August 1996, 20 U 139/95, Computer und Recht 1997 S. 536; Der Datenschutzberater, 1997 S. 17).

§ 203 Abs. 3 Satz 2 StGB (Einbeziehung berufsmäßig tätiger Gehilfen in die Verschwiegenheitspflicht) bietet keine Lösung. Danach müsste das eingesetzte Personal eine Gehilfenstellung im Sinne dieser Vorschrift erlangen. Gehilfen im Sinne dieser Vorschrift sind jedoch nur solche Personen, die an dem allgemeinen Vertrauen und der Verschwiegenheit des Arztes teilhaben. Selbst eine vertragliche Einbindung der Mitarbeiter des Archivierungsunternehmens in die Organisation des Krankenhauses vermag dies kaum zu begründen. Der notwendige unmittelbare innere Zusammenhang mit dem Behandlungsgeschehen dürfte fehlen.

Die Aufbewahrung von Patientenunterlagen bei einem externen Auftragnehmer in verschlossenen codierten Behältnissen wäre ebenfalls kritisch. Der Schutz vor unberechtigten Öffnungen wäre nur relativ. Die hinreichende Absicherung gegen die Kenntnisnahme Unbefugter bliebe fraglich.

Etwas anderes könnte gegebenenfalls dann gelten, wenn die Patientenunterlagen beim Auftragnehmer in eingebauten Schließfächern oder abgetrennten Räumen verwahrt würden, die grundsätzlich nur von bzw. unter Mitwirkung von Bediensteten des Krankenhauses geöffnet oder betreten werden können.

Demnach dürfte es praktisch nur äußerst schwer möglich sein, eine der ärztlichen Schweigepflicht entsprechende Aufbewahrung der Patientenakten eines Krankenhauses bei einer externen Stelle zu gestalten. Unbedenklich zulässig wäre die externe Archivierung von Patientendaten daher nur dann, wenn die betroffenen Patienten jeweils zuvor ihre Einwilligung in dieses Verfahren erklärt hätten.

12.10. Datenübermittlung per Telefax

Erneut ist der Landesbeauftragte mit der Problematik der Übermittlung personenbezogener Daten per Telefax befasst gewesen. Im konkreten Fall wurden von einer Behörde abgeforderte Unterlagen von einem Krankenhaus per Telefax an den Hauptsitz der Behörde gefaxt, obwohl diese von Mitarbeitern eines Nebenstandortes zur Aufgabenerfüllung benötigt wurden.
Der Landesbeauftragte weist daher erneut auf die diesbezüglich ausführlichen Erläuterungen im III. Tätigkeitsbericht (Ziff. 13.4) hin.
So sollte gerade bei medizinischen Daten, die einem besonderen Berufsgeheimnis unterliegen, nur in absoluten Ausnahmefällen und unter Einhaltung zusätzlicher Sicherheitsvorkehrungen (z. B. vorherige Abstimmung der Sendezeit mit dem Empfänger, damit Unbefugte am Empfängergerät keinen Einblick nehmen können) eine Übertragung per Telefax erfolgen.

13. Gewerbe und Wirtschaft

13.1. Neufassung des Ingenieurgesetzes Sachsen-Anhalt

Der Landesbeauftragte hatte bereits im Jahr 2005 Gelegenheit, das zuständige Ministerium vor der Novellierung des Ingenieurgesetzes umfänglich zu beraten. Am 22. Januar 2009 wurde das Ingenieurgesetz Sachsen-Anhalt novelliert (GVBl. LSA S. 6). Es dient der Umsetzung der Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen. Zwar wurde eine Anhörung durchgeführt, eine Beteiligung des Landesbeauftragten nach § 40 Satz 2 der Gemeinsamen Geschäftsordnung der Landesregierung erfolgte jedoch nicht. Der Landesbeauftragte hatte zuvor Kenntnis von einem Arbeitsentwurf des Ministeriums erhalten; hierzu hatte er von sich aus Stellung genommen.

So hatte er Gelegenheit, auf die Synchronisierung von Vorschriften zu Möglichkeiten des Widerspruchs durch Betroffene hinzuweisen.

Weiterhin kritisierte der Landesbeauftragte die Auskunftsregelungen zur Liste der beratenden Ingenieure. Dort war anders als in der allgemeinen Regelung zunächst vorgesehen, dass die Auskunft ohne Geltendmachung eines berechtigten Interesses verlangt werden konnte. Die Regelungen wurden angepasst.

Zudem hat der Landesbeauftragte darauf hingewiesen, dass die Auskunft und Veröffentlichung aus den nach den gesetzlichen Vorschriften zu führenden Listen nicht auf Angaben zum erfolgreichen Abschluss eines Studiums, zu praktischen Tätigkeiten als Ingenieur, zu Fortbildungsmaßnahmen bzw. zu Gesellschaftsvertragsinhalten oder Satzungsbestimmungen ausgedehnt werden sollten.

13.2. Änderung der Gewerbeordnung

Häufig erreichten den Landesbeauftragten in den vergangenen Jahren Anfragen zum Gewerberegister. Fast immer suchten die öffentlichen Stellen nach einer Lücke in der Bindung der Daten der Gewerbeanzeigen an die Zwecke der Entgegennahme der Gewerbeanzeige und die Überwachung der Gewerbeausübung. Der Landesbeauftragte musste stets auf § 14 Abs. 1 Gewerbeordnung alte Fassung (GewO a. F.) hinweisen, wo es hieß: „Die erhobenen Daten dürfen von der für die Entgegennahme der Anzeige und die Überwachung der Gewerbeausübung zuständigen Behörde nur für diesen Zweck verarbeitet oder genutzt werden.“ Auch die Liste der Stellen, denen nach § 14 Abs. 5 GewO a. F. durch die Gemeinden Daten der Gewerbeanzeigen übermittelt werden dürfen, war, so musste der Landesbeauftragte mehrmals mitteilen, eine abschließende Aufzählung. Selbst die Übermittlung ausschließlich der Grunddaten (Name, betriebliche Anschrift und angezeigte Tätigkeit) der Gewerbetreibenden an am Wettbewerb teilnehmende öffentliche Stellen scheiterte entweder mangels Erforderlichkeit zur Aufgabenerfüllung (§ 14 Abs. 6 GewO a. F.) oder hinsichtlich nicht-öffentlicher Stellen mangels berechtigtem Interesse (§ 14 Abs. 8 GewO a. F., falls der Gewerbetreibende der Datenübermittlung widersprochen hatte).
Doch mit Artikel 9 des Zweiten Gesetzes zum Abbau bürokratischer Hemmnisse insbesondere in der Mittelständischen Wirtschaft vom 7. September 2007 (BGBl. I S. 2246) wurde die Gewerbeordnung (GewO) entscheidend geändert, speziell § 14 Abs. 6 Gewerbeordnung neue Fassung (GewO n. F.). Seit dem 14. September 2007 gilt folgender Satz 2: „Der Name, die betriebliche Anschrift und die angezeigte Tätigkeit des Gewerbetreibenden dürfen allgemein zugänglich gemacht werden.“ Landmann/ Rohmer führen dazu in der Kommentierung der GewO in § 14 Rdnr. 74b folgendes aus: „§ 14 Abs. 6 Satz 2 in der Fassung des Änderungsgesetzes vom 07.09.2007 (BGBl. I S. 2246) hat die Grunddaten (Name, betriebliche Anschrift, angezeigte Tätigkeit) allgemein zugänglich gemacht.“ Auf Seite 91 der Gesetzesbegründung (BR-Drs. 68/07) heißt es hierzu: „Es besteht kein schutzwürdiges Interesse des Gewerbetreibenden an der Beschränkung der Weitergabe der Grunddaten. Der Gewerbetreibende legt sie im Geschäftsverkehr ohnehin offen und ist gem. § 15a und § 15b GewO zur Offenlegung des Namens grundsätzlich auch verpflichtet.“
Doch damit nicht genug: Da die Gemeinde nach der nun geltenden Rechtslage nicht mehr verpflichtet ist, Voraussetzungen irgendwelcher Art vor einer

Übermittlung der Grunddaten der Gewerbetreibenden an Dritte zu prüfen, könnte es zur Veröffentlichung dieser Grunddaten selbst im Internet, z. B. in einer Firmendatenbank, kommen. Die Grunddaten Name, betriebliche Anschrift und angezeigte Tätigkeit der Gewerbetreibenden sind nach § 14 Abs. 6 Satz 2 GewO n. F. allgemein zur Nutzung freigegeben.

14. Hinweise zum technischen und organisatorischen Datenschutz

14.1. Sicherung von Sozialdaten auf Laptops

Im Jahre 1996 waren aus öffentlichen Stellen des Landes laut polizeilicher Kriminalstatistik in 930 Fällen Computer gestohlen worden. Aufgrund der in den Folgejahren stetig verbesserten Absicherung der Dienstgebäude gegen solcherlei Ungemach und der wachsenden Sensibilität der Beschäftigten ist diese Zahl zwar kontinuierlich gesunken. Der Landesbeauftragte sieht jedoch weiter die Notwendigkeit, bei Fortbildungsveranstaltungen, Kontrollen und Beratungen immer wieder auf die grundsätzlich fortbestehende Problematik des Computerdiebstahls hinzuweisen und daran zu erinnern, dass mit den Computern personenbezogene Daten in die Hände Unbefugter gelangen können. Als Mittel dagegen, so empfiehlt er stets, könnte **Sicherheitssoftware** eingesetzt werden, die die gespeicherten personenbezogenen Daten durch Verschlüsselung zuverlässig schützt. Das gilt vor allem dann, wenn Computer in unsicherer Umgebung betrieben werden und für Laptops.

Die genannten Erfahrungen und Empfehlungen schlug das Ministerium für Gesundheit und Soziales bis zum Jahre 2007 schlicht in den Wind. In dem Jahr nämlich wurden zwei durch das Landesprüfungsamt des Ministeriums bei einer Kontrolle in der Allgemeinen Ortskrankenkasse Sachsen-Anhalt (AOK) genutzte Laptops durch Einbruchdiebstahl entwendet. Sicherheitssoftware zur Verschlüsselung der gespeicherten Daten war leider nicht installiert. Werden die Festplatten der gestohlen Laptops in einem anderen Gerät mit gestartet, wodurch die Eingabe des Benutzerkennwortes entfällt, können Unbefugte die gespeicherten Daten zur Kenntnis nehmen. Diese Daten hatten eine erhebliche datenschutzrechtliche Brisanz:

- Versicherten- bzw. Beschäftigtendaten
- Betriebs- und Geschäftsgeheimnisse von Arbeitgebern
- Daten aus Prüfungen, z. B.
  - im kassenärztlichen Bereich
  - der Pflegekasse bei der AOK und der Betriebskrankenkasse Sachsen-Anhalt
  - der Kassenzahnärztlichen Vereinigung

Das Ministerium hat inzwischen gehandelt und seine Prüfungslaptops mit einer Sicherheitssoftware ausgestattet, die folgende Funktionen bietet:

- Pre-Boot-Authentisierung
- komplette Festplattenverschlüsselung mit starken Algorithmen
- Verschlüsselung auch von externen Datenträgern (z. B. USB-Speichersticks)
- Sicherung auch des Ruhezustandes des Notebooks (erneute Authentisierung nach Beendigung dieses Zustandes)

Außerdem wurde bei diesen Laptops durch ein zusätzliches Laptopschloss die Diebstahlsicherheit verbessert.

Der Landesbeauftragte empfiehlt bei der Benutzung von Laptops, unabhängig davon, ob personenbezogene, aus anderen Gründen geheimzuhaltende oder wertvolle Daten gespeichert sind, eine Sicherheitssoftware zu installieren, die den o. g. Ansprüchen genügt. Dabei ist das Funktionieren dieser Software regelmäßig zu überprüfen.

14.2. Fernwartung einer Firewall

Im Rahmen der Kontrolle einer Stadtverwaltung hatte der Landesbeauftragte auch Fragen zum städtischen Datennetz gestellt. Beim Thema Netzwerksicherheit wurde ihm über die Administration der Firewall berichtet. Die anfallenden Administrator- und Wartungsarbeiten würden von einem gewerblichen Unternehmen schon seit Jahren zuverlässig erledigt.
Zu einer Firewall muss man Folgendes wissen: Eine Firewall - zu deutsch: Brandschutzmauer - sichert Datennetzwerke gegeneinander ab. Das können das städtische Datennetz und das Internet sein. Natürlich sind diese Netze dann nicht völlig getrennt, es gibt zwischen beiden Kommunikationsbeziehungen. Aufgabe der Firewall ist, den sie passierenden Datenverkehr bzw. die Datenpakete darauf hin zu überprüfen, ob sie den zuvor festgelegten Regeln für eine sichere Kommunikation entsprechen. Nur solche Pakete werden durchgelassen, die diesen Regeln entsprechen. Abhängig von der Richtung der Kommunikation und den genutzten Ports bzw. Diensten werden auch Pakete zurückgehalten. Damit kann eine Firewall das kommunale Netzwerk vor unerlaubten Zugriffen aus dem Internet schützen.
Eine Firewall bedarf jedoch der regelmäßigen Wartung. Häufig läuft auf einer Firewall bereits der erste Virenscanner eines Netzwerkes, der das Eindringen oder Einschleppen von Schadsoftware der unterschiedlichsten Art verhindern soll. Ein solcher Virenscanner muss in kurzen Abständen, möglichst mehrmals täglich, mit einer aktualisierten Virenmusterdatei versorgt werden. Das funktioniert in der Regel automatisch, sollte aber gleichwohl überwacht werden. Auch die Firewall-Software muss gelegentlich aktualisiert werden, und die Protokollierungsdateien sollten nach aufgetretenen Problemen oder Spuren von Angriffen durchsucht werden.
Alles in allem: Eine Firewall ist für das sichere und zuverlässige Funktionieren des von ihr geschützten Datennetzwerkes von essentieller Bedeutung. Eine unbemerkte Manipulation der Firewall könnte dabei ebenso katastrophale Folgen haben wie ihr Ausfall.
Vielleicht war das der vom Landesbeauftragten kontrollierten Stadtverwaltung bewusst, vielleicht auch nicht. Jedenfalls war ihr bei der Übertragung der administrativen und Wartungsarbeiten an ihrer Firewall auf den Dienstleister ein Fehler unterlaufen. Das Prozedere des Fernwartungszugriffs war so gestaltet, dass jeder, der über die entsprechenden Zugangsdaten verfügte, von jedem Ort der Welt über das Internet Zugriff auf die Firewall erhielt, und zwar ohne jede Mitwirkung der auftraggebenden Stadtverwaltung. Das Wartungsunternehmen hätte schalten und walten können, wie es wollte.

Der Landesbeauftragte empfiehlt, das Aufbauen einer Fernwartungsverbindung stets von der aktiven Mitwirkung eines Beschäftigten des Auftraggebers

abhängig zu machen. So ist vorstellbar, die Fernwartung so zu konfigurieren, dass sie nur durch einen von innen heraus geöffneten SSH-Tunnel (SSH = Secure Shell) möglich ist. Diese verschlüsselte Netzwerkverbindung sollte, wenn sie nicht manuell beendet wird, bei längerer Nichtbenutzung automatisch beendet werden. So bleibt ein Fernwartungszugriff unmöglich unbemerkt und ungewollt, da immer eine aktive Kommunikation, z. B. telefonisch, vorausgeht.

Die kontrollierte Stadtverwaltung hat die Wartung und Administration ihrer Firewall, nachdem der Landesbeauftragte sie auf das Problem aufmerksam gemacht hat, in die eigenen Hände genommen und den Wartungsvertrag gemäß den gesetzlichen Bestimmungen (§ 8 Abs. 7 DSG-LSA) angepasst.

14.3. Überarbeitung der Sicherheitsleitlinie der Verwaltungs-PKI des BSI

Der Arbeitskreis für technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder beauftragte 2007 eine Arbeitsgruppe zur Mitarbeit an der Überarbeitung der Verwaltungs-PKI des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Inhalt der Aufgaben der Arbeitsgruppe ist die Aktualisierung der Policy (Sicherheitsleitlinie) für die Verwaltungs-PKI und der zugehörigen Dokumente mit dem Ziel der Beteiligung von Datenschutzexperten bei der Fortentwicklung der Verwaltungs-PKI. Der Landesbeauftragte wirkt zusammen mit Kollegen des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und dem Vertreter des BSI in dieser Arbeitsgruppe unter Federführung des Hessischen Landesbeauftragten für den Datenschutz mit.

Thematisch wurden unter anderem die sichere Nutzung von sowohl qualifizierten als auch fortgeschrittenen elektronischen Zertifikaten erörtert und entsprechende Formulierungen für die Sicherheitsleitlinien der Verwaltungs-PKI festgeschrieben, die den datenschutzrechtlichen Anforderungen entsprechen. Es wurden Themen abgeleitet, welche ebenfalls beachtet und ggf. weiter untersucht werden müssen. In diesem Zusammenhang wurde auch das Key-Backup- und Key-Recovery-Konzept vorgestellt. Beide Konzepte sind aus datenschutzrechtlicher Sicht nicht zu beanstanden.

14.4. Sichere E-Mails mittels X.509-Zertifikat der PKI Sachsen-Anhalt

Kommunikation im Internet erfolgt größtenteils im Klartext. E-Mails an den Landesbeauftragten enthalten häufig schutzwürdige, sensible, personenbezogene Daten, die nicht für Dritte zugänglich sein dürfen. Diese sollten grundsätzlich nur verschlüsselt per E-Mail übertragen werden.

Auf der Homepage des Landesbeauftragten befindet sich seit 2000 ein PGP-Schlüssel, der von sicherheitsbewussten Bürgern bereits aktiv genutzt wird. Behörden verzichten derzeit immer noch auf spezielle Sicherungen ihrer Kommunikationsdaten. Selbst das kostenfreie PGP wird ignoriert. Für sensible Informationen wird das Medium E-Mail fast immer durch die Briefpost ersetzt.

Um mit gutem Beispiel voranzugehen und um eigene, praktische Erfahrungen mit dieser Technologie zu sammeln, ist der Landesbeauftragte seit 2007 im Besitz eines fortgeschrittenen X.509-Zertifikates der PKI des Landes Sachsen-Anhalt. Dieses kann alternativ zu PGP aktiv zur Absicherung der elektronischen Korrespondenz mit den Landesbeauftragten genutzt werden. Ziel ist es, eine sichere elektronische Kommunikation auch für behördliche E-Mails zu ermöglichen und den geringen Aufwand dafür zu zeigen.

Das Zertifikat kann im Verzeichnisdienst der TESTA-Zertifizierungsstelle oder dem der Europäischen Bridge-Zertifizierungsstelle unter Angabe der E-Mail-Adresse der Poststelle des Landesbeauftragten gefunden und heruntergeladen werden:
www.bridge-ca.de/eb-ca2/directory/

14.5. Die elektronische Signatur in der Verwaltung

Gemäß § 2 Nr. 1 Signaturgesetz (SigG) sind „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten (z. B. Dokumenten) beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen (vgl. VIII. Tätigkeitsbericht, Ziff. 4.3).

In Deutschland wurden mit dem 2001 novellierten SigG im Wesentlichen zwei Formen von Signaturen definiert, welche unter anderem unterschiedliche Prüfungsarten erfordern und für verschiedene Einsatzzwecke gedacht sind. Zum einen ist dies die qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG), welche gem. § 126a BGB der händischen Unterschrift unter einem Dokument gleichgestellt ist, und zum anderen die „nur“ fortgeschrittene elektronische Signatur, welche aufgrund geringerer Rechtsfolgen und auch wegen des verbundenen Prüfmodells nur als z. B. Transportverschlüsselung genutzt werden sollte. Nicht betrachtet wird die einfache elektronische Signatur (§ 2 Nr. 1 SigG).

Um die passende Signaturform auszuwählen und dem Einsatzzweck entsprechend zu verwenden, soll ein kurzer Überblick über Möglichkeiten und Grenzen der Verwendung elektronischer Signaturen gegeben werden. Auch in gesetzlichen Bestimmungen ist es wichtig, die richtige Signaturform vorzugeben. In der Regel wird dies die qualifizierte elektronische Signatur sein, auch wenn mit dieser Anwendungsform höhere Anforderungen verbunden sind – Sicherheit und Vertraulichkeit haben ihren Preis.

Zur Prüfung von elektronischen Signaturen gibt es verschiedene Gültigkeitsmodelle, nach deren Vorgaben eine Prüfung zu erfolgen hat. Qualifizierte elektronische Signaturen werden mit Hilfe des **Kettenmodells** (§ 2 Nr. 3a SigG) auf Gültigkeit zum Zeitpunkt der Erstellung der Signatur geprüft. Entscheidende Merkmale sind Echtheit und die dauerhafte Gültigkeit der Signatur, analog einer händischen Unterschrift. Bei einer fortgeschrittenen elektronischen Signatur wird nach dem **Schalenmodell** die Gültigkeit zum Zeitpunkt der Prüfung festgestellt. Diese völlig unterschiedlichen Prüfalgorithmen müssen bei der Beschaffung von Software zum Einsatz von Signaturen beachtet werden, um falsche Ergebnisse bei der Signaturprüfung zu vermeiden.

Beim Kettenmodell wird eine Vertrauenskette vom Wurzelzertifikat über die Zertifikate der Zertifizierungsdiensteanbieter bis hinab zum zur Signatur gehörenden Anwender-Zertifikat geprüft. Dabei wird zu jedem Zertifikat geprüft, ob das übergeordnete Zertifikat zum Zeitpunkt der Erstellung der jeweiligen (Zertifikats-)Signatur gültig war. Vorteil ist, dass die so erstellten Signaturen wie Unterschriften dauerhaft haltbar sind. Wichtig ist, dass das unmittelbar übergeordnete Zertifikat zum Zeitpunkt des Ausstellens der Signatur oder des untergeordneten Zertifikats gültig war.

Demgegenüber werden beim Schalenmodell sämtliche beteiligten Zertifikate zum Zeitpunkt der Prüfung der Signatur geprüft. Das bedeutet, dass eine solche Signatur in genau dem Moment ungültig wird, in dem ein beliebiges, übergeordnetes Zertifikat - sei es durch Sperrung oder durch Ablauf der Gültigkeitsdauer - ungültig wird. Da eine fortgeschrittene elektronische Signatur somit zwangsläufig nach relativ kurzer Zeit als ungültig erkannt werden wird, eignet sich das Verfahren nicht zum Signieren von dauerhaft gültigen Dokumenten. Aus diesem Grund müssen die Signaturen von Dokumenten (z. B. E-Mails) zeitnah überprüft werden.

Als drittes Prüfmodell existiert noch das Hybridmodell. Dieses ist seinem Wesen nach ein Schalenmodell, nur dass die Zertifikate nicht auf Gültigkeit zum Prüfzeitpunkt, sondern auf Gültigkeit zum Zeitpunkt der Signaturerstellung geprüft werden. Damit wäre dieses Modell zur Erteilung dauerhafter Signaturen geeignet. Nachteil ist allerdings, dass der Erstellungszeitraum für gültige Signaturen nicht allein vom Gültigkeitszeitraum des direkt übergeordneten Zertifikats abhängt, sondern von der gemeinsamen Schnittmenge der gültigen Zeiträume aller übergeordneten Zertifikate.

In den USA und auch in Ländern der EU (EU-Signaturrichtlinie) werden vielfach Programme eingesetzt, welche Signaturen nach dem Schalenmodell prüfen, was zu Problemen führen kann. Bei Nutzung solcher Programme in Deutschland sollte darauf geachtet werden, dass die Prüfung qualifizierter elektronischer Signaturen nach dem Kettenmodell erfolgt bzw. diese Fähigkeit nachgerüstet werden kann. Administratoren müssen sich mit den Prüfmethoden von Signaturen der eingesetzten Programme vertraut machen und für die jeweilige Signaturform ein passendes Programm auswählen. Sie müssen dessen Verhalten gezielt evaluieren, blindes Vertrauen in die Meldungen eines Programmes zur erfolgreichen Prüfung ist hier fehl am Platz. Bei Softwarebeschaffungen muss ggf. darauf geachtet werden, dass fortgeschrittene elektronische Signaturen auf den Zeitpunkt der Signaturerstellung geprüft werden können. Dies erfordert ggf. die Möglichkeit der Vorgabe des Prüfzeitpunkts, da eine Prüfung zum aktuellen Zeitpunkt sonst fälschlicherweise zu einem negativen Ergebnis führen kann.

Eine Prüfung nach Schalenmodell kann - wie beschrieben - problematisch sein, so dass sich hier die Frage stellt, ob es nicht sinnvoller ist, grundsätzlich das Kettenmodell in Verbindung mit einer qualifizierten elektronischen Signatur und passender Prüfsoftware zu verwenden.

14.6. Online Services Computer Interface 2.0 (OSCI 2.0)

Bund, Länder und Kommunen arbeiten intensiv an der Realisierung einer Vielzahl verschiedener eGovernment-Projekte mit ebenso verschiedenen Anforderungen an die Datenübertragung. Zur Sicherstellung von Vertraulichkeit und Integrität der Datenströme zwischen Fachverfahren, der öffentlichen Verwaltung, der Wirtschaft und auch dem Bürger wurde der Übertragungs-Standard OSCI-Transport 1.2 eingeführt (vgl. VIII. Tätigkeitsbericht, Ziff. 6.1). Er kann durch sachgemäße Nutzung von Signatur und Verschlüsselung einen datenschutzgerechten Datentransport und damit eine vertrauliche und rechtsverbindliche Kommunikation über das Internet sicherstellen. Typisch ist die Nutzung einer zentralen Vermittlungsstelle, eines sogenannten Intermediärs. Dieser erbringt Zusatzdienste, wie z. B. die Verwaltung eines Postkorbes für potentielle Empfänger, so dass z. B. asynchrone Übertragungen möglich werden. Damit können über eine OSCI-Verbindung Daten an einen Empfänger gesendet werden, selbst wenn dieser gerade nicht online ist. Die sichere Übermittlung ist durch Nutzung des Prinzips des „doppelten Umschlags“, bei dem die Nutzungsdaten in einem äußeren Umschlag und Inhaltsdaten in einem inneren Umschlag verschlüsselt transportiert werden, gewährleistet. Die Datenformate basieren auf Standards z. B. des World Wide Web Consortiums (XML, SOAP).

Immer mehr Gesetze und Normen schreiben die Nutzung von OSCI als Basis und Standard für eGovernment-Verfahren explizit vor. OSCI-Transport wird beispielsweise im Meldewesen auch in Sachsen-Anhalt erfolgreich eingesetzt. XMeld ist die erste bundesweite OSCI-Anwendung. Auch das Elektronische Gerichts- und Verwaltungspostfach (EGVP) verwendet OSCI.

Die Weiterentwicklung von OSCI-Transport 1.2 schreitet kontinuierlich voran. OSCI-Transport 2.0 wird neue Möglichkeiten bieten, um mittlerweile hinzugekommenen und künftigen Nutzungsszenarien gerecht zu werden. Der neue Standard soll insbesondere den Anforderungen von eGovernment-Anwendungen, Maschine-Maschine-Kommunikationen, Sicherheitsinfrastrukturen und den neuen Möglichkeiten der technischen Entwicklung Rechnung tragen. Erstmals wird z. B. ein „Einschreiben mit Rückschein“ elektronisch abbildbar sein und auch neue Nutzer- und Diensteverzeichnisse werden integriert werden können.

Aus Performancegründen werden nicht alle Einsatz-Profile das Prinzip des „doppelten Umschlags“ verpflichtend umsetzen. In diesen Fällen muss die Vertraulichkeit auch des äußeren Umschlags durch entsprechende Maßnahmen und Bedingungen auf z. B. Netzwerk- und Protokollebene erfolgen. Abhängig davon ist, wie welches OSCI-Profil den Anforderungen des Datenschutzes gerecht werden kann. Inwieweit mit OSCI-Transport 2.0 eine zu OSCI-Transport 1.2 gleichwertige Datensicherheit gewährleistet werden kann und der 1.2er Standard somit obsolet wird, kann derzeit noch nicht gesagt werden. Fest steht, dass OSCI 2.0 auf anderen Technologien basiert und damit völlig neu bewertet werden muss. Eine Arbeitsgruppe des Arbeitskreises für technische und organisatorische Datenschutzfragen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begleitet aus diesem Grund die Entwicklung von OSCI 2.0.

14.7. Sicherheit des Windows Encrypted File Systems (EFS)

Microsoft Windows Betriebssysteme bieten die Möglichkeit, das Dateisystem mit Bordmitteln zu verschlüsseln. Diese Verschlüsselung wird noch viel zu wenig genutzt und hat in den meisten Fällen keine merkliche Leistungseinbuße des Rechners zur Folge. Im Folgenden werden die Anforderungen an eine sichere Konfiguration beschrieben.

Das EFS ist unter Windows 2000 generell als unsicher anzusehen, da jeder lokale Administrator Zugriff als Data Recovery Agent (DRA) hat. Ab Windows XP gibt es keinen automatisch vom System vorgegebenen DRA und auch keinen Zwang zur Einrichtung eines lokalen DRA mehr. Da Windows 2000 Zugänge relativ einfach ausgehebelt werden können (das Rücksetzen des Passworts eines beliebigen Accounts erlaubt den Zugriff auf den Verschlüsselungs-Key des EFS), ist die EFS-Nutzung hier generell als unsicher zu betrachten.

Für moderne Windows-Systeme ist bei sensiblen Daten die Möglichkeit der EFS-Nutzung oft durchaus eine Alternative zu separaten Verschlüsselungsprogrammen wie dem als sehr sicher geltenden TrueCrypt, da das EFS keine zusätzliche Software und kein Container-Handling etc. erfordert und dennoch Schutz bietet.

Ab Windows XP wird das Backup des Benutzer-Schlüssels sicherer im Active Directory oder Offline auf einem Backup-Medium gespeichert. Damit kann ein Angreifer mit Zugriff auf das System die Dateien nicht mehr direkt entschlüsseln, sondern muss das **Passwort** des Nutzers ermitteln. Auch dies wurde deutlich erschwert.

Die Konfiguration des EFS unter Windows XP Professional muss mindestens folgenden Anforderungen genügen:

- Die Sicherheit steht und fällt mit einem guten Passwort!
- Die Security Account Manager (SAM)-Datenbank muss mit Hilfe des SYSKEY-Werkzeugs verschlüsselt worden sein, weil sie das gehashte Passwort enthält. Ab Windows 2000: Mit Syskey.exe auf Modus 2 oder 3 stellen und beachten, dass alle Passwörter anschließend neu vergeben werden müssen, da alte Passwörter so lange noch als Hash in der SAM-Datenbank enthalten sind. Ab Windows Vista ist das die Vorgabe-Einstellung. Um das EFS zu aktivieren, die Konten zu verschlüsseln und den Schlüssel lokal zu speichern, reicht z. B. der Aufruf von „syskey-L“.
- Autologon muss deaktiviert sein, da hierfür das Klartextpasswort in der Windows-Registry hinterlegt wird.
- In den Sicherheitseinstellungen der Gruppen-Policy muss Windows das Speichern des Passworts in Form von LM-Hashes untersagt werden.
- Passwörter werden zusätzlich als NTLM-Hashes (NT LAN Manager; für SMB) abgelegt. Diese sind mit Hilfe von Rainbow-Tabellen auffindbar. Einzige Abhilfe ist ein genügend langes Passwort, so dass die Tabellen die entsprechenden Hashes nicht mehr enthalten.

- Der Zugriff auf das Administrator-Konto muss ebenso gesichert werden, da über diesen das DRA-Zertifikat verändert werden kann. Alle anschließend verschlüsselten Dateien wären für einen Angreifer lesbar.
- Das EFS sollte mindestens auf Verzeichnisebene aktiviert werden, so dass auch z. B. temporäre Word-Dateien verschlüsselt werden. Bei einer Verschlüsselung wird die unverschlüsselte Datei im Anschluss gelöscht und ist u. U. wiederherstellbar. Windows speichert eine unverschlüsselte Sicherheitskopie, welche erst nach erfolgreicher Verschlüsselung gelöscht wird. Zum Löschen bietet das Windows-eigene Programm Cipher.exe die /W-Option. Das Programm gibt es ab Windows 2000 Security Rollup Package 1. Anwendungen von Drittanbietern könnten ebenfalls den Zweck erfüllen.

Zur Passwortlänge: Ab 14 Zeichen wird der LM-Hash nicht mehr in der SAM-Datenbank abgelegt. Zusätzlich wird der Angriff auf den NTLM-Hash erschwert. Um eine zur EFS-Verschlüsselung (3DES, AES) gleichwertige Sicherheit für den Nutzerzugang zu erreichen, ist ein mind. 20 Zeichen langes Passwort erforderlich.

Ab Windows Vista ist es möglich, statt einem Passwort zur Absicherung ein Zertifikat auf einer Smart Card zu verwenden. Diese Möglichkeit sollte genutzt werden, um Brute Force-Angriffe zur Passwortfindung ins Leere laufen zu lassen.

Alle Hinweise dienen nur der Absicherung der lokalen Dateien. Zugriffe über das Netzwerk oder mit Hilfe zusätzlicher Software sind parallel möglich und deren Absicherung ist zusätzlich zu bedenken.

14.8. Datenschutzgerechte Webserver-Logs

Das Speichern von IP-Adressen ist in den meisten Fällen nicht notwendig und nur im Ausnahmefall eingeschränkt erlaubt (vgl. Ziff. 14.9). Dennoch ist es oft gar nicht möglich, im täglichen Betrieb ohne Protokoll-Dateien (sog. Logdateien) auszukommen. Aus Sicherheitsgründen und zur Fehlersuche werden zeitlich auf das erforderliche Maß beschränkte Logs vom Landesbeauftragten daher toleriert. Zu statistischen Zwecken oder um das Nutzungsverhalten auf der Website abbilden zu können, ist oft jedoch auch ein Zugriff auf zusätzliche Daten wünschenswert.
Um Logdaten erfassen zu können, ist es notwendig, den Personenbezug durch Datenveränderung aus den Logs zu entfernen. Der Sächsische Datenschutzbeauftragte ließ ein Erweiterungs-Modul zur IP-Anonymisierung an Web-Servern (IIS 5 bis 7, Apache 1.3 bis 2.2) entwickeln. Es steht allen Interessierten unter der Adresse www.saechsdsb.de/ipmask für den freien Gebrauch zur Verfügung.

Technisch gesehen wird bei diesem Modul die letzte Ziffer der IP-Adresse auf 0 und zusätzlich ein beliebiger weiterer Teil bitweise auf 0 gesetzt, so dass in Logdateien konfigurierbar genaue Angaben abseits der kompletten IP-Adresse möglich werden. Damit kann auch Software, welche die Logdateien auswertet, in eingeschränktem Umfang mit den Daten umgehen, da

das Logdatenformat nicht verändert wird und auch sinnvolle Daten enthalten sind. Der Landesbeauftragte regt die Nutzung dieses Moduls an.

14.9. Webserver-Logs bei externen Dienstleistern

Mittlerweile hat es sich bei den meisten Behörden bereits herumgesprochen, dass das Protokollieren von IP-Adressen ein Problem aufwirft. Es handelt sich um personenbeziehbare Daten, die nur in engem Rahmen, z. B. zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage (§ 10 Abs. 4 DSG-LSA) - hierzu gehört auch ein Web-Server - für Zeiträume von 5 Tagen gesammelt werden dürfen (vgl. VIII. Tätigkeitsbericht, Ziff. 23.2).

In der freien Wirtschaft bieten einige Firmen externe Nutzer-Tracking-Dienstleistungen an. Ganz vorne mit dabei ist Google mit der Anwendung Google Analytics, einer webbasierten Oberfläche zur Erfassung und Analyse von **Logdaten**. Andere Anbieter treten deutlich weniger in Erscheinung. Zur Nutzung eines solchen Dienstes wird eine auf den Servern des Dienstleisters hinterlegte Grafik, häufiger jedoch eine JavaScript-Datei, in den Quelltext der Webseite eingebunden. Der Browser der Nutzer lädt solche Dateien im Kontext der eigentlichen Webseite mit und stellt diese dar. Wird eine solche externe Datei beim Seitenaufruf mitgeladen, werden Daten wie z. B. die IP-Adresse (das Herkunftsland des Nutzers bis hin zum Provider oder zum persönlichen Rechner), die Browserkennung, das Betriebssystem, Sprach- und Dateiformatpräferenzen u. a. in der Anfrage verborgen mitgesendet. Diese werden nicht dazu genutzt, die Antwort auf die Nutzeranfrage qualitativ zu verbessern, sondern um ein möglichst genaues Profil des Nutzers aufzubauen. Zusätzlich werden zur besseren Nutzerverfolgung Cookies eingesetzt.

Durch den Abruf vom externen Server fallen auf diesem die gleichen Logdaten an, als wäre das Log auf dem eigenen Server erstellt worden. Der Unterschied besteht darin, dass die Daten oft im Ausland lagern. Dadurch wird das deutsche Recht umgangen, der Anbieter des Nachverfolgungsdienstes kann diese Daten gezielt auswerten und mit anderen Daten verknüpfen und zusätzlich Präsentationsdienste anbieten. Die Daten der Nutzer der Website werden zur Profilbildung an Händler abgetreten. Diese Methoden sind (nicht nur) im behördlichen Umfeld nicht notwendig und sollten schon aufgrund der Vorbildwirkung staatlicher Institutionen nicht genutzt werden. Das Telemediengesetz erlaubt eine personenbezogene Auswertung des Nutzerverhaltens von Einzelpersonen über solche Dienste nicht. Prinzipiell müsste vorab eine Information der Betroffenen und Zustimmung zur Datenerhebung und -analyse eingeholt werden. Eine Anonymisierung der Daten wäre obligatorisch. Dies erfolgt allerdings nicht.

Aus sicherheitstechnischer Sicht soll besonders vor der Einbindung von JavaScript-Code in die eigenen Webseiten gewarnt werden, da die Gefahr besteht, dass damit die Kontrolle über die eigene Website abgegeben wird. Der Script erhält die komplette Kontrolle über das Browserfenster und kann dadurch noch mehr Daten abfragen. Allein der Dienstleister entscheidet, welcher Programmcode ausgeführt wird. Dadurch fallen nicht nur mehr Daten an (z. B. lässt sich so auch die Bildschirmauflösung ermitteln), sondern es wird

auch ein potentielles Einfallstor für Schadsoftware weit geöffnet. Im Extremfall könnte ein gehackter Tracking-Dienstleister Schadsoftware auf den Kunden-Webseiten ausführen lassen, welche die Besucher dieser Webseiten angreift. Aufgrund des massenhaften Einsatzes solcher Tracking-Dienste hätte ein erfolgreicher Angriff auf einen populären Anbieter schwerwiegende Folgen für das gesamte Internet.

Es soll ausdrücklich davor gewarnt werden, statt eigener Logdateien solche Dienstleister zu nutzen. Sowohl aus rechtlicher als auch aus technischer Sicht stellen sie keine Alternative dar. Ob die eigene Website betroffen ist, lässt sich im Quelltext der Webseite anhand von enthaltenem Quellcode von z. B. estat.com oder google-analytics.com erkennen.

Der Google Analytics Datensammler wird von Google treffend „urchin“ (Schmuddelkind, Straßenjunge) genannt. Es bleibt zu hoffen, dass nicht im gleichen Stil mit den Daten der Nutzer umgegangen wird.

Ein Nutzer kann seine Privatsphäre schützen, indem z. B. JavaScript abgeschaltet (was oft nicht praktikabel ist), entsprechende Browser-Erweiterungen installiert oder einzelne Namensauflösungen (wie die der Domain google-analytics.com) durch einen Werbeblocker oder die Hosts-Datei auf dem Rechner deaktiviert werden. Auch Firewalls können teilweise konfiguriert werden, Zugriffe auf solche Dienste zu erkennen und abzublocken. Nebeneffekt ist die schnellere Ladezeit der Webseiten, da weniger Zugriffe auf das Internet notwendig werden.

14.10. BlackBerry - Einsatz sicher gestaltbar

In immer mehr Behörden werden BlackBerry-Geräte des kanadischen Herstellers Research In Motion (RIM) als Ersatz für das herkömmliche Handy und den PDA genutzt. Aus Datenschutzsicht wird der Einsatz von BlackBerry-Geräten kritisch gesehen, da diese den Direktzugriff auf Dokumente erlauben, welche auf dem BlackBerry Enterprise Server (BES) hinterlegt sind. Der BES wiederum greift auf die Daten eines Microsoft Exchange Servers zu, so dass jeder BlackBerry zu jeder Zeit auf alle wichtigen Daten Zugriff hat. Dies ist ein großer Vorteil, gleichzeitig jedoch auch ein Sicherheitsrisiko.

Ein Vorteil ist es, dass der BES eine Dokumentenansicht erzeugt und live anzeigt und i. d. R. keine vollständigen Dokumente auf das mobile System kopiert werden. Durch diesen Push-Dienst ist ein sofortiges Reagieren auf E-Mails statt zeit- und kostenintensiver Anforderungen durch Polling (regelmäßiges Abfragen des Servers) möglich. Durch eine solche Push-Technologie werden Informationen von einem zentralen Server auf Basis der vom Client voreingestellten Parameter für diesen aufbereitet und anschließend ausgeliefert. Diese Informationen werden nach Erstellung auf dem Server sofort geliefert (gepusht), ohne dass der Client (z. B. das BlackBerry-Gerät) eine Anfrage starten muss. Dies ist ein wesentlicher Vorteil des Push-Dienstes.

Kritisiert wurde anfangs, dass der BES eine Verbindung zu zentralen RIM-Servern benötigt, um die verschlüsselte (3DES/AES) Datenübertragung zu gewährleisten. Ob die Ende-zu-Ende-Verschlüsselung durch RIM gebrochen

werden kann, war lange Zeit völlig unklar und führte in verschiedenen Firmen und Behörden teilweise zum Verbot der Geräte. RIM bemüht sich intensiv, solche Bedenken zu zerstreuen. So wurde eine umfangreiche Sicherheitsanalyse durch das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) durchgeführt, die zu dem Ergebnis kam, dass keine „verborgene Funktionen oder Hintertüren“ vorhanden sind.

Auch der Landesbeauftragte beschäftigte sich mit der Sicherheit von BlackBerry-Geräten. In einer 2008 durchgeführten Umfrage wurde ermittelt, dass einige Ressorts BlackBerry Geräte einsetzen (im Durchschnitt 5 Stück). Bei einem Informationsbesuch in einer obersten Landesbehörde wurde eine BES-Installation kontrolliert. Es wurde ein (soweit es in der Kürze feststellbar war) sauber aufgesetztes und kompetent betreutes System vorgefunden. Nachfragen bei Kollegen und bei RIM selbst brachten Informationen zur Konfiguration.

Wichtig ist, dass verlorene Geräte schnell gesperrt werden können und auch die Zugangspasswörter sicher sind und unter keinen Umständen Unbefugten zur Kenntnis gelangen. Das Zeitfenster unmittelbar nach einem Diebstahl bis zur Aktivierung des Bildschirmschoners ist als kritisch anzusehen. Eine Fernlöschung ist zwar möglich, kann aber umgangen werden. Das Gerät muss im Falle eines Verlustes immer schnellstmöglich gesperrt werden. Es sind Kriterien für die Passwortgestaltung und den Schlüsseltausch vorzugeben.

Die Sicherheit eines BES steht und fällt mit der sicheren Konfiguration desselben. Aus diesem Grund wird derzeit noch an Konfigurationsempfehlungen gearbeitet, um Administratoren Handlungsempfehlungen für einen sicheren Betrieb zu geben. Dies wird sich aber aufgrund der zahlreichen administrativen Möglichkeiten, notwendiger Übersetzungsleistung und der Notwendigkeit einer eigenen Referenzinstallation noch bis in den nächsten Tätigkeitsberichtszeitraum hinziehen. Hinzu kommt, dass in der Fachliteratur wesentlich strengere Vorgaben (Microsofts Checkliste zum Server Hardening, getrennte Server für Exchange und BES, etc.) gemacht werden, als in der Praxis üblich sind. Diese sollten auch berücksichtigt werden.

Abzuraten ist nach derzeitigem Erkenntnisstand von der Nutzung BlackBerry-kompatibler (Connect) Geräte an einem BES, da diese die Funktionalität und insbesondere die Sicherheitsfunktionen nur in Software nachbilden und daher ungleich gefährdeter sind als BlackBerry-Geräte des Herstellers RIM. Auch fehlen ggf. wichtige Funktionen, wie z. B. die Verschlüsselung der Daten auf den Endgeräten.

BlackBerry-Geräte des Herstellers RIM können vorläufig sicher genutzt werden. Voraussetzung ist aber die Nutzung und sorgfältige Einstellung aller Sicherheitsfunktionen, auch wenn diese beim Gebrauch durch den Nutzer etwas hinderlich sein sollten. Schwachstellen sind die Nutzer selbst (Sonderwünsche bei Einstellungen, Geräteverlust) und der BES, da dieser Zugriff auf die Daten des Exchange-Servers hat und wie dieser sorgfältig gewartet werden muss.

Nicht nur in letzter Zeit ist Berichten zu entnehmen, dass gerade wegen des Themas „Wirtschaftsspionage“ immer mehr Unternehmen in sensiblen Bereichen der Wirtschaft vom Einsatz von BlackBerry-Geräten Abstand nehmen. Der Landesbeauftragte empfiehlt deshalb auch den öffentlichen Stellen, dieses Thema weiter zu verfolgen, sorgfältig den Einsatz solcher Technik unter Einbeziehung des behördlichen Datenschutzbeauftragten zu prüfen. Den genannten Risiken sollte durch entsprechende organisatorische Regelungen zum Gebrauch der Geräte für die Nutzer sowie durch eine sichere Administration begegnet werden.

14.11. Offene Verteilerlisten in Rundschreiben per E-Mail

Im Berichtszeitraum beschäftigte sich der Landesbeauftragte mehrfach mit dem Problem offener Empfänger-Listen in E-Mail-Verteilern (vgl. VIII. Tätigkeitsbericht, Ziff. 12.5). Die Pressemitteilungen eines Polizeireviers wurden durch die Nutzung des CC-Feldes, anstatt des BCC-Feldes des E-Mail-Programms, verschickt, was dazu führte, dass alle Empfänger alle Adressen anderer Empfänger übermittelt bekamen. Richtig wäre die Nutzung der BCC-Empfängerliste gewesen, deren Empfänger alle dieselbe E-Mail im Durchschlag und ohne Offenbarung personenbezogener Daten anderer Empfänger erhalten hätten. Ein Petent informierte zuerst direkt die Behörde, die daraufhin den Fehler abstellte. Aufgrund von Abwesenheiten wurden aber nicht alle Mitarbeiter informiert. Einige Zeit später wurde wieder das falsche Feld genutzt, so dass das Problem erneut auftrat und sich der Petent an den Landesbeauftragten wandte.

Trotz der Hinweise des Landesbeauftragten in seinem VIII. Tätigkeitsbericht sind offenbar mitverschickte E-Mail-Verteilerlisten ein ständig wiederkehrender Fehler, der einer entsprechenden Sensibilisierung aller Mitarbeiter bei der Nutzung von E-Mail-Diensten bedarf. Gleichzeitig könnten aber auch E-Mail-Programme von sich aus auf derartige Fehler hinweisen oder über entsprechende „Listenmanagement-Funktionen“ diese bereits im Vorfeld ausschließen. Manuelles Einfügen von Empfängerlisten in das richtige Empfängerfeld fordert den Fehler geradezu heraus und sollte generell durch automatisierte Versendungen ersetzt werden. Hausverfügungen, Dienstanweisungen oder Rundschreiben an alle und die Hinweise des Landesbeauftragten werden nicht ausreichen, so dass sich der nächste Fall für den nächsten Tätigkeitsbericht sicher schon andernorts anbahnt.

14.12. Hinweise zur Absicherung von Wireless-LAN

Ein Wireless-LAN (WLAN, drahtloses Netzwerk, Funknetz) ist nicht nur eine preiswerte Alternative zu einem herkömmlichen LAN (lokales Festnetz), es wird auch immer häufiger in öffentlichen Einrichtungen eingesetzt. Im Folgenden sollen daher einige grundlegende Maßnahmen zur Gewährleistung eines sicheren Betriebs des eigenen WLAN aufgezählt werden.

Wichtig ist die Wahl einer sicheren Verschlüsselungsmethode. Wired Equivalent Privacy (WEP) ist schon lange unsicher. Mindestens Wi-Fi Protected Access (WPA) ist gefordert, aber auch WPA ist mit immer weniger Aufwand

kompromittierbar, so dass entweder zu Zusatzmaßnahmen (VPN, SSH-Tunnel) geraten wird oder besser gleich WPA2 zum Einsatz kommen sollte.

Die Authentifizierung des Nutzers im WLAN ist über das Extensible Authentication Protocol (EAP), einem Protokoll zur Authentifizierung von WLAN-Clients, möglich. Die erlaubten Nutzer können vom einem RADIUS-Server verwaltet werden. Eine Authentifizierung über die MAC-Adresse des drahtlosen Netzwerkadapters ist nur prinzipiell möglich. Eine MAC-Adresse ist eine 48-Bit lange, gerätespezifische Kennung, welche unter anderem eindeutige Angaben zu Hersteller, Produkt und Geräteart enthält und der Erkennung von Geräten im Netzwerk dient. Leider ist diese Kennung in gewissen Grenzen frei einstellbar, d. h. insbesondere im drahtlosen Netzwerk, so dass ein Teilnehmer nicht allein anhand seiner MAC-Adresse authentifiziert werden darf. Access Points erlauben in der Regel das Definieren einer Filterliste der erlaubten MAC-Adressen. Diese reicht damit nicht aus, denn im zweiten Schritt wird dem Teilnehmer eine IP-Adresse zugewiesen, damit dieser mit dem Access Point kommunizieren kann und schon ist er im Netzwerk. Benutzen Sie zur Authentifizierung bspw. einen RADIUS-Server oder einen Diameter-Authentifizierungsdienst. Für Zugänge in ein VPN bieten sich IPSec (IKE-Protokoll mit X.509 oder RADIUS) bzw. ein Layer 2-Protokoll (L2TP/IPSec, L2F, PPTP) bzw. SSH verbunden mit dem PPP-Protokoll (PAP/CHAP) zur Benutzer-Authentifizierung an. Eine passwortbasierte Authentifizierung (PAP/ CHAP) kann durch vorab verteilte Schlüssel (pre-shared Keys) oder X.509-Zertifikate vermieden werden.

Der Netzwerkschlüssel muss sicher sein. Es gelten gleiche Anforderungen wie an ein Passwort (die Zeichenmenge sollte ausgenutzt werden und möglichst lang sein).

Eine Standard-Netzwerkkennung (SSID), welche den Gerätetyp und damit eventuelle Sicherheitslücken benennt, sollte ausgetauscht werden. Ein Verbergen der SSID ist möglich, stellt jedoch kein Hindernis für einen Angreifer dar. Ab Werk eingestellte Passwörter am Router oder Access Point müssen vor Betriebsaufnahme ausgetauscht werden. Dabei sind auch die Funktionen zur Fernwartung abzusichern bzw. ganz zu deaktivieren.

Der unkontrollierte Einsatz von Funknetzen in Verbindung mit lokalen Netzwerken in Behörden stellt eine Gefährdung für diese dar.

14.13. Kontrolle von Wireless-LAN bei öffentlichen Stellen

Drahtlose Netzwerke (auch Funknetze genannt) werden nicht nur im privaten Bereich immer beliebter. Aufgrund der Einfachheit der Nutzung ist es auch dem Laien möglich, innerhalb kürzester Zeit ein Wireless-LAN (WLAN) einzurichten und zu verwenden. Eigenmächtige Einrichtungen von WLAN-Netzen mit Anbindung an lokale Netzwerke oder Arbeitsplätze sind immer ein Sicherheitsproblem, das durch den Administrator bereits im Vorfeld unterbunden werden muss. Aber auch offiziell errichtete und durch einen Administrator abgesicherte WLANs können nicht auf Dauer als sicher angesehen werden. Aufgrund des enormen Sicherheitsrisikos für die über ein WLAN zur Verfügung gestellten Daten des internen Netzwerks (LAN) ist immer eine ü-

ber die Möglichkeiten des WLAN hinausgehende Absicherung - z. B. durch die Nutzung von Virtual Private Networks (VPN) in Verbindung mit RADIUS- oder Diameter-Authentifizierungsdiensten notwendig. WLANs werden generell als Sicherheitsrisiko angesehen. Deshalb wird das Vorhandensein von WLANs vom Landesbeauftragten im Rahmen seiner regelmäßig stattfindenden Kontrollen von Behörden und öffentlichen Einrichtungen routinemäßig geprüft und auf die genutzte Verschlüsselungstechnik hin kontrolliert.

14.14. Telearbeit

Der behördliche Datenschutzbeauftragte einer Verwaltungsgemeinschaft wandte sich mit der Bitte um Prüfung einer Dienstvereinbarung zur Einführung alternierender Telearbeit an den Landesbeauftragten. Er hatte eine Dienstvereinbarung entworfen, die aus datenschutzrechtlichen Gründen die Nutzung privater Hard- und Software im Rahmen der Telearbeit untersagte. Der Leiter der Verwaltungsgemeinschaft war mit dieser nicht einverstanden und verlangte eine entsprechende Änderung der Dienstvereinbarung, damit die Nutzung privater Hard- und Software zulässig sei.

Der behördliche Datenschutzbeauftragte kam der Anweisung nach, wies jedoch darauf hin, dass mit dieser Dienstvereinbarung der Datenschutz nicht gewährleistet sei. Der Landesbeauftragten nahm wie folgt Stellung:

Öffentliche Stellen des Landes, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben gem. § 6 Abs.1 DSG-LSA alle technischen und organisatorischen Maßnahmen zu treffen, die nach den Absätzen 2 und 3 erforderlich sind. Bei der automatisierten Verarbeitung personenbezogener Daten sind insbesondere Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz gewährleisten.

Bei der Telearbeit werden dienstliche Aufgaben in den häuslichen Bereich verlagert, wodurch unter Umständen auch personenbezogene Daten die verantwortliche Stelle i. S. d. § 2 Abs. 8 DSG-LSA verlassen. Dies birgt Risiken, da in der Regel die infrastrukturellen Sicherheitsmaßnahmen dienststelleninterner Arbeitsplätze fehlen. Die Kontroll- und Einflussmöglichkeiten der Dienststelle werden erheblich erschwert, wenn nicht sogar unmöglich. Zugleich nehmen die Missbrauchs- und Einflussmöglichkeiten durch Dritte deutlich zu. Darüber hinaus sind weder IT- noch Datenschutzfachleute vor Ort, so dass die Überprüfung der richtigen Funktionsweise des Telearbeitsplatzes nur schwer realisierbar ist.

Die genannten Punkte führen zu einem ungleich größeren Risiko der möglichen Beeinträchtigung des Rechtes auf informationelle Selbstbestimmung der von einer solchen Datenverarbeitung Betroffenen. Aus diesem Grund sind an die technisch-organisatorischen Maßnahmen entsprechend hohe Anforderungen zu stellen.

Zu den grundsätzlichen Sicherheitsanforderungen - die im Übrigen den Gegebenheiten in einer Behörde entsprechen sollten - zählt, dass ausschließlich Hard- und Software zum Einsatz kommt, die der Dienstherr für den Tele-

arbeitsplatz getestet und freigegeben hat. Die Verwendung privater Hard- und Software sowie die private Nutzung der dienstlichen Arbeitsmittel ist zu untersagen. Es ist technisch sicherzustellen, dass verändernde Zugriffe auf die Betriebssystemebene und auf Konfigurationen nur durch den Systemadministrator ausgeführt werden.

Ebenso wie in einer Behörde die Verwendung privater Hard- und Software nicht gestattet werden sollte, ist dies aus folgenden Gründen auch bei einem Telearbeitsplatz zu untersagen:
Im Allgemeinen kann bei einem privaten PC nicht davon ausgegangen werden, dass die Installation und Konfiguration fachgerecht erfolgt ist. Insbesondere die Installation, Konfiguration und Aktualisierung von Sicherheitssoftware (z. B. Firewall, Virenscanner, Sicherheitspatches) ist für die Datensicherheit von erheblicher Bedeutung. Durch die IT-Abteilung der Behörde kann nicht ausreichend sichergestellt werden, dass sich keine Schadsoftware auf dem privaten PC befindet, die die Sicherheit des gesamten Behördennetzes bzw. anderer angeschlossener Netze gefährden kann. Die Möglichkeit, den PC mit Schadsoftware zu infizieren, erhöht sich außerdem durch die private Nutzung im familiären Umfeld (z. B. Nutzung des PC durch Kinder und Jugendliche).

Bei der automatisierten Verarbeitung personenbezogener Daten mittels Telearbeit ist zusammenfassend festzustellen, dass die Verwendung privater Hard- und Software sowie die private Nutzung der dienstlichen Arbeitsmittel zu untersagen ist, da die Vertraulichkeit, Integrität und Verfügbarkeit der Daten gefährdet werden könnte (siehe § 6 Abs. 2 DSG-LSA). Sieht sich die Behörde außer Stande, die erforderlichen technisch-organisatorischen Maßnahmen zu treffen, so hat die Telearbeit aus datenschutzrechtlicher Sicht zu unterbleiben.

15. Hochschulen

15.1. Studierendendaten im Internet

Große, zentrale Datensammlungen rufen bei Datenschützern häufig Skepsis hervor. Je größer die Sammlung, desto größer die Begehrlichkeiten und die Gefahr von Beeinträchtigungen durch zweckändernde Verwendungen, unberechtigte Zugriffe, technische Pannen usw. Solcherart geäußerte Befürchtungen werden jedoch in Gesetzgebungsverfahren häufig belächelt, da man ja Zweckbindungen im Gesetz festschreiben und die erforderlichen technischen Maßnahmen zur Sicherung der Daten treffen könne. Wasser auf die Mühlen der Datenschützer war daher die Einstellung von Datensätzen von über 40.000 Studierenden auf einen mit dem Internet verbundenen Webserver durch die Otto-von-Guericke-Universität in Magdeburg.

Das Hochschul-Informations-System der Universität nutzte eine zentrale Datenbank zur Verwaltung der Bewerbungs-, Studierenden- und Prüfungsdaten. Der Server des Hochschul-Informations-Systems befand sich in einem eigenständigen, von außen nicht zugänglichen Netz. Es bestand daher zu keinem Zeitpunkt die Möglichkeit, von außen auf einen Server der Universität, auf dem interne studentische Daten gespeichert waren, zuzugreifen.

Die Speicherung auf einem öffentlich zugänglichen Server erfolgte durch einen Mitarbeiter der Abteilung Datenverarbeitung der Verwaltung, der insoweit Administratorenrechte hatte. Einpflegearbeiten sollten durch Schaffung und Nutzung eines Programms automatisiert werden. Ein solches Programm muss während der Programmierung angepasst und getestet werden, um anschließend die gewünschte Aufgabe automatisch und fehlerfrei ausführen zu können.

Um die Arbeit schneller von zu Hause aus am Wochenende vollenden zu können, wurden die Daten über einen öffentlich zugänglichen Webserver transferiert. Der verantwortliche Mitarbeiter hatte jedoch die auf den Webserver hochgeladenen Daten nicht sofort gelöscht.

Betroffen war die Stammdatenbank zu den Studierenden. Sie enthielt neben Daten zu den aktiven ca. 13.000 Studenten auch Daten zu Ehemaligen. Insgesamt waren durch die Speicherung auf dem Webserver Daten von 42.861 Studentinnen und Studenten öffentlich zugänglich. Die Stammdatenbank umfasst 153 Datenfelder, von denen 113 belegt waren. Inhaltlich waren u. a. Angaben zu Namen, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Postanschrift, Beurlaubungsgrund, Hochschulzugangsberechtigung und Note der Zugangsberechtigung sowie Berufsabschluss umfasst.

Neben der Studierendenstammdatenbank waren im Internet weitere Tabellen zugänglich. Eine Tabelle mit privaten und universitären E-Mail-Adressen war ebenso verfügbar wie eine Identifikationstabelle zu Zuordnungszwecken (Identitätsnummer, Rolle, Verbindungsnummer) zu 59.902 Personen.

Die Fehlleistung führte dazu, dass Internet-Suchmaschinen den Server durchsucht und die darauf befindlichen Dateien gefunden, gespeichert und veröffentlicht haben. Somit bestand die Möglichkeit, auf die Daten u. a. über Google zuzugreifen. Innerhalb von 9 Tagen wurden 15 Zugriffe von Suchmaschinen registriert. Weiterhin fanden 220 anderweitige Zugriffe statt. Sie kamen aus dem Bereich der Universität, aber auch aus den Netzwerken privater Anbieter. Die Zugriffe erfolgten zum Teil auf einzelne Dateien, zum Teil auf alle.

Auch wenn es praktisch erscheinen mag, mit Echtdaten zu arbeiten, ist es beim Entwickeln von Anwendungen, die personenbezogene Daten verarbeiten sollen, wichtig, Tests und Probeläufe mit Testdaten durchzuführen. Gerade dies gibt auch die Gelegenheit, Testfehler und Extremfälle in die Daten einzuarbeiten und die Software somit robuster zu gestalten.
Daten, die einmal in das Internet gelangen, sind nicht mehr rückholbar. In diesem Fall war dank der schnellen Reaktion der Betroffenen selbst die Zahl der Zugriffe noch überschaubar. Dennoch kann nicht ausgeschlossen werden, dass die Daten auf irgendeiner lokalen Festplatte „gesammelt“ wurden und zu einem späteren Zeitpunkt genutzt werden.

Die Universität ist für die Daten der Studenten in den Studierendendatenbanken verantwortliche Stelle nach § 2 Abs. 8 DSG-LSA. Die Verpflichtung der Studenten zur Angabe der erforderlichen Daten gegenüber der Universität ergibt sich aus § 119 Hochschulgesetz (HSG LSA). Die Universität erhebt,

verarbeitet bzw. nutzt die Daten zur Erfüllung der Aufgaben des HSG LSA. Rechtsgrundlage hierfür sind mangels spezifischer Regelungen im Hochschulrecht (die Hochschuldatenverordnung ist durch Gesetz vom 18.11.2005 aufgehoben) die Vorschriften des DSG-LSA.

Durch die unverschlüsselte Ablage der Datenbanken auf dem Webserver erfolgte eine Übermittlung der betreffenden Daten. Übermitteln ist das Bekanntgeben an einen Dritten durch Weitergabe (vgl. § 2 Abs. 5 Satz 2 Nr. 3 a) aa) DSG-LSA). Dritter als Person außerhalb der Verantwortlichen Stelle (vgl. § 2 Abs. 9 DSG-LSA) war hier zunächst schon der Serverbetreiber, der auch die Möglichkeit der Kenntnisnahme hatte. Weiterhin erfolgt eine Übermittlung auch dadurch, dass Dritten die Daten bekannt gegeben wurden, indem sie zur Einsicht bereit gehalten wurden und die Dritten Einsicht nahmen (§ 2 Abs. 5 Satz 2 Nr. 3 a) bb) DSG-LSA).

Eine Rechtsgrundlage für die Datenübermittlung war nicht gegeben. § 12 Abs. 1 Nr. 1 DSG-LSA griff nicht ein, da die Übermittlung nicht zur Erfüllung der in der Zuständigkeit der Universität liegenden Aufgaben erforderlich war. Die Übermittlung an den Serverbetreiber zur Erledigung der Verwaltungsaufgaben der Programmentwicklung für die Einpflegearbeiten war unzulässig. Bereits der Rückweg der Daten zeigte, dass auch ein USB-Stick für den Transport hätte gewählt werden können, ohne Dritten die Möglichkeit der Kenntnisnahme zu verschaffen. Zudem wäre eine datenschutzgerechte Übermittlung auch durch verschlüsselte Versendung über den Server denkbar gewesen.

Besonders gravierend war, dass das Bereithalten der Daten (§ 2 Abs. 5 Nr. 3 a) bb) DSG-LSA) auf einem im Internet zugänglichen Server zu unzulässigen Übermittlungen an nicht in § 13 Abs. 1 DSG-LSA genannte Stellen im Ausland führen konnte.

Der Verstoß gegen datenschutzrechtliche Vorschriften war schon wegen der großen Zahl Betroffener erheblich. Es sind umfängliche Daten zu Studierenden der Öffentlichkeit preisgegeben worden, die zum Teil präzise Darstellungen der beruflichen Vita beinhalten. Die unbekannten Zugriffe und daraus folgende Verwendungen bleiben offen.
Der Umfang der Daten, die eine Universität zur Erfüllung ihrer Aufgaben verarbeiten muss, ist sehr groß. Die Studierenden sind zur Angabe verpflichtet und müssen darauf vertrauen dürfen, dass nur befugter und zweckgebundener Zugang zu ihren Daten erfolgt. Die gesetzlichen Verarbeitungsvorschriften und die erforderlichen Maßnahmen der technischen und organisatorischen Datensicherheit (§ 6 DSG-LSA) sind einzuhalten. Der Umgang mit den Daten erfordert daher eine erhebliche Sensibilität. Diese fehlte hier völlig. Nicht nur die Nachlässigkeit, sondern auch das versehentliche Unterlassen der Löschung, ist bedenklich. Schon der ungeschützte Transfer machte deutlich, dass im konkreten Fall in der für die Datenverarbeitung verantwortlichen Stelle der Universität ein entsprechendes Defizit bestand.

Die Universität hat diverse Maßnahmen ergriffen, um die Folgen der Zugänglichmachung zu begrenzen. Die Daten auf dem öffentlich zugänglichen Server wurden gelöscht.

Die Universität informierte die Betroffenen, soweit möglich, über eine E-Mail des Rektors, dann in einer Pressemitteilung. Eine auf der Homepage der Universität veröffentlichte Information unterrichtete dann detaillierter über den Vorgang und die getroffenen Maßnahmen.
Eventuell noch vorhandene Zugriffsmöglichkeiten wurden geprüft.

Von einer förmlichen Beanstandung konnte jedoch abgesehen werden (§ 24 Abs. 3 DSG-LSA).
Die Universität hatte die nötigen Maßnahmen umgehend getroffen und die Löschung der Daten im Netz bewirkt. Eine erkannte Gefahrenquelle weiterer Datenverwendungen wurde unterbunden. Den Transparenzerfordernissen wurde, wenn auch zögerlich, Rechnung getragen. Eine Beanstandung hätte daher keine über die getroffene Feststellung eines gravierenden Datenschutzverstoßes hinausgehende Wirkung gehabt.

15.2. Nachwirkungen des Hochschulmedizingesetzes

Im VIII. Tätigkeitsbericht (Ziff. 13.1) hatte der Landesbeauftragte die Auswirkungen des Hochschulmedizingesetzes (HMG) vom 12. August 2005 auf die Personalverwaltung dargestellt. Wegen der Rechtsform der Kliniken als Anstalten öffentlichen Rechts mit Dienstherrneigenschaft war die Trennung der Verwaltung des Personals der Hochschule und des Klinikums geboten. Die Hochschulen und Kliniken hatten mitgeteilt, dass sie nach Beratungen Wege gefunden haben, die Vorgaben im Wesentlichen umzusetzen.

Im Berichtszeitraum hat der Landesbeauftragte den Datenschutz in der Personalverwaltung eines Klinikums geprüft. Das Klinikum setzte Personalverwaltungssoftware ein. Kursorische Einblicke in die elektronischen Vorgänge ergaben einige datenschutzrechtlich bedenkliche Ergebnisse.

Zunächst war festgestellt worden, dass das Klinikum den Grundsatz der informationellen Gewaltenteilung in der Personalaktenbearbeitung faktisch umsetzte. Die Personalakten für den Sachbereich Ärzte und medizinisches Personal und den Sachbereich Pflege wurden in getrennten Räumen und durch nur hierfür zuständiges Personal geführt. Dies war auch geboten. Die Umsetzung des gesetzlich geforderten Personalaktengeheimnisses (vertraulich, keine unbefugte Einsicht) erfordert bei großen Einrichtungen, dass nicht alle Personalsachbearbeiterinnen auf den gesamten Personaldatenbestand zurückgreifen können. Demgemäß ist der Zugriff auf einen bestimmten Mitarbeiterbereich für einzelne Personalsachbearbeiterinnen und ihre Vertretung zu begrenzen.
Eine Mitarbeiterin, die für den Sachbereich Pflege zuständig war, wurde darum gebeten, mit Hilfe des Personalverwaltungssystems nach Namen zu suchen. Dabei war es der dortigen Mitarbeiterin, die nicht für den Sachbereich Ärzte und medizinisches Personal zuständig ist, möglich, lesend auf umfängliche Personaldaten zu Beschäftigten zuzugreifen, die dem Sachbereich Ärzte und medizinisches Personal angehörten. Dies war für Ihre Aufgabenerfüllung nicht erforderlich. Auch im Personalverwaltungssystem muss die Trennung jedoch durch entsprechende Zugangsberechtigungskonzepte sichergestellt werden. Demgemäß wurde auf den dringenden Handlungsbedarf zur Wahrung des Personalaktengeheimnisses hingewiesen.

Weiter wurde eine Mitarbeiterin gebeten, im Personalverwaltungssystem den Namen eines Professors, nach § 6 Abs. 1 HMG Personal der medizinischen Fakultät der Universität, zu suchen. Nach Eingabe des Nachnamens erschienen der Stammdatensatz (u. a. Name und Vorname) sowie weitere Ordner, die differenzierten Zugriff auf die Personaldaten des Hochschullehrers zuließen. Unter anderem konnte die Bankverbindung angesehen werden. Dies ließ sich auch für einen weiteren Hochschullehrer realisieren. Es handelte sich nicht lediglich um listenmäßige Sachakteninformationen zur Organisation des Arbeitsablaufs im Universitätsklinikum. Demgemäß bestand für die Personalsachbearbeitung des Universitätsklinikums als rechtlich selbständige Anstalt des öffentlichen Rechts ein unmittelbarer Zugriff auf Personalaktendaten von Personal eines anderen Dienstherrn.
Nach § 90 Abs. 1 Satz 1 2. Halbsatz Beamtengesetz LSA i. V. m. § 28 Abs. 1 DSG-LSA sind Personalakten vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Aus Sicht der Universität lag eine unzulässige Übermittlung vor. Obwohl die Rechtslage klar und bekannt war, war offensichtlich versäumt worden, die der Personalbewirtschaftung zugrundeliegende Informationstechnologie anzupassen. Es wurde daher darauf gedrungen, dass – unabhängig von der Frage der künftigen Ausgestaltung des IT-gestützten Zusammenwirkens von Universitätsklinikum und Medizinischer Fakultät – der umfassende einrichtungsübergreifende Zugang auf Personalaktendaten kurzfristig unterbunden werden muss. Die Universität hat zwischenzeitlich mitgeteilt, dass der unzulässige Zugriff im Zusammenwirken der Verantwortlichen der Universität und des Klinikums unter Einbeziehung der Datenschutzbeauftragten abgestellt wurde.

16. Kommunalverwaltung

16.1. Grundstückseigentümerangaben unklarer Herkunft

Eine Bürgerin staunte nicht schlecht, als sie von einer ca. 100 km von ihrem Wohnort entfernt gelegenen Verwaltungsgemeinschaft die Mitteilung erhielt, sie sei dort Eigentümerin eines Grundstücks. Die Verwaltungsgemeinschaft trübte die Freude der Bürgerin jedoch sogleich dadurch, dass sie ihr eine Verwarnung wegen fortgesetzten Verstoßes gegen die Straßenreinigungspflicht erteilte. Sie sei schließlich als Eigentümerin gemäß der entsprechenden kommunalen Satzung zur Straßenreinigung verpflichtet.

Die Bürgerin, selbstredend nicht Eigentümerin des von der Verwaltungsgemeinschaft bezeichneten Grundstücks, war wenig amüsiert, konstatierte die unrichtige Verarbeitung ihrer personenbezogenen Daten in der Verwaltungsgemeinschaft und bat den Landesbeauftragten, in den Datenbeständen der Verwaltungsgemeinschaft für Ordnung sorgen zu lassen.
Diese Aufgabe erwies sich als nicht trivial.

Auf Nachfrage des Landesbeauftragten erklärte die Verwaltungsgemeinschaft nämlich, Opfer eines Fehlers im automatisierten Liegenschaftsbuch geworden zu sein. Die von ihr nun als falsch anerkannten Eigentümerangaben seien aus dem vom Landesamt für Vermessung und Geoinformation gem. § 13 Abs. 2 Vermessungs- und Geoinformationsgesetz Sachsen-Anhalt

für das Gebiet der Gemeinde bereitgestellten automatisierten Liegenschaftsbuch entnommen worden. Das Landesamt stellte dem Landesbeauftragten nachvollziehbar dar, dass außer Name, Vorname, Geburtsname und Geburtsdatum im konkreten Fall keine darüber hinausgehende Angaben der Eigentümerin im Liegenschaftsbuch geführt und den Gemeinden keinesfalls mehr Eigentümerangaben mitgeteilt würden.
Das, durch den Landesbeauftragten der Verwaltungsgemeinschaft mitgeteilt und nach Fakten gefragt, brachte diese in Wallung. Die Verwaltungsgemeinschaft musste schließlich bekennen, dass sie die Adressdaten der angeblichen Eigentümerin manuell in ihren Datenbestand eingepflegt hatte. Dabei war den Verantwortlichen nicht einmal aufgefallen, dass der Vorname der Bürgerin in der Schreibweise doch eine kleine Abweichung aufwies, das Geburtsdatum um 11 Jahre und einige Monate differierte und der Geburtsname überhaupt nicht übereinstimmte. Das Bauamt hatte dies alles übersehen oder ignoriert und - auf inzwischen nicht mehr nachvollziehbarem Wege - recherchiert und irgendwann die Adresse der überraschten Bürgerin ermittelt und ungeprüft gespeichert.

Der Landesbeauftragte rät, personenbezogene Daten nur dann zu verarbeiten, wenn ihre Richtigkeit zuverlässig bekannt ist oder die Daten aus zuverlässiger Quelle stammen. Datenraten dagegen ist mit geordnetem Verwaltungshandeln nicht vereinbar.

16.2. Übermittlung der Namen der Gemeinderäte an private Dritte

Dem Landesbeauftragten wurde bekannt, dass die Kommunalaufsichtsbehörden die Kommunen des Landes dazu anhalten würden, die Namen, Anschriften und Telefonnummern von Gemeinderatsmitgliedern an private Dritte (wie z. B. interessierte Firmen) zu übermitteln.

Dem daraufhin um Stellungnahme gebetenen Ministerium des Innern war dieser Sachverhalt unbekannt. Es nahm die Schilderung des Landesbeauftragten aber zum Anlass, den Sachverhalt in einer gemeinsamen Beratung mit allen Kommunalaufsichtsbehörden zu besprechen. Dabei vertrat das Ministerium die Auffassung, dass zumindest die Übermittlung der Namen der Mandatsträger als Inhaber des öffentlichen Amts, neben der Angabe, welchen Ausschüssen sie angehören, als datenschutzrechtlich zulässige Aufgabenerfüllung der Kommune im Rahmen ihrer Öffentlichkeitsarbeit anzusehen sei.

An der Erforderlichkeit dieser „Aufgabenerfüllung“ zweifelt der Landesbeauftragte. Er sieht sich aber darin mit dem Ministerium einig, dass die Übermittlung darüber hinausgehender personenbezogenen Daten (wie Privatadresse, Telefonnummer) datenschutzrechtlich nicht gedeckt ist; es sei denn, jeder einzelne Betroffene habe darin eingewilligt.

16.3. Bezüge einzelner Geschäftsführer im Beteiligungsbericht

Gemeinden müssen ihren Gremien über Unternehmen, an denen sie beteiligt sind, entsprechend den Vorschriften der Gemeindeordnung für das Land Sachsen-Anhalt (GO LSA) einen sogenannten Beteiligungsbericht vorlegen.

Der Datenschutzbeauftragte einer Gemeinde hatte nun Bedenken, weil sich dem Beteiligungsbericht die Gesamtbezüge einzelner Geschäftsführer entnehmen ließen und wandte sich hilfesuchend an den Landesbeauftragten.

Der Landesbeauftragte hat zu diesem Sachverhalt eine umfangreiche Stellungnahme ausgearbeitet:

§ 118 Abs. 2 Satz 2 Nr. 4 GO LSA regelt ersichtlich nur die Angabe aggregierter Bezüge, insoweit dürfte es sich grundsätzlich um anonyme Daten (§ 2 Abs. 7 DSG-LSA) handeln. Nach der Darstellung der Gemeinde würden durch die faktische Reduktion der Gesamtbezüge auf eine einzelne Person deren sachliche Verhältnisse bestimmbar. Demnach käme in Betracht, nach § 118 Abs. 2 Satz 2 GO LSA auf die Daten im Beteiligungsbericht zu verzichten.

Grundsätzlich ist die umfassende Information der Mandatsträger notwendig, da sie für die grundlegenden Entscheidungen des kommunalen Gemeinwesens verantwortlich sind. Wahrnehmung von Verantwortung setzt Information voraus. Daher kann nur unter ganz besonderen Bedingungen die Unterrichtung der Mandatsträger unterbleiben. Ob allein das Faktum Einzeldatum ausreicht, um deswegen auf die Angabe der Bezüge gegenüber den Mandatsträgern zu verzichten, bedarf der genaueren Prüfung im Einzelfall. Nach §§ 10, 9 DSG-LSA könnte die Nutzung der Daten zulässig sein, wenn der Gemeinderat sie zur Erfüllung seiner Aufgaben benötigt.

Dies bedeutet jedoch nicht, dass diese Daten veröffentlicht werden dürfen. Auch wenn die sich aus dem Beteiligungsbericht ergebenden Zahlen keine Bewertung der wirtschaftlichen Gesamtsituation des betroffenen Geschäftsführers ermöglichen, stellen sie ein für den Betroffenen wesentliches Datum dar. Daher gebietet es § 50 Abs. 2 GO LSA, den Beteiligungsbericht insoweit nur in nicht-öffentlicher Sitzung zu behandeln. Dass dies bei der Befassung mit dem Beteiligungsbericht nötig werden kann, hat der Gesetzgeber durch den Hinweis in § 118 Abs. 2 Satz 3 GO LSA bereits berücksichtigt. Darauf, dass alle Mandatsträger gem. § 30 Abs. 2 GO LSA zur Verschwiegenheit verpflichtet sind, sei nur der Vollständigkeit halber hingewiesen. Damit kann den persönlichen Interessen des Geschäftsführers wie auch dem Informationsrecht des Gemeinderats in angemessener Weise genügt werden.

Schließlich zur Veröffentlichung des Beteiligungsberichts bzw. öffentlichen Information über diesen: Da keine spezielle gesetzliche Regelung in der GO LSA besteht, kann die Veröffentlichung und damit die Übermittlung der Bezüge eines Einzelnen an einen unbestimmten Empfängerkreis gem. §§ 12 Abs. 1 Nr. 1, 10 Abs. 2 Nr. 2 DSG-LSA nur erfolgen, wenn der Betroffene eingewilligt hat (vgl. § 4 Abs. 1 DSG-LSA). Im Unterschied zu den handelsrechtlichen Berichten gemäß §§ 286 Abs. 4 i. V. m. § 285 Abs. 9 a) HGB, die zur Veröffentlichung bestimmt sind, ist dies beim kommunalen Beteiligungsbericht nicht zwingend vorgesehen. Da nach dem Gesetzeswortlaut die Gemeinde die Einwohner über den Beteiligungsbericht lediglich in geeigneter Form zu unterrichten hat (§ 118 Abs. 3 GO LSA), ist eine Mitteilung personenbezogener Daten unnötig.

Mit dem gleichen Ergebnis hat sich auch der Landesrechnungshof gegenüber der Gemeinde geäußert.

17. Personalwesen

17.1. Gesetz zur Neuordnung des Landesbeamtenrechts

Aufgrund der im Grundgesetz im Zuge der Föderalismusreform geänderten Regelungen zur Gesetzgebungskompetenz hat der Bund mit dem Beamtenstatusgesetz die beamtenrechtlichen Grundstrukturen festgelegt. Es trat am 1. April 2009 in Kraft. Die weitergehenden Regelungen oblagen dem Landesgesetzgeber.

Das Ministerium des Innern hatte den Landesbeauftragten zu einem Referentenentwurf eines Gesetzes zur Neuordnung des Landesbeamtenrechts im Sommer 2008 beteiligt. Eine weitere Beteiligung im Rahmen der Anhörung erfolgte leider nicht.

Der Landesbeauftragte wies auf einzelne Aspekte des Personalaktenrechts hin, die teilweise in den Entwurf der Landesregierung (LT-Drs. 5/1710) eingearbeitet wurden.

Zunächst war positiv festzustellen, dass eine sehr detaillierte Regelung des Personalaktenrechts unter Einbeziehung der bewährten Regelungen des Beamtengesetzes des Landes (BG LSA) vorgesehen war. Auch nach den hiesigen Erfahrungen im Rahmen von Prüfungen stellen die bisherigen Vorschriften eine gute Unterstützung bei der sachdienlichen und datenschutzkonformen Bearbeitung von Personalvorgängen dar.

Zur Regelung des Inhalts der Personalakte wurde angeregt, ergänzend klarzustellen, dass in die Personalakte die Unterlagen gehören, die den Beamten betreffen, soweit sie mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen (Personalaktendaten). Das Kriterium, das den materiellen Personalaktenbegriff festlegt, war für die praktische Differenzierung hilfreich. § 50 Satz 2 Beamtenstatusgesetz sieht dies allerdings bindend vor. Auch der Begründung ist nicht zu entnehmen, dass ein Abweichen von dem materiellen Personalaktenbegriff gewollt ist.

Weiter wurde empfohlen, erneut die Regelung aus § 90 Abs. 1 Satz 1 BG LSA vorzusehen, wonach die Personalakte vertraulich zu behandeln und vor unbefugter Einsicht zu schützen ist. Bisher galt das in § 90 BG LSA formulierte Personalaktengeheimnis als ein besonderes, gesteigertes Geheimnis. Allerdings gibt § 50 Satz 3 Beamtenstatusgesetz die vertrauliche Behandlung vor. Der Begründung ist auch hier nicht zu entnehmen, dass ein Abweichen von dem Personalaktengeheimnis gewollt ist.

Weiterhin hatte der Landesbeauftragte darauf hingewiesen, dass der bisherige Anspruch des Beamten auf Überlassung eines Ausdrucks der zu seiner Person automatisiert gespeicherten Personalaktendaten (§ 90c Abs. 3 Satz 2 letzter Halbsatz BG LSA) erhalten bleiben sollte. Darauf war zunächst ver-

zichtet worden, weil sich der Anspruch hinreichend aus dem Einsichtsrecht selbst ergebe. Nunmehr ist ein entsprechender Anspruch formuliert.

Das ursprüngliche Anliegen, personenbezogene Daten aus der Personalakte ohne Einwilligung an andere beauftragte Stellen weitergeben zu dürfen, um u. a. Besoldungs-, Versorgungs- und Beihilfevorgänge zu erledigen, erschien bedenklich. Demgemäß wies der Landesbeauftragte darauf hin, dass insbesondere bei Beihilfedaten personenbezogene Daten besonderer Art betroffen sind (Gesundheitsdaten), die landes-, bundes- und europarechtlich besonderen Schutz genießen. Der Wortlaut „beauftragte Stelle“ hätte aber zugelassen, auch eine private Einrichtung zu beauftragen. Dies erscheint im Hinblick auf die Sensibilität der betreffenden Daten und den Anspruch des Beamten auf vertraulichen Umgang mit diesen Daten durch seinen Dienstherrn nicht vereinbar.

17.2. Personalmanagementsystem

Das Land beabsichtigt, ein IT-gestütztes Personalmanagementsystem (PMS) für die gesamte Landesverwaltung zu beschaffen. Das System soll ressortübergreifend Aufgaben im Bereich der Personalverwaltung, der Personalentwicklung und -planung, der Dienstposten- und Arbeitsplatzverwaltung, der Stellenbewirtschaftung sowie der Verwaltung der Personalausgaben und der Personalkostenhochrechnung wahrnehmen. Zur Umsetzung des komplexen Vorhabens wurden eine Projektlenkungsgruppe und eine Projektarbeitsgruppe mit den im Bereich Personal fachlich versierten Bediensteten der Ressorts gebildet. Zunächst wurde eine detaillierte Leistungsbeschreibung erarbeitet, die Grundlage für die Auftragsvergabe werden sollte. Später folgten Unterarbeitsgruppen, die die im Rahmen der Einführung des PMS benötigten Konzepte aus fachlicher Sicht vorbereiteten.

Der Landesbeauftragte wurde frühzeitig in das Projekt einbezogen. Er hat das federführende Finanzministerium beraten, nimmt an den Sitzungen der Projektlenkungsgruppe teil und berät auch in der Unterarbeitsgruppe „Rollen- und Berechtigungskonzept“.

Zunächst konnte auf die Handlungsempfehlungen „Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung“ der Datenschutzbeauftragten des Bundes und der Länder hingewiesen werden, in denen grundlegende Anforderungen formuliert sind. In den Beratungen wurden schon vor Fertigstellung der Leistungsbeschreibung datenschutzrechtliche Aspekte erörtert.

Das Verhältnis des geplanten PMS und seiner zentralen Datenbank zu den Datenlieferanten wurde angesprochen. Wegen datenschutzrechtlicher und insbesondere beamtenrechtlicher Vorgaben müssen die Zugriffe auf die personenbezogenen Daten im Ergebnis in der Verantwortung der jeweils datenschutzrechtlich verantwortlichen Stelle, der personalaktenführenden Stelle, verbleiben. Das Rechenzentrum bzw. die zentrale Datenbank könnte als zentraler Service die Datenhaltung im Sinne einer Hilfsfunktion übernehmen. Auch eine Auslagerung der reinen Datenhaltung könnte bei entsprechender Ausgestaltung, z. B. mittels Verschlüsselung, ggf. mit dem Beamtengesetz

vereinbar sein. Das Bewusstsein der Ressorts und personalverwaltenden Dienststellen dafür, dass es sich um ihre eigenen Daten handelt, müsse geschärft werden.
Ergänzend wurde darauf hingewiesen, dass die Strukturierung, die beamtenrechtlichen Vorgaben und die differenzierten Zugriffsrechte bereits im Anforderungskatalog für die Anbieter deutlich gemacht werden sollten, um das System von vorn herein an den gesetzlichen Anforderungen auszurichten.
Infolge der beamtenrechtlichen Vorgaben müsse es für die zentrale Auswertung bei anonymisierten bzw. **aggregierten** Daten verbleiben.

Auch allgemeine datenschutzrechtliche Rahmenbedingungen wurden erörtert, wie beispielsweise die Problematik der unzulässigen Doppeldatenspeicherung bzw. die allgemeine Problematik von Hybridakten. Weiter wurden die Notwendigkeit der Beachtung von Löschungsfristen und die archivrechtlich vorgesehene Anbietung an das Landesarchiv angesprochen.

Im Rahmen eines Customizing war angedacht, dass ein Bearbeiter den Datenkatalog um eigene Felder erweitern können soll. Dies erschien schon im Hinblick auf die Datensparsamkeit datenschutzrechtlich problematisch. Es sollte sich jedoch nicht um ein Blankofeld handeln, sondern vielmehr um die Möglichkeit, den spezifischen Anforderungen an die Sachbearbeitung in einzelnen Ressorts im Rahmen der Beschreibung des Feinkonzepts Rechnung zu tragen. Für bestimmte fachliche Aufgaben (Untersuchung medizinisch-technischer Angestellter, Schlussprüfung) sind Felder erforderlich.
Wichtig ist, dass die Datenzugriffe des jeweiligen Sachbearbeiters nur auf „seine“ Daten begrenzt werden. Dies ist bei der Umsetzung im Rahmen eines **Berechtigungskonzepts** zu berücksichtigen.

Im Rahmen der Personalverwaltung soll das System Entscheidungsgrundlagen für die Personalauswahl liefern, automatische Synopsen erstellen und letztlich nach Auswahl bestgeeigneter Bewerber Einladungsschreiben zu Auswahlgesprächen selber elektronisch generieren. Hierzu wurde auf § 90g Abs. 4 BG LSA hingewiesen. Personalentscheidungen dürfen nicht ausschließlich aufgrund automatisiert verarbeiteter personenbezogener Daten erfolgen. Möglich ist lediglich, die persönliche Entscheidung zu unterstützen.

Die Beteiligung der Personalvertretung war ebenfalls Thema, wie auch die notwendige Transparenz unter Bezug auf § 90g Abs. 5 BG LSA.

Der Landesbeauftragte wird die Ausgestaltung weiter begleiten. Insbesondere bei der praktischen Umsetzung der Zuweisung von Rollen und Zugriffsberechtigungen an einzelne Beschäftigte wird im Detail die datenschutzrechtliche Zulässigkeit zu prüfen sein.

17.3. Fortbildungsmanagement

Die Landesregierung beabsichtigte, ein zentrales Programm, genannt TIS, zur Planung, Verwaltung, Abrechnung und Auswertung von Fortbildungsmaßnahmen sowie der Kosten- und Leistungsrechnung und Inventarverwaltung einzuführen. Dieses Fortbildungsmanagementsystem war als Leitprojekt

Bestandteil des eGovernment-Konzepts des Landes. Der Landesbeauftragte wurde beteiligt.

In den Beratungen wurde die Absicht deutlich, den Personalstammdatenbestand der zentralen Bezügestelle für das Fortbildungsprogramm nutzbar zu machen. Dem Bezügeabrechnungssystem sollten bestimmte Personaldaten wie Name, Vorname, Geburtsjahr, Privat- und Dienstanschrift entnommen werden, da die anderweitige Erfassung zu aufwändig sei.

Allerdings fehlte für eine Datenübermittlung in der beschriebenen Art durch Übertragung eines umfangreichen Personalstammdatensatzes aller Beschäftigten von der Bezügestelle an das Landesinstitut für Lehrerfortbildung, Lehrerweiterbildung und Unterrichtsforschung (LISA - seit 1. März 2009 Landesinstitut für Schulqualität und Lehrerbildung), welches das Programm landesweit einsetzen sollte, eine Rechtsgrundlage.
Die Einwilligung aller Beschäftigten lag nicht vor, ihre Einholung war unpraktikabel.
Eine Weitergabe im Wege der Datenverarbeitung im Auftrag (§ 8 Abs. 1 Satz 1 DSG-LSA) schien ebenfalls problematisch. Eine jeweilige Beauftragung wäre erforderlich gewesen. Zudem hätten lediglich „Hilfsfunktionen“ ausgeführt werden dürfen. Da ein zentrales Fortbildungsmanagement vorgesehen war, war nicht von einer Datenverarbeitung im Auftrag auszugehen.

Die Bezügestelle verfügt auf besoldungsrechtlicher Grundlage über die zur Berechnung und Zahlbarmachung der Bezüge/Vergütung erforderlichen Personaldaten. Diese sind wegen des inneren unmittelbaren Zusammenhangs mit dem Beschäftigungsverhältnis als Personalaktendaten i. S. d. § 90 Abs. 1 Satz 2 BG LSA zu qualifizieren. § 90 Abs. 1 Satz 3, Abs. 3 BG LSA, der die Verwendung von Personalaktendaten für Zwecke der Personalverwaltung und Personalwirtschaft erfasst, kommt als Grundlage einer Weitergabe der Bezügestammdaten an das LISA nicht in Betracht, da § 90 Abs. 3 BG LSA nur die Zugangsberechtigung innerhalb der Behörde regelt, bei der die Personalakte bzw. Nebenakte geführt wird. Die Vorlage an andere Behörden oder Dritte bestimmt sich nach § 90d BG LSA.
§ 90d Abs. 1 BG LSA erlaubt eine Übermittlung über die Ressortgrenzen hinweg nur, wenn die andere Behörde an einer Personalentscheidung mitzuwirken hat. Es ging jedoch nicht um eine konkrete Personalentscheidung, sondern das Einpflegen der Daten aller Beschäftigten.
Zudem dürfte eine Personalstammdatenbank mit Informationen u. a. zu Geburtsjahr und Privatanschrift beim LISA nicht mit dem Gebot der Datensparsamkeit und Datenvermeidung (§ 1 Abs. 2 Satz 1 DSG-LSA) zu vereinbaren sein. Das Vorhaben begegnete auch im Hinblick auf die Unzulässigkeit einer Vorratsdatenspeicherung Bedenken, da kaum alle Beschäftigten des Landes an einer Fortbildung teilnehmen würden.

Eine Eingabe aller Beschäftigten von Hand, insbesondere der Lehrkräfte, war jedoch nicht zu bewältigen. Es war daher notwendig, beim erstmaligen selbständigen Zugang der Beschäftigten über das Internet eine Prüfung der Berechtigung (Landesbediensteter) vorzunehmen, wofür das Programm die entsprechenden Referenzdaten braucht.

Letztlich wurde nach umfänglichen Erörterungen mit Hinweisen auch zu technisch-organisatorischen Maßnahmen der Datensicherheit unter Einbeziehung aller Beteiligten auf die Dateneinpflege vom Bezügesystem verzichtet. Die Anmeldung erst bei Bedarf wurde akzeptiert.
Die Anmeldung der Lehrkräfte erfolgt online über das Portal. Die Zugangsberechtigung wird durch eine Kennung nachgewiesen, die der Bezügemitteilung aufgedruckt ist. So wird die Gefahr eines missbräuchlichen Zugangs auf ein angemessenes Maß reduziert.
Die Anmeldung anderer Beschäftigter erfolgt jeweils, soweit erforderlich, durch die jeweilige personalführende Dienststelle. Hierfür erhalten die Dienststellen die entsprechende Software.

17.4. Durchsuchung der Zentralablage

Anonyme Schreiben an verschiedene Einrichtungen warfen der Leitung des Ministeriums für Landwirtschaft und Umwelt unsachliche und rechtswidrige dienstliche Entscheidungen vor. Als Absender der Schreiben waren Mitarbeiter des Ministeriums bzw. Mitarbeiter des Personalreferates aufgeführt. Um den Urheber der Schreiben zu ermitteln, wurde ein Suchlauf auf der Zentralablage des Servers durchgeführt. Der Landesbeauftragte wurde um Prüfung des Vorgangs gebeten.
Der elektronische Suchlauf auf dem Server des Ministeriums erfasste die Zentralablage des Servers (die Abteilungs- und Referatsablage und die Nutzerablage). Passwortgeschützte Dateien, lokale Laufwerke und der E-Mail-Server wurden nicht durchsucht. Aber es waren auch Speicherungen des Personalrats betroffen. Die mit Standardsoftware durchgeführte Suche nach Dateinamen richtete sich auf das Auffinden von zwei Stichworten. Es wurde kein Treffer erzielt.

Im Hinblick auf das Ergebnis des Suchlaufs war festzustellen, dass mangels Treffers kein datenschutzrechtlich relevanter Erhebungs-, Verarbeitungs- oder Nutzungsvorgang stattgefunden hat. Objektiv betrachtet war daher zunächst auch kein Datenschutzverstoß feststellbar.

Der Suchlauf hatte aber eine datenbezogene Rechenoperation in Gang gesetzt, die im Trefferfall zu personenbezogenen Daten hätte führen können. Gegen die Verpflichtung des Ministeriums, die Ausführung der Vorschriften des Datenschutzes sicher zu stellen, wäre verstoßen worden, wenn es für eine Erhebung im Trefferfall keine Rechtsgrundlage gegeben hätte.
Trotz Bedenken konnte im Ergebnis jedoch festgestellt werden, dass für eine solche Datenerhebung eine Rechtsgrundlage (§ 9 Abs. 2 Nr. 2 a) DSG-LSA) gegeben gewesen wäre.

Die Verhältnismäßigkeit der Maßnahme war indessen zweifelhaft.

Nach dem verfassungsrechtlichen **Grundsatz der Verhältnismäßigkeit** darf ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung nicht außer Verhältnis zum angestrebten Ziel stehen (Verhältnismäßigkeit im engeren Sinne). Maßgeblich für Verhältnismäßigkeit eines solchen Eingriffs ist u. a. das Gewicht des Eingriffs (Persönlichkeitsrelevanz) und, ob der Betroffene einen zurechenbaren Anlass für die Maßnahme gegeben hat. Werden

Personen, die keinen Anlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, kann dies zu Einschüchterungseffekten führen. Die Einbeziehung von Personen, die in keiner Beziehung zum Tatvorwurf stehen, kann zu einer die Eingriffsintensität merklich erhöhenden Streubreite führen.
Demgemäß erfordern Eingriffe bestimmte Gefahrenstufen. Die Verhältnismäßigkeit gebietet, dass selbst bei einer drohenden Rechtsgutsbeeinträchtigung größten Ausmaßes das Erfordernis einer hinreichenden Wahrscheinlichkeit des Gefahreneintritts berücksichtigt wird. Grundrechtseingreifende Ermittlungen „ins Blaue hinein“ sind mit der Verfassung nicht zu vereinbaren.
Staatliches Eindringen in die Privatsphäre aufgrund reiner Spekulation, begründet die Gefahr maßloser Ermittlungen. Erhebt man einen Generalverdacht, erfasst man viele, trifft es Unbeteiligte. Bei Vorfeldermittlungen mit großer Streubreite sind konkrete Fakten hinsichtlich einer konkreten Gefahrenlage zu dokumentieren.

Im vorliegenden Sachverhalt wurden durch die Suche alle Nutzer der Zentralablage, auf der nach Vorgaben des Ministeriums aus Sicherheitsgründen zu speichern war, erfasst. Fast alle Bediensteten mit dienstlichen und ggf. auch privaten Speicherungen wurden also einbezogen. Die Reaktion der Personalräte und die nachfolgende öffentliche Diskussion sowie die Debatte im Landtag zeigten, dass vielfach das Gefühl unangemessener Überwachung entstand.

Die Frage nach der Verhältnismäßigkeit gebietet jedoch auch eine Abwägung mit den legitimen Interessen des Dienstherrn.
Es war zu berücksichtigen, dass auf der Zentralablage grundsätzlich dienstliche Korrespondenz zu speichern ist. Die Kenntnisnahme dieser Korrespondenz als Teil der Behördenkommunikation steht der Hausleitung grundsätzlich zu.
Zudem wurde der Suchlauf für interne Zwecke der Wahrnehmung von Aufsichts- und Kontrollbefugnissen durchgeführt.
Zunächst bestand die Notwendigkeit, die leitenden Mitarbeiter vor weiteren Anschuldigungen in dieser Form zu schützen.
Zudem wiesen die Schreiben auf Verfasser aus dem Haus hin, so dass auch den insoweit Beschäftigten gegenüber die Notwendigkeit bestand, den Verdacht auszuschließen, dass Mitarbeiter des Ministeriums als Verfasser ernsthaft in Betracht kommen.
Auch die Verteilung der anonymen Schreiben machte ein Einschreiten erforderlich. Die Vorwürfe kursierten in der Justiz, der Regierung sowie in weiteren unbestimmten Kreisen. Sie waren auch im ganzen Haus bekannt. Damit war das Ansehen der Ministeriumsleitung in breiten, nicht näher eingrenzbaren Bereichen tangiert. Rufschädigungen ist entgegen zu treten.

Weiter war zu berücksichtigen, dass die tatsächliche Beeinträchtigung der Nutzer der Zentralablage letztlich eher gering war. Dies ergab sich aus dem durchgeführten Verfahren und den verwendeten Suchbegriffen.
Der Suchlauf wurde nur durch die Administratorin durchgeführt. Es wären auch nur Treffer gemeldet worden. Eine Grundrechtsbeeinträchtigung der Vielzahl der „Unbescholtenen“ war gemäß der Rechtsprechung des Bundes-

verfassungsgerichts nicht gegeben, denn die Nutzer der Zentralablage blieben infolge des Vorgehens anonym; es wurden keine Datenspuren erfasst.
Die Suchbegriffe waren sehr spezifisch ausgewählt worden, so dass eine Trefferwahrscheinlichkeit bei Beschäftigten, die keines der anonymen Schreiben auf Ihrer Ablage gespeichert hatten, relativ gering war.
Eine besondere Reduktion erfuhr die Betroffenheit dadurch, dass nur ein Suchlauf nach Dateinamen, nicht nach Dateiinhalten durchgeführt wurde, der die Wahrscheinlichkeit eines Treffers extrem verkleinerte. Nur bei den als „Treffer“ gemeldeten Fällen wäre für den Betroffenen eine „Entlastung“ notwendig geworden.

Datenschutzrechtlich bedenkliche Kontrollmaßnahmen, die zur merklichen Beeinträchtigung des Persönlichkeitsrechts geführt hätten, lagen im Ergebnis nicht vor. Datenschutzrechtlich problematische Nutzungen dienstlicher Kommunikationstechnik zur Mitarbeiterüberwachung wären i. d. R. erst bei Maßnahmen gegeben, die aufgrund ihres Umfangs und der tatsächlichen Betroffenheit des Einzelnen mit dem Schutz des Persönlichkeitsrechts der Beschäftigten nicht mehr vereinbar sind.

Die Verhältnismäßigkeit stand noch deshalb in Frage, weil das Ministerium es vor der Veranlassung des Suchlaufs versäumt hatte, den Personalrat zu beteiligen. Auch die Zulässigkeit besonderer Formen der Datenerhebung unterliegt dem allgemeinen Verhältnismäßigkeitsgrundsatz.
Die Dienstvereinbarung sah grundsätzlich keine Leistungs-/Verhaltenskontrollen der Beschäftigten vor. Ausnahmen bedürfen der Zustimmung des Personalrats. Dienstvereinbarungen schaffen grundsätzlich personalvertretungsrechtlich eine verbindliche Grundlage.
In der Gesamtschau war die Verhältnismäßigkeit dennoch gegeben.
Die Recherchen des Landesbeauftragten ergaben, dass der Dienstvereinbarung ein klares Verdikt gegen die Durchführung eines Suchlaufs ohne vorherige Zustimmung des Personalrats nicht zu entnehmen war. Das Ministerium hätte den Personalrat im Trefferfall beteiligt.
Erst im Fall weiterer Maßnahmen wäre aber eine spürbare Intensivierung der Grundrechtsbeeinträchtigung der Betroffenen erfolgt. Zuvor war die Beeinträchtigung eher gering. Im Hinblick auf den für die Verhältnismäßigkeit wesentlichen Aspekt der Intensität der Beeinträchtigung erschien die Verschiebung einer Beteiligung auf konkretere Maßnahmen noch akzeptabel.
Auch wenn die Unterlassung einer frühzeitigen Information aus personalvertretungsrechtlicher Sicht möglicherweise kritisch war, lag noch keine Unverhältnismäßigkeit in datenschutzrechtlicher Hinsicht vor.

Die Verhältnismäßigkeit des Suchlaufs war auch insoweit zu würdigen, als Daten hätten zu Tage treten können, die der Verschwiegenheit der Personalvertretung unterliegen. Die Verschwiegenheit der Personalvertretung dient aber vornehmlich dem Schutz der persönlichen Daten derer, die Objekte personalvertretungsrechtlichen Handelns sind. Die Wahrscheinlichkeit, dass Daten von Beschäftigten erfasst würden , die sich vertrauensvoll an die Personalvertretung gewandt hatten, war jedoch äußerst gering. Wegen der Suche von spezifischen Begriffen in Dateinamen wären herkömmliche Personalratsunterlagen kaum betroffen gewesen.

Der Landesbeauftragte hat gegenüber dem Ministerium und in der Öffentlichkeit deutlich gemacht, dass die besonderen komplexen Umstände dieses Einzelfalls und die dazu vorgenommenen Erwägungen keine Verallgemeinerung hinsichtlich einer grundsätzlichen datenschutzrechtlichen Zulässigkeit von Datensuchläufen zur Beschäftigtenüberwachung erlauben.

17.5. Daten bei der Personalvertretung

Der Presse war zu entnehmen, dass bei der Beschlagnahme eines privaten Laptops beim Vorsitzenden eines Hauptpersonalrates auch Informationen zur Personalratstätigkeit betroffen gewesen waren. Der Landesbeauftragte befragte daraufhin das zuständige Ministerium zur Datenverarbeitung bei der Personalvertretung zu Vorgaben der Datenspeicherung, zu deren Sicherung und zum Umgang mit mobilen Datenträgern.

Zunächst hatte die Befragung ergeben, dass sich auf dem beschlagnahmten privaten Laptop keine personenbezogenen Daten, sondern lediglich Notizen zu sachlichen Überlegungen im Zusammenhang mit der Personalratstätigkeit befunden haben.
Zudem verfügte die Hauptpersonalvertretung über einen von der Dienststelle zur Verfügung gestellten Laptop. Dieser sei nicht netzfähig, Daten würden darauf jedoch unverschlüsselt gespeichert. Der Landesbeauftragte hat in einem Gespräch mit dem Ministerium und den Personalvertretungen dazu dargelegt, dass die Verschlüsselung von Daten auf mobilen Datenträgern aus Gründen der technisch-organisatorischen Sicherheit der Daten geboten ist. Gerade bei mobilen Datenträgern ist die Gefahr des Verlustes bzw. Abhandenkommens und der dadurch bedingten Möglichkeit der Kenntnisnahme der Daten durch Unbefugte gegeben. Einzelheiten der Verschlüsselungsmöglichkeiten wurden erörtert.

Im Hinblick auf die Nutzung des privaten Laptops wurde festgestellt, dass die Nutzung im Ministerium durch eine von den Beschäftigten zu unterzeichnende Erklärung untersagt ist. Hierzu wurde angeregt, dies ggf. durch eine allgemeine Anordnung oder im Rahmen einer Dienstvereinbarung deutlich zu machen. Für den Ressortbereich wurde ebenfalls angeregt, hinsichtlich der Nutzung privater Laptop eine klare Regelung zu treffen.

Im Zuge der Erörterungen wurde von den Personalvertretungen der Wunsch geäußert, die Speicherungen der elektronischen Dokumente der Personalvertretungstätigkeit, die vielfach dem besonderen Vertrauensschutz unterliegen, in besonderer Weise zu sichern und unbefugtem Zugriff zu entziehen. Hierzu hat das Ministerium der örtlichen Personalvertretung die Möglichkeit eingerichtet, die Unterlagen verschlüsselt auf dem zentralen Server abzulegen, so dass ein Zugriff auf die Informationen durch Dritte, auch Systemadministratoren, ohne Zutun der Personalvertretungsmitglieder nicht möglich ist. Der Hauptpersonalvertretung wurde ebenfalls angeboten, Verschlüsselungsprodukte zur Verfügung zu stellen. Zudem wurde die Prüfung einer sicheren Anbindung an einen zentralen Server von außerhalb zugesagt.

17.6. Personaldaten im Internet

Das Organigramm einer Landkreisverwaltung, welches im Internet veröffentlicht wurde, war in Vorstandsbereiche, Fachbereiche und Sachgebiete strukturiert. Bis zur Ebene der Sachgebietsleiter wurden die Beschäftigten mit Name und Telefonnummer benannt. Es handelte sich allerdings um eine pdf-Datei, deren Inhalt von Suchmaschinen nicht erfasst wird.
Dazu wurde der Landkreisverwaltung die Problematik von Personaldaten im Internet unter Hinweis auf den VI. Tätigkeitsbericht (Ziff. 16.1) erläutert.
Nach neuester Rechtsprechung ist es im Interesse einer transparenten bürgernahen öffentlichen Verwaltung für den Dienstherrn grundsätzlich möglich, Namen, Funktion und dienstliche Erreichbarkeit jedenfalls solcher Beamter, die mit Außenkontakten betraut sind, auch ohne deren Einverständnis im Internet bekannt zu geben. Etwas anderes gilt lediglich dann, wenn einer solchen Bekanntgabe Sicherheitsbedenken entgegenstehen.
Behörden haben daher grundsätzlich hinsichtlich der modernen Präsentation der Behörde in der Öffentlichkeit einen erheblichen Ermessensspielraum. Auch die Ausübung von Ermessen muss jedoch verfassungsrechtliche Grenzen, wie etwa den Grundsatz der Verhältnismäßigkeit, respektieren. Einerseits kann bei hohen Funktionsträgern und typischen (telefonischen) Ansprechpartnern das legitime Interesse des Dienstherrn an der Präsentation gegenüber dem Schutz des Persönlichkeitsrechtes des betroffenen Beschäftigten gerade in Bezug auf sog. Funktionsträgerdaten überwiegen. Andererseits ist zu berücksichtigen, dass mit der Veröffentlichung im Internet Angaben zu Amt, Status, Einkünften und Beschäftigungsort der Betroffenen weltweit bekannt gemacht werden. Demgemäß ist bei der Bewertung der Erforderlichkeit und der Abwägung der beteiligten Interessen Zurückhaltung geboten. Der Schwerpunkt einer solchen Serviceleistung der Verwaltung liegt in der Sicherung eines kompetenten Ansprechpartners zum angegebenen Sachgebiet unter einer angegebenen Telefonnummer. Der Name des Beschäftigten ist, wie schon regelmäßige behördeninterne Personalumsetzungen dokumentieren, für den Erstkontakt von außen in der Regel nebensächlich.
Daher wurde empfohlen, die Erforderlichkeit der Nennung der Namen bis zur Ebene der Sachgebietsleiter im Internet zu überprüfen. Rein vorsorglich ist ergänzend auf die Einwilligung als Rechtsgrundlage der Internetveröffentlichung personenbezogener Informationen verwiesen worden, soweit zuvor eine hinreichende Aufklärung erfolgt ist und die Verweigerung der Einwilligung keine Nachteile bewirkt (vgl. § 4 DSG-LSA).

17.7. Einstellungstests

Ein Landkreis bediente sich bei Verfahren der Personalauswahl einer Gesellschaft für Personalwesen. Dort werden Einstellungstests für Auszubildende durchgeführt, die mit Ergebnisbögen im Umfang von zwei DIN-A4-Seiten enden. In diesen Ergebnissen werden verschiedene Anforderungsbereiche mit Punkten bewertet. Für das Auswahlverfahren werden somit einheitliche und über den Kreis hinausgehend objektive Maßstäbe angewandt. Die Ergebnisse dieses Personalauswahlverfahrens fließen in die Einstellungsentscheidung mit ein. Die Unterlagen werden zur Personalakte genommen und sollen auch der Evaluation des Auswahlverfahrens dienen, denn nach Abschluss

der Ausbildung soll überprüft werden, ob sich die im Auswahlverfahren ergebenen Annahmen bestätigt haben.

Ob im Hinblick auf den unmittelbaren Zusammenhang mit der Einstellungsentscheidung die Aufnahme eines Gesamtergebnisses (Einzeldatum) in die Personalakte vertretbar ist, konnte wegen des Umfangs der Ergebnisbögen dahinstehen. Die Aufnahme von Testunterlagen in Personalakten begründet grundsätzlich die Gefahr, dass die Ergebnisse bei künftigen Personalentscheidungen auf der Grundlage der Personalakte möglicherweise nachteilige Auswirkungen auf den Betroffenen haben. Dies gilt insbesondere, soweit umfängliche Test mit detaillierten Aussagen aus vielfältigen Unterlagen gesammelt werden. Im Unterschied zu langfristig erworbenen Befähigungsvoraussetzungen ergeben Einstellungstests lediglich eine Momentaufnahme, deren Aussagegehalt nach Abschluss der Ausbildung bzw. nach Aufnahme von Beurteilungen in die Personalakte erheblich an Wert verliert.

Zudem ist der Zweck des Auswahlverfahrens und der damit im Zusammenhang stehenden Datenerhebung bereits mit der Entscheidung über die Einstellung oder Ablehnung des Bewerbers erreicht. Einstellungstests gehören demgemäß grundsätzlich nicht in die Personalakte. Sie können allenfalls in Sachakten aufbewahrt werden. Dies ist zunächst jedenfalls insoweit erforderlich, wie das Verfahren noch nicht bestandskräftig abgeschlossen und mit evtl. Konkurrentenverfahren zu rechnen ist.
Gegenstand der dauerhaft aufzubewahrenden Personalakten sind lediglich die Bewerbungsunterlagen.
Schriftverkehr, Test- und Ablehnungsschreiben als allgemeine Unterlagen in den Sachakten unterliegen der Löschung, soweit sie nicht mehr erforderlich sind.
Die Aufbewahrung von Ergebnissen aus Personalauswahlverfahren der Gesellschaft für Personalwesen erschien daher allenfalls für einen angemessen kurzen Zeitraum bis zur Evaluation des Auswahlverfahrens gerechtfertigt. Von der Aufnahme in die Personalakten wurde daher abgeraten.

17.8. Polizeiliche Auskunftssysteme und Zentralregisterauskunft für Bewerbungsverfahren

Eine Eingabe betraf die Nutzung polizeilicher Auskunftssysteme für Zwecke der Personalwirtschaft. Ein Bewerber um eine Einstellung in den gehobenen Polizeivollzugsdienst hatte nicht angegeben, dass gegen ihn ein polizeiliches Ermittlungsverfahren als Beschuldigter anhängig war. Er hatte aber eine Einverständniserklärung zur Einholung der polizeilichen Auskunft bei der für ihn zuständigen Polizeidienststelle und deren Nutzung bei der Eignungsüberprüfung abgegeben. Nachdem der Bewerber den ersten Teil des Auswahlverfahrens bestanden hatte, wurde die Auskunft eingeholt. Danach ergab sich, dass gegen ihn zwei Jahre zuvor ein Ermittlungsverfahren wegen unerlaubten Entfernens vom Unfallort geführt wurde. Über die Verwertung dieser Information war der Petent verwundert, da er angab, von einer unbekannten Person angezeigt worden zu sein, keinen Unfall gehabt zu haben und nach der Protokollierung seiner Befragung durch die Polizei vor eineinhalb Jahren die Einstellungsverfügung erhalten zu haben.

Die Frage nach strafrechtlichen Ermittlungsverfahren ist zu Zwecken der Prüfung der Gesamtpersönlichkeit des Bewerbers im Rahmen der Eignung für die angestrebte Laufbahn grundsätzlich vertretbar. Allerdings ist auch bei derartigen Fragen der Grundsatz der Verhältnismäßigkeit zu wahren. Die Abfrage von Ermittlungsverfahren ohne zeitliche und inhaltliche Eingrenzung scheint in diesem Zusammenhang nicht verhältnismäßig, da sämtliche Verfahren (auch Bagatellfälle und bereits eingestellte Verfahren) damit erfasst sind. Das Informationsinteresse des Dienstherrn ist in solchen Fällen in der Regel nicht höher zu bewerten als der Schutz des Persönlichkeitsrechts.

Aufgrund der Hinweise zu dem vorgenannten Einzelvorgang wurde dem Landesbeauftragten Gelegenheit gegeben, zu den Vorschlägen für ein künftiges Eignungsauswahlverfahren Stellung zu nehmen. Dieses sah folgende Kriterien vor:

Für Bewerber, die nach Auswahlgesprächen und dem Führungszeugnis nach §§ 30 ff Bundeszentralregistergesetz (BZRG) in die engere Wahl kommen, sollte die oberste Landesbehörde gemäß § 41 Abs. 1 Nr. 2 BZRG eine unbeschränkte Auskunft aus dem Bundeszentralregister ohne Einwilligung des Betroffenen einholen. Die oberste Landesbehörde sollte dann die Auskunft auswerten und ggf. die Zustimmung dafür erteilen, dass der Bewerber für eine Ernennung in Frage kommt. Vorsorglich sollten die Bewerber ihr Einverständnis für eine Übermittlung des Inhalts der unbeschränkten Auskunft durch die oberste Landesbehörde an die Einstellungsbehörde erklären.

Gegen das beabsichtigte Auswahlverfahren bestanden datenschutzrechtliche Bedenken, obwohl hinsichtlich der Anzahl der Bewerber zunächst eine Vorauswahl getroffen wurde. Unerheblich war auch, dass durch die oberste Landesbehörde lediglich eine Zustimmung zum weiteren Verfahren auf der Grundlage der Auskunft erfolgt. Schon mit der Zustimmung, spätestens jedoch im Falle eines gerichtlichen Verfahrens nach einer Ablehnung würden die entsprechenden Auskünfte zum Bestandteil des Personalbewerbungsverfahrens.

Das Verfahren konnte auch nicht durch die Einwilligung als Rechtsgrundlage getragen werden. Die Erklärung des Einverständnisses des Bewerbers in die Übermittlung der Inhalte einer unbeschränkten Auskunft durch die oberste Landesbehörde an die Einstellungsbehörde bedürfte zur Rechtswirksamkeit der Freiwilligkeit der Entscheidung des Betroffenen. Diese dürfte hier im Hinblick auf die Situation des Bewerbungsverfahrens nicht gegeben sein.
Zudem erscheint die Einbeziehung der erweiterten Auskunft nach § 41 BZRG in das Bewerberauswahlverfahren als Umgehung der Vorschriften des BZRG, da die Verwendung der unbeschränkten Auskünfte nach § 41 Abs. 1 Nr. 2 BZRG durch oberste Bundes- oder Landesbehörden begrenzt ist (§ 43 BZRG). Die Zulässigkeit der Verwendung für die Personalauswahl ist dort abschließend aufgeführt (u. a. Bewachungspersonal).
Die Beratungen mit den zuständigen Behörden dauern noch an.

17.9. Personalservicecenter

Das Personalservicecenter (PSC) der Landesverwaltung wird auf der Grundlage des Gemeinsamen Runderlasses vom 15. März 2007 (MBl. LSA S. 333) tätig. Sein Aufgabenbereich umfasst neben der Information, Öffentlichkeitsarbeit und Beratung die Vermittlung und Qualifizierung (Erarbeitung von Besetzungsvorschlägen, Vermittlung von Personalaustauschgesuchen, individuelle Qualifizierungs- und Umschulungsmaßnahmen). Für die Vermittlung sind neben Meldungen interessierter Beschäftigter auch Meldungen der Ressorts unter Verwendung von Vordrucken vorgesehen. Personenbezogene Angaben umfassen neben dem Namen unter anderem die Dienststelle, die Besoldungs-/Entgeltgruppe, die Teilzeitbeschäftigung sowie Angaben zur Ausbildung sowie über Kenntnisse und Befähigungen, die grau unterlegt waren. Zudem ist eine Einwilligungserklärung zur ausschließlichen Verarbeitung von Daten im PSC vorgesehen, um freie Arbeitsplätze möglichst schnell zu besetzen. Ergänzt wird die Erklärung durch den Hinweis, dass bei einer Verweigerung der Zustimmung die Daten durch die meldende Stelle an das PSC gesandt werden, die „...nach datenschutzrechtlichen Bestimmungen einer Einwilligung nicht bedürfen“.

In einer Beratung des Landesbeauftragten mit dem PSC wurde festgestellt, dass die zuvor genannten, grau unterlegten Informationen stets auch ohne Unterzeichnung der Einwilligung und somit gegen den Willen der Betroffenen übermittelt werden. Ein gewisser Datenumfang sei für die Erfüllung der Aufgaben des PSC erforderlich.

Seitens des Landesbeauftragten wurde darauf hingewiesen, dass es nicht nur um die Erhebung der Daten für die Aufgabenerfüllung des PSC im Rahmen der Erforderlichkeit gehe. Vielmehr seien mangels **Einwilligung** die begrenzten Übermittlungsregelungen des § 90d BG LSA (ggf. i. V. m. § 28 DSG-LSA) zu berücksichtigen. Es geht weitgehend um ressortübergreifende Übermittlungen, die nach § 90d BG LSA nur zulässig wären, wenn das PSC zur Mitwirkung an einer Personalentscheidung berufen wäre. Hier bestanden aber im Hinblick auf die Anzahl der Betroffenen (keine Einzelfälle) Bedenken. Zudem würde die „Mitwirkung“ voraussetzen, dass die Zustimmung bzw. das Einvernehmen des PSC für die Personalmaßnahme erforderlich ist, was nach der Erlaßlage äußerst fraglich erschien. Beispiele ressortübergreifender Personalserviceagenturen in anderen Ländern beruhten daher auch auf einer gesonderten gesetzlichen Grundlage. Zudem wurde das PSC auf die Voraussetzungen einer Einwilligung nach § 4 Abs. 2 DSG-LSA hingewiesen. Abschließend wurde die Notwendigkeit der Prüfung einer Löschung bzw. Sperrung von nicht zulässig erhobenen Daten (§ 16 DSG-LSA) erörtert.

In einer späteren Beratung teilte das PSC mit, dass man sich nunmehr vorwiegend mit Qualifizierungsmaßnahmen auf freiwilliger Grundlage, mit Ausschreibungen und der Thematik der Negativbescheide befasse. Eine Optimierung des Erlasses zum PSC war dagegen leider noch im Entwurfsstadium.
Allerdings gingen seit geraumer Zeit keine personenbezogenen Daten ohne Einwilligung der Betroffenen allein auf der Grundlage des Runderlasses vom 15. März 2007 beim PSC ein. Aufgrund des ersten Gesprächs habe man im

PSC die vorhandenen Vorgänge daraufhin überprüft, ob Daten ohne Einwilligung auf der Grundlage des Runderlasses eingegangen sind. Diese Daten habe man aus dem Bestand genommen. Daher seien derzeit keine unfreiwillig übermittelten Daten gespeichert. In fast allen Fällen hätten ohnehin die Einwilligungen vorgelegen.

Seitens des Landesbeauftragten wurde auf den kurzfristigen Optimierungsbedarf im Hinblick auf die nach dem Runderlass vorgesehene Einwilligungserklärung der Betroffenen hingewiesen (Bezug auf die Vorschriften des DSG-LSA, Einhaltung der Anforderungen des § 4 Abs. 2 DSG-LSA, hinreichende Aufklärung der Betroffenen usw.). Auf die mögliche Unterstützung durch behördliche Datenschutzbeauftragte wurde hingewiesen. Das PSC erklärte die Absicht, kurzfristig eine Mustereinwilligungserklärung in Anlehnung an das Muster der Verwaltungsvorschriften zum DSG-LSA zu entwerfen und zur Diskussion zu stellen.

Intensiv wurde die Frage erörtert, ob und inwieweit für eine Übermittlung aus den personalaktenführenden Dienststellen an das PSC eine gesetzliche Grundlage erforderlich erscheint. Nach Auffassung des Landesbeauftragten könnte zukünftig eine gesetzliche Grundlage für eine umfängliche Tätigkeit des PSC sinnvoll sein, um im präzise bestimmten und unerlässlichen Umfang mit personenbezogenen Daten arbeiten zu können.

17.10. Eingliederungsmanagement und Personalvertretung

Bei längerer Erkrankung eines Beschäftigten ist der Arbeitgeber bzw. Dienstherr gehalten, ein Eingliederungsmanagement nach § 84 Abs. 2 Satz 2 SGB IX vorzusehen. Dazu werden zumeist der Betroffene und die Personalvertretung gleichzeitig zu einem Gespräch eingeladen, wobei auf die Freiwilligkeit des Verfahrens hingewiesen wird.

Nach § 84 Abs. 2 Satz 6 und Satz 7 SGB IX kann die Personalvertretung Klärung verlangen und wacht darüber, dass der Arbeitgeber die ihm nach der Vorschrift obliegenden Verpflichtungen erfüllt. Unter Beteiligung der Interessenvertretung hat der Arbeitgeber zu klären, wie die Arbeitsunfähigkeit überwunden und erneuter Arbeitsunfähigkeit vorgebeugt werden kann. Nach § 84 Abs. 2 S. 3 SGB IX ist der Arbeitgeber verpflichtet, den Betroffenen über das Ziel des betrieblichen Eingliederungsmanagements sowie auf Art und Umfang der hierfür verwendeten Daten hinzuweisen.

Gerichtliche Entscheidungen erster Instanz enthalten die Auffassung, dass der Arbeitgeber dem Personalrat ohne Zustimmung des jeweils Betroffenen aus § 84 Abs. 2 S. 7 SGB IX mitzuteilen verpflichtet ist, welche Beschäftigten der Dienststelle innerhalb eines Jahres länger als sechs Wochen ununterbrochen oder wiederholt arbeitsunfähig waren. Dies sei nötig, um ein Eingliederungsmanagement anzustoßen. Die Personalvertretung müsse so überprüfen können, ob in jedem Fall ein dem Satz 3 entsprechender Hinweis an den Betroffenen ergangen ist. Demgemäß sei eine frühzeitige Information grundsätzlich zulässig.

Ein derartiges Verfahren wird allerdings den Interessen der Betroffenen nicht unbedingt gerecht. Sollte sich der Betroffene vollständig verweigern und keine entsprechenden Datenflüsse wünschen, sollte dies respektiert werden. Die Mitarbeit der betroffenen Person im jeweiligen Verfahren ist freiwillig (§ 84 Abs. 2 Satz 1 SGB IX „mit Zustimmung und Beteiligung der betroffenen Person“). Diese Regelung des Satzes 1 ist dem Satz 7 zumindest systematisch vorrangig. Zudem besagt Satz 3 des § 84 Abs. 3 SGB IX ausdrücklich, dass die betroffene Person „zuvor“, also vor der Prüfung der Möglichkeiten mit der Interessenvertretung die Hinweise zum Eingliederungsmanagement erhalten soll.

Demgemäß stellen andere erstinstanzliche Urteile fest, dass ein Anspruch der Personalvertretung auf Unterrichtung vor Zustimmung des Betroffenen an dessen Persönlichkeitsrechten scheitert. Maßgeblich für die Information der Personalvertretung sei das Landespersonalvertretungsrecht. Ein bundesrechtlicher Anspruch einer Personalvertretung sei schon im Hinblick auf die Gesetzgebungskompetenz fraglich. Zudem ist zwischen der Vertraulichkeit von Personalakteninformationen und dem Informationsrecht der Personalvertretung abzuwägen, wobei unverhältnismäßige Eingriffe in die Rechte des einzelnen Beschäftigten unzulässig sind. So ist auch grundsätzlich die Personalakteneinsicht von der Zustimmung abhängig.

Obergerichtliche Entscheidungen stehen noch aus. Es wäre jedoch sinnvoll, unabhängig von der Frage der Zulässigkeit vorzeitiger Beteiligung im Einvernehmen mit der Personalvertretung erst dann eine namentliche Information vorzunehmen, wenn der Betroffene seine Zustimmung gegeben hat. Andernfalls kann auf die Zahl von Fällen verwiesen werden, in denen die Voraussetzungen des Eingliederungsmanagements gegeben waren und entsprechende Hinweise nach Satz 3 erfolgt sind. Würde der Arbeitgeber die Zahlen absichtlich unkorrekt übermitteln, würde er wohl auch die gerichtlich festgestellte Pflicht zur namentlichen Nennung umgehen. Im Rahmen des vertrauensvollen Zusammenwirkens dürfte daher auch eine Handhabung der Kontrolle durch den Personalrat möglich sein, die die Persönlichkeitsrechte der Betroffenen respektiert.
Es ist daher zu empfehlen, die namentliche Information an die Personalvertretung im Zusammenhang mit der Einladung zu einem Gespräch erst dann vorzunehmen, wenn die Zustimmung des Betroffenen vorliegt.

18. Polizei

18.1. Änderung des SOG LSA

Im vorherigen Tätigkeitsbericht (VIII. Tätigkeitsbericht, Ziff. 17.1) wies der Landesbeauftragte auf den aus datenschutzrechtlicher Sicht bestehenden Änderungsbedarf am Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) hin. Insbesondere die richterlichen Entscheidungen zum Kernbereichsschutz bei Telekommunikations- (Bundesverfassungsgericht vom 27. Juli 2005; BVerfGE 113, 348) und Wohnraumüberwachung (Verfassungsgerichtshof Rheinland-Pfalz vom 29. Januar 2007; VGH B 1/06, DVBl. 2007, 569) und zur Rasterfahndung (Bundesverfas-

sungsgericht vom 4. April 2006; BVerfGE 115, 320) müssen Eingang in das SOG LSA finden.

In ihrer Stellungnahme zum VIII. Tätigkeitsbericht (LT-Drs. 5/1097) führte die Landesregierung zu den Hinweisen des Landesbeauftragten aus: *„Nach Abschluss der Polizeistrukturreform ist vorgesehen, im Jahr 2009 einen Entwurf zur Änderung des SOG LSA vorzulegen. Dabei wird auch zu entscheiden sein, inwieweit den Anregungen des Landesbeauftragten gefolgt werden kann. Eine besondere Dringlichkeit besteht nicht. Das SOG LSA enthält keine Regelung zur präventiven Überwachung der Telekommunikation. Die akustische oder optische Wohnraumüberwachung kann in der Praxis so gestaltet werden, dass keine Eingriffe in den unantastbaren Kernbereich privater Lebensgestaltung erfolgen. Rasterfahndung ist die absolute Ausnahme; sie lässt sich auch ohne ausdrückliche Festlegung im Gesetzestext auf das Vorliegen konkreter Gefahren beschränken."*

Der Landesbeauftragte teilt die Auffassung der Landesregierung hinsichtlich einer kaum gegebenen Dringlichkeit einer Überarbeitung des SOG LSA nicht. In verschiedenen Bereichen entspricht die Rechtslage nicht den Anforderungen an die Verfassungsmäßigkeit von Gesetzesregelungen. Das allein ist Grund genug, eine Anpassung nicht auf die lange Bank zu schieben. Den Kernbereichsschutz in eine künftige Regelung anforderungsgemäß einzubinden, dürfte schon juristisch einen gewissen Anspruch stellen. Wie es dann ohne eine durchdachte Rechtsgrundlage in der Praxis bereits jetzt möglich sein soll, Eingriffe in den Kernbereich zu vermeiden, erschließt sich nicht offensichtlich. Zur Rasterfahndung ist der Landesregierung insoweit zu folgen, dass eine Rasterfahndung nicht zur alltäglichen Aufgabenwahrnehmung der Polizei gehört. Letztlich bleibt auch hier festzustellen, dass verfassungsgemäß und sachgerecht ausgestaltete Normen zwingend sind. Mit Blick auf die Entscheidungsdaten der angeführten gerichtlichen Verfahren besteht nicht nur Handlungsbedarf; es ist Eile geboten, auch und vor allem für die Anwender des SOG LSA.

18.2. Datenschutz bei der Polizei

In seinem letzten Tätigkeitsbericht wies der Landesbeauftragte darauf hin, dass u. a. die Zusammenarbeit mit den Polizeibehörden des Landes in Teilen dadurch erschwert wurde, dass für Stellungnahmen der Dienstweg über das Ministerium des Innern einzuhalten war (VIII. Tätigkeitsbericht, Ziff. 2.3). Die Einhaltung des Dienstweges kostet Zeit und wird der Verpflichtung der öffentlichen Stellen zur Unterstützung des Landesbeauftragten nach § 23 Abs. 1 DSG-LSA nicht gerecht.

Im Oktober 2007 wandte sich das Ministerium des Innern mit dem Entwurf eines Erlasses „Regelungen zum Datenschutz bei den Polizeibehörden und Polizeieinrichtungen; Änderung" an den Landesbeauftragten. Beabsichtigt war, die im November 2007 auslaufenden Regelungen zum Datenschutz bei der Polizei ohne inhaltliche Überarbeitung schlicht zu verlängern. Der Landesbeauftragte äußerte sich zur beabsichtigten Verlängerung, indem er unter Verweis auf seine Ausführungen im VIII. Tätigkeitsbericht inhaltliche Veränderungen anregte.

Nach umfassendem Schriftverkehr und vielfachen Telefonaten wurde letztendlich eine Erlassfassung erarbeitet, die zwar nicht allen Anforderungen des Gesetzes gerecht wird, als Zwischenergebnis aber zumindest vorläufig tragbar ist. Als Abschnitt II des Runderlasses (Runderlass des MI vom 27. August 2008 - 21.11-0555/1020101-P; MBl. LSA 2008 S. 676 f.) wird das „Verfahren bei Kontrollbesuchen und Auskunftsersuchen sowie bei Besprechungen mit dem Landesbeauftragten für den Datenschutz“ geregelt. Soweit es Kontrollen durch den Landesbeauftragten betrifft, sind die Stellungnahmen nach wie vor auf dem Dienstweg über das Ministerium des Innern vorzulegen. Bei Auskunftsersuchen - und insoweit kann von einer Verbesserung zugunsten des Datenschutzes gesprochen werden - sind künftig die schriftlichen Auskünfte der Dienststellen grundsätzlich nur noch nachrichtlich dem Ministerium des Innern zu übermitteln. In der Praxis bedeutet das, dass die Auskünfte dem Landesbeauftragten und dem Ministerium des Innern parallel übersendet werden. Damit tritt eine deutliche Zeitersparnis ein. Allerdings sind von dieser Regelung Auskunftsersuchen, die einer vorherigen Unterrichtung oder Beteiligung des Ministeriums des Innern bedürfen, insoweit ausgenommen. Einer vorherigen Beteiligung bedürfen nach Auffassung des Ministeriums des Innern Auskunftsersuchen, bei denen Stellung genommen wird z. B. zur Umsetzung von Erlassen und Weisungen, zum organisatorischen und technischen Datenschutz bei automatisierten Verfahren mit landesweiter Bedeutung oder bei erheblichen Auswirkungen auf den Haushalt der Polizei. Letztlich räumt aber auch das Ministerium des Innern in seiner Erlassregelung ein, *„... dass die Beachtung der Regelungen dieses Abschnitts nicht zu einer Behinderung des Landesbeauftragten für den Datenschutz oder seiner Mitarbeiterinnen und Mitarbeiter bei der Durchführung ihrer gesetzlichen Aufgaben ...“* führen darf.

Die Regelungen stoßen beim Landesbeauftragten vor allem deshalb auf Kritik, weil sie die eigenverantwortliche Verpflichtung der öffentlichen Stellen gegenüber dem Landesbeauftragten verkennen (vgl. §§ 2 Abs. 8, 23 Abs. 1 DSG-LSA). Den Landesbeauftragten bei seiner Aufgabenwahrnehmung nicht zu behindern, ist nicht mit der Verpflichtung aus § 23 Abs. 1 DSG-LSA zu seiner Unterstützung gleichzusetzen. Der Landesbeauftragte wird diesen Unterschied gegenüber dem Ministerium des Innern weiterhin unterstreichen und versteht die derzeitige Fassung des Erlasses als Zwischenergebnis, welches es auszubauen gilt.

18.3. Änderung des Bundeskriminalamtgesetzes

Mit Gesetz vom 25. Dezember 2008 (BGBl. I 2009 S. 3083) wurde dem Bundeskriminalamt die Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus übertragen. Nicht nur der Aufgabenumfang des Bundeskriminalamtes wurde mit diesem Gesetz erweitert, auch die Befugnisse, die für die Aufgabenwahrnehmung zur Verfügung stehen, haben ein neues Ausmaß angenommen. Um all die neuen Befugnisse in das Gesetz einzupassen, wurde eigens ein neuer Unterabschnitt gebildet, der mit den §§ 20a bis 20x des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) allerhand Möglichkeiten bereithält.

Zu der Befugnis aus § 20k BKAG fand eine besonders intensive Auseinandersetzung statt. § 20k BKAG ist mit „Verdeckter Eingriff in informationstechnische Systeme“ überschrieben und bezeichnet damit nichts anderes als die **Online-Durchsuchung.**

Die Online-Durchsuchung begegnet aus datenschutzrechtlicher Sicht erheblichen Bedenken. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder bereits in ihrer Entschließung anlässlich der 74. Konferenz im Oktober 2007 **(Anlage 4)** auf diese Bedenken hingewiesen. *„Die heimliche Online-Durchsuchung führt ... zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen. ... Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. ... Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.“*

Das Bundesverfassungsgericht hat in seiner Entscheidung vom 27. Februar 2008 (NJW 2008, 822) zu einer entsprechenden Befugnis zur Online-Durchsuchung im nordrhein-westfälischen Verfassungsschutzgesetz seine verfassungsrechtlichen Bedenken hinsichtlich solcher Maßnahmen deutlich gemacht und ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als Teil des allgemeinen Persönlichkeitsrechts formuliert (vgl. Ziff. 1). *„Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. Überragend wichtig sind Leib, Leben und Freiheit der Person oder solche Güter der Allgemeinheit, deren Bedrohung die Grundlagen oder den Bestand des Staates oder die Grundlagen der Existenz der Menschen berührt. ... Die heimliche Infiltration eines informationstechnischen Systems ist grundsätzlich unter den Vorbehalt richterlicher Anordnung zu stellen. Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.“*

Im April 2008 haben die Landesbeauftragten des Bundes und der Länder unter dem Eindruck dieser Entscheidung des Bundesverfassungsgerichtes eine Entschließung gefasst, die den Gesetzgeber auf die Beachtung der durch das Bundesverfassungsgericht entwickelten Grundsätze hinweist **(Anlage 8).** *„Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass das Bundesverfassungsgericht die Regelung zur Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalen für nich-*

tig erklärt hat. Hervorzuheben ist die Feststellung des Gerichts, dass das allgemeine Persönlichkeitsrecht auch das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme umfasst. ... 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. ... 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."

Über diese Feststellungen zur Online-Durchsuchung hinaus haben sich die Datenschutzbeauftragten des Bundes und der Länder im April 2008 auch zur Novellierung des BKAG geäußert **(Anlage 9).** Die Ausstattung des Bundeskriminalamtes mit Befugnissen zur Online-Durchsuchung war in diesem Zusammenhang nur ein Aspekt, wenn auch ein bedeutender. *„Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken. Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits. ... Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes. Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung" vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung", sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln."*

Trotz aller Bedenken und Hinweise wurde das Gesetz mit der Befugnis zur Online-Durchsuchung beschlossen. Zwar wurde die ursprüngliche Fassung der Befugnisnorm im Rahmen des Gesetzgebungsverfahrens angepasst, so dass die Anordnung einer Online-Durchsuchung nunmehr ausnahmslos dem

Richtervorbehalt unterstellt ist. Zweifel bleiben trotzdem, ob die Eingriffstiefe, die eine Online-Durchsuchung verursacht, vor dem Hintergrund des verfolgten Zwecks gerechtfertigt erscheint. Letztlich wird wohl auch im Fall der Befugnis zur Online-Durchsuchung durch das Bundeskriminalamt das Bundesverfassungsgericht entscheiden, ob die bestehende Regelung verfassungskonform ist.

18.4. Bundespolizeigesetz

Im Dezember 2007 wurde das Dritte Gesetz zur Änderung des Bundespolizeigesetzes (BGBl. I S. 3214) erlassen. Zum einen wurde § 27 des Bundespolizeigesetzes (BPolG) neu gefasst. Vor der Änderung waren durch selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte aufgezeichnete personenbezogene Daten unverzüglich zu vernichten, soweit sie nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt wurden. Jetzt ist die Frist bei unerlaubten Grenzübertritten auf zwei und bei Gefahren im Zusammenhang mit gefährdeten Objekten sogar auf 30 Tage ausgedehnt worden. Da es sich jeweils um Maximalfristen handelt, bleibt zu hoffen, dass die Polizei ihr Ermessen adäquat ausübt und diese Fristen nicht regelmäßig ausschöpft.

Zum anderen wurde in Umsetzung der Richtlinie 2004/82/EG des Rates vom 29. April 2004 (ABl. EU Nr. L 261 S. 24) über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln, ein § 31a in das BPolG neu eingeführt. Seit dem 1. April 2008 haben alle Luftfahrtunternehmen, die Fluggäste über die Schengen-Außengrenzen in das Bundesgebiet befördern, die in § 31a Abs. 3 BPolG genannten personenbezogenen Daten der Passagiere zu erheben und an die Bundespolizeibehörde zu übermitteln.

Obwohl die Erhebung all dieser Daten zu jedem Flugpassagier grundsätzlich kritisch betrachtet werden kann, wurde datenschutzrechtlichen Bedenken insoweit Rechnung getragen, dass kurze Löschfristen vorgesehen wurden. Nach § 31a Abs. 5 BPolG werden die erhobenen Daten 24 Stunden nach ihrer Übermittlung beim Luftfahrtunternehmen und grundsätzlich 24 Stunden nach der Einreise der Betroffenen bei der Bundespolizeibehörde gelöscht. Ausnahmen gibt es allerdings für die Löschung bei der Bundespolizeibehörde. Diese greifen dann, wenn die Daten für die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs bzw. für Maßnahmen der Strafverfolgung weiterhin benötigt werden.

18.5. Videoüberwachung öffentlicher Plätze

Über die Videoüberwachung öffentlicher Plätze hat der Landesbeauftragte zuletzt in seinem VIII. Tätigkeitsbericht (Ziff. 17.5) berichtet. Schwerpunkt bildete dabei die Entscheidung des Bundesverfassungsgerichtes zur Videoüberwachung eines Kunstwerkes im öffentlichen Raum vom 23. Februar 2007 (Bundesverfassungsgericht vom 23. Februar 2007, 1 BvR 2368/06, DVBl. 2007, 497). Im Berichtszeitraum dieses Tätigkeitsberichtes gab es vergleichbar grundlegende Entscheidungen in Sachen Videoüberwachung

öffentlicher Plätze nicht. Deshalb konzentriert sich dieser Beitrag auf die tatsächlichen Begebenheiten in Sachsen-Anhalt.

Bereits im dritten Quartal 2007 hatte sich der Landesbeauftragte eine Übersicht zu den damals aktuellen Standorten polizeilicher Videoüberwachungsanlagen vorlegen lassen. 2007 waren 14 polizeiliche Videoüberwachungsanlagen für öffentliche Plätze in Betrieb. Um die Entwicklung in diesem Bereich beurteilen zu können, forderte der Landesbeauftragte 2008 erneut eine entsprechend aktualisierte Übersicht an. Aus der übersandten Übersicht ergab sich, dass nunmehr 17 polizeiliche Anlagen arbeiteten. Allerdings ist nicht allein die Gesamtzahl der betriebenen Videoüberwachungsanlagen von Bedeutung. Vielmehr prüft der Landesbeauftragte anhand solcher Übersichten auch, wie lange die jeweilige Anlage in Betrieb ist. Denn die Dauer des Betriebs muss sich begründen lassen. Wie § 16 Abs. 2 SOG LSA zu entnehmen ist, sind Videoaufzeichnungen nur an bestimmten gefährlichen Orten oder gefährdeten Objekten zulässig.

Gefährliche Orte sind solche, an denen erfahrungsgemäß u. a. Straftaten begangen werden. Dass eine bestimmter Ort auch ein gefährlicher Ort i. S. d. § 16 Abs. 2 SOG LSA ist, muss z. B. durch entsprechende statistische Erhebungen belegbar sein.

Bei der Auswertung der Übersichten fiel z. B. auf, dass eine polizeiliche Videoüberwachungsanlage bereits seit 1999 ununterbrochen in Betrieb war. Bei solchen Zeiträumen muss hinterfragt werden, ob der Betrieb einer Videoüberwachungsanlage unter Berücksichtigung der vorstehend erläuterten rechtlichen Grundlagen gerechtfertigt ist und ob sie das geeignete Mittel zum Erreichen des Überwachungszwecks darstellt. Videoüberwachungsanlagen dienen ja nicht dem Selbstzweck. Sie werden errichtet, um die bestehende Gefährlichkeit eines Ortes einzudämmen. Wenn die Gefährlichkeit über Jahre allerdings unbenommen einer Videoüberwachungsanlage sehr hoch ist, stellt sich die Frage danach, ob der verfolgte Zweck der Verminderung von Straftaten mittels Videoüberwachungsanlage überhaupt erreicht werden kann oder ob nicht andere Maßnahmen, wie insbesondere eine häufigere Bestreifung durch die Polizei, in Betracht gezogen werden müssen.

Der Landesbeauftragte wird die Entwicklung weiter verfolgen und inhaltlich begleiten. Er wird insbesondere die „Dauerüberwachungsanlagen“ immer wieder hinterfragen.

18.6. Videoüberwachung am Hasselbachplatz in Magdeburg

Silvester 2007/2008 wurde am Hasselbachplatz in Magdeburg das neue Jahr nicht nur mit den üblichen Böllerschüssen begrüßt. Es kam zu regelrechten Krawallen. 15 bis 20 teils vermummte Randalierer griffen ein Polizeifahrzeug an und verletzten Polizisten. 19 Personen wurden unmittelbar nach den Krawallen festgenommen. Aus diesen Vorkommnissen und der Erkenntnis, dass sich der Hasselbachplatz über die letzten Jahre zu einem Kriminalitätsschwerpunkt in der Stadt Magdeburg entwickelt hat, zog die Polizei nunmehr Konsequenzen.

Entsprechenden Presseberichten Anfang Januar 2008 war zu entnehmen, dass die Polizei Videokameras am Hasselbachplatz installiert hat. Der Landesbeauftragte forderte daraufhin die zuständige Polizeidirektion Sachsen-Anhalt Nord (PD Nord) mit Schreiben vom 8. Januar 2008 zu einer Stellungnahme auf. Am 14. Januar 2008 nahm der Landesbeauftragte die errichtete Videoüberwachungsanlage in den Räumen der PD Nord in Augenschein. Er informierte sich insbesondere hinsichtlich der Beobachtungsbereiche und der Reichweite der Kameras. Die Feststellungen vor Ort lassen sich wie nachfolgend geschildert zusammenfassen.

Durch die Polizei wurden innerhalb der ersten zwei Kalenderwochen des Jahres 2008 zwei Kameras auf bzw. an Gebäuden am Hasselbachplatz installiert. Die Bilder werden auf Videokassetten aufgezeichnet. Beim Test der technischen Möglichkeiten der Kameras musste festgestellt werden, dass es durch Zoomen möglich war, in Wohnungen der Häuser am Hasselbachplatz Einblick zu nehmen. Den Bediensteten sei mittels Dienstanweisung allerdings untersagt, die Wohnungen zu beobachten. Bereits bei dieser Inaugenscheinnahme der Videoüberwachungsanlage wurde durch den Landesbeauftragten auf die rechtlichen Grenzen solcher Maßnahmen hingewiesen. So stellt die Einsichtnahme in Wohnungen einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung dar. Bereits die Möglichkeit des Einblicks in Wohnungen ist eine Grundrechtsverletzung, unabhängig davon, ob diese Möglichkeit letztlich genutzt wird. Auch wurde auf eine Entscheidung des Verwaltungsgerichtes Hamburg (VG Hamburg vom 24. Mai 2007, Az.: 4 K 2800/06) aufmerksam gemacht, die einen vergleichbaren Fall auf der dortigen Reeperbahn thematisiert. In dem im Nachgang zu diesem Termin ergangenen Schreiben des Landesbeauftragten wurde zudem auf die unzureichende Beschilderung des Hasselbachplatzes hingewiesen. Der Zugang zum Platz hätte mit ausreichend großen und verständlichen Hinweisschildern, die auf die Videoüberwachung aufmerksam machen, versehen sein müssen.

Dem Termin Anfang Januar 2008 folgte ein umfassender Schriftverkehr zu allen datenschutzrechtlichen Belangen einer solchen Videoüberwachung und am 22. Februar 2008 einer erneuter Vor-Ort-Termin. Im Ergebnis all dieser Bemühungen konnte ein rechtmäßiger Zustand hergestellt werden. Die beiden Kameras wurden durch Endschalter in ihren Schwenkbereichen so eingeschränkt, dass ein Einsehen in die Wohnungen der Häuser am Hasselbachplatz nicht möglich ist. Auch die Löschfristen wurden datenschutzrechtlichen Erfordernissen angepasst. Die Löschung der Videoaufzeichnungen erfolgt nach 48 Stunden. Für Zwecke der Strafverfolgung können in diesem Zeitraum als Beweisstücke Ausschnitte kopiert oder Bilder gefertigt werden.

Auch in Zukunft wird der Landesbeauftragte die Entwicklungen in Sachen Videoüberwachung rund um den Hasselbachplatz im Auge behalten. Die polizeiliche Anordnung für die Videoüberwachung erfolgte in der Vergangenheit halbjährlich. Der Landesbeauftragte hat und wird sich in Zukunft unterrichten lassen, welche Erkenntnisse bzw. Vorfälle zur Rechtfertigung der Videoüberwachung herangezogen werden.

18.7. Kopien von Videoaufzeichnungen für künstlerische Zwecke

Im April 2008 erreichte den Landesbeauftragten eine eher ungewöhnliche Anfrage. Im Rahmen des Internationalen Theaterfestivals „Theater der Welt“ in Halle (Saale) sollte u. a. die Überwachung des öffentlichen Raumes hinterfragt werden. Für die Umsetzung des künstlerischen Konzeptes eines Installationskünstlers sollte der Landesbeauftragte mitteilen, ob Bürgerinnen und Bürger das Recht haben, eine Kopie von Videoaufzeichnungen des Marktplatzes in Halle (Saale) zu erhalten.

Der Landesbeauftragte führte zur Anfrage aus, dass Rechtsgrundlage für Videoüberwachungsmaßnahmen der Polizei § 16 SOG LSA bildet. Die Polizei darf die so erhobenen personenbezogenen Daten der Bürgerinnen und Bürger grundsätzlich nur für die Zwecke nutzen, für die sie auch erhoben wurden (§ 26 SOG LSA). Eine Übermittlung dieser personenbezogenen Daten an eine nichtöffentliche Stelle - wie sie das Internationale Theaterinstitut Berlin als Initiator des Theaterfestivals darstellt - käme nur unter den Voraussetzungen des § 28 SOG LSA in Betracht.

Die Übermittlung personenbezogener Daten an eine nichtöffentliche Stelle durch die Polizei des Landes Sachsen-Anhalt für künstlerische Zwecke ist jedoch in diesen Vorschriften nicht vorgesehen.

Soweit die Anfrage darauf gerichtet war, ob ein auf der Videoaufzeichnung abgebildeter Betroffener Anspruch auf die Aushändigung einer Kopie der Aufzeichnung hat, ist auch dies zu verneinen. Zwar steht jedem Betroffenen ein Auskunftsrecht über die zu seiner Person gespeicherten Daten nach § 15 des Gesetzes zum Schutz personenbezogener Daten der Bürger (DSG-LSA) zu. Dieser Anspruch richtet sich aber nicht auf das Überlassen von Kopien der entsprechenden Unterlagen. Selbst wenn eine Überlassung von Unterlagen in Betracht käme, würde sich der Anspruch im Fall einer Videoaufzeichnung nur auf die Sequenzen beziehen können, in denen der Betroffene tatsächlich alleine zu sehen ist. Die Überlassung einer Komplettkopie käme nicht in Betracht, weil damit zwangsläufig die personenbezogenen Daten diverser anderer Personen mit übermittelt würden.

Personenbezogen könnten die Daten auf Videoaufzeichnungen ggf. genutzt werden, wenn die Betroffenen der Nutzung der Daten für künstlerische Zwecke zugestimmt hätten. Es dürfte allerdings bereits aus rein praktischen Erwägungen nicht umsetzbar sein, dass alle auf einem Videoband abgebildeten Personen ermittelt und um ihre Einwilligung gebeten werden.

Für die Überlassung einer durch Bildbearbeitung erstellten anonymisierten Kopie wäre das DSG-LSA nicht mehr anwendbar, weil es sich in einem solchen Fall nicht mehr um personenbezogene Daten handeln würde. Die Anonymisierung der Daten entsprechend § 2 Abs. 7 DSG-LSA wäre allerdings durch die Behörde bzw. von ihr Beauftragte vorzunehmen und so auszuführen, dass sie nicht mehr rückgängig zu machen ist. Ob und ggf. mit welchem Aufwand eine solche Kopie erstellt und überlassen werden kann, hätte die zuständige (Polizei-)behörde zu beurteilen.

18.8. Beschwerdestelle Polizei

Wie der Landesbeauftragte im April 2008 aus Presseberichten erfuhr, sollte der Innenminister angekündigt haben, eine zentrale Beschwerdestelle Polizei beim Landespräventionsrat zu schaffen. Um die Meldung zu überprüfen, wandte sich der Landesbeauftragte an das Ministerium des Innern.

Als Anlage zu seiner Stellungnahme übermittelte das Ministerium des Innern die „Konzeption einer Zentralen Beschwerdestelle Polizei“. Aus dieser ließ sich zunächst erschließen, dass die Einrichtung der Zentralen Beschwerdestelle dazu dienen soll, „... eventuell verloren gegangenes Vertrauen in die objektive Beschwerdebearbeitung innerhalb der Polizei wieder zurück gewinnen zu können, ...“. Nach der Konzeption soll Bürgerinnen und Bürgern des Landes, aber auch Polizeibeamtinnen und Polizeibeamten eine alternative, zentrale Ansprechstelle für den Fall geboten werden, dass ihnen eine Beschwerde auf anderem Weg nicht verfolgbar erscheint.

Der Landesbeauftragte beschäftigte sich im Rahmen seiner Prüfung der Konzeption nicht mit den verfolgten Absichten, sondern vielmehr mit deren praktischer Umsetzung. Nach dem Willen des Ministeriums des Innern sollte die Zentrale Beschwerdestelle beim Landespräventionsrat eingerichtet werden, weil dieser „... aufgrund seiner personellen Zusammensetzung ein hohes Maß an Objektivität und Professionalität erwarten ...“ lasse. Um die einschlägigen Rechtsvorschriften für die Übermittlung personenbezogener Daten an den Landespräventionsrat festzustellen, war es zunächst erforderlich, seine Rechtsform und seine Stellung innerhalb oder zur Landesverwaltung zu klären. In Abstimmung mit dem für Landesorganisation zuständigen Referat des Ministeriums des Innern war im Ergebnis festzustellen, dass es sich bei dem Landespräventionsrat um einen nicht rechtsfähigen Verein handelt, der nicht Teil der Verwaltung des Landes Sachsen-Anhalt ist. Damit ist er datenschutzrechtlich als nichtöffentliche Stelle i. S. d. DSG-LSA anzusehen.

In seiner Stellungnahme gegenüber dem Ministerium des Innern führt der Landesbeauftragte u. a. aus: „Sollte die Zentrale Beschwerdestelle Polizei wie geplant eingerichtet werden, würde sich die Übermittlung personenbezogener Daten vom Ministerium des Innern an die Zentrale Beschwerdestelle Polizei an den Vorgaben des § 12 DSG-LSA messen lassen müssen. Auch wenn nach dem Wortlaut der Konzeption anscheinend davon ausgegangen wird, dass keine personenbezogenen Daten - zumindest nicht ohne das Einverständnis des Beschwerdeführers - übermittelt werden, erscheint es wenig praxisnah, dass Beschwerden über polizeiliches Handeln grundsätzlich ohne personenbezogene bzw. -beziehbare Daten bearbeitet werden können. Letztlich sind aber nicht nur die personenbezogenen Daten der Beschwerdeführer zu schützen. Auch die personenbezogenen Daten der Polizeibediensteten, über die sich ggf. beschwert wurde, sind schutzwürdig. Insofern würde meine Kontrolle beim Ministerium des Innern ansetzen.“

Dem Landesbeauftragten wurde auf seine Stellungnahme hin mitgeteilt, dass die Prüfung hinsichtlich der Einrichtung der Zentralen Beschwerdestelle noch nicht abgeschlossen ist. Zunächst solle auf Anregung des Landespräventionsrates eine Veranstaltung an der Fachhochschule der Polizei in Aschers-

leben unter dem Titel „Beschwerdemanagement in der Polizei“ stattfinden. Im Januar 2009 wurde die in Aussicht gestellte Veranstaltung unter Beteiligung u. a. des Landesbeauftragten durchgeführt. Durch die Diskussionsteilnehmer wurden verschiedene Formen der Organisation eines Beschwerdemanagements vorgestellt. Zum einen wurde zum „Berliner Modell“ erläutert, dass hier die zentrale Beschwerdestelle im Stab des Polizeipräsidenten im Stabsbereich Personal angesiedelt ist. Darüber hinaus gibt es in Berlin Beschwerdesachbearbeiter in den einzelnen Organisationseinheiten, die aber dem Stabsbereich Personal angegliedert sind. Zum anderen wurde über die auf gesetzlicher Grundlage eingerichtete „Hamburger Polizeikommission“ berichtet. Diese Kommission, die aus ehrenamtlichen vom Senat berufenen Mitgliedern bestand, die in Ausübung ihrer Amtsbefugnisse an Aufträge und Weisungen nicht gebunden waren, existiert allerdings nicht mehr. Auch die seitens des Ministeriums des Innern favorisierte Anbindung der Beschwerdestelle beim Landespräventionsrat wurde ebenso wie der Vorschlag zur Einrichtung einer unabhängigen Arbeitsstelle im Ministerium des Innern thematisiert. Der Landesbeauftragte mahnte für den Fall einer externen Anbindung mit Blick auf § 28 SOG LSA und das Personalaktengeheimnis eine **gesetzliche Regelung** an.

Wegen rechtlicher - insbesondere datenschutzrechtlicher - Bedenken wurde inzwischen die ursprünglich vom Ministerium des Innern bevorzugte Angliederung einer zentralen Beschwerdestelle beim Landespräventionsrat verworfen. Im Ergebnis soll zwar eine zentrale Beschwerdestelle eingerichtet werden, allerdings soll dies beim Ministerium des Innern geschehen. Ausweislich einer Stellungnahme vom Mai 2009 soll die zentrale Beschwerdestelle organisatorisch als Stabsstelle beim Staatssekretär des Ministeriums des Innern eingerichtet werden. Räumlich soll die Unterbringung der vorgesehenen drei Mitarbeiter jedoch nicht im Dienstgebäude des Ministeriums des Innern erfolgen. Nach der Besetzung der Stelle des Leiters der zentralen Beschwerdestelle soll in Abstimmung mit den Behörden und Einrichtungen der Polizei ein Feinkonzept erarbeitet werden.

Der Landesbeauftragte wird die Fortentwicklung der Angelegenheit weiter begleiten und sich nach der Einrichtung der zentralen Beschwerdestelle auch vor Ort ein Bild machen.

18.9. Datenübermittlung an nichtöffentliche Stellen

Zu Beginn des Jahres 2008 hat der Landesbeauftragte bei den drei Polizeidirektionen des Landes Sachsen-Anhalt um die Übersendung der nach § 28 Abs. 3 des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) zu führenden Übermittlungsverzeichnisse für Datenübermittlungen im Rahmen polizeilicher Aufgaben an private Dritte nachgesucht. Nur eine der Polizeidirektionen konnte ein entsprechendes Verzeichnis vorlegen. Dabei ist die Verpflichtung nach dem SOG LSA eindeutig und auch nicht neu. Die Polizeibehörden und das für diese zuständige Ministerium des Innern haben ohne weiteres Zutun des Landesbeauftragten erkannt, dass dieser gesetzwidrige Zustand umgehend beseitigt werden muss.

Die beiden Polizeidirektionen, die in der Vergangenheit keine Verzeichnisse geführt haben, teilten bereits in ihren Stellungnahmen mit, dass die erforderlichen Verzeichnisse ab sofort geführt werden. Zum Teil wurden entsprechende Verfügungen an die Dienststellen im Zuständigkeitsbereich der Polizeidirektion gleich mit übersandt. Auch das Ministerium des Innern stellte eine kurzfristige Prüfung auf die Notwendigkeit fachaufsichtlicher Maßnahmen in Aussicht.

Im Ergebnis dieser Prüfung verfasste das Ministerium des Innern kurzfristig einen Erlass an die ihm nachgeordneten Polizeibehörden. Die Behörden wurden auf die bestehende Verpflichtung zum Führen eines besonderen Verzeichnisses hingewiesen. Darüber hinaus wurde den Behörden ein Muster für ein Verzeichnisblatt zur Verfügung gestellt, welches landeseinheitlich zu verwenden ist.

18.10. Schutz vor haftentlassenen Sexualstraftätern

In seinem VIII. Tätigkeitsbericht (Ziff. 17.7) hat der Landesbeauftragte über Bestrebungen zur Errichtung einer öffentlich zugänglichen Sexualstraftäterdatei und deren Verfassungswidrigkeit berichtet. Das in Sachsen-Anhalt zuständige Ministerium des Innern hat auf Anfrage des Landesbeauftragten im November 2007 mitgeteilt, dass zur Klärung von Fragen nach notwendigen Maßnahmen zum Schutz der Bevölkerung eine Arbeitsgruppe unter Beteiligung des Ministeriums des Innern, des Ministeriums der Justiz und des Ministeriums für Gesundheit und Soziales eingerichtet wurde. Die Arbeitsgruppe sei einvernehmlich zu dem Ergebnis gelangt, dass eine gesonderte „Sexualstraftäterdatei“ nicht erforderlich sei. Vielmehr sollen die Polizeibehörden angehalten werden, die bestehenden Dateien im Rahmen ihrer Zweckbindung intensiver zu nutzen.

Um die Zusammenarbeit insbesondere zwischen der Justiz und der Polizei zu optimieren, wurde ein gemeinsamer Erlass „Maßnahmen zur Verbesserung des Schutzes der Bevölkerung vor Straftaten von haftentlassenen rückfallgefährdeten Sexualstraftätern“ erarbeitet.

Die letztendlich veröffentlichte Fassung des Erlasses (MBl. LSA 2008 S. 196) ist mit dem Landesbeauftragten abgestimmt. Der Erlass stellt die bereits bestehenden Übermittlungsbefugnisse aus dem Strafgesetzbuch und der Strafprozessordnung zusammen und schafft damit für den Anwender mehr Übersichtlichkeit. Über die gesetzlich vorgesehenen Übermittlungsbefugnisse hinaus werden keine zusätzlichen geschaffen.

18.11. Archivierungssysteme der Polizei

Im Rahmen der Bearbeitung einer Eingabe stellte der Landesbeauftragte fest, dass eine Polizeidirektion des Landes Sachsen-Anhalt zur Begründung erkennungsdienstlicher Maßnahmen auf personenbezogene Daten aus einer Archivierungsdatenbank zurückgegriffen hat. In den sonstigen polizeilichen Datenbanken waren zur Person des Betroffenen keine Daten mehr gespeichert. Für den Betroffenen konnte die Situation geklärt werden. Allerdings blieb die Frage nach dem grundsätzlichen Umgang der Polizei mit personen-

bezogenen Daten in Archivierungsdatenbanken zunächst offen. Das Ministerium des Innern sicherte zu dieser Fragestellung von grundsätzlicher Bedeutung im Mai 2008 eine gesonderte Stellungnahme zu.

Aus der zwischenzeitlich vorliegenden Stellungnahme vom Mai 2009 geht hervor, dass die Polizei Archivierungssysteme im Sinne einer klassischen Vorgangsverwaltung nicht mehr unterhält. Vielmehr würden **„Mischdateien“** geführt, die neben der reinen Vorgangsverwaltung auch der Erfüllung polizeilicher Aufgaben und der Strafverfolgung dienen. Für diese „Mischdaten“ sollen nach Auffassung des Ministeriums des Innern die Regelungen über das Löschen von Daten zur Erfüllung polizeilicher Aufgaben und zur Strafverfolgung Anwendung finden.

Zum Redaktionsschluss dieses Tätigkeitsberichtes war die Prüfung der Unterlagen noch nicht abschlossen. Der Landesbeauftragte wird die Angelegenheit weiter verfolgen.

18.12. Automatisierte Kfz-Kennzeichenerfassung durch die Polizei

Bereits 2002 erlangte der Landesbeauftragte davon Kenntnis, dass in einzelnen Bundesländern Tests mit automatischen Kennzeichenerkennungssystemen durchgeführt werden. In den folgenden Jahren hat sich der Arbeitskreis Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder immer wieder mit der Thematik befasst.

In einer Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aus dem Jahr 2004 wurden die datenschutzrechtlichen Bedenken deutlich. *„Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können. ... Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. ... Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.“*

Rechtsgrundlagen für den dauerhaften Einsatz automatischer Kennzeichenerfassungsgeräte wurden u. a. in den Bundesländern Hessen und Schleswig-Holstein geschaffen. Die Zulässigkeit dieser Regelungen wollten mehrere Kraftfahrzeughalter aus beiden Bundesländern überprüft wissen und erhoben Verfassungsbeschwerde. Mit Urteil vom 11. März 2008 hat das Bundesverfassungsgericht die angegriffenen Vorschriften in beiden Bundesländern für nichtig erklärt, da sie das allgemeine Persönlichkeitsrecht der Beschwerdeführer in seiner Ausprägung als Grundrecht auf informationelle Selbstbestimmung verletzen (BVerfG, NJW 2008, 1505).

Das Gericht stellte fest, dass die Regelungen nicht dem Gebot der Normenbestimmtheit und Normenklarheit genügen. Sie benennen weder den Anlass

noch den Ermittlungszweck, dem die Erhebung und der Abgleich dienen sollen. Die Normen werden wegen ihrer unbestimmten Weite auch dem verfassungsrechtlichen Gebot der Verhältnismäßigkeit nicht gerecht. Sie ermöglichen schwer wiegende Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen, ohne die grundrechtlich geforderten gesetzlichen Eingriffsschwellen hinreichend zu normieren. *„Mit dem Grundsatz der Verhältnismäßigkeit ist es insbesondere nicht vereinbar, dass die angegriffenen Vorschriften aufgrund ihrer unbestimmten Weite anlasslos erfolgende oder ... flächendeckend durchgeführte Maßnahmen der automatisierten Erfassung und Auswertung von Kraftfahrzeugkennzeichen ermöglichen."*
„Eine automatisierte Kennzeichenerfassung, die unterschiedslos jeden nur deshalb trifft, weil er mit einem Fahrzeug eine ohne besonderen Anlass oder gar dauerhaft eingerichtete Stelle zur automatisierten Erfassung von Kraftfahrzeugkennzeichen passiert, vermittelt den Eindruck ständiger Kontrolle. Das sich einstellende Gefühl des Überwachtwerdens kann ... zu Einschüchterungseffekten und in der Folge zu Beeinträchtigungen bei der Ausübung von Grundrechten führen." Der Entscheidung des Bundesverfassungsgerichtes lagen gemäß dessen Pressemitteilung im Wesentlichen nachfolgende Erwägungen zu Grunde:

I. „Die automatisierte Kennzeichenerfassung greift in den Schutzbereich des Grundrechts auf informationelle Selbstbestimmung ein, wenn das Kennzeichen nicht unverzüglich mit dem Fahndungsbestand abgeglichen und ohne weitere Auswertung sofort wieder gelöscht wird. ..."
II. „Eingriffe in das Grundrecht auf informationelle Selbstbestimmung müssen auf einer verfassungsmäßigen gesetzlichen Grundlage beruhen. Die angegriffenen Vorschriften erfüllen diese Voraussetzung nicht. ..."
III. „Den Landesgesetzgebern stehen verschiedene Möglichkeiten zur Verfügung, um eine im Rahmen ihrer Zuständigkeit verbleibende und sowohl hinreichend bestimmte als auch angemessene Eingriffsermächtigung zu schaffen. Für eine die Verhältnismäßigkeit wahrende Regelung der Voraussetzungen der automatisierten Kennzeichenerfassung scheidet ein weit gefasster Verwendungszweck beispielsweise dann nicht aus, wenn er mit engen Begrenzungen der Eingriffsvoraussetzungen kombiniert ist, wie es die derzeitige brandenburgische Regelung vorsieht. Möglich sind ferner Kombinationen von enger gefassten Zweckbestimmungen, die die Kennzeichenerfassung auf nicht eingriffsintensive Verwendungszwecke begrenzen, mit entsprechend geringeren Voraussetzungen für die Aufnahme in den Fahndungsbestand und die Voraussetzungen für den Erhebungsanlass. ..."

Ein Jahr nach dem Urteil hat der Allgemeine Deutsche Automobil-Club e. V. ein Gutachten in Auftrag gegeben, welches die aktuelle Rechtslage und die Überwachungspraxis in allen Bundesländern darauf hin überprüft, ob die Vorgaben des Bundesverfassungsgerichtes umgesetzt wurden. Das Gutachten vom März 2009 stellt fest, dass in fünf Bundesländern weiterhin nach nicht verfassungskonformen Regelungen gescannt wird, dass vier Bundesländer in der Praxis nicht mehr scannen, aber ihre nicht verfassungskonformen Regelungen nicht geändert oder aufgehoben haben, und dass sieben Bundesländer entweder verfassungskonforme Regelungen haben oder gänzlich auf Kennzeichenscanning verzichten. Erfreulich aus datenschutzrechtli-

cher Sicht ist, dass Sachsen-Anhalt zu den Bundesländern zählt, die auf Kennzeichenscanning verzichten.

18.13. Protokollierung von Datenabfragen beim Technischen Polizeiamt

Im Rahmen der Prüfung einer Eingabe wurde dem Landesbeauftragten bekannt, dass zumindest punktuelle Probleme bei der Protokollierung von Datenabfragen der Polizei durch das Technische Polizeiamt (TPA) bestanden haben.

Gegenstand der Eingabe war die Prüfung der Zulässigkeit einer Datenabfrage durch Bedienstete der Polizei. Zu klären war, ob an einem bestimmten Tag zu einem bestimmten Kfz-Kennzeichen eine Datenabfrage durch Bedienstete der Polizei veranlasst wurde. Zu diesem Zweck richtete der Landesbeauftragte - wie üblich - eine Anfrage an das Landeskriminalamt (LKA), welches die eigentliche Datenselektion beim TPA durchführen lässt. Parallel zu dieser Abfrage wandte sich der Landesbeauftragte an das Kraftfahrtbundesamt (KBA). Die Abfragen der Polizeien z. B. nach Kfz-Kennzeichen werden automatisiert an das KBA gerichtet, weil dort das zentrale Fahrzeugregister geführt wird. Alle Anfragen an das KBA werden bei der jeweiligen Polizei - für Sachsen-Anhalt beim TPA - und beim KBA protokolliert.

Die Ergebnisse der beiden Anfragen verblüfften den Landesbeauftragten. Vom LKA erhielt er die Auskunft, dass an dem bestimmten Tag zu dem bestimmten Kfz-Kennzeichen keine Abfrage erfolgt sei. Das KBA bestätigte jedoch eine Abfrage. Es lieferte Datum, Uhrzeit, den codierten Anlass der Anfrage und die Kennung des anfragenden Bediensteten.

Zur Aufklärung der fehlerhaften Protokollierung beim TPA richtete der Landesbeauftragte eine weitere Anfrage an das LKA. Dieses teilte im Ergebnis mit, dass eine nochmalige Prüfung und die Wiederholung der Recherche durch das TPA erfolgt, eine Abfrage in den Protokolldaten aber dennoch nicht nachweisbar sei. Es müsse von einem programmtechnischen Einzelfehler ausgegangen werden, dessen Ursache trotz intensiver Bemühungen nicht lokalisiert werden könne. Zur Vermeidung einer Fehlerwiederholung soll die Protokollierung von der zuständigen Stelle überprüft werden. Gegebenenfalls könnte sich in der Folge der Überprüfung die Notwendigkeit von Programmveränderungen ergeben. Nach erfolgter Überprüfung wurde mitgeteilt, dass nicht von einer systematischen Fehlfunktion der Protokollierungssoftware auszugehen sei. Mit hoher Wahrscheinlichkeit habe es sich um eine einmalige technische Fehlfunktion im komplexen Gesamtzugriffs- und Protokollierungssystem des Landes gehandelt. Die Notwendigkeit einer vollständigen Protokollierung soll in den entsprechenden Dienstberatungen thematisiert werden.

Gegenüber dem Ministerium des Innern des Landes Sachsen-Anhalt, als dem TPA und LKA vorgesetzte Behörde, hat der Landesbeauftragte abschließend nochmals auf die grundlegende Bedeutung einer fehlerfreien Protokollierung hingewiesen. Sie bildet nicht nur die Voraussetzung für eine effektive Datenschutzkontrolle, sie ist auch und gerade für die Sicherheit des Systems elementar.

18.14. Ermittlungsgruppe Schulweg

Über die Ermittlungsgruppe Schulweg hat der Landesbeauftragte in seinem VIII. Tätigkeitsbericht (Ziff. 18.10) bereits ausführlich berichtet. Er hat auch deutlich gemacht, dass gegen die Maßnahmen der Ermittlungsgruppe keine Bedenken bestanden haben. Darüber hinaus hat der Landesbeauftragte angekündigt, die rechtzeitige Löschung der Daten und die Vernichtung des Materials im Rahmen seiner Zuständigkeiten zu kontrollieren. Diese angekündigte Kontrolle wurde im April 2008 bei der Polizeidirektion Sachsen-Anhalt Süd (PD Süd), bei der die Ermittlungsgruppe eingerichtet ist, durchgeführt.

Im Ergebnis der Kontrolle wurde die PD Süd mit Schreiben des Landesbeauftragten von Anfang Mai 2008 aufgefordert, zu Fragen Stellung zu nehmen bzw. Abhilfe zu schaffen.

Einwilligungserklärungen

Als Formular für die Einwilligungserklärung wurden die Formblätter entsprechend der Anlagen zum gemeinsamen Runderlass des Ministeriums des Innern und des Ministeriums der Justiz vom 31. März 2006 verwendet. Diese Formblätter stellen aber in ihrem Wortlaut nicht auf den Reihengentest nach § 81h der Strafprozessordnung (StPO) ab. Vielmehr beziehen sich die Formblätter auf die §§ 81c und 81e StPO. Durch die Verwendung dieser Formblätter werden die Betroffenen nicht in die Lage versetzt, die Tragweite und Bedeutung ihrer Einwilligungserklärung zu verstehen. Die Betroffenen erlangen keine Kenntnis von der Rechtsgrundlage der Maßnahme. Dieser Umstand ist zum einen datenschutzrechtlich nicht zu vertreten. Die Betroffenen sind - zumal es sich hier um eine freiwillige Maßnahme handelt - angemessen über ihre Rechte, Pflichten und Möglichkeiten aufzuklären. Nach Auffassung des Landesbeauftragten führt die mangelnde Aufklärung zum anderen aber auch dazu, dass sich die Betroffenen an den Landesbeauftragten wenden, weil sich ihnen das Vorgehen der Polizei nicht erschließt. Mit einem auf die konkrete Rechtslage angepassten Formblatt ließen sich Missverständnisse vermeiden, was sich auf die Ermittlungsarbeit förderlich auswirken würde.

Verfahrensverzeichnis

Einzelne Angaben im Verfahrensverzeichnis stimmten mit den tatsächlichen Verhältnissen nicht überein. Im Einzelnen handelte es sich um den Kreis der Betroffenen und die Angaben hinsichtlich der Löschung der Daten. Als Kreis der Betroffenen wurden „Zeugen, Hinweisgeber und Geschädigte“ angegeben. Bei den Personen, die freiwillig eine Speichelprobe abgegeben haben, handelt es sich aber nicht um Zeugen. Sie sind auch keine Tatverdächtigen. Sie sind als Dritte anzusehen, die keiner der Gruppen zuzuordnen sind. Insoweit war das Verfahrensverzeichnis zumindest unvollständig und anzupassen. Hinsichtlich der Löschfristen war zum einen festgelegt, dass die Daten nach Beendigung des Ermittlungsverfahrens zu löschen sind. Zum anderen erfolgte jedoch auch eine Festlegung, dass hinsichtlich der Erforderlichkeit der weiteren Speicherung eine regelmäßige Prüfung der Daten im Rahmen der ständigen Aktualisierung vorgenommen wird. Im Gespräch vor Ort konnte nicht hinreichend nachvollziehbar erläutert werden, für welche Fallgestaltungen diese Regelung Anwendung finden soll. Der Landesbeauftragte bat

deshalb, das Verfahrensverzeichnis entsprechend anzupassen, was durch die PD Süd zugesichert wurde.

In der seitens der PD Süd abgegebenen Stellungnahme wurde die Überarbeitung der Einwilligungserklärung angezeigt. Vor einer Nutzung sind solche landeseinheitlichen Vordrucke jedoch von der Vordruckkommission des Landes Sachsen-Anhalt zu genehmigen. Durch die PD Süd wurde die überarbeitete Fassung der Kommission vorgelegt. Darüber hinaus hat die PD Süd das Verfahrensverzeichnis in den benannten Punkten überarbeitet und dem Landesbeauftragten vorgelegt. An dem überarbeiteten Verfahrensverzeichnis wurden durch den Landesbeauftragten keine Mängel festgestellt.

18.15. Zuverlässigkeitsüberprüfungen bei der Deutschen Bundesbank

Im Mai 2007 erhielt der Landesbeauftragte davon Kenntnis, dass die Deutsche Bundesbank seit 2004 in erheblichem Umfang Sicherheitsüberprüfungen für Fremdpersonal (z. B. Reinigungskräfte) durchführen soll, die nicht dem Anwendungsbereich des Sicherheitsüberprüfungs- und Geheimschutzgesetzes (SÜG) unterfallen. Aufgrund einer Einwilligungserklärung der Betroffenen würden die Landeskriminalämter um die Übermittlung von Erkenntnissen gebeten. Für die Datenübermittlung durch die Landeskriminalämter seien mit diesen Vereinbarungen geschlossen worden.

Der Landesbeauftragte wandte sich daraufhin an das Landeskriminalamt. Dieses teilte mit, dass die Deutsche Bundesbank im Oktober 2004 um den Abschluss einer Vereinbarung über die Durchführung von Zuverlässigkeitsüberprüfungen von bankfremden Personen nachsuchte. Nach Prüfung der Rechtslage hat das Landeskriminalamt festgestellt, dass aus rechtlichen Gründen der Abschluss einer solchen Vereinbarung nicht möglich ist.

Als Rechtsgrundlage einer Übermittlung an die Deutsche Bundesbank könnte nach Auffassung des Landesbeauftragten allenfalls das Gesetz über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) herangezogen werden, weil das SÜG die dargestellten Fälle nicht erfasst. Im SOG LSA findet sich aber keine Ermächtigung für eine Datenübermittlung an eine öffentliche Stelle sozusagen „zur Vorbeugung“. Eine Datenübermittlung käme nur dann in Betracht, wenn von einer konkreten Gefahr auszugehen ist. Diese konnte von der Deutschen Bundesbank allerdings nicht belegt werden. Das Landeskriminalamt ist dem Ansinnen der Deutschen Bundesbank nach Abschluss einer Vereinbarung zu Recht nicht nachgekommen. Aus datenschutzrechtlicher Sicht ist eine Beteiligung des Landeskriminalamtes Sachsen-Anhalt an derartigen Überprüfungen nicht zulässig.

Die Deutsche Bundesbank, die dieses Verfahren angeregt und mit verschiedenen Bundesländern entsprechende Vereinbarungen abgeschlossen hat, untersteht der datenschutzrechtlichen Kontrolle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. Nach Prüfung des Vorgehens der Deutschen Bundesbank kam der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu dem Ergebnis, dass die Zuverlässigkeitsüberprüfungen durch die Deutsche Bundesbank rechtlich unzulässig sind und bat, von der bisherigen Praxis abzusehen und die insoweit rechtswidrig erhobe-

nen personenbezogenen Daten zu löschen und zu vernichten. Das lehnte die Deutsche Bundesbank mit Verweis auf ihre mit dem Bundesministerium des Innern übereinstimmende Auffassung ab. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat letztendlich im November 2008 das Verfahren bei der Deutschen Bundesbank förmlich beanstandet.

18.16. Speicherung im polizeilichen Informationssystem INPOL

Am 16. Dezember 2008 hat das Niedersächsische Oberverwaltungsgericht in einem Urteil (Az: 11 LC 229/08, DVBl. 2009, 466) ausgeführt, dass die personenbezogenen Daten eines Klägers aus der Datei „Gewalttäter Sport“ zu löschen sind, weil es bislang mangels einer Rechtsverordnung nach § 7 Abs. 6 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKAG) an einer wirksamen Rechtsgrundlage für die Erhebung und Speicherung der Daten fehlt. Das Urteil hat aber nicht nur Auswirkungen auf die Speicherung personenbezogener Daten in der Datei „Gewalttäter Sport“, sondern auch auf alle sonstigen in INPOL geführten Verbunddateien.

Mit dieser Entscheidung des Gerichts wird die seitens der Datenschutzbeauftragten des Bundes und der Länder vertretene Auffassung zur Speicherung personenbezogener Daten im polizeilichen Informationssystem INPOL bestätigt. Die Datenschutzbeauftragten betrachten im Gegensatz zum Bundesministerium des Innern den Erlass einer Rechtsverordnung nach § 7 Abs. 6 BKAG als Zulässigkeitsvoraussetzung für die Datenverarbeitung in den Verbunddateien. Auf die Erforderlichkeit einer solchen Rechtsverordnung wird bereits seit 1997 hingewiesen (17. und 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit). Am 1. August 1997 trat das BKAG in Kraft, welches seither in § 7 Abs. 6 den Erlass einer entsprechenden Rechtsverordnung vorsieht. Bis heute hat das Bundesministerium des Innern die erforderliche Rechtsverordnung nicht erlassen.

Vor diesem Hintergrund haben die Datenschutzbeauftragten anlässlich der 77. Tagung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung erneut auf ihren Standpunkt hingewiesen und Konsequenzen aus dem Urteil des Niedersächsischen Oberverwaltungsgerichts angemahnt **(Anlage 30).**

19. Rechtspflege

19.1. Allgemeines

Sowohl aus Kontrollen als auch aus einzelnen Beschwerden ergeben sich Auffälligkeiten, welche wegen ihrer allgemeinen Bedeutung vorab dargestellt werden sollen.

- Das erste Problem betrifft die gesetzlich geforderte Erstellung von **Verfahrensverzeichnissen** (§ 14a DSG-LSA). Teils wurden Verfahrensverzeichnisse gar nicht erstellt und damit interessierten Bürgerinnen und Bürgern die rechtlich vorgesehene Informationsmöglichkeit über die Verarbeitung eventuell auch ihrer persönlichen Daten vorenthalten. Teils

konnte der mit den Verzeichnissen verbundene wesentliche weitere Zweck nicht erreicht werden, nämlich deren essentielle Funktion zur Selbstkontrolle der verantwortlichen Stellen, zur Selbstvergewisserung bei Einführung personenbezogener EDV-Maßnahmen in den Dienststellen. Insbesondere die Notwendigkeit, in den Festlegungen zum Verfahrensverzeichnis die Rechtsgrundlage zu benennen, dürfte in manchen Fällen zu einer Änderung der Praxis geführt haben. Soweit Verfahrensverzeichnisse erstellt wurden, litten die Festlegungen zum Verfahrensverzeichnis häufig an Mängeln. Zwar war zumeist ein Zweck der Verarbeitung bzw. Nutzung personenbezogener Daten genannt. Die Benennung einer Rechtsgrundlage fehlte indessen häufig oder es wurde nur eine Verwaltungsvorschrift aufgeführt. Diese ist jedoch keine Rechtsnorm und kann damit nicht als rechtliches Fundament für einen Eingriff in die Grundrechte der Betroffenen herangezogen werden. Schließlich dienen die Verfahrensverzeichnisse auch als Grundlage für Kontrollen durch den behördlichen Datenschutzbeauftragten wie auch den Landesbeauftragten.

- Der andere grundsätzliche und leider immer wieder anzutreffende Problemfall betrifft die Vergabe von **Datenverarbeitung im Auftrag**. Nach § 8 Abs. 6 DSG-LSA hat die zuständige öffentliche Stelle als Auftraggeberin den Landesbeauftragten für den Datenschutz über die Vergabe einer Datenverarbeitung im Auftrag zu unterrichten, wenn auf den Auftragnehmer die Vorschriften des DSG-LSA nicht anwendbar sind (z. B. Privatfirmen, Unternehmen). Nur aufgrund dieser Mitteilung wird der Landesbeauftragte regelmäßig in die Lage versetzt, auch ohne dass ein konkreter Einzelfall dazu Anlass gibt, Kontrollen bei diesen Auftragnehmern durchzuführen. Es war auch im Bereich der Justizdienststellen festzustellen, dass dieser gesetzlichen Pflicht nicht nachgekommen wird.

Der Landesbeauftragte hält es für geboten, dass das Justizministerium auf seinen Geschäftsbereich entsprechend einwirkt - auch damit die Aufgabenerfüllung des Landesbeauftragten nicht unnötig erschwert oder in Teilbereichen gar unmöglich gemacht wird.

19.2. Telekommunikationsüberwachung überarbeitet - Vorratsdatenspeicherung eingeführt

Überwiegend zum 1. Januar 2008 ist das Gesetz zur Neuregelung der Telekommunikationsüberwachung (TKÜ) und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG in Kraft getreten (Gesetz vom 9. November 2007, BGBl. I S. 3198). Damit wurde unter anderem die o. g. Richtlinie des Europäischen Parlaments und des Rates vom 15. März 2006 in nationales Recht umgesetzt.
Trotz fundierter und zahlreicher kritischer Äußerungen unter anderem von der Ministerin der Justiz, die sich kritisch zur Vorratsdatenspeicherung von Nutzerdaten geäußert hat, wie auch von den Datenschutzbeauftragten des Bundes und der Länder zu den Entwürfen (siehe Entschließung vom 8. Juni 2007, **Anlage 1**) wurden mit dem Gesetz umfangreiche Änderungen vor allem der Strafprozessordnung (StPO) und des Telekommunikationsgesetzes (TKG, siehe hierzu Ziff. 24.1) vorgenommen. Die Forderung der Daten-

schutzbeauftragten, nur verhältnismäßige Eingriffstatbestände zu schaffen, wurde vom Bundesgesetzgeber überwiegend nicht berücksichtigt.
Besonders bedauerlich ist, dass die Chance vertan wurde, den verfassungsrechtlichen Schutz des Kernbereichs privater Lebensgestaltung für alle verdeckten Ermittlungsmaßnahmen einheitlich einzuführen. Dies hätte sich insbesondere angeboten, nachdem das Bundesverfassungsgericht in seinem Beschluss vom 11. Mai 2007 - 2 BvR 543/06 (NJW 2007, 2753) - festgestellt hatte, dass die Neuregelung einer anderen verdeckten Überwachungsmaßnahme, nämlich der akustischen Wohnraumüberwachung, hinsichtlich des Kernbereichsschutzes grundrechtlichen Ansprüchen genügt.
Immerhin sind Ermittlungsmaßnahmen allein gegen Strafverteidiger, Geistliche und Abgeordnete grundsätzlich unzulässig (§ 160a Abs. 1 StPO). Ausnahmen sind nur vorgesehen, wenn geschützte Geheimnisträger selbst einer einschlägigen Straftat verdächtig sind. Warum die Gesetzesänderung andere Berufsgeheimnisträger wie Rechtsanwälte (soweit sie nicht als Strafverteidiger handeln), Ärzte und auch Journalisten nicht in den besonderen Schutz einbezieht, ist nicht verständlich. Kaum war diese missliche Regelung in Kraft, wurden Pläne des Bundesinnenministeriums bekannt, für das Bundeskriminalamt auch die Befugnis zur präventiven Überwachung der Telefongespräche von Strafverteidigern, Geistlichen und Abgeordneten zu schaffen. Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer Berliner Erklärung im April 2008 **(Anlage 6)** unterstrichen, dass u. a. die Regelungen zum großen Lauschangriff, zur Telekommunikationsüberwachung und zur Vorratsspeicherung von Telekommunikationsdaten die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet haben. Es erleichtert sicherlich nicht die Akzeptanz gesetzgeberischer Entscheidungen, wenn diese regelmäßig durch das Bundesverfassungsgericht korrigiert werden müssen, da sie offenkundig Grundrechte der Bürgerinnen und Bürger zu weit beschränken. Bedauerlich ist zudem, dass vor Verschärfung der bestehenden freiheitsbegrenzenden Regelungen anscheinend keine unabhängige Evaluation des bereits bestehenden Rechtsinstrumentariums umgesetzt wurde. Auch die Forderung des Bundesverfassungsgerichts (BVerfG NJW 2007, 351 - IMSI-Catcher, vgl. VIII. Tätigkeitsbericht Ziff. 18.3), vor neuerlicher Ausdehnung von Ermittlungsmethoden deren unabweisbare Notwendigkeit im Hinblick auf die Grundrechtspositionen unbeteiligter Dritter zu prüfen, scheint in den gesetzgeberischen Vorüberlegungen nicht ausreichend bedacht worden zu sein.

Die in der Neuregelung vorgenommenen datenschutzfreundlichen Änderungen der StPO sind dagegen von ihrer Anzahl her eher übersichtlich.
So teilt der Landesbeauftragte die Einschätzung der Landesregierung in ihrer Stellungnahme zum VIII. Tätigkeitsbericht nur begrenzt, dass hinsichtlich der neu formulierten Benachrichtigungspflicht Betroffener grundsätzlich Rechtsklarheit erreicht sein dürfte. Künftig sind nach einer Abhörmaßnahme in Wohnungen z. B. nur die „erheblich mitbetroffenen Personen“ zu benachrichtigen (§ 101 Abs. 4 Satz 4 StPO). Die weitere Konkretisierung der Begrifflichkeit bleibt der Rechtsanwendung überlassen. Dass Betroffenen nur eine Frist von 14 Tagen zugestanden wurde, um nach der Information über die Abhörmaßnahme eine Rechtmäßigkeitsprüfung veranlassen zu können (§ 101 Abs. 7 Satz 2 StPO), erscheint schon verwunderlich. Ob es ihnen in dieser

Zeitspanne möglich ist, eine entsprechende Entscheidung, zumal nach anwaltlicher Beratung, treffen zu können, ist eher zweifelhaft. Wie sich die Neuregelung in der Praxis auswirkt, wird noch zu prüfen sein.

Weiterhin ist nach § 100a Abs. 1 StPO die TKÜ nur zulässig, wenn die verfolgte Tat u. a. auch im Einzelfall schwerwiegend ist und der Verdacht einer „Katalogstraftat“ besteht. Dieser Katalog von Straftaten ist in § 100a Abs. 2 StPO niedergelegt. Es wurde zwar das Erfordernis einer „schwerwiegenden Straftat“ festgeschrieben, der Straftatenkatalog jedoch zugleich deutlich ausgeweitet.

Letztlich dürfte die Neuregelung ein, gerade im Hinblick auf unbeteiligte Dritte (also des größten Teils der Bevölkerung), nicht wünschenswertes deutliches Anwachsen der Anzahl verdeckter Ermittlungsmaßnahmen und der damit bewirkten Grundrechtseingriffe auslösen. Eine nachvollziehbare Evaluation mit nachfolgender öffentlicher Diskussion ist daher unabdingbar erforderlich. Dies hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im November 2008 nachdrücklich eingefordert, nachdem insbesondere das vom Max-Planck-Institut für ausländisches und internationales Strafrecht im Auftrag des Bundesministeriums der Justiz erstellte Gutachten (Zur Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung) ausgewertet worden war (vgl. Entschließung der 76. Konferenz, **Anlage 22**).
Auch der Landtag hat die Problematik aufgegriffen und die Landesregierung gebeten, ihm in den Ausschüssen für Recht und Verfassung sowie Inneres über die Nutzung der Telekommunikationsverkehrsdaten im Rahmen von § 100g StPO zu berichten.

Der Landesbeauftragte würde es begrüßen, wenn die Landesregierung im Rahmen ihrer Mitwirkungsmöglichkeiten eine qualitätsvolle und vor allem unabhängige Überprüfung der Regelungen befördern könnte.

19.3. Verfolgung der Absicht der Vorbereitung von Terrordelikten

Als ob im Zusammenhang mit der Neuregelung im Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen (vgl. zu Ziff. 19.2) nicht schon genug Maßnahmen zur weiteren Beschränkung der Grundrechte vorgesehen worden wären, legte die Bundesregierung im Januar 2009 mit einem Gesetzentwurf nach, welcher neue Straftatbestände in das Strafgesetzbuch einführen soll, die so unbestimmt formuliert erscheinen, dass Zweifel am eigentlichen Zweck allen Strafrechts, nämlich durch die Drohung mit Strafe Taten zu verhindern und im Falle eines Falles Täter verurteilen zu können, aufkeimen (BT-Drs. 16/12428).
In der Süddeutschen Zeitung wurde treffend formuliert, dass mit dem Terror-Camp-Gesetzentwurf „*die noch nicht konkrete Vorbereitung von noch nicht konkreten Straftaten*“ unter Strafe gestellt werde. Der Schluss, den der Autor dieses Artikels zog, dass eigentlicher Hintergrund der Regelung nur sei, die z. B. in der Strafprozessordnung (StPO) vorgesehenen Eingriffsmöglichkeiten nutzen zu können, ist nicht von der Hand zu weisen. Sollte der Entwurf nämlich Gesetzeskraft erlangen, würde damit zugleich unter anderem den Ermittlungsbehörden die Möglichkeit eingeräumt, die gesamte Klaviatur der

strafverfahrensrechtlichen und damit grundrechtseingreifenden Maßnahmen zu nutzen, welche die StPO bietet. Damit würde z. B. auch auf die vorratsgespeicherten Daten der Telekommunikation zugegriffen werden können, denn der neue Straftatbestand soll als sog. schwere Straftat in den Katalog der Straftaten des § 100a StPO aufgenommen werden.

Angesichts der im Mai 2009 erfolgten Verabschiedung des Gesetzes durch den Bundestag könnte nur noch eine ablehnende Entscheidung im Bundesrat verhindern, dass letztlich erneut eine Entscheidung des Bundesverfassungsgerichts zum Korrektiv werden muss; doch dieser stimmte zu.

19.4. Videotechnik in der Justiz

Nachdem am 10. September 2008 an den Landesbeauftragten ein Hinweis gegeben worden war, dass das Verhalten von Bediensteten am Zeiterfassungsgerät im Justizzentrum Magdeburg per Videoüberwachung aufgezeichnet und arbeitsrechtlich ausgewertet werde, wurde am selben Tag ein kurzfristiger Kontrollbesuch durchgeführt. Im Haupteingangsbereich wurde eine kaum als Überwachungskamera erkennbare sog. Dome-Kamera vorgefunden. Solche Geräte wirken, je nach Anbringungsstelle, eher wie Wand- oder Deckenlampen. Dieses Gerät war zwar in einiger Höhe, aber direkt über einem Zeiterfassungsgerät angebracht worden. Die Nutzung dieser Zeiterfassung erfolgte im Aufnahmebereich der Kamera. Weitere Kameras befinden sich an zwei Außenseiten des Gebäudekomplexes, in der Tiefgarage, im Innenhof, in den Zufahrten und im Bereich organisierte Kriminalität der Staatsanwaltschaft. Hinweisschilder auf die Videoüberwachung fanden sich weder im Eingangsbereich noch auf den öffentlichen Wegflächen rund um das Justizzentrum. Lediglich auf einer Zufahrtsschranke an der Zufahrt zum Innenhof des Justizzentrums befand sich ein textlicher Hinweis. Diesen hätte ein unbefangener Besucher jedoch nur mit der Zufahrtskontrolle, aber nicht mit anderen Überwachungen in Verbindung bringen können. Neben der optischen schien auch eine akustische Beobachtung möglich zu sein.
Die optischen Aufnahmen sind von sehr guter Qualität, der Ton der Kamera im Außenbereich wurde durch Straßengeräusche beherrscht. Eine Mithörmöglichkeit der im Innenbereich installierten Kameras soll wegen der Montagehöhe nicht möglich gewesen sein. Die akustische Funktionalität der Kameras wurde kurz nach der Kontrolle des Landesbeauftragten dauerhaft zerstört.
Die optischen Aufzeichnungen waren für einen längeren Zeitraum gespeichert worden, akustische sollen nicht möglich gewesen sein. Ein Zugriff auf die vorhandenen Speicherungen war u. a. jedem Wachtmeister in der Eingangswache möglich. Die gespeicherten Daten konnten auf mobile Datenträger übertragen werden, eine Begrenzung der Berechtigung hierfür bestand im Kontrollzeitpunkt nicht.
Da die Überwachung nicht als Erfassung personenbezogener Daten gesehen wurde, fand naturgemäß weder eine datenschutzrechtlich vorgeschriebene Vorabkontrolle (§ 14 Abs. 2 DSG-LSA) statt, noch war eine Festlegung für dieses Verfahren zum Verfahrensverzeichnis gem. § 14 Abs. 3 DSG-LSA erstellt worden. Nach einem etwas zögerlichen und verharmlosenden Einstieg in die Problematik hat sich das Justizministerium auf eine aktive Rolle besonnen und beabsichtigt nunmehr den Datenschutz in der Justiz, auch un-

ter Zuhilfenahme externer Beratung, auf sichere und einheitliche Füße zu stellen. Einige Sofortmaßnahmen, wie die Begrenzung der Speicherdauer, die Löschung unzulässig erhobener Daten und die Zerstörung der Tonerfassungsfunktionalität der Kameras wurden umgehend veranlasst (vgl. § 30 DSG-LSA). Dies soll auch bei anderen Justizeinrichtungen geschehen sein. Das Justizzentrum in Magdeburg ist nämlich noch nicht einmal die Justizeinrichtung mit den meisten Überwachungskameras.
Neben dem bereits angesprochenen externen Gutachter (der allerdings bis zum Redaktionsschluss dieses Tätigkeitsberichts noch keinen Auftrag erhalten hat - die Bereitschaft des Landesbeauftragten zur Kooperation mit dem Gutachter konnte so leider noch nicht wirksam werden), benannte das Justizministerium zunächst noch weitere sieben Punkte, auf welche es sein besonderes Augenmerk richten will:

- Die Dienstvereinbarung der Nutzer des Justizzentrums soll hinsichtlich der Zuständigkeit für den Datenschutz konkretisiert werden.
- Den behördlichen Datenschutzbeauftragten sollen technisch versierte Helfer zur Seite gestellt werden.
- Die Einhaltung datenschutzrechtlicher Standards soll Bestandteil der turnusmäßigen Geschäftsprüfungen werden.
- Jährlich soll eine Datenschutzkonferenz der behördlichen Datenschutzbeauftragten beim Oberlandesgericht stattfinden.
- Es wird eine Begründungspflicht für die Anschaffung neuer Videotechnik eingeführt.
- Zur Verlängerung der Speicherdauer (bei Vorfällen) soll das Vier-Augen-Prinzip gelten.
- Die Aus- und Fortbildungsmaßnahmen zu Datenschutzfragen im Justizbereich sollen ausgeweitet werden. (Der Landesbeauftragte wirkt hierbei mit.)

Nachdem dem Landesbeauftragten schließlich alle während verschiedener Informationsbesuche erbetenen Unterlagen vorgelegt worden waren, konnte der Sachverhalt „Videoüberwachung im Justizzentrum Magdeburg“ abschließend bewertet werden.

Der Landesbeauftragte sah letztlich von einer förmlichen Beanstandung ab.
Zwar ist ihm, insbesondere durch die geführten zahlreichen Gespräche, deutlich geworden, dass es an der notwendigen Sensibilität schon hinsichtlich des Umstands, ob personenbezogene Daten berührt sein könnten, gefehlt hat. Bereits bei der Installation der Kameras scheint es den handelnden Personen nicht zu Bewusstsein gekommen zu sein, dass ihre Maßnahmen immer auf Menschen und deren soziale Interaktion gerichtet waren und damit regelmäßig deren Rechtskreis berühren mussten. Auch war festzustellen, dass etliche Gesprächspartner übersehen haben, dass nicht nur eine tatsächlich umgesetzte optische oder akustische Erfassung, sondern auch schon die technisch eingerichtete, sozusagen drohende Möglichkeit hierzu einen Grundrechtseingriff darstellt.
Allerdings geht der Landesbeauftragte davon aus, dass das gesamte Geschehen nach der ersten Kontrolle im September 2008 die nötige Warnfunktion für die Bediensteten bei der künftigen Bearbeitung von solchen Verwaltungsvorhaben erfüllen wird. Eine weitergehende Wirkung wäre auch durch

eine förmliche Beanstandung nicht zu erreichen gewesen. Die datenschutzrechtlichen Verstöße wurden einvernehmlich als gravierend bewertet.

Auch die schnelle und - nachdem einige justizinterne Missverständnisse geklärt waren - in der Folgezeit konsequente und umfassende Aufarbeitung der Missstände hat die getroffene Entscheidung ermöglicht. Dass nicht nur das Justizzentrum in Magdeburg, sondern auch die übrigen Justizdienststellen im Lande in den Blick genommen wurden, ist ebenso positiv hervorzuheben, wie die Tatsache, dass das Amtsgericht Magdeburg als bewirtschaftende Dienststelle des Justizzentrums u. a. die Anregung des Landesbeauftragten aufgegriffen hatte, das Zeiterfassungsterminal im Eingangsbereich des Justizzentrums aus dem Erfassungsbereich der Eingangskamera zu verlegen.

Der Landesbeauftragte hat seiner Entscheidung insbesondere folgende weitere Aspekte zugrunde gelegt:

- Die dargelegten Gründe rechtfertigen grundsätzlich die im Justizzentrum eingerichteten optischen Überwachungsmaßnahmen. Der Erkennbarkeit der Überwachung wurde durch Anbringen entsprechender Piktogrammschilder genüge getan.
- Eine Aufzeichnung von Gesprächen erfolgte nicht. Eine akustische Überwachung mit Hilfe der Kameras im Windfangbereich des Justizzentrums und an anderen Stellen soll aufgrund deren Montagehöhe nicht möglich gewesen sein. Die Audiofunktion der Kameras wurde dauerhaft deaktiviert (die zunächst getroffene Formulierung einer Deaktivierung der „Tonaufzeichnungen“ wurde begrifflich klargestellt).
- Der bisher vergleichsweise einfache Zugriff auf die Videoaufzeichnungen wurde umgehend ebenso begrenzt wie der Erfassungsbereich der Kameras.
- Die nunmehr vorgenommenen differenzierten Festlegungen zur Speicherdauer der per Kamera aufgezeichneten personenbezogenen Daten sind weitgehend angemessen.
- Die unzulässige Nutzung der Überwachungsaufzeichnungen als Drohinstrument gegenüber einer Bediensteten wurde vom Amtsgericht bzw. auf Veranlassung des Justizministeriums angemessen beurteilt und einer weiteren personalrechtlichen Bewertung zugeführt.
- Die technisch-organisatorischen Vorkehrungen zur Sicherung insbesondere des Überwachungsnetzwerks scheinen nach derzeitigem Kenntnisstand ausreichend zu sein.
- Hinsichtlich der Überwachungspraxis an anderen Gerichtsstandorten wurden eine Überprüfung und die notwendigen Schritte zur Herstellung eines rechtmäßigen Zustands durch das Justizministerium umgehend veranlasst. Inwieweit die vorgeschriebenen Feststellungen zu den Verfahrensverzeichnissen erstellt wurden, wird ggf. Gegenstand späterer Kontrollen durch den Landesbeauftragten sein.
- Die Erforderlichkeit der Überwachungsmaßnahmen soll einer regelmäßigen Überprüfung unterzogen werden. Dass die Erfüllung dieser schon von Verfassungs wegen zu gewährleistenden Maßnahme zum Gegenstand der justizinternen Geschäftsprüfungen werden soll, sichert die Regelmäßigkeit.

Der Landesbeauftragte unterstreicht die Feststellung der Justizministerin, dass Datenschutz nicht nur eine Angelegenheit des behördlichen Datenschutzbeauftragten, sondern aller Bediensteten ist. Für die Verantwortung der Behördenleitung gilt dies besonders (§ 14 Abs. 1 DSG-LSA).
Er weist in diesem Zusammenhang erneut darauf hin, dass eine Trennung der Funktionen des behördlichen Datenschutzbeauftragten und des für IuK-Angelegenheiten Verantwortlichen notwendig ist. Die Trennung dieser Funktionen sollte sich aus Geschäftsverteilungsplänen ebenso entnehmen lassen wie die besondere Stellung der behördlichen Beauftragten i. S. v. § 14a Abs. 2 DSG-LSA.

Bei der zusammenfassenden Beurteilung dieses Vorfalls kann der Landesbeauftragte nur mit Verwunderung feststellen, dass, obwohl die Kameras offenkundig nicht zur Beobachtung und Überwachung technischer Prozesse, sondern ausschließlich zur Beobachtung und Überwachung von Personen angeschafft und betrieben wurden, keiner der Beteiligten hierin einen die Rechte des Einzelnen berührenden Vorgang erkannte. Die notwendige Empfindsamkeit für solche Rechtsbeeinträchtigungen scheint - auch bei qua Berufsbild eigentlich aufmerksameren Zeitgenossen - durch die allgegenwärtigen Überwachungssituationen doch bereits erheblich herabgesetzt zu sein. Dieser Eindruck wird noch dadurch verstärkt, dass kurz zuvor im Bereich der Polizei eine Videoüberwachungsmaßnahme am unweit vom Justizzentrum gelegenen Hasselbachplatz für öffentlichkeitswirksamen Wirbel gesorgt hatte (vgl. Ziff. 18.6). Trotzdem löste das keine Reaktion im Justizzentrum aus. Es wurde sozusagen vergessen, dass beim Beob“achten“ das besondere Augenmerk immer auch auf dem Achten der Grundrechte der Beobachteten liegen muss. Die bereits eingangs dieses Tätigkeitsberichts allgemein angesprochene unerlässliche Stärkung des Datenschutzbewusstseins bleibt daher ebenfalls ein notwendiger Appell im Bereich der Justiz.

19.5. Namen von Verfahrensbeteiligten auf Monitoren im Eingangsbereich eines Justizzentrums

Wie der Landesbeauftragte anlässlich eines Informations- und Kontrollbesuchs in einem Justizzentrum feststellte, wurden dort auf einer elektronischen Tafel im öffentlichen Eingangsbereich vollständig und undifferenziert Namen und Vornamen Verfahrensbeteiligter der gerichtlichen Verfahren aufgelistet.
Dies erschien dem Landesbeauftragten nicht so unproblematisch wie dem Gesprächspartner beim kontrollierten Gericht. Allein dessen Hinweis darauf, dass dies automatisiert durch das EDV-System EUREKA erfolge, kann natürlich unzulässige Datenverarbeitungen nicht rechtfertigen - ganz im Gegenteil ist das EDV-System so zu konfigurieren, dass u. a. nur das Erforderliche an Informationen Dritten übermittelt wird.
Zweck einer solchen (elektronischen) Terminsrolle ist zum einen den Zugang zu den Verhandlungen zu erleichtern und damit zum anderen auch den Grundsatz der Öffentlichkeit von Gerichtsverhandlungen zu gewährleisten.
Allerdings dürfte schon die öffentliche Wiedergabe des Vornamens für diese Zwecke nicht erforderlich sein. Schließlich werden an einem Tage nicht unzählige Verfahren beim gleichen Gericht unter gleichem Nachnamen mit gleichem Rechtsanwalt geführt werden.

Daher bestehen an der Erforderlichkeit schon dieser Form namentlicher Nennung Zweifel. Bei nicht-öffentlichen Verfahren könnte zudem durch die Namenswiedergabe die Verletzung von Schutznormen verursacht werden. Durch eine solche Bekanntmachung würde ohne Not ein wesentlicher Teil der Nichtöffentlichkeit beseitigt. Wenn auf der Terminsrolle im Justizzentrum z. B. bei Strafverfahren gegen Jugendliche, in Sozialgerichtsverfahren oder auch bei Verfahren zur Abgabe der eidesstattlichen Versicherung Namen der Verfahrensbeteiligten genannt werden, zu deren Schutz die Nichtöffentlichkeit festgeschrieben wurde, könnten Dritte unberechtigt Kenntnis von personenbezogenen Daten erlangen. Dies gilt auch hinsichtlich personenbezogener Daten, die aufgrund besonderer Regelungen nicht ohne weiteres veröffentlicht oder gar an Dritte übermittelt werden dürfen, insbesondere Sozialdaten.
Der Landesbeauftragte hat angeregt, diese Thematik im Rahmen der Nutzerbesprechung des Justizzentrums aufzugreifen und darauf hingewiesen, dass auf der Terminsrolle hinsichtlich nicht öffentlicher Sitzungen lediglich Terminstag, die Terminsstunde, das Aktenzeichen sowie ggf. die Bezeichnung der Vorsitzenden bzw. des Vorsitzenden, die Namen der mitwirkenden Richterinnen und Richter sowie die Saalnummer ersichtlich sein sollten. Die erbetene Stellungnahme konnte bis zum Ende des Berichtszeitraums nicht vorgelegt werden.

19.6. Schülergremien

Der Landesbeauftragte hatte im vergangenen Berichtszeitraum (VIII. Tätigkeitsbericht, Ziff. 18.7) darüber informiert, dass das Justizministerium im Land sog. Schülergremien, landläufig Schülergerichte genannt, eingeführt hat.
Auf seine Anfrage hin informierte das Justizministerium den Landesbeauftragten inzwischen ausführlich über das Projekt „Schülergremien“.

Als Handlungsgrundlage u. a. zur Übermittlung von im Ermittlungsverfahren gewonnen Daten zu Tat, Täter oder Täterin und deren Persönlichkeit solle danach nicht nur die Einverständniserklärung der Beschuldigten und deren Erziehungsberechtigten zur „freiwilligen“ Teilnahme am Schülergerichtsverfahren sowie zur Akzeptanz der Entscheidung des Schülergerichts dienen. Grundlage sei die gesetzlich in § 45 Abs. 2 Jugendgerichtsgesetz vorgesehene Möglichkeit der Staatsanwaltschaft, als Herrin des Ermittlungsverfahrens von der weiteren Strafverfolgung abzusehen, wenn eine erzieherische Maßnahme bereits durchgeführt oder eingeleitet ist und eine richterliche Beteiligung nicht erforderlich scheint. Diese strafverfahrensrechtliche Befugnisnorm ist als Rechtsgrundlage für eine Datenübermittlung an private Dritte, nichts anderes sind die Schülerrichterinnen und Schülerrichter, ebenso wenig geeignet wie die Regelungen der §§ 12 ff. des Einführungsgesetzes zum Gerichtsverfassungsgesetz. Allerdings dürften die Bestimmungen von §§ 12, 10 DSG-LSA im Falle der Einwilligung von Beschuldigten und ggf. deren Erziehungsberechtigten eine angemessene Grundlage für die Übermittlung der erforderlichen Daten sein.

Das vom Justizministerium vorgesehene Verfahren zur Verschwiegenheitsverpflichtung von Schülerrichterinnen und Schülerrichtern nach dem Ver-

pflichtungsgesetz unter Beteiligung von deren Erziehungsberechtigten erscheint geeignet, die besondere Verantwortung auch hinsichtlich der Daten von Beschuldigten deutlich werden zu lassen.
Zweifel an der rechtlichen Wirksamkeit der Verpflichtungserklärung gegenüber Minderjährigen bestehen zwar fort, der wesentliche Sinn des Verpflichtungsvorgangs, nämlich seine besondere Warnfunktion und damit auch seine Schutzfunktion hinsichtlich der im Schülergremium bekannt werdenden persönlichen Daten, wird allerdings in der Regel erreicht werden können. Ob im Falle einer Verschwiegenheitsverletzung durch eine Schülerrichterin oder einen Schülerrichter die Verpflichtungserklärung tatsächlich als Grundlage strafrechtlicher Folgeschritte zu dienen vermag, ist im Verhältnis zu dieser Warnfunktion nicht erheblich.

19.7. Zustellungen durch Gerichtsvollzieher

Im Rahmen einer Eingabe hatten sich Petenten beim Landesbeauftragten darüber beschwert, dass ein Gerichtsvollzieher durch seine Verfahrensweise anlässlich von Ersatzzustellungen an Dritte diesen ermöglicht habe, von den die Petenten betreffenden Pfändungsbeschlüssen Kenntnis zu erlangen. Es war nachvollziehbar, dass dies den Petenten in besonderer Weise unangenehm sein musste, handelte es sich bei diesen Dritten doch um (auch befristet beschäftigte) Bedienstete ihres jeweiligen Arbeitgebers. Trotz einer nachdrücklichen Bitte des Rechtsanwalts der Petenten, die notwendige Diskretion zu wahren, habe der Gerichtsvollzieher erneut in der kritisierten Weise beim Arbeitgeber der Petenten Pfändungsunterlagen ohne Briefumschlag übergeben.

Das zuständige Amtsgericht hat den zu beanstandenden Sachverhalt bestätigt. So habe der zuständige Gerichtsvollzieher vorläufige Zahlungsverbote zwar grundsätzlich entsprechend der „gesetzlichen“ Vorgaben in der Verwaltungsvorschrift für die Geschäftstätigkeit der Gerichtsvollzieher jeweils im Wege der Ersatzzustellung an eine in den Geschäftsräumen anwesende und bei dem Adressaten beschäftigte Person zugestellt. Allerdings habe der Gerichtsvollzieher entgegen § 36 Nr. 3 Abs. 1 der Geschäftsanweisung für Gerichtsvollzieher die Ersatzzustellung nicht im verschlossenen Umschlag vorgenommen.

Da der Verstoß nach Mitteilung des Gerichts auch zum Anlass genommen worden war, die Gerichtsvollzieher im Gerichtsbezirk gesondert auf eine rechtlich einwandfreie Verhaltensweise bei Zustellungen hinzuweisen, konnte nach § 24 Abs. 3 DSG-LSA von einer formellen Beanstandung abgesehen werden.

19.8. Justizaktenaufbewahrung

Wie im VIII. Tätigkeitsbericht (Ziff. 18.6) berichtet, hatten die Datenschutzbeauftragten des Bundes und der Länder seit Jahren eine gesetzliche Grundlage für die Aufbewahrung, Löschung etc. von Akten und Dateien in der Justiz gefordert.
Zwar hatten die Landesjustizverwaltungen nur sukzessive eine Regelungsnotwendigkeit anerkannt. Schließlich wurde aber doch federführend von ei-

nem Land ein gemeinsamer Gesetzesentwurf zur Aktenaufbewahrung von Justizakten erarbeitet. Letztlich konnte am 19. Juni 2008 auch für Sachsen-Anhalt ein Schriftgutaufbewahrungsgesetz für die Justiz (JSchrG LSA) veröffentlicht werden (GVBl. LSA S. 236). Leider fehlte die nach § 2 JSchrG LSA zu erlassende Rechtsverordnung bis Ende des Berichtszeitraums immer noch.

Allerdings wurde dem Landesbeauftragten kurz vor Ende des Berichtszeitraums der Entwurf einer Rechtsverordnung zugeleitet. Dieser bezog sich aber lediglich auf die Aufbewahrungsfristen in der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaft, dem Justizvollzug und dem Sozialen Dienst der Justiz.
Ein Entwurf für die Fachgerichtsbarkeiten bedürfe nach Mitteilung des Justizministeriums noch umfangreicherer Abstimmungen.
Der Landesbeauftragte hofft, dass die Verordnungen - an welchen nach der Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht bereits seit 2007 gearbeitet werde - wie zu Jahresbeginn 2009 angekündigt noch in diesem Jahr vorliegen werden.

19.9. Abfrage von Kreditkartendaten in einem Ermittlungsverfahren

Am 17. Februar 2009 hat das Bundesverfassungsgericht beschlossen, die Verfassungsbeschwerden bezüglich der Abfrage von Kreditkartendaten in einem Ermittlungsverfahren nicht zur Entscheidung anzunehmen (BVerfG NJW 2009, 1405). Hintergrund dieses Verfahrens sind die Ermittlungen der Staatsanwaltschaft Halle (Saale), die unter der Bezeichnung „Mikado“ 2006 und 2007 bundesweite Bekanntheit erlangten. Der Landesbeauftragte hatte in seinem VIII. Tätigkeitsbericht (Ziff. 18.11) ausführlich über die Ermittlungen und deren datenschutzrechtliche Dimension informiert.

Das Bundesverfassungsgericht stellt in seinem Beschluss u. a. das Folgende fest:
„Die Datenabfrage der Staatsanwaltschaft und die sie bestätigenden Gerichtsentscheidungen verletzen die Beschwerdeführer nicht in ihrem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG.“
„Die Abfrage der Kreditkartendaten durch die Staatsanwaltschaft war kein Eingriff in das Recht auf informationelle Selbstbestimmung der Beschwerdeführer, deren Kreditkartendaten bei den Unternehmen nur maschinell geprüft, mangels Übereinstimmung mit den Suchkriterien aber nicht als Treffer angezeigt und der Staatsanwaltschaft daher nicht übermittelt wurden.“ „Für die Annahme eines Eingriffs genügt es nicht, dass die Daten bei den Unternehmen in einen maschinellen Suchlauf mit eingestellt wurden, da ihre Daten anonym und spurenlos aus diesem Suchlauf ausgeschieden wurden und nicht im Zusammenhang mit dieser Ermittlungsmaßnahme behördlich zur Kenntnis genommen wurden ...“.
„Bei der vorliegenden Maßnahme handelte es sich nicht um eine Rasterfahndung im Sinne von § 98a StPO oder eine ähnliche Maßnahme, die an den Voraussetzungen dieser Ermächtigungsgrundlage zu messen wäre. Datenermittlungen wie die hier vorliegende, welche die besonderen Merkmale

einer Rasterfahndung nicht aufweisen und sich auf andere Ermächtigungsgrundlagen stützen lassen, werden dagegen durch § 98a StPO nicht ausgeschlossen....“
„Die Rasterfahndung ist eine besondere Fahndungsmethode unter Nutzung der elektronischen Datenverarbeitung. Die Strafverfolgungsbehörde lässt sich von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln, um einen automatisierten Abgleich (Rasterung) mit anderen Daten vorzunehmen.“ „Dagegen liegt keine Rasterfahndung vor, wenn die Strafverfolgungsbehörde von privaten Stellen Auskünfte zu speziellen Täter-Daten erhält, also nicht die Gesamtdateien zum weiteren Abgleich mit anderen Dateien übermittelt bekommt ....“ „Die Wirkung und Eingriffsintensität der Anfrage der Staatsanwaltschaft und der dadurch veranlassten Übermittlung der Daten entspricht auch nicht der einer Rasterfahndung, so dass kein Anlass für eine entsprechende Anwendung der §§ 98a, 98b StPO besteht ....“

Die umstrittene Ermittlungsmaßnahme der Staatsanwaltschaft Halle (Saale) hat sich damit - wie auch vom Landesbeauftragten festgestellt - als rechtmäßig herausgestellt.

19.10. Zwangsversteigerung und Internet

Im Rahmen einer Eingabe hatte sich ein Petent darüber beschwert, dass ohne seine Zustimmung im Rahmen eines Zwangsversteigerungsverfahrens durch den gerichtlich beauftragten Gutachter Bilder seiner Wohnung ins Internet eingestellt und damit seine personenbezogenen Daten weltweit an unbestimmte Dritte übermittelt werden. Da das Gericht in seinem Antwortschreiben an den Petenten auf dessen Vorhalte hin meinte, es seien keine personenbezogenen Daten weitergegeben worden, wies der Landesbeauftragte bereits in seiner Bitte um Stellungnahme gegenüber dem Gericht darauf hin, dass der aus den Bildern ersichtliche Wohnungseinrichtungsstil ein personenbezogenes Datum darstellen könnte. Auch könnte eine Zuordnung zu Personen dadurch möglich werden, dass die Räume den Gebäudegeschossen und diese den Bewohnern zugeordnet werden könnten.

Zur Veröffentlichung der Zwangsversteigerungsimmobilie bediente sich das Gericht offenkundig eines privaten Dritten, um die Gutachten ins Internet einzustellen. Auch wenn dieser u. U. mit dem vom Gericht bestellten Sachverständigen identisch ist, stellt die weitergehende Veröffentlichung einen eigenständig zu bewertenden Vorgang dar.
Durch die Nutzung privater Dritter dürfte sich das Gericht einer Datenverarbeitung im Auftrage bedienen. Die Regelungen des Gesetzes über die Zwangsversteigerung und die Zwangsverwaltung (ZVG) geben zwar grundsätzliche die Befugnis, u. a. Wertgutachten in bestimmten elektronischen Informationssystemen bekannt machen zu dürfen. Die derzeitige Verfahrensweise dürfte aber einer eigenen Rechtfertigung bedürfen.

Das zuständige Amtsgericht hat in seiner Antwort bestätigt, dass sich auf der Internetseite die aus dem Gutachten ersichtlichen Bilder befinden. Eine konkrete Zuordnung zu einzelnen Personen sei nicht möglich, da im Gutachten die Namen der Beteiligten - so auch der des Petenten - entfernt worden seien.

Dem Petenten wurde vom Landesbeauftragten erläutert, dass, wenn aufgrund des weitergehenden Informationsgehalts der im Internet einsehbaren Bilder u. U. ein Personenbezug hergestellt werden könnte, dies nur dann problematisch wäre, wenn die Weitergabe solcher indirekten Informationen unzulässig wäre. Der Gesetzgeber hat jedoch die Befugnis zur Internetveröffentlichung in § 38 Abs. 2 ZVG vorgesehen. Dass er dabei auch die Möglichkeit einer Bestimmbarkeit von Personen durch indirekte Informationen übersehen hat, ist nicht anzunehmen. Wie die Gesetzesbegründung belegt, hat er mit dieser Bestimmung die Verwertungsmöglichkeiten in der Zwangsversteigerung verbessern wollen. Dies dient auch den Interessen der Eigentümer, hier des Petenten. Zu bedenken war auch, dass bei der Begutachtung der Immobilie der Sohn des Petenten anwesend war. Er hatte der Erstellung der Lichtbilder nicht widersprochen. Demzufolge konnte der anwesende Rechtspfleger davon ausgehen, dass keine Bedenken gegen die Aufnahmen bestanden hatten.
Letztlich konnte das Verhalten des Gerichts aufgrund der geltenden Gesetzeslage durch den Landesbeauftragten nicht kritisiert werden. Die Verfassungswidrigkeit des hier wesentlichen § 38 Abs. 2 ZVG könnte nur durch das Bundesverfassungsgericht festgestellt werden.
Gleichwohl war der Sachverhalt dem Landesbeauftragten Anlass, zu den praktischen Umständen und rechtlichen Bezügen bei der Bearbeitung von Zwangsversteigerungsangelegenheiten das Justizministerium, insbesondere hinsichtlich der Internetveröffentlichung im Wege der Auftragsdatenverarbeitung, um Stellungnahme zu bitten. Die Stellungnahme stand zum Ende des Berichtszeitraums noch aus, sie wurde bereits im Dezember 2008 erbeten.

20. Schulen

20.1. Prüfung in Schulen

In diesem Berichtszeitraum hat der Landesbeauftragte Sekundarschulen und Gymnasien hinsichtlich der Einhaltung der datenschutzrechtlichen Vorschriften geprüft.
Wie bereits im VIII. Tätigkeitsbericht (Ziff. 19.4.1) dargelegt, musste auch in den nunmehr besuchten Schulen festgestellt werden, dass teilweise keine behördlichen Datenschutzbeauftragten gem. § 84a Abs. 2 SchulG LSA i. V. m. § 14a DSG-LSA bestellt waren, die Schülerdatenerhebung häufig über das erforderliche Maß des § 84a Abs. 3 Satz 1 SchulG LSA hinaus ging und private Lehrer-PC dienstlich ohne die erforderliche Genehmigung der Schulleitung genutzt wurden.
Die datenschutzrechtlichen Hinweise und Empfehlungen des Landesbeauftragten wurden von den Schulen unverzüglich umgesetzt.

Ein Fall fiel besonders auf:
Im Sommer 2006 hat der Landesbeauftragte in einer Sekundarschule die Einhaltung der datenschutzrechtlichen Vorschriften geprüft und u. a. festgestellt, dass das verwendete Schülerstammblatt nicht den Voraussetzungen des § 84a Abs. 3 Satz 1 SchulG LSA entspricht. Die Erforderlichkeit der Datenerhebung von der Nationalität, Anzahl der Geschwister, Bekenntnis bis

zur Art des Verhältnisses zum Schüler und Ursache für die Zurückstellung vom Schulbesuch war aus Sicht des Landesbeauftragten nicht gegeben.
Da die Sekundarschule die Vordrucke des Schülerstammblattes vom Schulträger, einer Stadt, zur Verfügung gestellt bekommt, hat sich der Landesbeauftragte im Januar 2007 an diesen selbst gewandt.
Im Rahmen des Schriftwechsels hat der Landesbeauftragte der Stadt erläutert, dass sie nach § 14 Abs. 1 DSG-LSA für ihren Organisationsbereich sicherzustellen hat, dass die datenschutzrechtlichen Vorschriften eingehalten werden. Der Stadt obliegt es, die materiell-sächlichen Bedingungen zur Sicherung des Schulbetriebes vorzuhalten. Dazu gehört auch die Beschaffung und Bereitstellung von Formularen, wie z. B. des Schülerstammblatts. Der Landesbeauftragte hat diesbezüglich darauf hingewiesen, dass die Beschaffung von Formblättern für Schulen nicht ausschließlich unter wirtschaftlichen Gesichtspunkten erfolgen darf. Ein Eingriff in das Grundrecht der informationellen Selbstbestimmung ist nur aufgrund eines Gesetzes zulässig. Dies ist demnach entsprechend des § 84a Abs. 3 Satz 1 SchulG LSA nur im tatsächlich erforderlichen Umfang möglich. Die Erhebung nicht erforderlicher Informationen ist unzulässig. Sie darf daher erst recht nicht durch die Verwendung entsprechender Formulare gefördert werden.
Die Stadt bestritt zunächst eine Mitverantwortung, da schließlich die Schulen die Daten erheben. Sie räumte jedoch im Juni 2007 ein, die Schulen in ihrer Trägerschaft mittels Erfassungshilfen entsprechend sensibilisieren zu wollen. Der Landesbeauftragte merkte dazu an, dass diese Hinweise nur vorläufige Maßnahmen sein können.

Aufgrund einer erneuten datenschutzrechtlichen Prüfung in einer anderen Sekundarschule der Stadt im September 2008 musste der Landesbeauftragte dann jedoch feststellen, dass mehr als ein Jahr nach der Zusicherung des Schulträgers an den Schulen noch immer derselbe Vordruck zum Schülerstammblatt verwandt wurde, ohne dass die Schulen Einfluss auf die Auswahl dieses Formblattes haben. Darüber hinaus behauptete die Schule, dass keine Hinweise oder Erfassungshilfen des Schulträgers vorlägen.
Die Stadt konnte dann jedoch nachweisen, die Schulen auf die Rechtsgrundlagen der Datenerhebung und -verarbeitung hingewiesen zu haben.
Der Landesbeauftragte wirkte darauf hin, dass der Schulträger nur noch solche Vordrucke beschafft und an die Schulen gibt, die den Voraussetzungen des § 84a Abs. 3 Satz 1 SchulG LSA entsprechen.

20.2. Umstellung der Schulstatistik auf Individualdaten (Kerndatensatz)

Bereits im VIII. Tätigkeitsbericht (Ziff. 19.1) hatte der Landesbeauftragte über das Vorhaben ausführlich berichtet.

Am 15. August 2007 hat die zweite Besprechung von Vertretern der Datenschutzkonferenz mit der AG Kerndatensatz/Datengewinnung der Kommission für Statistik (KomStat) der Kultusministerkonferenz (KMK) stattgefunden. Grundlage war das überarbeitete Konzeptpapier KMK, das diese am 14./15. Juni 2007 gebilligt hatte.
Im Ergebnis bestand in vielen Punkten noch immer erheblicher Klärungsbedarf (z. B. was versteht die KMK unter einer „hochwertigen Pseudonymisierung der Datensätze“). Insbesondere bezüglich der Frage der Totalerhebun-

gen zur Durchführung von Bildungsverlaufsuntersuchungen bestanden die Auffassungsunterschiede fort.

Mit Schreiben vom 30. Juni 2008 hat der Vorsitzende der KomStat der KMK dem Vorsitzenden der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein überarbeitetes Konzept für die länderübergreifende Nutzung der schulstatistischen Einzeldaten mit der Bitte um Wiederaufnahme und Weiterführung der Gespräche übersandt. Hierzu haben die Datenschutzbeauftragten dem Vorsitzenden der KomStat der KMK im Oktober 2008 geantwortet.
Zusammenfassend wurde mitgeteilt, dass nach wie vor erhebliche Zweifel an der Notwendigkeit der beabsichtigten Totalerhebung bestehen, da eine hinreichende Begründung dafür weiterhin nicht gegeben wurde. Es war nicht ersichtlich, weshalb gründliche fachwissenschaftliche, einen hinreichend großen Datensatz einbeziehende Untersuchungen bezogen auf eine kleine Stichprobe den anerkanntermaßen bestehenden Bedarf an Erkenntnissen für Verbesserungen im Schulwesen nicht ebenso befriedigen können.
Darüber hinaus fehlten weiterhin die Vorgaben für das notwendige statistikrechtliche Instrumentarium in den Ländern.
Hinsichtlich einer Hash-Verschlüsselung der Schülerdaten bleiben Fragen offen, z. B. Bildung des Hash-Wertes u. a. auf Basis des Schülernachnamens, der sich nicht selten ändern kann; Kenntnis des Schlüssels bei allen beteiligten Stellen.
Die Entwicklung dieses Projektes wird vom Landesbeauftragten daher weiter kritisch verfolgt.

20.3. Schulverwaltungssoftware

Sachsen-Anhalt beabsichtigt, flächendeckend eine einheitliche Schulverwaltungssoftware einzuführen. Sie soll zu einer erheblichen Verwaltungsvereinfachung führen und ist Voraussetzung für die Umsetzung der von der Kultusministerkonferenz im Mai 2003 beschlossenen Einführung des Kerndatensatzes (siehe Ziff. 20.2, VIII. Tätigkeitsbericht, Ziff. 19.1). Die Informationen der Schulaufsicht für Planung und Statistik sollen aus den Schulverwaltungsdaten extrahiert werden.

Die Schulen erhalten auf der Grundlage einer Rahmenkooperationsvereinbarung zwischen dem Kultusministerium und den Kommunalen Spitzenverbänden Kommunikationscomputer. Dies ist die Grundlage für den landesweiten Einsatz der entwickelten Software. Die von den Schülern und Lehrern erhobenen Daten werden in einer Datenbank in der Schule gespeichert (dezentrale Datenhaltung). Über eine Schnittstelle sollten an festgelegten Stichtagen bestimmte Daten zu Planungs- und Statistikzwecken an ein zentrales System übermittelt werden.
Eine zentral von einer Clearingstelle vergebene landeseinheitliche Schüler-Identifikationsnummer (Schüler-ID) sei erforderlich, um im Rahmen der Schulverwaltung Plausibilitätskontrollen durchzuführen (z. B. Sicherung der Eindeutigkeit). Außerdem solle der Kerndatensatz „Abfallprodukt“ dieses Projektes sein.

Ein erster Arbeitsentwurf vom 4. April 2008 mit Änderungen des § 84a SchulG LSA als Grundlage der Datenverarbeitung wurde mit dem Landesbeauftragten beraten, der auf Folgendes hinwies:

Bedenklich erschien eine Regelung, nach der eine oder mehrere Stellen mit Aufgaben schulübergreifender Verwaltungszwecke beauftragt werden können, die dann die erforderlichen personenbezogenen Daten von Schülern verarbeiten. Die rechtliche Struktur der Einbindung dieses Dienstleisters war offen. Soweit diesbezüglich eine Datenverarbeitung im Auftrag angedacht war, wäre keine Schaffung bzw. Änderung der Rechtsgrundlage erforderlich gewesen, da rechtlich gesehen keine Datenübermittlung stattfindet (vgl. § 8 DSG-LSA). Würde eine solche Stelle beim Landesverwaltungsamt angesiedelt werden, hätte dies bedeutet, dass jede einzelne verantwortliche Schule hinsichtlich der Datenverarbeitung gegenüber dem Landesverwaltungsamt weisungsbefugt wäre (vgl. Nr. 8.3 VV-DSG-LSA zu § 8 DSG-LSA).
Zudem sind bei der Speicherung von Daten für schulübergreifende Verwaltungszwecke die verfassungsrechtlichen Aspekte der Datensparsamkeit und Datenvermeidung zu berücksichtigen. Fragwürdig erschienen daher die Schaffung einer operativen Datenbank und die Generierung einer landesweit eindeutigen Schüler-ID für die Vermeidung von Doppelerfassungen. Es dürften stets nur die Daten und nur so lange gespeichert werden, wie dies für die konkrete Aufgabenerfüllung erforderlich, also unerlässlich ist. Der Gesamtumfang schulstatistischer Individualdaten (Sprache, Wahlfächer, Noten, Telefonnummern usw.) dürfte weder für einzelne, noch für mehrere gleichzeitig zu erledigende Verwaltungsaufgaben erforderlich sein. Identifikationsverfahren, die eine individuelle Zuordnung gewährleisten, sind mit wenigen Daten denkbar.

Darüber hinaus wurde auf das Trennungsgebot von Verwaltung und Statistik hingewiesen, das gegen die Anbindung bei einer datenschutzrechtlich verantwortlichen Stelle sprach (operative Datenbank im Schulreferat, statistische Datenbank „Amtliche Schuldaten“ im Statistikreferat).
Im Hinblick auf die Erstellung amtlicher Statistiken wurde angeregt, die Aufgabe bei einer Stelle anzubinden, die dem Statistikgeheimnis unterliegt. Bezüglich des Vorhabens, Verlaufsstatistiken zu bilden, wurde darauf hingewiesen, dass der Gefahr der Reidentifizierbarkeit statistischer Datensätze (Datenumfang, Schulnummer) zu begegnen ist. Zudem wäre zu berücksichtigen, dass eine umfängliche Registrierung und Katalogisierung auch in der Anonymität der Statistik verfassungsrechtlich bedenklich wäre.

20.4. Medienkompetenz und Datenschutzbewusstsein von Schülern

Aufgrund der Vorbereitungen und Ergebnisse des Europäischen Datenschutztages am 28. Januar 2008 (siehe auch oben Ziff. 3.3) mit dem Thema „Datenschutz macht Schule“ hat die 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder beschlossen, sich noch intensiver mit diesem Thema in einer Arbeitsgruppe zu beschäftigen. Ziel dieser Arbeitsgruppe ist es, Vorschläge zur Verbesserung der Medienkompetenz und des Datenschutzbewusstseins von Schülern zu entwickeln. Die von der Arbeitsgruppe vorbereitete und auf der 75. Konferenz der Datenschutzbeauftragten gefasste Entschließung „Medienkompetenz und Datenschutzbewusstsein in

der jungen online-Generation“ **(Anlage 7)** fordert die für schulische Bildung zuständigen Minister der Landesregierungen auf, bei der Förderung der Medienkompetenz von Schülern auch deren Datenschutzbewusstsein zu stärken. Die Arbeitsgruppe stellt eine Linkliste mit Informationsmaterial und Unterrichtshilfen zusammen, die auf der Homepage des Landesbeauftragten zur Verfügung steht. Mit dem Recht von Kindern auf ein sicheres Online-Umfeld, das ihre Privatsphäre respektiert, hat sich auch die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre befasst und in der „Entschließung zum Schutz der Privatsphäre von Kindern im Internet“ Forderungen (erzieherische Ansätze, Schutzvorschriften) formuliert **(Anlage 47).**

Bei der notwendigen Förderung von Medienkompetenz gerade bei der jungen Online-Generation sind informationeller Selbstschutz und **Datenschutzbewusstsein** zu wecken und zu stärken. Dabei geht es nicht nur um Datensicherheit, sondern um das zugrunde liegende Grundrechtsverständnis. Mit der Wissensvermittlung geht die **Wertevermittlung** einher. Selbstbestimmung, Privatheit und Verhaltensfreiheit sind Gemeinwohlbelange und Funktionsbedingung der freiheitlichen Demokratie, zumal gegen heimliche Überwachung und Einschüchterungseffekte. Datenschutz gehört so zum Bildungsauftrag von Schule, und das nicht nur in den Fächern Moderne Medienwelten und Informatik (zu kurz greift insofern die Bekanntmachung des Kultusministeriums vom 12. März 2009, Schulverwaltungsblatt 2009, 76), sondern vor allem in den Fächern Sozialkunde, Rechtskunde und auch Ethik. Darüber hinaus gehört Datenschutz zur politischen Bildung in der Demokratie.

Anknüpfend an die Aktivitäten der Konferenz hat der Landesbeauftragte auch im Land Sachsen-Anhalt zunächst die Kontakte u. a. zum Kultusministerium, Landesinstitut für Schulqualität und Lehrerbildung (bis 28. Februar 2009 Landesinstitut für Lehrerfortbildung, Lehrerweiterbildung und Unterrichtsforschung), zur Landesmedienanstalt, Staatskanzlei und Landeszentrale für politische Bildung verstärkt. Ziel soll ein multiplikatorisches Hineinwirken in die Schulen und die Unterstützung der Demokratieinitiative der Landesregierung sein.

Erste gemeinsame Projekte wurden vorbereitet und durchgeführt.
Der Landesbeauftragte wirkt z. B. bei Angeboten der Lehrerfortbildung des Landesinstituts für Schulqualität und Lehrerbildung mit. Außerdem sollen die schulfachlichen Referenten und die schulischen Datenschutzbeauftragten entsprechend geschult werden.
Im Rahmen des Safer Internet Day 2009 hat der Landesbeauftragte zusammen mit dem Staatssekretär des Kultusministeriums Schülerinnen und Schüler in einer Sekundarschule besucht. Die Jugendlichen haben Projekte zum Thema „Cyber Mobbing“ vorgestellt. Anschließend wurde mit ihnen und den Lehrern zu den Themen Datenschutzbewusstsein und Internetnutzung diskutiert.
Weitere Projekte dieser Art sind in der Planung. Insbesondere hat der Landesbeauftragte sein Angebot an Schulen zu Vorträgen und Unterrichten erneuert (vgl. hierzu VI. Tätigkeitsbericht, Ziff. 19.5, VII. Tätigkeitsbericht, Ziff. 19.1). Dies wird von den Schulen im Land nunmehr gern aufgegriffen.

20.5. Soziale Netzwerke

Soziale Netzwerke gehören zu den beliebtesten Instrumentarien moderner Kommunikation auf der Grundlage von Anwendungen oder Portalen im Web 2.0. Sie bieten den Beteiligten die Möglichkeit, Profile in das Netz zu stellen und die Zugriffsberechtigten festzulegen. Sie gewähren u. a. die Kontaktaufnahme, die Versendung und den Empfang von Nachrichten, das Einstellen von Bildern und Blogs. Dies bewirkt auch Risiken für die Privatsphäre. Darauf sollten gerade die jungen Nutzer besonders hingewiesen werden. Bedeutsam sind u. a. grundlegende Einstellungen, z. B. zum Zugriff auf die Profildaten, zum Zugriff von Suchmaschinen, zur Nutzung der Daten zu Werbezwecken und zur Löschung der Daten. Hierzu ist auf den Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich „Datenschutzkonforme Gestaltung sozialer Netzwerke“ **(Anlage 36)** hinzuweisen. Auch die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre hat in der „Entschließung zum Datenschutz in Sozialen Netzwerkdiensten“ Empfehlungen zum Persönlichkeitsschutz formuliert **(Anlage 46).**

20.6. Bewertungsportale

Bewertungsportale, wie „spickmich.de“ oder „meinprof.de“, erfreuen sich bei Schülern und Studenten größter Beliebtheit. Von der Möglichkeit, die Lehrer bzw. Hochschullehrer im Internet zu benoten, wird gern und umfänglich Gebrauch gemacht. Die Rechtsprechung neigt bisher dazu, die Benotung von Lehrkräften grundsätzlich nicht als Verletzung des allgemeinen Persönlichkeitsrechts bzw. als Verstoß gegen datenschutzrechtliche Bestimmungen anzusehen. Das zivilgerichtlich mittels einstweiliger Verfügungen geltend gemachte Unterlassungsbegehren von Lehrkräften gegenüber den Portalbetreibern hatte in der obergerichtlichen Rechtsprechung bisher keinen Erfolg. Dies hat der Bundesgerichtshof mit Urteil vom 23. Juni 2009 (VI ZR 196/08) in einem Einzelfall bestätigt.
Demnach können Lehrkräfte grundsätzlich weiterhin unter Benennung ihres Namens und der Lehreinrichtung nach bestimmten fachlichen Kriterien (u. a. guter Unterricht, fachlich kompetent, faire Noten, vorbildliches Auftreten) mit Schulnoten versehen werden. Die dortigen Meinungsäußerungen fallen nach Auffassung der Rechtsprechung in den Schutzbereich des Grundrechts auf Meinungsfreiheit gem. Artikel 5 Abs. 1 GG. Die Vermeidung einer Persönlichkeitsbeeinträchtigung, die durch die Bewertung entstehen kann, kann die Einschränkung der Meinungsfreiheit nicht rechtfertigen. Voraussetzung war, dass die Beurteilungskriterien die Lehrkraft nicht in ihrem Erscheinungsbild oder in ihrer allgemeinen Persönlichkeit betreffen, sondern auf die konkrete Ausübung der beruflichen Tätigkeit abstellen. Die Grenze liegt im Bereich von Schmähkritik oder Formalbeleidigungen.

Gegenüber den Tendenzen der Rechtsprechung haben die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich im April des Jahres 2008 zu Recht auf Folgendes hingewiesen (siehe dazu: Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-

öffentlichen Bereich „Internetportale zur Bewertung von Einzelpersonen“, **Anlage 35**):
Die Beurteilungen und Bewertungen von Lehrkräften in Internetportalen enthalten vielfach sensible Informationen und subjektive Werteurteile, die jederzeit von jedermann abgerufen werden können, ohne dass die Urheber erkennbar sind. Die Portale müssen jedoch das Bundesdatenschutzgesetz berücksichtigen. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Es bleibt demnach Aufgabe der beteiligten öffentlichen Stellen, bei den nutzenden Schülern und Studenten ein entsprechendes Datenschutzbewusstsein zu wecken. Auch den Nutzern muss deutlich sein, dass es bei der Ausübung ihres Rechts auf Meinungsfreiheit geboten ist, den Persönlichkeitsrechten der Betroffenen in angemessenem Umfang Rechnung zu tragen.

20.7. Gesamtbeurteilungsbogen

Die Bundesagentur für Arbeit wollte die Zusammenarbeit zwischen den Agenturen für Arbeit und den Förder-/Sonderschulen verbessern. Zur Umsetzung gehörte auch ein vom Klassenlehrer des betroffenen Schülers auszufüllender Gesamtbeurteilungsbogen, in dem die Lehrkraft u. a. die schulischen Leistungen des Schülers bewerten und Angaben zur Persönlichkeitsstruktur und zu seiner körperlichen Konstitution eintragen sollte.
Die Datenschutzbeauftragten des Bundes und der Länder beteiligten sich an der datenschutzrechtlichen Optimierung des Vordrucks (u. a. zum Datenumfang und Verwendungszweck und zur Formulierung der Einwilligungen). Nachdem die Anregungen der Datenschutzbeauftragten in die Formulargestaltung eingeflossen waren, konnte der Landesbeauftragte dem zuständigen Ministerium auf dessen Anfrage mitteilen, dass gegen die Verwendung keine datenschutzrechtlichen Bedenken bestehen.

20.8. Hospitation

Den Landesbeauftragten erreichte eine Anfrage zur Hospitation eines Stadtrates im Unterricht einer Sekundarschule.

Dazu war zunächst festzustellen, dass durch die Hospitation personenbezogene Daten zu den beteiligten Schülerinnen und Schülern und Lehrkräften an die hospitierende Person übermittelt werden. Dafür ist eine Rechtsgrundlage bzw. die Einwilligung der Betroffenen notwendig (§ 4 Abs. 1 DSG-LSA).

Für die Eltern gibt es aufgrund der verfassungsrechtlichen Position eine schulgesetzliche Grundlage zur Hospitation (§ 59 Abs. 6 SchulG LSA).

Eine spezialgesetzliche Regelung für die Hospitation von Stadträten, die nicht Eltern eines der betroffenen Schüler sind, war jedoch nicht ersichtlich.
Eine kommunalrechtliche Hospitationsbefugnis ist auch aus der Gemeindeordnung nicht abzuleiten. Die Informationsansprüche des Stadtrates auf

der Grundlage des § 44 Abs. 6 GO LSA beziehen sich zwar auf einzelne Angelegenheiten der Gemeinde. Schulträger der Sekundarschulen sind gemäß § 65 Abs. 2 Satz 1 SchulG LSA die Landkreise und kreisfreien Städte. Eine Stadt kann ggf. gemäß § 65 Abs. 3 SchulG LSA die Schulträgerschaft übertragen erhalten. Die Schulträgerschaft umfasst jedoch nur Aufgaben der Vorhaltung des Schulangebots und der Schulanlagen (im Einzelnen § 64 SchulG LSA). Die inhaltlichen Aufgaben der Unterrichtsmethodik und der Beobachtung und Steuerung des Sozialverhaltens obliegen jedoch im Rahmen der Vorgaben der Schule § 10 SchulG LSA i. V. m. § 24 SchulG LSA. Die Entscheidungen werden von der Schulleitung bzw. den Konferenzen (§ 25 SchulG LSA) getroffen. Die inhaltliche Beobachtung des Schulunterrichts gehört damit nicht zum Informationsgegenstand des Stadtrates nach § 44 Abs. 6 GO LSA. Das schulpolitische Interesse eines Stadtrates korrespondiert daher nicht mit den Aufgaben einer Stadt als Schulträger.

Mangels entsprechender Zuständigkeiten eines Stadtrates in seiner öffentlich-rechtlichen Funktion kam auch eine Übermittlung auf der allgemeinen Grundlage des § 84a Abs. 2 SchulG LSA i. V. m. § 11 Abs. 1 DSG-LSA nicht in Betracht.

Der mit der Hospitation einhergehende Datenfluss begegnete auch auf der Grundlage des § 84a Abs. 2 SchulG LSA i. V. m. § 12 Abs. 1 Nr. 2 DSG-LSA Bedenken. Zwar könnte der schulpolitische Informationsbedarf ggf. bei entsprechender Darlegung als berechtigtes Interesse des Stadtrates gewertet werden. Es dürften jedoch die schutzwürdigen Interessen der betroffenen Schülerinnen und Schüler und Lehrkräfte - schon zahlenmäßig - einer Übermittlung entgegenstehen.

Eine Hospitation war daher nur mit Einwilligung der betroffenen Schüler (bzw. Erziehungsberechtigten) und Lehrer möglich.

20.9. Ersatzschulverordnung

Das zuständige Ministerium gab dem Landesbeauftragten Gelegenheit, zum Entwurf der Ersatzschulverordnung (ESch-VO) eine Stellungnahme einzureichen. Der Landesbeauftragte wies auf einige datenschutzrechtlich fragwürdige Aspekte hin, die überwiegend jedoch nicht berücksichtigt wurden.

In den notwendigen Angaben im Antrag zur Genehmigung des Betriebs war unter anderem für Schulleitung und Lehrkräfte die Angabe der Staatsangehörigkeit vorgesehen. Die Erforderlichkeit der Abfrage einer konkreten Staatsangehörigkeit als Voraussetzung der Genehmigung einer Ersatzschule oder gar als Versagungsgrund erscheint im Hinblick auf die Voraussetzungen nach § 16 SchulG LSA fraglich.

Dem Antrag zur Genehmigung war u. a. der Gesellschaftsvertrag der Träger beizufügen. Aus dem Vertragswerk dürften sicher einige Aspekte genehmigungsrelevant sein (z. B. Hinweise zu Bildungs-, Ausbildungs- und Erziehungszielen, Gestaltung der zu tragenden Schule, besondere pädagogische, religiöse oder weltanschauliche Prägung). Andererseits kann ein Gesellschaftsvertrag vielfältige Beziehungen aus dem persönlichen Bereich bzw. im

Bereich von Betriebs- und Geschäftsgeheimnissen regeln, die nicht genehmigungsrelevant sind. Im Hinblick auf die Verhältnismäßigkeit wurde eine Prüfung angeregt. Alternativ könnten die Informationen, die für die Genehmigung gebraucht werden, konkret bezeichnet und abgefragt werden. Der Nachweis könnte dann ggf. (neben anderen Möglichkeiten) durch Vorlage von Auszügen aus dem Gesellschaftsvertrag erfolgen. An die Möglichkeit der Schwärzung nicht erforderlicher Informationen sollte gedacht werden.

Die Erforderlichkeit der Beifügung aktueller Arbeitsverträge (mit ggf. persönlichen Informationen wie Schwerbehinderung) zum Antrag auf Anerkennung als Ersatzschule erschien fraglich, da die fachliche Qualifikation der Leiter und Lehrkräfte dann bereits nachgewiesen ist, die Muster der Verträge mit dem Lehrpersonal vorliegen und wesentliche Änderungen bei Arbeitsverträgen anzuzeigen gewesen wären.

Auch die Notwendigkeit der Erhebung von personenbezogenen Daten durch die Vorlage von Schulverträgen erschien fraglich. Weder die Gewähr für das dauernde Erfüllen der Genehmigungsvoraussetzungen noch die nähere Bestimmung der Anerkennungsvoraussetzungen legen den Bedarf an personenbezogenen Informationen über Zahlen hinaus nahe. Dies wurde aufgegriffen. In § 6 Abs. 3 Nr. 4 ESch-VO vom 16. Dezember 2008 ist nun vorgesehen, dem Antrag lediglich die Muster der Schulverträge beizufügen.

§ 9 Abs. 5 ESch-VO begegnete insoweit Bedenken, als Schülerlisten und Klassenlisten dem Landesverwaltungsamt für die abschließende Festsetzung der Finanzhilfe nach Abschluss des Schuljahres und nicht erst für eine Prüfung im Einzelfall vorliegen müssen.
Nach § 18a Abs. 1 SchulG LSA richtet sich der Zuschuss der Finanzhilfe nach der Zahl der Schülerinnen und Schüler. Gemäß § 18a Abs. 8 Nr. 2 SchulG LSA enthält die Verordnung Bestimmungen über das Antragsverfahren, wozu auch die Ermittlung der zu berücksichtigenden Zahl gehört. Auch die Materialien zur gesetzlichen Regelung stellen nur auf die Ermittlung der einzubeziehenden Schüler ab, wozu Stichtage einzuführen seien. Die abschließende Bestimmung des Umfangs der Verordnung wird betont. Eine Abkehr von der rein zahlenmäßigen Errechnung ohne personenbezogene Benennung der Schülerinnen und Schüler liegt damit nicht vor. Die Regelung der Erhebung personenbezogener Schülerdaten in Schülerlisten bereits für die Festsetzung des Zuschusses entbehrt daher wohl einer hinreichenden gesetzlichen Grundlage.

Auch aus einer grundsätzlich notwendigen Prüfung der Abrechnungen dürfte keine Grundlage folgen, die schon eine personenbezogene Vorlage zur Festsetzung gestattet. Zwar bestehen gegen haushaltsrechtlich vorgegebene und wirksame Kontrollen keine Bedenken. Nachweise für den Zuschuss stehen nach § 18a Abs. 8 Nr. 12 SchulG LSA jedoch im Zusammenhang mit der Verwendungsprüfung. Eine wirksame Prüfung, die haushaltsrechtlichen Anforderungen entspricht, dürfte zudem stets auch einen Abgleich vor Ort notwendig machen (unter anderem Prüfung anhand der zunächst nicht vorliegenden aktuellen Schulverträge, ob die Schüler in den jeweils berechneten Monaten tatsächlich nach der Vertragslage auch anwesend waren). Die Schulträger sind verpflichtet, Schülerlisten aufzubewahren (§ 11 Abs. 7). Ab-

rechnungsangaben, Schülerliste und Verträge lassen sich vor Ort dann abgleichen.

21. Sozialwesen

21.1. Arbeitslosengeld II

Bereits im VII. Tätigkeitsbericht (Ziff. 20.1) und im VIII. Tätigkeitsbericht (Ziff. 20.3 - 20.5) hat der Landesbeauftragte zur Entwicklung im Bereich des SGB II Stellung genommen.

Einer der Problemkreise betraf die Antragsvordrucke und Ausfüllhinweise, die von der Bundesagentur für Arbeit entwickelt werden. Sie dienen den vom Landesbeauftragten datenschutzrechtlich zu kontrollierenden Arbeitsgemeinschaften (ARGEn) als Arbeitsgrundlage. Vor der Veröffentlichung gibt die Bundesagentur dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Gelegenheit zur Stellungnahme. Der Bundesbeauftragte beteiligt seinerseits die Landesbeauftragten für den Datenschutz. So konnte auch der Landesbeauftragte die Möglichkeit nutzen und sich mit Anregungen gegenüber dem Bundesbeauftragten an der datenschutzrechtlichen Optimierung der Antragsvordrucke beteiligen. Der Bundesbeauftragte koordiniert dann die Hinweise und wirkt gegenüber der Bundesagentur auf die datenschutzkonforme Ausgestaltung hin.

Weiter war die Problematik der Umsetzung der Datenschutzkontrolle bei den ARGEn erörtert worden, die auf der besonderen Konstruktion der ARGEn nach § 44b SGB II und der Zuständigkeitsregelung in § 50 Abs. 2 SGB II basierte. Infolge der bestehenden Rechtsunsicherheit wurde die grundsätzliche Kontrollzuständigkeit der Landesbeauftragten bei den ARGEn zwischen Bundesministerium, Bundesagentur und Datenschutzbeauftragten einvernehmlich festgelegt. Danach bezog sich die Kontrollkompetenz auf alle Leistungen der ARGEn. Der Bundesbeauftragte war dagegen für die zentralen IT-Verfahren der Bundesagentur zuständig. Die ARGEn wurden darauf hingewiesen. Im Berichtszeitraum hatte der Landesbeauftragte daher bei der Umsetzung der Datenschutzkontrollen vor Ort keine Schwierigkeiten.

Mit Urteil vom 20. Dezember 2007 hat das Bundesverfassungsgericht die durch § 44b SGB II vorgegebene Mischstruktur der ARGEn, mit der die Aufgaben der beiden Träger für Grundsicherung (Bund, kommunale Träger) einheitlich wahrgenommen werden, für mit der Verfassung nicht vereinbar erklärt (BVerfG, Urteil vom 20. Dezember 2007, 2 BvR 2433, 2434/04; NVwZ 2008, 183). Durch die organisatorische und personelle Verflechtung sei eine eindeutige Zuordnung des staatlichen Handelns zu einem der Leistungsträger nicht möglich. Bis Ende 2010 müsse daher eine Neuregelung erfolgen.
Die Einrichtung von „Zentren für Arbeit und Grundsicherung“ auf der Grundlage einer Verfassungsänderung wird seither politisch kontrovers diskutiert.

21.2. Kontroll- und Beratungsbesuche in Arbeitsgemeinschaften (ARGEn)

Auch im vergangenen Berichtszeitraum hat der Landesbeauftragte bei den ARGEn vor Ort Beratungen und Kontrollen durchgeführt. Beratungen betreffen zumeist Einzelfälle. Kontrollen hat der Landesbeauftragte in der Regel fallunabhängig durchgeführt, um sich allgemein einen Überblick über das Datenschutzniveau in den ARGEn zu verschaffen.

Grundsätzlich kann davon ausgegangen werden, dass die ARGEn und auch die Optionskommunen nach § 6a SGB II datenschutzkonform verfahren. Offensichtliche Mängel wurden während der Überprüfungen nicht festgestellt. Lediglich in Einzelfällen bedurfte es der Vermittlung bzw. Beratung durch den Landesbeauftragten. Insbesondere bei den von den ARGEn bzw. Optionskommunen erstellten eigenen Vordrucken war gelegentlich noch Klärungs- bzw. Erörterungsbedarf gegeben.

21.3. Anforderung von Kontoauszügen

Bereits im VIII. Tätigkeitsbericht (Ziff. 20.2) hat der Landesbeauftragte die Anforderung von Kontoauszügen bei der Bearbeitung von Anträgen auf Sozialleistungen problematisiert und auf die von mehreren Landesbeauftragten entwickelten Empfehlungen zur Vorlage von Kontoauszügen hingewiesen. Diese Empfehlungen können auf der Homepage des Landesbeauftragten unter „Service“ eingesehen werden.

Die Problematik prägte auch im Berichtszeitraum mehrere Beratungen und Eingaben. Ein Petent machte sich sogar die Mühe, eine Vielzahl von Gerichtsentscheidungen zu zitieren, nach denen die Anforderung von Kontoauszügen der letzten drei Monate ohne Begründung rechtswidrig sei, wenn der Antragsteller im Antragsformular alle für die Bearbeitung notwendigen Angaben gemacht habe und keine Anhaltspunkte für die Unrichtigkeit der Angaben bestünden. Weitere Entscheidungen besagten, dass zumindest die Speicherung von Kontendaten rechtswidrig und unzulässig sei. Eine obergerichtliche Entscheidung gehe sogar davon aus, dass der Antragsteller nicht einmal zur Vorlage verpflichtet sei, wenn das Antragsformular vollständig ausgefüllt ist.

Die Rechtsprechung war im Zusammenhang mit der Einsicht in und Speicherung von Kontoauszügen bisher nicht einheitlich. Bei der Bewertung ist zu berücksichtigen, dass die Leistungsträger grundsätzlich infolge der Amtsermittlung gehalten sind, den Sachverhalt aufzuklären (§ 20 SGB X) und der Antragsteller grundsätzlich im Rahmen der Mitwirkung verpflichtet ist, die erforderlichen Mitteilungen zu machen und die Beweismittel zu bezeichnen und vorzulegen (§ 60 Abs. 1 SGB I). Dies steht allerdings unter dem Vorbehalt der Vorschriften über die Zulässigkeit der Erhebung von Sozialdaten (§ 37 Satz 3 SGB I) und damit der Erforderlichkeit.

Die Erhebung personenbezogener Sozialdaten insbesondere durch die Abforderung von Kontoauszügen ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung (Art. 6 Abs. 1 der Landesverfassung bzw. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG). Sie ist auf der Grundlage des § 51b Abs. 1

Satz 1 Nr. 1 SGB II bzw. § 67a Abs. 1 SGB X zulässig zur Durchführung der anstehenden Aufgaben. Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gestattet dabei jedoch nur das unerlässlich Notwendige.
Besonders zu beachten ist, dass die Verpflichtung Betroffener zur Vorlage von Kontoauszügen gemäß § 60 SGB I noch keine Befugnis zur Speicherung dieser Daten darstellt. Nach § 67c Abs. 1 Satz 1 SGB X steht auch das Speichern abermals unter dem Vorbehalt, dass es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden gesetzlichen Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind.

Mit den o. g. Regelungen macht der Gesetzgeber deutlich, dass er das nachvollziehbare und auch haushaltsrechtlich gebotene Anliegen respektiert, bei der Ausreichung von öffentlichen Mitteln für Sozialleistungen in angemessenem Umfang nachzuprüfen, ob die Auszahlungsvoraussetzungen tatsächlich vorliegen. Konkret gebotene Nachweisprüfungen zur Abwehr von Schäden für öffentliche Haushalte und zur Vermeidung von Missbrauch sind daher nicht zu beanstanden.

Die Einsicht in Kontoauszüge zu einem aussagefähig kurzen - nicht historischen - Zeitraum ist daher grundsätzlich vertretbar. Aktuelle Kontoauszüge dokumentieren den Vermögensstand und die Ein- und Ausgabeverhältnisse zwecks Prüfung von Vermögen und Einkommen. Dabei sind nicht nur auffällig große Summen, sondern oftmals auch kleine, ggf. aber regelmäßige Beträge von Bedeutung, da sie Anlass geben können, im Hinblick auf Vermögensgegenstände bzw. Ansprüche Nachfragen zu stellen. Andererseits sind bloße Informationen zum Ausgabeverhalten, beispielsweise zu Abonnements im Medienbereich oder zu Beiträgen zu einer konkreten Partei oder Gewerkschaft für die Entscheidung unerheblich. Sie dürfen nicht erhoben werden, die Angaben können grundsätzlich geschwärzt werden. Hierauf sind die Antragsteller hinzuweisen. Vollkontrollen sind stets unangemessen.

Da Kontoauszüge regelmäßig eine Vielzahl von Kontobewegungen enthalten, die für die Feststellung des Bedarfs von Betroffenen nicht relevant sind, ist eine Speicherung dieser Daten grundsätzlich bedenklich. Insbesondere ist eine Speicherung nicht schon deshalb gerechtfertigt, weil nachgewiesen werden soll, dass die Belege vorgelegen haben. Insoweit reicht regelmäßig ein Sachbearbeitungsvermerk. Vielmehr dürfen die Daten nur dann gespeichert werden, wenn diese zur Aufgabenerfüllung im Einzelfall erforderlich sind. Ein vager Verdachtsmoment oder geringfügige Auffälligkeiten reichen grundsätzlich nicht aus, Kontoauszüge zur Akte zu nehmen. Nur wenn im Einzelfall ein begründeter Anlass besteht, beispielsweise um Bedenken nachzugehen, können Speicherungen nötig sein. Wie schon vor der Einsicht gilt hier insbesondere die Notwendigkeit, dem Betroffenen Gelegenheit zur Schwärzung der nicht erforderlichen Informationen zu geben.

Letztendlich darf auch das Kopieren kompletter Kontoauszüge wegen des Arbeitsanfalls an Sprechtagen kein regelmäßiger Speicherungsgrund sein, sondern muss auf extrem seltene Ausnahmen beschränkt bleiben. Das vorsorgliche Kopieren und Abheften führt zu - teilweise - unzulässiger, da nicht erforderlicher Datenerhebung und -speicherung.

Die oben genannten Empfehlungen bleiben grundsätzlich auch für die Vorlage von Kontoauszügen bei Fortzahlungsanträgen bestehen. Die Vorgabe, erst nach einem Hilfezeitraum von mindestens 12 Monaten Auszüge für nur 6 Monate (bzw. nach 6 Monaten für 3 Monate) zu fordern, dient dem Zweck, dass gerade eine Vollkontrolle (Vorlage sämtlicher Kontoauszüge) aus Gründen der Verhältnismäßigkeit vermieden werden soll. Liegt dagegen ein konkreter Verdacht vor, bestehen keine Bedenken, diesen Sachverhalt unter Vorlage von Kontoauszügen zu klären. Mit dem Argument, dass Betroffene „möglicherweise etwas vergessen“ haben könnten, ist allerdings eine Intensivierung der Überwachung nicht zu begründen.

Solche Maßstäbe ergeben sich insoweit nunmehr auch aus der Entscheidung des Bundessozialgerichts vom 19. September 2008 (B 14 AS 45/07 R, NZS 2008, XVIII). Wer Sozialleistungen nach dem SGB II beantragt oder erhält, ist grundsätzlich verpflichtet, eine Kontenübersicht und Kontoauszüge (im vorliegenden Fall: für die letzten drei Monate) vorzulegen. Diese Pflicht ist nicht auf Verdachtsfälle beschränkt. Auch die Regelungen über den Sozialdatenschutz schränken die Vorlagepflicht nicht ein. Dem Leistungsempfänger ist nach der Entscheidung aber die Möglichkeit einzuräumen, auf der Ausgabenseite die Empfänger von Zahlungen zu schwärzen oder unkenntlich zu machen, wenn die Zahlungen besondere personenbezogene Daten betreffen; die überwiesenen Beträge müssen dennoch für den Grundsicherungsträger erkennbar bleiben.

21.4. Erhebung von Sozialdaten des Ehepartners

Eine Petentin machte den Landesbeauftragten darauf aufmerksam, dass ihr eine ARGE ein Formular „Arbeitspaket zur Vorbereitung eines Integrationsgespräches“ übergeben hatte, obwohl lediglich ihr Ehemann Leistungen der Grundsicherung für Arbeitssuchende erhalte und sie selbst versicherungspflichtig beschäftigt sei.

Das SGB II geht von der spezifischen Konstruktion der Bedarfsgemeinschaft aus. Es kommt auf den Gesamtbedarf der Bedarfsgemeinschaft an. Nach § 7 Abs. 3 Nr. 1 und Nr. 3. a) SGB II bildete die Petentin mit ihrem Ehemann als erwerbsfähigem Hilfebedürftigen eine Bedarfsgemeinschaft. Grundsätzlich ist im Rahmen der Vollmachtsvermutung in § 38 SGB II, soweit abweichende Anhaltspunkte nicht entgegenstehen, der „Hauptleistungsberechtigte“ befugt, Leistungen für die mit ihm in einer Bedarfsgemeinschaft lebenden Personen zu beantragen und in Empfang zu nehmen.

Folgerichtig erhält die Petentin gemäß § 7 Abs. 2 SGB II als Mitglied der Bedarfsgemeinschaft ebenfalls Leistungen nach § 4 SGB II. Dies können sowohl Geldleistungen gemäß § 4 Abs. 1 Nr. 2 SGB II als auch beispielsweise Dienstleistungen nach § 4 Abs. 1 Nr. 1 SGB II sein. Unter Dienstleistungen sind Information, Beratung und umfassende Unterstützung mit dem vorrangigen Ziel der Beendigung oder Verringerung der Hilfebedürftigkeit der gesamten Bedarfsgemeinschaft zu verstehen. Die Bestimmung der Leistungsart erfolgt im Rahmen pflichtgemäßer Ermessensausübung auf Grundlage der Eingliederungsvereinbarung (§§ 3, 15, 16 SGB II) durch die ARGE. Infolge-

dessen war die ARGE grundsätzlich zu erforderlichen Datenerhebungen berechtigt.

Während der „Teil 1 - Persönliche Daten“ des Arbeitspakets allgemein der Erfassung von Sozialdaten nach § 51b Abs. 1 Nr. 1 i. V. m. Absatz 2 Nr. 4 SGB II (u. a. für statistische Zwecke) dient, wird „Teil 2 - Vorbereitung Vermittlungsgespräch“ als Grundlage für ein Integrationsgespräch mit den einzelnen Mitgliedern der Bedarfsgemeinschaft verwendet.

Die konkrete Anforderung u. a. auch kompletter Bewerbungsunterlagen war aber datenschutzrechtlich problematisch. Nach Information der Bundesagentur für Arbeit steht der ARGE die Nutzung des Arbeitspakets im Rahmen der Umsetzungsverantwortung frei.
Es ist bereits schwer, Arbeitslose einzugliedern. Daher wäre es wohl kaum darstellbar, besonderen Aufwand für die Vermittlung von versicherungspflichtig beschäftigten Bedarfsgemeinschaftsmitgliedern zu betreiben. Im Rahmen des verhältnismäßigen Vorgehens dürfen daher allenfalls sehr wenige Informationen zur Klärung des Sachverhalts erhoben werden (qualifikationsangemessene Beschäftigung). Dabei ist zu berücksichtigen, ob tatsächlich beabsichtigt ist, die Vermittlung auch von Beschäftigten durchzuführen.

Im Beratungsgespräch mit der ARGE konnte der Landesbeauftragte erreichen, dass künftig Hinweise zum Arbeitspaket erarbeitet werden, die den Mitgliedern der Bedarfsgemeinschaft im Rahmen der Neuantragstellung zusammen mit dem Arbeitspaket zur Verfügung zu stellen sind. Mit ihnen soll dargelegt werden, aus welchen Gründen die ARGE die Informationen benötigt. Die ARGE hat ihr Verfahren unter Berücksichtigung der Hinweise angepasst. Insbesondere bei Betroffenen, die einer Berufstätigkeit nachgehen, ist der „Teil 2 – Vorbereitung Vermittlungsgespräch“ des Arbeitspakets zunächst nicht auszufüllen.

21.5. Löschung der Telefonnummer

Ein Petent beklagte sich darüber, dass ein Leistungsträger nach dem Zweiten Buch Sozialgesetzbuch (SGB II) eine von ihm freiwillig angegebene Telefonnummer nicht nach § 84 Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) löschen wollte, da der Leistungsträger die Auffassung vertrat, dass die Speicherung der Telefonnummer für die Erfüllung der Aufgaben nach dem SGB II, insbesondere für die Eingliederung in Arbeit, erforderlich sei. Eine effektive Vermittlung sei zum größten Teil nur kurzfristig möglich und könne in diesen Fällen nur über eine telefonische Kontaktaufnahme realisiert werden.

Nach intensiven Bemühungen des Landesbeauftragten hatte der zuständige Leistungsträger den Bescheid zurückgenommen und die Löschung der Telefonnummer veranlasst.
Insbesondere konnte dem Leistungsträger verdeutlicht werden, dass die Erhebung von Sozialdaten nur dann zulässig ist, wenn die Voraussetzungen des § 67a SGB X erfüllt sind. Betroffene haben nach § 35 Erstes Buch Sozialgesetzbuch einen Anspruch darauf, dass die sie betreffenden Sozialdaten nach § 67 Abs. 1 SGB X von Leistungsträgern nicht unbefugt verarbeitet werden.

Der Argumentation des Leistungsträgers, dass die im Antrag des Betroffenen freiwillig angegebene Telefonnummer über das Internet und das örtliche Telefonbuch abrufbar sei, begründet jedoch nicht die Zulässigkeit der Erhebung der Telefonnummer. Grundsätzlich sind Sozialdaten gemäß § 67a Abs. 2 Satz 1 SGB X beim Betroffenen zu erheben. Darüber hinaus hatte der Landesbeauftragte aufgrund eigener Recherchen festgestellt, dass die Telefonnummer des Petenten gerade nicht über das Internet verfügbar war.

Den Bedenken des Leistungsträgers, dass durch Löschung der Telefonnummer die Akte manipuliert werde, konnte nicht gefolgt werden. Nach § 84 Abs. 2 Satz 1 SGB X sind Sozialdaten zu löschen, wenn ihre Speicherung unzulässig ist. Es wurde jedoch der Hinweis gegeben, in der Akte zu dokumentieren, dass die Telefonnummer nach § 84 Abs. 2 Satz 1 SGB X gelöscht wurde.

Letztendlich sieht auch die Erreichbarkeits-Anordnung der Bundesagentur für Arbeit wegen der Pflicht, Vorschlägen zur beruflichen Eingliederung zeit- und ortsnah Folge leisten zu können, lediglich die Erreichbarkeit durch Briefpost vor (§ 1 Abs. 1 Satz 2). In der Regel kann davon ausgegangen werden, dass Briefe die Betroffenen nach 1 bis 3 Tagen erreichen.

Dem Anliegen des Petenten konnte damit Rechnung getragen werden.

21.6. Grundsicherung für Selbständige

Generell wird mit jedem erwerbsfähigen Hilfebedürftigen eine Eingliederungsvereinbarung nach § 15 SGB II abgeschlossen. Zu den Erwerbsfähigen in § 7 Abs. 1 Nr. 2 SGB II zählen sowohl Arbeitnehmer als auch Selbständige. Für die Erhebung der Daten wird für Selbständige ein Formular mit Basisinformation verwendet. Dies wäre nach § 51b Abs. 1 Satz 1 Nr. 1 und 2, Abs. 2 SGB II bzw. § 67 a SGB X im Rahmen des Erforderlichen grundsätzlich zulässig. Regelungen zum Datenumfang enthält § 51b Abs. 2 SGB II.
Die nach dieser Regelung vorgesehene Datenerhebung ist sehr weitgehend. Der Fallmanager soll allein aufgrund des Datenbestandes in die Lage versetzt werden, die bisherigen Betreuungs- und Eingliederungsmaßnahmen und die Beschäftigungsverhältnisse des Erwerbsfähigen bei seinen Entscheidungen über die weitere Betreuung zu berücksichtigen.
Ein bei einer Prüfung bekannt gewordener Basisfragebogen stellte jedoch darüber hinaus kritische Fragen: „Wie zufrieden bin ich mit meiner derzeitigen Situation?“, „Konnte ich die letzte Frage sofort beantworten?“. „Schiebe ich Entscheidungen insgesamt lieber eine Weile vor mir her?“, „Wie reagiere ich, wenn ein Kunde kommt, um eine Reklamation auszusprechen?“ usw. Nach Angaben der geprüften ARGE sollte der Fragebogen dem für den jeweiligen betroffenen Leistungsbezieher zuständigen Fallmanager einen Eindruck darüber verschaffen, ob ihm weiterhin eine zum aktuellen Zeitpunkt unrentable, selbständige, gewerbliche Tätigkeit zugestanden werden soll.
Diese Vorgehensweise erscheint dann gerechtfertigt, wenn selbständige Gewerbe über einen längeren Zeitraum keine Gewinne erwirtschaften und vermieden werden soll, dass ein unrentables Gewerbe einer sinnvolleren Vermittlung in den Arbeitsmarkt entgegensteht. Insofern soll mit Hilfe des

Fragebogens geklärt werden, in welcher Form das ausgeübte Gewerbe strukturiert ist und welche Gründe einer wirtschaftlichen Ausübung entgegenstehen.

Der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit gestattet jedoch nur unerlässliche Datenerhebungen. Zulässige Recherchen im Fragebogen beziehen sich auf die künftige Einrichtung der gewerblichen Tätigkeit und ihre Rahmenbedingungen, also auf eine individuelle Chancen- und Risikoeinschätzung.

Einzelne Fragen im Basisfragebogen sind jedoch eher mittelbar ökonomisch orientiert und richten sich dem Schwerpunkt nach mehr auf Motivation und Empfinden und damit auf die Persönlichkeit des Antragstellers aus. Sie sind aus datenschutzrechtlicher Sicht bedenklich. Auch wenn die Bewertung der Persönlichkeit des Antragstellers als Kriterium des wirtschaftlichen Erfolges eine Rolle bei der Prognose spielen kann, sollten die externen Fakten im Vordergrund stehen.
Eine stärker sachlich-ökonomische Orientierung bzw. die Möglichkeit, einzelne unangenehme Fragen nicht beantworten zu müssen, könnte zudem der Akzeptanz bei den Betroffenen und damit der Effizienz dienen.

21.7. Angaben zum Leistungsbezug im Adressfeld von Briefsendungen

Eine Eingabe einer Petentin wies darauf hin, dass bei Briefsendungen einer ARGE regelmäßig im Brieffenster zu erkennen war, dass sie Leistungsbezieherin ist.

Die darauf angesprochene ARGE änderte ihr Formular so, dass ein Bezug zu Sozialdaten grundsätzlich auszuschließen bzw. bei der Falzung des Vordruckes der Bereich „Alg II-Bezieher“ im Briefkopffenster nicht mehr zu erkennen war.

Einige Monate später wandte sich die Petentin wieder an den Landesbeauftragten, da sie erneut Briefsendungen der ARGE mit dem Aufdruck zum Leistungsbezug erhielt. Der Landesbeauftragte suchte nunmehr das persönliche Gespräch mit der ARGE. In diesem Zusammenhang konnte festgestellt werden, dass eine Mitarbeiterin der ARGE den „alten“ Vordruck verwendet hatte.

Grundsätzlich hat der Sozialleistungsträger dafür Sorge zu tragen, dass die nach § 78a Zehntes Buch Sozialgesetzbuch (SGB X) i. V. m. der Anlage zu § 78a erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um zu verhindern, dass ein Datenträger (hier: Brief) von Unbefugten ganz oder teilweise gelesen werden kann (vgl. u. a. Ziffer 4 der Anlage zu § 78a SGB X).

Da durch die zweite Eingabe erkennbar war, dass die bisher getroffenen Maßnahmen nicht ausgereicht haben, hat die ARGE eine Dienstanweisung an die Mitarbeiterinnen und Mitarbeiter erlassen, die nunmehr den Postversand von Formularen beschreibt. Künftig wird ein Vorblatt als Adressblatt verwendet.

21.8. Netzwerk bei Projekt „Zukunftswerkstatt 50plus“

In einer Eingabe beklagte sich ein Betroffener über den Druck durch eine ARGE, die Zuwendungen zu kürzen, wenn keine hinreichende Mitwirkung erfolge. Der Betroffene war nicht damit einverstanden, dass seine sämtlichen vermittlungsrelevanten Daten in ein regionales Netzwerk eingestellt werden.

Gegen das Vorgehen der ARGE bestanden zumindest im Ergebnis keine grundsätzlichen datenschutzrechtlichen Bedenken. Sie hatte dargelegt, dass ein Bildungsträger als Projektleitung beauftragt war, in der dortigen Region das Projekt im Rahmen der Initiative Perspektive 50plus des Bundesministeriums für Arbeit und Soziales zu leiten. Die vertragliche Gestaltung zur Umsetzung der zweiten Programmphase dieses Bundesprogramms lag vor. Darin waren auch umfängliche datenschutzrechtliche Vorgaben enthalten. Der Projektträger arbeitete auf der Basis eines Zuwendungsbescheides mit weiteren notwendigen Kooperationspartnern zusammen, die insgesamt im Rahmen einer Netzwerkarbeit für die korrekte Umsetzung des Bundesprogramms tätig sind. Nach Darstellung der ARGE war die Weitergabe der personenbezogenen Daten innerhalb des Netzwerkes unabdingbare Voraussetzung im Rahmen der dem Konzept entsprechenden phasenweisen Prozessabläufe im Projekt „Zukunftswerkstatt 50plus“. Die Verarbeitung beziehe sich lediglich auf ausschließlich vermittlungsrelevante Daten. Im Hinblick auf die Verpflichtung zur Mitwirkung berief sich die ARGE auf § 38 SGB III, wonach Arbeitsuchende die für eine Vermittlung erforderlichen Auskünfte zu erteilen und Unterlagen vorzulegen haben.

Soweit tatsächlich lediglich die Daten verarbeitet werden, die für Vermittlungstätigkeiten unerlässlich sind, bestanden dagegen keine grundsätzlichen Bedenken. Sowohl nach § 6 Abs. 1 Satz 2 SGB II als auch nach § 37 Abs. 1 SGB III ist es gestattet, im Rahmen von Eingliederungs- und Vermittlungsleistungen der Sozialleistungsträger Dritte mit der Wahrnehmung von Aufgaben zu beauftragten. Eine Begrenzung auf einen einzelnen Dritten ist den Regelungen nicht zu entnehmen. Die verfassungsrechtlichen Grenzen der Erforderlichkeit und Verhältnismäßigkeit sind aber zu beachten.

Auch gegen die Übermittlung von personenbezogenen Daten von einem beteiligten Bildungsträger an einen anderen beteiligten Bildungsträger bestanden keine Bedenken. Hierzu war auf § 50 Abs. 1 SGB II zu verweisen, der u. a. für die an Leistungen des SGB II beteiligten Träger und die mit der Wahrnehmung von Aufgaben beauftragten Dritten eine Datenübermittlungsbefugnis schafft. Soweit dies zur Erfüllung der Aufgaben nach dem SGB II oder dem SGB III und damit auch für Vermittlungsaufgaben erforderlich ist, dürfen personenbezogene Daten übermittelt werden. Der Gesetzgeber bezieht damit auch die Dritten in den Aufgabenverbund mit ein.

Da somit eine gesetzliche Grundlage für die Übermittlung von personenbezogenen Daten der Betroffenen gegeben ist, war die Einholung einer Einwilligung genau genommen nicht erforderlich. Lediglich wenn Daten übermittelt werden sollen, die nicht zwingend erforderlich, aber ggf. für die Vermittlung nützlich sind, wäre die Einholung der Einwilligung der Betroffenen geboten.

Darüber hinaus wäre die Erteilung der Einwilligung des Betroffenen grundsätzlich dann erforderlich, wenn Daten nicht im Kreise der von § 50 Abs. 1 SGB II genannten, sondern an unbeteiligte Dritte übermittelt werden sollen. Hierfür besteht keine gesetzliche Grundlage. Dies dürfte auch der Anlass dafür sein, dass durch die Bildungsträger gern mit dem Instrument der Einwilligung gearbeitet wird. Es wurde jedoch gegenüber der ARGE angeregt, dort, wo auf gesetzlicher Grundlage Daten verarbeitet werden können, auf die Verwendung von Vordrucken zu verzichten, die durch den Bezug auf die Freiwilligkeit zu Missverständnissen führen.

21.9. Elektronischer Entgeltnachweis

Millionen Empfänger von Sozialleistungen erhalten von 2012 an nur noch mit einer elektronischen Unterschrift Geld vom Staat. Dieses Szenario verbirgt sich hinter dem Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz vom 28. März 2009, BGBl. I S. 634).
Zunächst wird das Verfahren für sechs Bescheinigungen aus den Bereichen Arbeitslosengeld I, Bundeselterngeld und Wohngeld Anwendung finden. Später sollen weitere Bescheinigungen und Nachweise nach dem Sozialgesetzbuch folgen.
Die Arbeitgeber sollen die Einkommensdaten ihrer Beschäftigten an eine zentrale Speicherstelle elektronisch übermitteln.
Bei einer Beantragung von Sozialleistungen können dann die entsprechenden Behörden unter Verwendung einer elektronischen Signaturkarte die Daten von der zentralen Speicherstelle elektronisch abfordern.
Dieses Verfahren bedeutet allerdings, dass Daten auf Vorrat gespeichert werden, ohne dass absehbar ist, ob und inwieweit sie jemals verwendet werden. Die Einkommensinformationen über denjenigen, der nie eine von den im Gesetz vorgesehenen Sozialleistungen beantragt, werden jahrelang nutzlos gespeichert. Zudem konnte die eher geringe Anzahl der Personen, die tatsächlich einen Antrag stellen, trotz mehrfacher Nachfrage von den Verantwortlichen nicht beziffert werden.
Nach Ansicht des Landesbeauftragten stellt dies einen unverhältnismäßigen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Zuletzt hat die 76. Konferenz der Datenschutzbeauftragten nochmals auf dieses Problem in ihrer Entschließung „Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren“ vom November 2008 hingewiesen **(Anlage 18).**
Besondere Brisanz erhält diese Datensammlung im Hinblick auf die Begehrlichkeiten, die bei Dritten geweckt werden. Zwar ist derzeit eine strenge Zweckbindung im Gesetz vorgesehen, aber Gesetze kann man, wie die Erfahrung zeigt, ändern.

21.10. Steuerungsprogramme der gesetzlichen Krankenversicherung

Die Reformen der gesetzlichen Krankenversicherung sollen u. a. über die Einführung von Wettbewerbsmechanismen zu mehr Qualität und Effizienz führen. Maßnahmenkomplexe finden sich u. a. auf dem Gebiet des Versorgungsmanagements, der Patientenschulung oder der strukturierten Behandlungsprogramme. Kernelement der Maßnahmen ist die Freiwilligkeit. Dies umfasst auch die Beteiligung privater Dienstleister bei der Umsetzung der Maßnahmen. Hierfür ist die vorherige Einwilligung der Versicherten einzuho-

len. Ferner darf die Krankenkasse nur Daten für die Gewinnung der Versicherten verwenden, wenn dies ausdrücklich gesetzlich vorgesehen ist. Hierzu hat die 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder die Entschließung „Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten“ gefasst **(Anlage 21).**

21.11. Beeinflussung von Patienten

Durch eine Eingabe erhielt der Landesbeauftragte Hinweise, dass eine Krankenkasse nach Auffassung von Patienten deren Daten verwende, um sie hinsichtlich ihres Nutzungsverhaltens zu beeinflussen. So habe ein Patient besondere Mischspritzen benötigt. Der Patient habe sich an die Krankenkasse gewandt, die die Spritzen für zu teuer befand. Wenn der Patient allerdings bei einer bestimmten Apotheke einkaufe, wäre das Medikament billiger und der Patient könne es erhalten. Eine andere Patientin wies darauf hin, dass sie von einer Mitarbeiterin der Krankenkasse besucht worden sei. Diese habe Kopien der bisherigen Rezepte dabei gehabt, auf die hohen Kosten verwiesen, hohe Zuzahlungen thematisiert und mitgeteilt, dass die Krankenkasse beschlossen habe, die Medikamente seien jetzt von einer Sammelstelle (der auch im vorigen Fall benannten Apotheke) zu beziehen.

Zunächst hatte der Landesbeauftragte den Petenten erläutert, dass sich Fragen des Anspruchs der Versicherten auf Versorgung mit bestimmten Medikamenten und durch bestimmte Leistungserbringer einer datenschutzrechtlichen Bewertung entziehen. Eher problematisch wäre die abgenötigte Offenbarung sensibler Daten gegenüber einer bestimmten Apotheke.

Aus datenschutzrechtlicher Sicht fraglich war aber die Nutzung von bei der Krankenkasse vorliegenden Abrechnungsinformationen in Gesprächen mit den einzelnen Mitgliedern. Rechtsgrundlage für die Nutzung der im Wege der Arzneimittelabrechnung nach § 300 SGB V erhaltenen Informationen ist die Regelung des § 284 Abs. 3 SGB V. Danach dürfen die rechtmäßig erhobenen und gespeicherten versichertenbezogenen Daten für Zwecke der Aufgaben nach Abs. 1 des § 284 SGB V im jeweils erforderlichen Umfang verarbeitet und genutzt werden. Damit ist eine abschließende Zweckbindung vorgegeben. Zu den Aufgaben des Abs. 1 gehören nach Nr. 4 die Prüfung der Leistungspflicht und der Erbringung von Leistungen an Versicherte, die Bestimmung des Zuzahlungsstatus und die Durchführung der Verfahren bei der Kostenerstattung, Beitragsrückzahlung und der Ermittlung der Belastungsgrenze sowie nach Nr. 9 die Überwachung der Wirtschaftlichkeit der Leistungserbringung. Daher kann es unter Umständen zulässig sein, mit Mitgliedern Einzelfragen aus dem Aufgabenkanon des § 284 Abs. 1 SGB V unter Verwendung von einzelnen Abrechnungsinformationen zu erörtern.

Demgemäß hat die Krankenkasse darauf hingewiesen, dass Mitarbeiter gelegentlich Versicherte nach vorheriger Abstimmung aufsuchen. Die Aufgaben dienen der Erfüllung des gesetzlichen Auftrages zur Information, Beratung und Aufklärung. Gesprächsthema kann beispielsweise die Frage nach der Zuzahlung sein. Dabei ist die sog. Belastungsgrenze zu berücksichtigen (§ 62 i. V. m. § 61 SGB V). Für die Frage der Ermittlung der Belastungsgrenze der jeweiligen Versicherten müssen neben den Bruttoeinnahmen auch die

zu leistenden Zuzahlungen geprüft werden. Deshalb kann es erforderlich sein, dass den jeweiligen Versicherten betreffende Aufkommen an zuzahlungspflichtigen Leistungen zu betrachten. Demgemäß könnte es auch notwendig erscheinen, in diesem Zusammenhang auf den bisherigen Verordnungsstand zurückzugreifen.

Grundsätzlich ging jedoch auch die Krankenkasse davon aus, dass das umfängliche Mitführen von tatsächlichen Verordnungen beim Besuch beim Versicherten als Fehlverhalten anzusehen sei. Es dürfte sich bei den Beschwerdefällen um Missverständnisse zwischen dem Versicherten und dem Mitarbeiter gehandelt haben. Die Krankenkasse habe gegenüber den in den entsprechenden Bereichen tätigen Mitarbeitern klargestellt, dass medizinische Verordnungen nicht zu Beratungszwecken genutzt werden sollen. Weiterhin hat die Krankenkasse mitgeteilt, dass sie die freie Wahl des Versicherten unter den Apotheken nach § 31 Abs. 1 Satz 4 SGB V respektiere.

21.12. Landesrechnungshof und Landesprüfungsamt

Der Landesrechnungshof beabsichtigte, die Aktivitäten des Landesprüfungsamts für Sozialversicherung zu untersuchen. Dazu erschienen ihm dessen Prüfberichte von Bedeutung. Sie wurden ihm jedoch zunächst vorenthalten. Das zuständige Ministerium war der Auffassung, dass datenschutzrechtliche Erwägungen der Aushändigung der Prüfberichte entgegenstünden. Das Landesprüfungsamt prüfe z. B. Geschäftsunterlagen der Krankenkassen, die sich im Wettbewerb mit anderen Kassen befänden (vgl. § 274 Abs. 1 SGB V). Zudem wären in den Prüfberichten auch Sozialdaten der Versicherten enthalten. Solange es um Prüfungsgegenstand und -umfang gehe, müssten Inhaltsverzeichnisse der Berichte und Prüfungshandbücher in Sinne der Datensparsamkeit ausreichen. Demgegenüber verwies der Landesrechnungshof auf seinen verfassungsrechtlichen und gesetzlichen Prüfungsauftrag, der ihm die Entscheidung gewähre, welche Unterlagen zu Prüfungen einzusehen seien.

Der Landesbeauftragte hat die Problematik mit dem Ministerium und dem Landesrechnungshof erörtert. Zunächst konnte er darauf hinweisen, dass er bereits im I. Tätigkeitsbericht (Ziff. 16.6) zur Prüfkompetenz des Landesrechnungshofs Ausführungen gemacht hat. Danach bestimmt der Landesrechnungshof die für die Erfüllung seiner unabhängigen und umfassenden Prüfaufgaben erforderlichen Unterlagen grundsätzlich selbst. Sie sind ihm gemäß § 95 Landeshaushaltsordnung vorzulegen. Andererseits ist auch der Landesrechnungshof an die verfassungsrechtlichen Vorgaben des Grundrechts auf informationelle Selbstbestimmung gebunden. Bei der Anforderung von Unterlagen mit personenbezogenen Informationen hat er daher den Verhältnismäßigkeitsgrundsatz, insbesondere das Übermaßverbot zu beachten.

Die umfassende Erörterung führte zu dem Ergebnis, dass das Ministerium seine Bedenken zurückstellte. Dabei wurde neben den vorgenannten Aspekten insbesondere berücksichtigt, dass auch der Sozialdatenschutz der Durchführung der Rechnungsprüfung - im erforderlichen Umfang - nicht entgegensteht. Aus § 69 Abs. 5 i. V. m. 67c Abs. 3 SGB X ergibt sich, dass die

Übermittlung von Sozialdaten für die Erfüllung der gesetzlichen Aufgaben der Rechnungshöfe zulässig ist.

21.13. Private Abrechnungsstellen

Eine besondere Betonung erfuhr der Sozialdatenschutz in der Entscheidung des Bundessozialgerichts (BSG) vom 10. Dezember 2008 (Az.: B 6 KA 37/07 R). Dort wurde festgestellt, dass es einer Kassenärztlichen Vereinigung (KV) gestattet ist, die Abrechnung eines an der vertragsärztlichen Versorgung teilnehmenden Krankenhauses zu verweigern, wenn sich das Krankenhaus einer privaten Abrechnungsstelle bedient hat. Die KV hatte mit den Verbänden der Krankenkassen einen Honorarverteilungsvertrag geschlossen, der vorsah, dass die Abrechnung persönlich zu erfolgen habe und eine Einschaltung von Dritten, insbesondere Verrechnungsstellen, unzulässig sei. Obwohl das Krankenhaus die Einwilligung der Patienten zur Einschaltung der Abrechnungsstelle einholte, sah das BSG dies als unzulässigen Verstoß gegen den Sozialdatenschutz an.

Durch die Einschaltung Dritter sei die Abrechnung „formal unrichtig“. Es fehle an der Rechtsgrundlage für die Übermittlung der Patientendaten durch das Krankenhaus an die Abrechnungsstelle, auch wenn der Patient eingewilligt habe. Die Entstehungsgeschichte der bereichsspezifischen datenschutzrechtlichen Regelungen im Sozialgesetzbuch und gerade in der gesetzlichen Krankenversicherung belege die hohe Bedeutung, die der Gesetzgeber dem Sozialdatenschutz zumesse. Anhand vieler in der Entscheidung aufgeführter Beispiele begründet das BSG den Grundsatz des „Verbots mit Erlaubnisvorbehalt“. Es werde wiederholt im Gesetz, in den Begründungen und den Materialien auch zu Gesetzesänderungen deutlich, dass die Befugnisse enumerativ aufgeführt seien. Für die Übermittlung von Patientendaten durch Leistungserbringer an externe Abrechnungsstellen fehle - von wenigen Ausnahmen abgesehen - die gesetzliche Grundlage. Die lediglich punktuellen und differenzierten Regelungen rechtfertigten den Schluss, dass die Datenweitergabe von Leistungserbringern im Übrigen nur an die Sozialleistungsträger (§ 35 SGB I) erfolgen dürfe.

Infolge des spezialgesetzlichen Ausschlusses sei auch nicht auf die Einwilligung des Patienten abzustellen. Zwar sähen auch §§ 67d i. V. m. 67b Abs. 1 SGB X eine Einwilligung als Ermächtigungsgrundlage vor. Dies betreffe aber nur die Stellen nach § 35 SGB I. Auch auf allgemeine datenschutzrechtliche Grundsätze könne nicht zurückgegriffen werden, da der Gesetzgeber nur in wenigen besonderen Fällen die Zulässigkeit einer auf Einwilligung gestützten Datenübermittlung durch Leistungserbringer ausdrücklich geregelt habe.

Aufgrund der prinzipiellen Aussagen zum Sozialdatenschutz stellt die Entscheidung über den Bereich der Abrechnung durch Leistungserbringer hinaus Maßstäbe zur Verfügung. Dies ist zu begrüßen, auch wenn die informationelle Selbstbestimmung in Gestalt des Einverständnisses betroffen ist. Grundsätzlich bedarf es des Schutzes der Versichertendaten durch gesetzliche Grundlagen, wo sie gezwungenermaßen in die gesetzliche Krankenversicherung einbezogen werden. Einwilligungen in Datenverarbeitungen sind nunmehr noch präziser zu prüfen. Gerade bei der Einschaltung externer Ab-

rechnungsstellen kann jedoch von einer freiwilligen Einwilligung in die Datenverarbeitung aufgrund der faktischen Verhältnisse ohnehin kaum ausgegangen werden.

21.14. Feuerwehr-Unfallkasse-Mitte

Nach der Fusion im Bereich der Rentenversicherung wurden auch die Feuerwehr-Unfallkassen der Länder Sachsen-Anhalt und Thüringen fusioniert. Die Feuerwehr-Unfallkasse Mitte hat ihren Sitz in Magdeburg. Sachsen-Anhalt ist als aufsichtsführendes Land bestimmt.
Dementsprechend ist der Landesbeauftragte für den Datenschutz Sachsen-Anhalt künftig für die Beratung und Kontrolle der Feuerwehr-Unfallkasse Mitte in datenschutzrechtlichen Fragen zuständig, auch für Petenteneingaben aus Thüringen.

21.15. Kinder- und Jugendhilfe

Wie bereits im VIII. Tätigkeitsbericht (Ziff. 20.19) beschrieben, werden derzeit auf Bundes- und Landesebene zahlreiche Möglichkeiten zur Vermeidung und besseren Erkennung von Kindeswohlgefährdungen diskutiert.

Auf Bundesebene ist diesbezüglich bereits das Gesetz zur Erleichterung familiengerichtlicher Maßnahmen bei Gefährdungen des Kindeswohls in Kraft getreten (BGBl. I 2008 S. 1188), welches u. a. regelt, dass Familiengerichte künftig früher bei Anzeichen von Kindesmisshandlung oder -vernachlässigung eingreifen können. So ist auch die Eingriffsvoraussetzung des elterlichen Erziehungsversagens aus dem Gesetz gestrichen worden. Die Gerichte können den Eltern konkrete Auflagen erteilen (z. B. Annahme von Hilfen der Jugend- und Gesundheitsfürsorge).

Darüber hinaus liegt ein umstrittener Entwurf eines Kinderschutzgesetzes des Bundes vor (BT-Drs. 16/12429). Unter anderem sind danach Personen, die der Schweige- oder Geheimhaltungspflicht unterliegen, zur Einschätzung der Gefährdung des Kindeswohls befugt, eine erfahrene Fachkraft hinzuzuziehen und die dafür erforderlichen Daten anonymisiert oder pseudonymisiert zu übermitteln. Zur Gefährdungseinschätzung bzw. -abwehr kann das Jugendamt beteiligt werden, wenn die Personensorgeberechtigten nicht bereit oder in der Lage sind mitzuwirken. Entsprechendes soll für andere Berufsgruppen gelten (Ausbildung, Erziehung oder Betreuung von Kindern und Jugendlichen).
Im Übrigen werden die Jugendämter durch eine Änderung des § 8a SGB VIII bei der Gefährdungseinschätzung stärker in die Pflicht genommen. Im Zuge der Beratungen wurde zwecks Schutzes der Vertrauensbeziehung die Verpflichtung zu Hausbesuchen auf das fachlich gebotene Maß reduziert. Aber auch dieser Regelungsvorschlag blieb im Hinblick auf den Kontrollcharakter und fehlende Präventionsansätze umstritten; das Gesetz kam nicht mehr zustande.

Überdies hat der Gemeinsame Bundesausschuss das Früherkennungsprogramm zur möglichst frühzeitigen Erkennung von Krankheiten um die zusätz-

liche Untersuchung U7a erweitert, die im 34. bis 36. Lebensmonat als Leistung der gesetzlichen Krankenversicherung angeboten wird.

Auch auf Landesebene wurden in dieser Hinsicht vielfältige Projekte initiiert. Der Landesbeauftragte konnte bei einigen Vorhaben mitwirken (Leitfaden für Ärzte und Ärztinnen zu Gewalt gegen Kinder und Jugendliche; Fortbildung von Hebammen).

21.16. Kinderschutzgesetz des Landes

Mit dem Entwurf eines Gesetzes zur Verbesserung des Schutzes von Kindern und zur Förderung der frühkindlichen Bildung (LT-Drs. 5/1331) beabsichtigte die Landesregierung, die Kinder besser vor Misshandlung und Verwahrlosung zu schützen. Der Gesetzesentwurf sah u. a. die Einrichtung lokaler Netzwerke Kinder- und Jugendschutz, die Förderung der Fehlbildungserfassung von Neugeborenen, Sprachstandsfeststellungen im vorletzten Jahr vor Beginn der Schulpflicht und die Förderung der Teilnahme an Vorsorgeuntersuchungen vor.

Hinsichtlich dieser Früherkennungsuntersuchungen war vorgesehen, dass eine zentrale Stelle von den Kinderärzten Meldungen über die durchgeführten Früherkennungsuntersuchungen erhalten und diese Daten mit den von den Meldeämtern übermittelten Meldedaten abgleichen sollte. Die gesetzlichen Vertreter der Kinder, die aufgrund des Abgleichs herausgefiltert wurden, weil sie nicht an der Untersuchung teilgenommen haben, sollten von der Zentralen Früherkennungsstelle einmal gebeten werden, diese Untersuchung nachzuholen. Wäre auch dann keine ärztliche Meldung eingegangen, hätte das jeweils zuständige Jugendamt informiert werden sollen. Das Jugendamt sollte dann eigenständig entscheiden, welche Maßnahmen es ergreift.

Der Landesbeauftragte wurde frühzeitig beteiligt. Seine Anregungen wurden vom zuständigen Ministerium nur teilweise in den Entwurf aufgenommen bzw. deren Berücksichtigung in den Regelungen der notwendigen Rechtsverordnung zugesagt. Verbesserungen betrafen u. a. die Bestimmungen zur Datenlöschung und die vorgesehene Evaluation. Grundlegende verfassungsrechtliche Bedenken musste der Landesbeauftragte im Rahmen der Anhörung vor dem Ausschuss für Soziales des Landtags von Sachsen-Anhalt geltend machen.

Zunächst galt es angesichts der Debatte in der Öffentlichkeit deutlich zu machen, dass Formulierungen wie „Kinderschutz vor Datenschutz“ zwar einprägsam, aber inhaltlich verquer sind. Auch führen sie dazu, den Blick auf die eigentlich zu lösenden Probleme zu verstellen.

Verfassungsrechtlich zweifelhaft erschienen die vorgesehene Datenerfassung und der Abgleich im Hinblick auf die Eignung, Erforderlichkeit und Verhältnismäßigkeit im engeren Sinne.

Die **Eignung** des Verfahrens, die Förderung des Kindeswohls zum Schutz vor Missbrauch und Vernachlässigung erreichen zu können, wurde in der öffentlichen Diskussion und in parlamentarischen Anhörungen im Bund wie in

den Ländern durch Fachleute in Frage gestellt. Die Vorsorgeuntersuchungen stellen nur Momentaufnahmen mit großen Intervallen dar. Ein wissenschaftlich nachweisbarer Zusammenhang zwischen verbindlichen Vorsorgeuntersuchungen und wirksamen Vorkehrungen gegen Kindesvernachlässigung ist nicht gegeben. Die Untersuchungen dienen nach Aussagen von Fachkräften der Krankheitsfrüherkennung, nicht der Prävention. Wesentliche Bereiche des Schutzbedarfs (seelische Schädigungen) werden überwiegend nicht erkannt. Zudem ist angesichts der bekannten Belastung der Jugendämter fraglich, ob eingehende Meldungen ohne weitere Ausstattung umgesetzt werden können.

Hielte man das Verfahren dennoch für geeignet, bliebe die **Erforderlichkeit** fraglich. Denn es kämen alternative Möglichkeiten zur Zweckerreichung in Betracht (Allianz für Kinder, weitere Aufklärungsmaßnahmen, Netzwerke, Hilfsangebote, Anreizsysteme, Ausstattung der Jugendämter usw.). Bei der Würdigung alternativer Hilfemaßnahmen ist insbesondere auch das Vertrauensverhältnis zwischen Jugendamt und Familie zu berücksichtigen. Das Jugendamt soll auch nach den bundesrechtlichen Vorgaben in erster Linie Helfer, nicht Kontrolleur sein.

Auch die **Verhältnismäßigkeitsprüfung** konnte bei Beachtung der Rechtsprechung des Bundesverfassungsgerichts nur negativ ausfallen:
„Die Anforderungen an die Ermächtigungsgrundlage richtet sich nach dem Gewicht des Eingriffs, das insbesondere von der Art der erfassten Informationen, dem Anlass und den Umständen ihrer Erhebung, dem betroffenen Personenkreis und der Art der möglichen Verwertung der Daten beeinflusst wird. ...
Informationserhebungen gegenüber Personen, die den Eingriff durch ihr Verhalten nicht veranlasst haben, sind grundsätzlich von höherer Eingriffsintensität als anlassbezogene...
Werden Personen, die keinen Erhebungsanlass gegeben haben, in großer Zahl in den Wirkungsbereich einer Maßnahme einbezogen, können von ihr auch allgemeine Einschüchterungseffekte ausgehen, die zu Beeinträchtigungen bei der Ausübung von Grundrechten führen können...
Die Unbefangenheit des Verhaltens wird insbesondere gefährdet, wenn die Streubreite von Ermittlungsmaßnahmen dazu beiträgt, dass Risiken des Missbrauchs und ein Gefühl des Überwachtwerdens entstehen...
In dem Spannungsverhältnis zwischen der Pflicht des Staates zum Rechtsgüterschutz und dem Interesse des Einzelnen an der Wahrung seiner von der Verfassung verbürgten Rechte ist es dabei zunächst Aufgabe des Gesetzgebers, in abstrakter Weise den Ausgleich der widerstreitenden Interessen zu erreichen...
Dies kann dazu führen, dass Grundrechtseingriffe einer bestimmten Eingriffsintensität erst von bestimmten Verdachts- oder Gefahrenstufen an vorgesehen werden dürfen...
Selbst bei höchstem Gewicht der drohenden Rechtsgutsbeeinträchtigung kann allerdings auf das Erfordernis einer hinreichenden Wahrscheinlichkeit nicht verzichtet werden. Grundrechtseingreifende Ermittlungen "ins Blaue hinein" lässt die Verfassung nicht zu..."
(BVerfG, Urteil vom 11.03. 2008, 1 BvR 2074/05, 1 BvR 1254/07 – NJW 2008, 1505)

Es war daher fraglich, ob es gerechtfertigt ist, alle Eltern und Kinder zu erfassen, somit eine Art Generalverdacht auszusprechen und so eine große Streubreite zu erzielen, ohne dass in der weit überwiegenden Zahl der Familien irgendein tatsächlicher Anhaltspunkt einer Kindeswohlgefährdung vorliegt. Auch in der Begründung des Gesetzesentwurfs wurde lediglich angenommen, dass eine Nichtteilnahme an den Untersuchungen ein Hinweis auf eine Gefährdung sein „kann“. Die vom Bundesverfassungsgericht geforderte Gefahrenschwelle, wie sie z. B. in § 8a SGB VIII normiert ist, wird weit verfehlt (auf diese vorgenannten Aspekte wurde im Urteil des Verfassungsgerichtshofs Rheinland-Pfalz vom 28. Mai 2009 - VGH B 45/08 - zu einem dort ähnlich ausgestalteten Einladungs- und Erinnerungsverfahren nicht näher eingegangen).
Nur ein geringer Prozentsatz nimmt nicht an den Untersuchungen teil. Dennoch werden alle erfasst. Es müssten sich aber diejenigen gegen „Verdächtigungen“ rechtfertigen, die z. B. nicht von den Ärzten gemeldet wurden. Dies kann aber auch am Umgang des Arztes mit der zunehmenden Bürokratie oder daran liegen, dass er mit Sitz im benachbarten Bundesland nicht der Meldepflicht unterliegt. Es muss vermieden werden, dass einige Betroffene, die aus fachlich akzeptablen Gründen nicht an einer Untersuchung teilnahmen oder versehentlich nicht gemeldet wurden, über unbestimmte Zeit hinaus in Vorgängen des Jugendamtes als potentielle Vernachlässiger von Kindeswohl geführt werden.
Zudem gibt es keine Verpflichtung zur Teilnahme an den Untersuchungen, so dass sich selbst die wenigen, die nicht teilnehmen, legal verhalten.

Der Gesetzgebungs- und Beratungsdienst des Landtages hatte ebenfalls eine Verletzung des Grundsatzes der Verhältnismäßigkeit festgestellt und empfohlen, die Regelungen zum Einladungswesen für Früherkennungsuntersuchungen im Entwurf zu streichen. Der Teil des Gesetzentwurfes zur Verbesserung des Schutzes von Kindern, der u. a. das verbindliche Einladungswesen für Früherkennungsuntersuchungen vorsehen sollte, wurde daraufhin in den Ausschüssen unter Hinzuziehung von Gutachten und Prüfung alternativer Regelungen zurückgestellt.

Das am 1. Januar 2009 in Kraft getretene Gesetz zur Förderung der frühkindlichen Bildung (GVBl. LSA 2008, S. 448) regelt vor allem die Sprachstandsfeststellung im vorletzten Jahr vor Beginn der Schule und die bei Bedarf stattfindende Sprachförderung in Kindertageseinrichtungen. Hierfür wurden das Schulgesetz des Landes Sachsen-Anhalt und das Kinderförderungsgesetz geändert. Das nähere Verfahren soll in einer Verordnung geregelt werden, die derzeit von einer Arbeitsgruppe, in der auch der Landesbeauftragte beteiligt ist, erarbeitet wird.

21.17. Projekt „Frühwarnsystem Pädiatrie“

Bei diesem vom Land unterstützten Projekt handelt es sich um eine Kooperation einer Universitätsklinik für Kinder- und Jugendmedizin und einer unter anderem in sozialen Belangen engagierten Stiftung. Ziel dieses Projektes ist es, Risikofamilien direkt nach der Geburt des Kindes zu identifizieren und ehrenamtliche oder professionelle Hilfen an diese Familien zu vermitteln.

Dafür werden mittels eines standardisierten Erhebungsbogens bei der Aufnahme in der Klinik Anamnesen und Befunde erhoben. Dazu gehören z. B. auch freiwillig angegebene Daten zur Sozialanamnese (z. B. berufliche Tätigkeit der Eltern). Aufgrund dieser Daten werden vom Behandlerteam Risikofaktoren ermittelt und bewertet. Während der Vorsorgeuntersuchung U2 wird allen Familien dann ein entsprechendes Hilfeangebot unterbreitet.
Angeboten werden Leistungen von Familienpaten und Familienhebammen. Dieses Projekt wird von der Stiftung durchgeführt. Eine Teilnahme am Familienpatenprojekt ist freiwillig. Datenübermittlungen an die Familienpaten erfolgen auf der Grundlage der Einwilligung, die Familienhebammen erheben die benötigten Daten selbst.

Der Landesbeauftragte ist dem Wunsch der Klinik nach Beratung gern nachgekommen. Er konnte darauf hinwirken, dass sich der Umfang der erhobenen und verarbeiteten Daten an strengen Maßstäben der Erforderlichkeit orientiert. Zudem sollte den Ärzten eine Ausfüllanleitung zur Verfügung stehen. Es wurde darauf hingewiesen, dass für Datenübermittlungen im Rahmen der späteren Kooperation mit Sozialleistungsträgern Schweigepflichtentbindungen notwendig sind. Abgesehen von Notstandssituationen ist die Einwilligung der Betroffenen nach vorheriger umfassender Aufklärung die Rechtsgrundlage der Datenverarbeitung. Der Landesbeauftragte machte zudem deutlich, dass auch das Verfahren zur Weiterverwendung der Daten bei Sozialleistungsträgern den Anforderungen der Datensparsamkeit genügen muss.

21.18. Klientenverwaltungssystem für Integrationsfachdienste

Wie im VIII. Tätigkeitsbericht (Ziff. 20.23) angekündigt, hat der Landesbeauftragte auch in diesem Berichtszeitraum die Thematik beobachtet.

Es konnte erreicht werden, dass die wesentlichen festgestellten datenschutzrechtlichen Bedenken ausgeräumt wurden. So wurde beispielsweise im zweiten Quartal 2008 im Integrationsamt und in den Integrationsfachdiensten die Verschlüsselungssoftware GnuPG installiert, um die Exportdatenbank bei der Übertragung zu verschlüsseln.

Noch zu klären ist das Problem der Speicherung nicht mehr zur Verfügung stehender Kontaktpersonen in der Kontaktpersonendatenbank. Die Lösung soll eine Weiterentwicklung vom Klientenverwaltungssystem für Integrationsfachdienste (KLIFD 3) sein, welches den gegenwärtigen und zukünftigen Anforderungen, auch in datenschutzrechtlicher Hinsicht, entsprechen soll. Mit einer Implementierung in Sachsen-Anhalt ist jedoch frühestens im dritten Quartal 2009 zu rechnen.

21.19. Bundeselterngeld- und Elternzeitgesetz

Das Gesetz zum Elterngeld und zur Elternzeit (Bundeselterngeld- und Elternzeitgesetz - BEEG) trat zum 1. Januar 2007 in Kraft und sieht vor, dass die Länder für die Ausführung dieses Gesetzes zuständig sind.
Aus datenschutzrechtlicher Sicht waren diesbezüglich im Berichtszeitraum die Antragsformulare und die Evaluation zu erörtern.

Der Landesbeauftragte hatte die Antragsformulare geprüft und die festgestellten datenschutzrechtlichen Mängel dem zuständigen Ministerium mitgeteilt.
So sollten nach § 22 Abs. 2 Nr. 13 BEEG zwar bestimmte Daten (Familienstand und Angaben über weitere Kinder) erhoben werden, jedoch nicht bei den Eltern, sondern bei den nach § 12 BEEG zuständigen auskunftspflichtigen Stellen. Da jedoch die genannten Daten für die ordnungsgemäße Antragsbearbeitung in der Regel nicht erforderlich sind und eine Datenerhebung ausschließlich zu statistischen Zwecken auch auf freiwilliger Basis bei den Eltern nach dem Bundesstatistikgesetz (BStatG) ausgeschlossen ist, konnten diese Daten dem Statistischen Bundesamt nicht mitgeteilt werden. § 9 Abs. 1 BStatG legt nämlich fest, dass eine Rechtsvorschrift, die eine Bundesstatistik anordnet, (hier das BEEG) außer den Erhebungs- und Hilfsmerkmalen u. a. den Kreis der zu Befragenden zu bestimmen hat. Der Kreis der zu Befragenden war in § 23 BEEG tatsächlich bestimmt worden, aber er erstreckte sich eben nicht auf die antragstellenden Eltern.
Der Gesetzgeber hat mit dem Ersten Gesetz zur Änderung des Bundeselterngeld- und Elternzeitgesetzes vom 17. Januar 2009 (BGBl. I. S. 61) in das BEEG einen neuen § 23 Abs. 2 eingeführt, der nun auch die antragstellenden Eltern zu Auskunftspflichtigen für die Bundesstatistik bestimmt. Leider werden damit die mit der Durchführung des BEEG betrauten Verwaltungsstellen gleichzeitig zu Erhebungsstellen für eine Bundesstatistik. Um dem verfassungsrechtlich geforderten Trennungsgebot von Verwaltungsvollzug und Statistik doch noch irgendwie zu entsprechen, sollen nach dem BEEG-Änderungsgesetz die von den Verwaltungsstellen ausschließlich zu Statistikzwecken erhobenen Daten der Antragsteller nun durch technische und organisatorische Maßnahmen getrennt von den Verwaltungsdaten verwendet und nach der Übermittlung an das Statistische Bundesamt gelöscht werden.

Im Rahmen des BEEG war eine Evaluation vorgesehen. Dazu sollten die Elterngeldstellen Adressdaten der Betroffenen an ein Sozialforschungsinstitut übermitteln, damit dieser die Telefonnummern der Betroffenen ermitteln könne, um telefonisch die Einwilligungen zur Teilnahme an der Befragung einzuholen.
Der Landesbeauftragte hat gegen diese Vorgehensweise datenschutzrechtliche Bedenken geltend gemacht, da bei einer Sozialdatenübermittlung nach § 75 Abs. 1 SGB X der Grundsatz der Priorität der Einwilligung gilt. Das Vorliegen hinreichender Gründe, die die Einholung einer Einwilligung unzumutbar im Sinne von § 75 Abs. 1 SGB X gemacht hätten, schien aber fraglich. Zwar wurde durch die beteiligten Forschungseinrichtungen eingewandt, dass ein auf Einwilligung und Mitwirkung beruhendes Adressmittlungsverfahren nicht in Betracht komme, da ein Erinnerungsverfahren notwendig sei. Auch sei ein Verfahren gewählt worden, bei dem die Einrichtung, die mit dem Fragebogen arbeitet, diesen anonym erhalte. Der Fragebogen werde ohne ID-Nummer in einem Briefumschlag mit ID-Nummer an eine beteiligte Einrichtung gesandt, die die Umschläge und Bögen voneinander trenne und an die Forschungseinrichtung weiterleite. Der Fragebogen lasse keinen Personenbezug zu, dennoch könne anhand der ID-Nummern ein sachgerechtes Erinnerungsverfahren durchgeführt werden. Ein derartiges Verfahren sei in anderen Bundesländern für vertretbar erachtet worden.

Dennoch sollten allgemeine Argumente, wie z. B. der Einwand höherer Kosten oder enge zeitliche Vorgaben, grundsätzlich keinen Eingriff in das Grundrecht auf informationelle Selbstbestimmung rechtfertigen (vgl. auch Ziff. 10.3). Der Landesbeauftragte schlug daher vor, zumindest ein Widerspruchsverfahren zu realisieren. Dies hätte bedeutet, dass die Elterngeldstellen die betroffenen Eltern schriftlich darüber informieren, dass vorgesehen ist, ihre Adressen an ein Forschungsinstitut zu übermitteln. Soweit binnen einer gesetzten Frist kein Widerspruch der Betroffenen erhoben worden wäre, wären diese Adressdaten dann übermittelt worden. Das zuständige Ministerium hat sich nach umfänglichen Beratungen dennoch dazu entschieden, den Antrag des Forschungsinstitutes nach § 75 SGB X zu genehmigen.

21.20. Antragsformular für die Gewährung der besonderen Zuwendung für Haftopfer

Durch eine Länderumfrage wurde der Landesbeauftragte darüber informiert, dass u. a. auch in Sachsen-Anhalt ein bestimmtes Antragsformular für die Gewährung der besonderen Zuwendung für Haftopfer (Opferpension) nach § 17a Strafrechtliches Rehabilitierungsgesetz (StrRehaG) verwandt wird.

Einzelpunkte des Vordruckes, insbesondere Fragen zum Einkommen sowie zur Erklärung der wirtschaftlichen Verhältnisse, begründeten datenschutzrechtliche Bedenken. Es war fraglich, warum vom Antragsteller Angaben zum Bezug einer Rente und deren Höhe abgefragt wurden, obwohl nach § 17a Abs. 2 Satz 2 zweiter Halbsatz StrRehaG Renten wegen Alters, verminderter Erwerbsfähigkeit, Arbeitsunfall oder Berufskrankheit sowie wegen Todes oder vergleichbarer Leistungen unberücksichtigt bleiben. So sah auch das Hinweisblatt die Pflicht zur Angabe von Renten und vergleichbaren Leistungen vor.

Grundsätzlich fallen zwar Renten und vergleichbare Leistungen unter den Einkommensbegriff des § 82 SGB XII; dies jedoch nur so lange, wie sie nicht durch gesetzliche Grundlage - wie in § 17a Abs. 2 Satz 2 zweiter Halbsatz StrRehaG geschehen - von der Berücksichtigung ausgeschlossen sind.

Nach Erörterung mit der zuständigen Behörde wurde auf die Abfrage zur Höhe der jeweiligen anrechnungsfreien Rente verzichtet.

Auch die weitere Abfrage zur Art der Rente erschien bedenklich. Die Abfrage damit zu begründen, dass sie die Voraussetzungen dafür schaffe, dass die Verwaltung selbst entscheiden könne, ob es sich um eine anrechnungsfreie Rente nach § 17a Abs. 2 Satz 2 zweiter Halbsatz StrRehaG handelt, hielt der Landesbeauftragte für bedenklich. Gemäß § 9 Abs. 1 DSG-LSA dürfen personenbezogene Daten nur erhoben werden, wenn ihre Kenntnis zur Erfüllung der Aufgaben (hier: Prüfung der wirtschaftlichen Verhältnisse) erforderlich ist. Die in § 17a Abs. 2 Satz 2 zweiter Halbsatz StrRehaG aufgeführten Renten sind nicht bei der Einkommensprüfung zu berücksichtigen, so dass es bereits an der Erforderlichkeit der Erhebung mangelt.

Die vorsorgliche Erhebung von Daten zu dem Zweck, sich die erforderlichen Informationen aus dem Angebot herauszusuchen, ist datenschutzrechtlich nicht akzeptabel. Soweit Bedenken bestehen, dass Antragsteller anrechen-

bare Bezüge für nicht anrechenbar halten und deshalb verschweigen, ist durch weniger einschneidende Maßnahmen zu begegnen.
Hierzu verwies der Landesbeauftragte auf § 25 Verwaltungsverfahrensgesetz. Danach hat die Behörde im Verwaltungsverfahren grundsätzlich die Pflicht, Auskünfte über die Rechte und Pflichten der Beteiligten im Verwaltungsverfahren zu erteilen. Die Beratungs- und Auskunftspflicht ist Teil der Fürsorgepflicht der Behörde gegenüber den direkt Beteiligten im allgemeinen Verwaltungsverfahren.
Der konkrete Umfang der zu erteilenden Auskunft richtet sich nach dem Empfängerhorizont der Beteiligten und der Komplexität der Sachlage.

Kennt jemand die für die Verfolgung seiner Rechte wesentlichen Vorschriften nicht oder hat er aus Unerfahrenheit oder Unkenntnis gar kein Problembewusstsein und kann daher nicht um Auskunft bitten, muss die Behörde den Beteiligten über seine Rechte und Pflichten im Verfahren belehren (Beratungspflicht). Diese Vorgaben treffen auch auf das Antragsformular und den Einkommensfragebogen zu (vgl. hierzu auch die Konkretisierung für den Bereich des Sozialversicherungsrechts in § 17 Abs. 1 SGB I).

Demgemäß wäre es zunächst erforderlich, im Antragsformular bzw. in erläuternden Hinweisen klarzustellen, welche Renten nicht anrechnungsfrei und damit anzugeben sind. Selbst wenn es tatsächliche Erfahrungen hinsichtlich einzelner Rentenarten gäbe, die mit nicht anrechenbaren häufig verwechselt werden, könnte konkret nach dieser anrechenbaren Rente gefragt werden.

22. Statistik

22.1. EU-weiter Zensus 2011

Bereits in seinem VIII. Tätigkeitsbericht (Ziff. 21.1) hatte der Landesbeauftragte über die EU-initiierte Volks-, Gebäude- und Wohnungszählung berichtet. Im Berichtszeitraum sind die Vorbereitungen von Gesetzgebern und Verwaltungen an diesem Mammutprojekt weiter vorangeschritten. Natürlich werden die Vorbereitungsarbeiten am Zensus 2011 als eine der umfangreichsten statistischen Erhebungen seit der Volkszählung im Jahre 1987 auch bei den Datenschutzbeauftragten des Bundes und der Länder mit besonderer Aufmerksamkeit bedacht.

Meilenstein im Rahmen der Vorbereitungsarbeiten am Zensus 2011 war die Erarbeitung eines Zensustestgesetzes. Mit diesem Gesetz sollen Erfahrungen mit den neuen Erhebungsinstrumentarien, die für den Zensus 2011 konzipiert wurden, gesammelt werden. So gab es bisher kaum Erfahrungen in Bezug auf die Zusammenführung und Auswertung so großer **Register** wie der Adressdatenbank der Bundesagentur für Arbeit und von Daten aus den Melderegistern.
Der Landesbeauftragte hatte im Rahmen einer zum Entwurf eines Zensusvorbereitungsgesetzes abgegebenen Stellungnahme u. a. bemängelt, dass eine Durchbrechung von Statistik und Verwaltungsvollzug vorgesehen sei. Es war nämlich beabsichtigt, dass die Statistischen Ämter der Länder, in denen jeweils die Landesdaten gesammelt und verknüpft werden sollen, die Meldebehörden unter Nennung der entsprechenden Adressbereiche über

Anhaltspunkte auf unvollständige oder fehlerhafte Meldedaten aufmerksam machen sollen. Diese Rückinformation aus der Statistik in den Verwaltungsvollzug, die in Widerspruch zu den bisher geübten Grundsätzen der entsprechenden Trennung in der Statistik steht, wurde mit dem Zensusvorbereitungsgesetz 2011 vom 8. Dezember 2007 (BGBl. I S. 2808) tatsächlich Rechtswirklichkeit. Allerdings konnten die Datenschutzbeauftragten verhindern, dass die Meldebehörden die Datendifferenzen durch Einzelprüfungen vor Ort beseitigen. Lediglich eine erneute Überprüfung der eigenen Datenbestände soll nun durchgeführt werden.

Während man in Deutschland bereits eifrig den nationalen Teil des europaweiten Zensus 2011 vorbereitete, lag eine entsprechende europäische Verordnung über eine Volks- und Wohnungszählung lange überhaupt nicht vor. Grund war ein heftiger Streit zwischen der EU-Kommission und dem Ausschuss für Beschäftigung und soziale Angelegenheiten des Europäischen Parlaments um die Abfrage zahlreicher freiwilliger Angaben, z. B. über das Sexualleben, Computerkenntnisse oder die Lese- und Schreibkompetenz der Befragten, alles wegen nicht genügend dargelegter Erforderlichkeit letztendlich datenschutzrechtlich höchst bedenklich. Schließlich nahmen die EU-Parlamentarier den Vorschlag des Beschäftigungs- und Sozialausschusses an, diesen freiwilligen Teil der Befragung entfallen zu lassen. Die EG-Verordnung über Volks- und Wohnungszählungen trat im September 2008, ohne diese Fragen zu regeln, in Kraft.

Durch die Verordnung wird nun erstmals der Rahmen exakt bezeichnet, den die EU für die nationalen Datenerhebungen setzt. Parallel dazu wird aktuell an einem Zensusanordnungsgesetz gearbeitet. Der Landesbeauftragte hatte bereits im Mai 2008 zu dem damals vorliegenden Gesetzentwurf, in dem für Deutschland der Umfang des Zensus 2011 beschrieben wird, eine ausführliche Stellungnahme abgegeben. Als datenschutzrechtlich bedenklich hatte er damals u. a. die Erhebung der Religionszugehörigkeit der in der Stichprobe persönlich zu Befragenden (maximal 8 % der Bevölkerung, also rund 8,5 Millionen zu Befragende) zum Zweck der Feststellung des Bedarfes an religiös zu nutzenden Gebäuden genannt. Auch die Frist von 4 Jahren nach dem Zensusstichtag für die Löschung der Hilfsmerkmale (z. B. die Namen, Vornamen und Anschriften der für die Gebäude- und Wohnungszählung Auskunftspflichtigen) erschien ihm zu lang.

Im Dezember 2008 erreichte den Landesbeauftragten ein überarbeiteter Entwurf für ein Zensusanordnungsgesetz, der bereits eine Fülle von noch im Mai 2008 festgestellten datenschutzrechtlichen Kritikpunkten nicht mehr umfasste. Allerdings enthält der im März 2009 in den Bundestag eingebrachte Gesetzentwurf (BT-Drs. 16/12219) weiterhin einige datenschutzrechtlich bedenkliche Regelungen. So beinhaltet der Gesetzentwurf der Bundesregierung in § 7, der die Haushaltstichprobe regelt, zunächst nicht mehr die Erhebung des Merkmals Religionszugehörigkeit. Der Bundesrat forderte in seiner Stellungnahme (BR-Drs. 3/09 (Beschluss)) die Bundesregierung auf, diese Angabe gleichwohl zu erheben. In ihrer Gegenäußerung (enthalten in (BT-Drs. 16/12219)) lehnte die Bundesregierung dies mit der Begründung ab, die entsprechende EG-Verordnung sehe diese Erhebung nicht vor. Der Innenausschuss des Bundestages forderte in seiner Beschlussempfehlung/seinem

Bericht (BT-Drs. 16/12711) nicht nur, die rechtliche Zugehörigkeit zu einer öffentlich-rechtlichen Religionsgemeinschaft zu erheben, sondern außerdem noch das Bekenntnis zu anderen Religionen, Glaubensrichtungen oder Weltanschauungen, wie dem Buddhismus oder dem alevitischen Islam, um nur einige zu nennen. Der Landesbeauftragte erinnert in diesem Zusammenhang daran, dass nach dem Urteil des Bundesverfassungsgerichts zur verfassungsrechtlichen Überprüfung des Volkszählungsgesetzes 1983 vom 15. Dezember 1983 (BVerfGE 65,1) Einschränkungen des Rechts auf informationelle Selbstbestimmung, wie sie eine Statistik wie der Zensus 2011 zwangsläufig mit sich bringt, nur im überwiegenden Allgemeininteresse zulässig sind. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, bei der der Gesetzgeber den Grundsatz der Verhältnismäßigkeit zu beachten hat.
Ein anderes Problem des Gesetzentwurfes war in § 8 Abs. 1 und 4 die Erhebung von Individualdaten in Sonderbereichen, z. B. in Obdachlosenunterkünften. Bei in diesen Einrichtungen untergebrachten Personen wurde die Erhebung der Hilfsmerkmale Name und Vorname vorgeschrieben. Der Landesbeauftragte sah dadurch die Gefahr der sozialen Abstempelung der Betroffenen gegeben und empfahl eine anonyme Datenerhebung.
Bundestag und Bundesrat hielten letztendlich an den umstrittenen Regelungen fest.

Die Vorbereitung und Durchführung des Zensus 2011 - der Landesgesetzentwurf zur Umsetzung wird noch in 2009 erwartet - wird der Landesbeauftragte weiter begleiten.

22.2. Trennung von Erhebungs- und Hilfsmerkmalen

Einer der Grundsätze der amtlichen Statistik ist die Abtrennung der im Wesentlichen der Plausibilitätsprüfung dienenden häufig personenbezogenen Hilfsmerkmale von den eigentlich statistikrelevanten Erhebungsmerkmalen. Diese Abtrennung führt letztendlich zur Anonymisierung der zu einer Statistik gemachten Einzelangaben und sollte rechtsstaatlich selbstverständlich sein. So hat der Bundesgesetzgeber in § 12 Abs. 1 Bundesstatistikgesetz (BStatG) bestimmt, dass die Hilfsmerkmale, soweit nichts anderes gilt, zu löschen sind, „sobald bei den Statistischen Ämtern die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist. Sie (die Hilfsmerkmale) sind von den Erhebungsmerkmalen zum frühestmöglichen Zeitpunkt zu trennen und gesondert aufzubewahren.“ Dies gilt im Übrigen gem. § 10 Abs. 3 Landesstatistikgesetz Sachsen-Anhalt auch für Landesstatistiken.

Allerdings war diese eigentlich eindeutige Vorschrift durch die amtliche Statistik im Fall einer Erhebung anders ausgelegt worden, als der Gesetzgeber dies nach Meinung einer großen Zahl von Datenschutzbeauftragten beim Bund und Ländern beabsichtigt hatte. Der Datenschutzbeauftragte eines anderen Bundeslandes stellte nämlich folgendes fest: Bei der Strukturerhebung im Dienstleistungsbereich (Dienstleistungsstatistik, angeordnet durch ein Bundesgesetz) sei es in seinem Land unmöglich gewesen, den Teil des Fragebogens, der die Hilfsmerkmale (Name und Anschrift des Auskunftspflichtigen, Name eines Ansprechpartners für Rückfragen) enthält, von dem Teil mit

den Erhebungsmerkmalen (Umsatz, Zahl der Beschäftigten, gezahlte Steuern usw.) zu trennen. Grund war, dass ein Teil der Erhebungsmerkmale auf der Rückseite der Hilfsmerkmale notiert und eine physische Trennung damit unmöglich sei. Diese Trennung, so stellte der Landesbeauftragte fest, wäre bei den in Sachsen-Anhalt verwendeten Fragebögen durchaus möglich. Allerdings wurde sie nicht praktiziert!
Im Rahmen der schriftlichen Unterrichtung der zu Befragenden gem. § 17 BStatG, die Annex des Fragebogens zur Dienstleistungsstatistik ist, teilte das Statistische Landesamt den zu Befragenden nämlich folgendes mit: „Die Fragebogen, auf denen sich diese Hilfsmerkmale befinden, werden spätestens nach Abschluss der nächsten Erhebung vollständig gelöscht." Bei genauerer Lektüre des Erhebungsbogens stellt der Interessierte dann überrascht fest, dass die Dienstleistungsstatistik eine jährliche Statistik ist, der Abschluss der nächsten Erhebung kann also durchaus noch weit über ein Jahr in der Zukunft liegen. Erst dann würden also die Hilfs- und mit ihnen die Erhebungsmerkmale gelöscht. Das steht nach Meinung des Landesbeauftragten im krassen Gegensatz zum BStatG und ist viel zu spät.
Erwartungsgemäß sah das Statistische Landesamt das anders. In seiner Stellungnahme gab es dem Landesbeauftragten gegenüber zunächst an, seinen Unterrichtungspflichten gem. § 17 BStatG nachgekommen zu sein. Die zu Befragenden würden richtig über die Trennung und Löschung der Hilfsmerkmale spätestens nach Abschluss der nächsten Erhebung unterrichtet. Und diese lange Frist stehe durchaus im Einklang mit § 12 BStatG. Nach § 12 Abs. 2 BStatG dürfen nämlich bei periodischen Erhebungen die zur Bestimmung des Kreises der zu Befragenden erforderlichen Hilfsmerkmale gesondert aufbewahrt werden, soweit sie für nachfolgende Erhebungen benötigt würden. Sie seien nach dieser Vorschrift nach Beendigung des Zeitraums der wiederkehrenden Erhebung zu löschen. Dass der Gesetzgeber in § 12 Abs. 2 BStatG gefordert hatte, die Hilfsmerkmale von den Erhebungsmerkmalen gesondert - also getrennt - aufzubewahren, focht das Statistische Landesamt in keiner Weise an. Es hielt sich auf dem richtigen Wege. Die statistisch-fachliche Erforderlichkeit der weit über ein Jahr hinausgehenden Aufbewahrung der personenbezogenen Erhebungsdaten konnte es dagegen nicht hinreichend darlegen.

Da das Problem offenbar in der Mehrzahl der Bundesländer gleichermaßen auftrat, wurde der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit gebeten, gemeinsam mit dem Statistischen Bundesamt nach einer einvernehmlichen Lösung zu suchen. Dieses erklärte zunächst zur Rechtfertigung, dass bei periodischen Erhebungen in vielen Fällen eine abschließende Plausibilitätsprüfung erst nach Vorliegen der Angaben aus der Folgeerhebung möglich sei. Es hielt im Widerspruch zu § 12 Abs. 1 BStatG es durchaus für zulässig, bei jährlichen Erhebungen den Zeitpunkt der Trennung von Erhebungs- und Hilfsmerkmalen mit dem Löschzeitpunkt der Hilfsmerkmale zusammenzulegen.
Im Rahmen der weiteren Diskussion konnte das Statistische Bundesamt schließlich zum Einlenken gebracht werden. Gemäß der getroffenen Vereinbarung werden künftig in allen Statistischen Landesämtern die Erhebungsbögen zur Dienstleistungsstatistik spätestens nach Abschluss der Erhebung des aktuellen Berichtszeitraums vernichtet werden. Das Statistische Landesamt sagte dem Landesbeauftragten zu, entsprechend zu verfahren.

23. Strafvollzug

23.1. PPP-Projekt Justizvollzugsanstalt Burg

23.1.1. Vorgeschichte

Der Landesbeauftragte hatte im VIII. Tätigkeitsbericht (vgl. dort Ziff. 22.1) über das Vorhaben zum Bau und Betrieb einer Justizvollzugsanstalt im Rahmen einer sog. public-private-partnership (PPP) berichtet. Die gegen Ende des Berichtszeitraums des vergangenen Tätigkeitsberichts auf Datenträger übersandten Verträge und Ausführungsvereinbarungen wurden geprüft.
Der Landesbeauftragte hatte hierzu zunächst im Allgemeinen angemerkt, dass die vorgesehene sehr weitgehende Übertragung von Aufgaben im Strafvollzug an Private erheblichen verfassungsrechtlichen Bedenken begegnet. Es gibt wenige Aufgabenfelder, in denen sich das Gewaltmonopol des Staates vergleichbar intensiv und dauerhaft ausdrückt, wie in diesem Bereich. Nicht ohne Grund hatte der Bundesgesetzgeber in § 155 Strafvollzugsgesetz eine Wahrnehmung von Aufgaben in Justizvollzugsanstalten nur aus besonderen Gründen durch vertraglich verpflichtete Personen zugelassen. Als solcher besonderer Grund kommt vor allem die Verfügbarkeit von besonderem Fachpersonal, etwa aus dem Bereich der Medizin, in Betracht. Fiskalische Gründe allein rechtfertigen ein solches Vorgehen nicht. Die dauernde Wahrnehmung von Aufgaben durch Außenstehende weicht das staatliche Monopol unvertretbar auf. Dem Landesbeauftragten erscheint zudem eine strikte Trennung in hoheitliche und andere Aufgabenbereiche im Tatsächlichen schwer umsetzbar. Datenschutzrechtlich ist dies praktisch vielfältig von Bedeutung.

23.1.2. Nichthoheitliche und hoheitliche Tätigkeit im hoheitlichen Strafvollzug?

In Folge einer gemeinsamen Besprechung im September 2007 sicherte das Justizministerium zu, im Zuge der Erarbeitung der Dienstanweisungen für das private Personal nochmals im Detail zu prüfen, ob ggf. einzelne Segmente aus den in den Vereinbarungen beschriebenen Leistungen beim Land bleiben sollten. Ein ausdrückliches Ergebnis dieser Prüfung wurde nicht mitgeteilt.
Das Justizministerium ist der Auffassung, dass eine klare und praktikable Trennung der in einer Strafvollzugseinrichtung anfallenden Aufgaben in einen hoheitlichen und einen nicht hoheitlichen Teil möglich sei, auch wenn es zugesteht, dass in Einzelbereichen, z. B. bei den der Vollzugshilfsdiensten, die Tätigkeit des privaten Personals den grundrechtlichen Bereich der Gefangenen am Rande tangieren kann. Dadurch sei indes in keinem Fall der Kernbereich der Grundrechte betroffen. Die Eingriffsintensität liege daher deutlich unterhalb solcher Eingriffe, wie sie beispielsweise auf Flughäfen durch das Kontrollpersonal von jeher praktiziert würden. Der Landesbeauftragte geht zwar davon aus, dass insoweit keine Änderung der Auffassung zu erwarten ist. Er hält diese Ansicht - wie auch den unpassenden Vergleich - für unzutreffend und weist nachdrücklich darauf hin, dass die Grundrechte - entgegen der Darstellung des Justizministeriums - in ihrer Schutzwirkung nicht auf einen Kernbereich reduziert werden können. Ganz im Gegenteil unterstreicht

die Feststellung des Bundesverfassungsgerichts, in den Kernbereich privater Lebensgestaltung dürfe unter keinen Umständen durch die staatliche Gewalt eingegriffen werden, dass Eingriffe außerhalb des Kernbereichs allenfalls im Rahmen verfassungsgemäßer Regelungen zulässig sind. Dies heißt, dass im vorliegenden Fall schon ein „Tangieren“ grundrechtlicher Bereiche der Gefangenen - u. U. auch Bediensteter - einen Eingriff darstellt.
Der Landesbeauftragte hob, wie auch der Justizbediensteten-Verband, hervor, dass es zwangsläufig zu vielfältigen Kontakten privater Mitarbeiter mit Gefangenen in nahezu allen Lebenslagen innerhalb der Justizvollzugsanstalt kommen muss. Durch diese „Nähe“ im Strafvollzugsalltag ist eine weitgehende Information über persönliche Daten nahezu unvermeidbar.

23.1.3. Absicherung des Datenschutzes durch Vertragsgestaltung?

Ob die im Rahmenvertrag verankerte Möglichkeit zur fristlosen Kündigung bei Verstößen gegen die einschlägigen datenschutzrechtlichen Regelungen und die durch eine Verpflichtung nach dem Verpflichtungsgesetz untermauerte Pflicht zur Verschwiegenheit eine ausreichende Motivation darstellt, mit Daten sensibel umzugehen und keinerlei Informationen an Unbefugte weiterzugeben, bleibt zu hoffen.
Auch in Details der Vereinbarungen fanden sich bereits problematische Regelungen. So ist faktisch eine bis in den Intimbereich reichende umfassende Überwachung und Auswertung persönlicher Daten angedacht, die sich auch durch elektronische (RFID-)Chips an persönlicher Wäsche etc. realisiert. Dies erscheint verfassungsrechtlich nicht akzeptabel - auch unter den besonderen Bedingungen des Strafvollzugs. Die Gefangenen werden dadurch letztlich auf eine Zahl, auf einen betriebswirtschaftlichen Faktor reduziert.
Hierzu verwies das Justizministerium in seiner Stellungnahme lediglich auf die ausgeschriebene Leistung (Reinigung der Anstaltswäsche), die eine Wäschekennzeichnungsvariante umfassen sollte. Personenbezogene Anstaltskleidung solle danach mit RFID-Chips versehen werden. Welche Wäscheteile als personenbezogen gelten, sei noch festzulegen. Im übrigen werde ein Verbrauchsverhalten ausschließlich über die Bestands- und Lagerführung ermittelt. Beim Waschen würden lediglich beschädigte Wäscheteile individuell erfasst. Eine weitere rechtliche Bewertung nahm das Justizministerium nicht vor, äußerte jedoch, dass das konkrete Verfahren noch diskutabel sei und datenschutzrechtliche Bedenken noch berücksichtigt würden. Weitergehende Informationen lagen bis zum Redaktionsschluss nicht vor.

23.1.4. Datenverarbeitung im Ausland?

Der Landesbeauftragte wies weiter darauf hin, dass jede Verarbeitung und Nutzung personenbezogener Daten in einem Land außerhalb der Europäischen Union sowie jeder Zugriff aus einem Land von außerhalb der Europäischen Union unterbleiben muss. Gleich ob die Datenverarbeitung und -nutzung im Auftrag des Auftragnehmers oder durch diesen unmittelbar erfolgt. Es reicht nicht aus, nur die Übermittlung an Drittstaaten auszuschließen, wie es in einem „Konzept gebäudebezogener Dienstleistung“ vorgesehen ist. Denn innerhalb eines theoretisch denkbaren (Unter-) auftragsverhältnisses käme es im Rechtssinne u. U. nicht zu einer Übermittlung von Daten an den (Unterauftrags-)datenverarbeiter, sondern nur zur Datennutzung.

Dies sah das Justizministerium ebenso. Die Einhaltung datenschutzrechtlicher Vorgaben sei Grundvoraussetzung für die Leistungsvergabe an einen Nachunternehmer. Personenbezogene Daten würden nicht außerhalb der Europäischen Union bzw. in Staaten übermittelt, ohne dass ein angemessenes Schutzniveau im Sinne der EG-Datenschutzrichtlinie (Richtlinie 95/46/EG) gewährleistet sei.

23.1.5. Die Beteiligung des Landesbeauftragten im Übrigen

Das Justizministerium begrüßte zwar das Angebot des Landesbeauftragten, einen leitenden Mitarbeiter aus seinem Technikreferat in die Projektgruppe Justizvollzugsanstalt Burg zur Beratung zu entsenden. Es wurde aber nicht in Anspruch genommen. Der Landesbeauftragte bedauert auch, dass ihm nicht, wie vereinbart, die Dienstanweisungen für das private Personal spätestens im 3. Quartal 2008 zur Kenntnis gegeben wurden. Auch das seit 2007 angekündigte umfassende Datenschutzkonzept, welches erst eine angemessene Beurteilung der Verarbeitung personenbezogener Daten erlauben würde, lag bis Juni 2009 nicht vor.

23.1.6. Handflächenvenenerkennung und Berechtigungskonzeption

Ende Dezember 2008 wurde ein Berechtigungskonzept für das Unterstützungsprogramm BASIS vorgelegt. Zugleich informierte das Justizministerium über ein biometrisches Erkennungssystem, welches zur Zu- und Abgangskontrolle der Besucher dienen soll und auf dem Scannen der Handvenen der Besucher beruht.
Ob das biometrische Erkennungssystem aufgrund der technisch-funktionalen Ausgestaltung akzeptabel sein könnte, muss noch geprüft werden. Es soll als Schlüssel- und Anwesenheitskontrolle für Besucher dienen. Von Besuchern soll ein verschlüsseltes Muster ihrer Handvenen erstellt werden. Nur wenn die biometrischen Referenzdaten beim Aufenthalt mit dem dann erstellten neuerlichen Scan übereinstimmen, werden Durchgangsschleusen geöffnet. Das gespeicherte Muster soll mit Verlassen der Justizvollzugsanstalt gelöscht werden; eine Zuordnung zu den Akten besuchter Strafgefangener soll nicht erfolgen. Das mit der Erhebung der Handvenen durch digitale Verschlüsselung hergestellte Muster soll nur dann auf eine Person rückführbar sein, wenn nur noch ein einziger Besucher in der Justizvollzugsanstalt anwesend ist. Ob auch bei zwei oder mehr Besuchern bei deren persönlicher Anwesenheit ein Bezug zwischen Muster und Person hergestellt werden kann, wäre zu klären. Ein verschlüsseltes Muster der Handflächenvenen könnte ein pseudonymisiertes Datum darstellen. Wie lange dieses Muster gespeichert wird, würde, bei Löschung des Templates mit Verlassen der Justizvollzugsanstalt, ausschließlich vom Besucher abhängen.
Allerdings ändert die Verfahrensweise nichts am Eingriff in das Datenschutzgrundrecht der Besucher. Die zur Rechtfertigung des Systems angeführten Gründe sind entweder rechtstatsächlich nicht belegt oder reichen als rein wirtschaftliche Erwägungen für einen Grundrechtseingriff nicht aus. So sind aus Einrichtungen, die „klassische“ Zugangskontrollen nutzen - außer einem einzigen benannten Fall trickreichen Entweichens, auf den sich das Justizministerium bezog - keine weiteren Fälle mitgeteilt worden, die gegen das bisherige Besuchsprozedere sprächen. Auch eine Information der Besucher ü-

ber die Wirkungsweise des Systems bewirkt für sich noch keine Rechtfertigung. Ob dies und die vom Justizministerium bisher benannten personalwirtschaftlichen Erwägungen ausreichen, einen Grundrechtseingriff - auch im Hinblick auf den Einschüchterungseffekt - zu fundieren, wird noch zu diskutieren sein.
Bislang wurden von der (künftigen) Leitung der Justizvollzugsanstalt für diesen Vorgang noch keine Ausführungen zu einer Feststellung zum Verfahrensverzeichnis gemacht. Auch wurden noch keine Strukturpläne überlassen, die belegen könnten, dass eine Verknüpfungsmöglichkeit der im Hintergrund des biometrischen Systems agierenden Datenbank mit anderen Informationssystemen nicht besteht. Ein völlig autark arbeitendes System wäre aus datenschutzrechtlicher Sicht zu begrüßen. Die für eine abschließende Bewertung dieses biometrischen Systems notwendigen technischen Unterlagen und Netzpläne sowie Informationen über die Datenbank (Feldinhalte, verschlüsselte Speicherung, Löschung, Zugriffsschutz, usw.) lagen noch nicht vor.

Kritisch fiel auch eine erste Beurteilung des Rollen- und Berechtigungskonzepts für das Programm BASIS (Buchhaltungs- und Abrechnungssystem im Strafvollzug) aus. Innerhalb dieses Systems sollen anscheinend auch Bedienstete der privaten Firma zum Teil sehr weitgehende Befugnisse haben. Dies betrifft in Sonderheit die Funktion der EDV-Administratoren. Dieser Funktionsbereich ist, gleich ob öffentlich bediensteter oder externer Administrator, regelmäßig besonders kritisch zu beleuchten. Denn diese Personengruppe wird in der Regel sämtliche Einstellungen, Zugangsberechtigungen, Kontrollroutinen, etc. einrichten und verändern können - kurz, ein Administrator könnte im System alles veranlassen, ohne dass dies kontrollierbar bzw. nachvollziehbar wäre. Dabei besteht auch das Risiko, dass Inhalte von Datensätzen eingesehen werden könnten, künftig u. U. auch sensible Daten besonderer Art, wie u. a. Krankendaten der Gefangenen und ggf. auch der Bediensteten. Das bekannte Beispiel des EDV-Systems einer amerikanischen Großstadt, welches durch einen ehemaligen Administrator völlig blockiert werden konnte, mag insoweit als Warnung dienen. Daher hat der Landesbeauftragte immer wieder darauf hingewiesen, dass, außer einem eventuell einzurichtenden Vieraugenprinzip, die eigentlichen Arbeitsdateien verschlüsselt abgelegt werden sollten. Damit bestünde auch für Administratoren nicht mehr die Gefahr, unabsichtlich sensible Daten zur Kenntnis nehmen zu müssen. Mit dieser Notwendigkeit verträgt sich allerdings die Festlegung im Rollen- und Berechtigungskonzept nicht, nach dem für die Rolle „Administrator“ alles sichtbar sein soll.
Der Landesbeauftragte hat mit Zustimmung zur Kenntnis genommen, dass das Justizministerium die datenschutzrechtliche Notwendigkeit sieht, einen staatlichen namentlich bezeichneten Systemadministrator einzusetzen. Inwieweit für diesen tatsächlich die Notwendigkeit besteht, auch mit unverschlüsselten Datensätzen umgehen zu müssen, wird ggf. Gegenstand weiterer Erörterungen und späterer Kontrollen sein.

Neben der Rolle der Systemadministration schienen dem Landesbeauftragten auch einige andere Rollen angesichts ihrer Bezeichnung problematisch zu sein. Mit Rollen wie „Global ohne Notfallbogen“ oder „eingeschränkt sichtbar“ könnten auch dem Personal des privaten Dienstleisters Personendaten

einsehbar werden, ohne dass aus den vorgelegten Unterlagen des Rollen- und Berechtigungskonzepts zu ersehen wäre, welchen Zweck und Umfang die denkbaren Informationsweitergaben haben sollen.
Auf Nachfrage teilte das Justizministerium Ende März 2009 mit, dass die genannten Rollen keinen Zugriff auf Daten, sondern nur auf allgemeine Grundfunktionen und die Menüstruktur ermöglichen würden.

Der Landesbeauftragte hat im Zusammenhang mit der Übersendung eines Fragenkatalogs an das Justizministerium auch das in Aussicht gestellte Datenschutzkonzept angemahnt, welches insbesondere die Verantwortlichkeit der öffentlichen Stelle wiederspiegeln müsste. Die speziellen Unterlagen etwa „EDV-Systembetreuung“ oder „Bereichsbezogene Dienstanweisung EDV-Systembetreuung“ des privaten Partners können ein entsprechendes Datenschutz- und Sicherheitskonzept der Justizvollzugsanstalt, als der verantwortlichen Stelle nach dem DSG-LSA, nicht ersetzen. Der Landesbeauftragte wies bereits auf zahlreiche konkrete inhaltliche Mindestinhalte und offene Fragen hinsichtlich eines solchen Datenschutzkonzepts hin.
Er stellte zudem klar, dass auch eine Formulierung im Vertrag über die EDV-Systembetreuung, nach welcher der private Vertragspartner die Einhaltung der Datenschutzvorschriften gewährleistet, das Land Sachsen-Anhalt als Auftraggeber nicht von der eigenen Verantwortung und den Verpflichtungen aus § 8 DSG-LSA (Datenverarbeitung im Auftrag) entbinden kann. Hierzu gehören insbesondere die Erfüllung der gesetzlichen Anforderungen des § 8 Abs. 2, 6 und 7 DSG-LSA.
Der Landesbeauftragte hatte darum gebeten, ihm - auch rechtstatsächlich - die Auftragssituation darzulegen. Die Beziehungen zwischen Justizministerium, der Projektgruppe, der Justizvollzugsanstalt und privaten Dienstleistern erschweren nämlich durch in sich verwobene Auftrags- und Unterauftragsverhältnisse die Zuweisung von rechtlicher Verantwortlichkeit. In einer ersten Antwort des Justizministeriums wurde zwar dargestellt, dass eine datenschutzrechtlich bedeutsame Auftragssituation nicht gegeben sei. Zugleich wurde aber auf die Wartungstätigkeit des privaten Betreibers hingewiesen. Ob dieser dadurch zwangsläufig personenbezogene Daten zur Kenntnis bekommt, wurde noch nicht mitgeteilt, vgl. § 8 Abs. 7 DSG-LSA.

23.1.7. Personalaktenbearbeitung durch private Dritte?

Aus den Entwürfen der Dienstanweisungen des privaten Betreibers ließ sich noch ein weiteres Tätigkeitsfeld entnehmen, welches rechtlich in unmittelbarer Landesverantwortung liegen müsste:
In der Dienstanweisung für die Verwaltungshilfsdienste sind als Aufgaben u. a. die Bearbeitung von Bewerbungen, Anträgen für Reisekostenabrechnung, Trennungsgeld und anderen anfallenden Formularen im Antragswesen beschrieben. Da der Begriff Trennungsgeld typischerweise im öffentlichen Dienst verwendet wird, könnte dies bedeuten, dass die Mitarbeiter der privaten Firma die beschriebenen Aufgaben auch hinsichtlich der Landesbediensteten wahrnehmen sollen. Eine telefonische Nachfrage beim Aufbaustab der Justizvollzugsanstalt Burg bestätigte diese Vermutung.
Wenn mit dieser Tätigkeit eine aus datenschutzrechtlicher Sicht als Übermittlung von Personalaktendaten an Dritte zu wertende Handlung verbunden wäre, könnte dies lediglich unter den Voraussetzungen des § 90d BG LSA oder

auf spezialgesetzlicher Grundlage zulässig sein. So enthalten insbesondere Unterlagen zu Trennungsgeld, Reise- und Umzugskostenvergütungen Personalaktendaten.
Die Voraussetzungen für eine Datenübermittlung an bzw. Datennutzung durch eine private Firma waren allerdings nicht ersichtlich. Eine spezialgesetzliche Regelung zur Übertragung von Aufgaben der Personalverwaltung an Dritte besteht - abgesehen von der schon fraglichen verfassungsrechtlichen Zulässigkeit einer solchen Bestimmung - nicht. Auch § 8 DSG-LSA käme als Rechtsgrundlage für eine Auftragsdatenverarbeitung von Personalaktendaten nicht in Betracht. Denn nach § 3 Abs. 3 S. 2 DSG-LSA bleibt die Verpflichtung zur Wahrung besonderer Amtsgeheimnisse (hier: Personalaktengeheimnis) unberührt.
Dem DSG-LSA unterliegen daher lediglich Sachaktendaten. Dies sind Unterlagen, die besonderen von der Person und dem Dienstverhältnis sachlich zu trennenden Zwecken dienen (§ 90 Abs. 1 Satz 4 BG LSA). Ob und inwieweit Vorgänge bzw. Daten aus Personalakten in Sachakten fließen, unterliegt einer von der Fürsorgepflicht des Dienstherrn gesteuerten Wertung. Die verfassungsrechtlichen Vorgaben des Schutzes der Persönlichkeit und die Wertung des Gesetzgebers, tendenziell die Weitergabe von personenbezogenen Daten aus Personalakten möglichst einzuschränken, sind dabei mit besonderem Gewicht zu berücksichtigen.
Es bedarf daher der Prüfung im Einzelfall, ob und inwieweit Daten zu Einzelaufgaben aus den o. g. Komplexen übermittelt bzw. im Weg der Datenverarbeitung im Auftrag überlassen werden können (z. B. die Prüfung einzelner Angaben von Anträgen). Ende März 2009 äußerte das Justizministerium, dass der Einsatz der Verwaltungshilfsdienste u. a. zur Prüfung eingereichter Unterlagen auf Vollständigkeit erfolge. Dies wird ggf. Gegenstand späterer Kontrollen sein. Denn zu einer Vollständigkeitsprüfung dürfte eine umfassende Erfassung des Sachverhalts notwendig sein. Ob dann den bestehenden gesetzlichen Regelungen entsprochen wird, ist zumindest zweifelhaft.

Der Landesbeauftragte anerkennt das grundsätzliche Interesse des Justizministeriums an einer auch datenschutzgerechten Verwirklichung des Projekts der Justizvollzugsanstalt Burg. Allerdings konnten noch längst nicht alle Fragen geklärt werden. Ggf. wird hierzu im folgenden Tätigkeitsbericht zu referieren sein.

23.2. Kontrolle in Justizvollzugsanstalt: Licht und Schatten

Der Landesbeauftragte kontrollierte im September 2007 eine Justizvollzugsanstalt. Auch nachdem er das Justizministerium gebeten hatte, aufgrund der unzureichenden Stellungnahme der Anstalt und des Umstands, dass eventuell weitere Justizstellen zu beteiligen wären, eine Ergänzung der Stellungnahme zu veranlassen, blieben auch nach Übersendung von weiteren Informationen noch Fragen offen.

Zunächst ergab die Prüfung der Justizvollzugsanstalt vor Ort eine beispielhaft positive Verfahrensweise beim Nutzen der Gefangenenpersonalakten. So wurde die Entnahme von Gefangenenpersonalakten aus der Vollzugsgeschäftsstelle von den betreffenden Bediensteten auf einem der jeweiligen Gefangenenpersonalakte beigefügten Entnahmeblatt abgezeichnet. Bei Ent-

nahme der Gefangenenpersonalakten wurde dieses Blatt an zentraler Stelle in der Vollzugsgeschäftsstelle abgelegt. Nach Rückgabe wurde auf dem gleichen Formular von dem Mitarbeitenden der Geschäftsstelle gegengezeichnet und das Blatt wieder der zurückgereichten Gefangenenpersonalakte beigeheftet. Durch dieses Verfahren ist auf einen Blick die Nutzung von Akten durch nicht in der Vollzugsgeschäftsstelle beschäftigtes Personal sowie der Verbleib der Akten und ggf. deren noch nicht erfolgter Rücklauf feststellbar. Nicht nur zur Sicherung des Aktenbestands, sondern auch für Kontrollzwecke stellt diese Verfahrensweise eine gute Grundlage dar. Durch die erfreulich unkomplizierte und nachvollziehbare Praxis wird zudem auch belegt, dass ein solches Verfahren ohne größere Beeinträchtigung der Verwaltungsabläufe eingehalten werden kann.
Die stichprobenweise Auswertung der zum Entnahmetermin aus der jeweiligen Gefangenenpersonalakte ersichtlichen weiteren Veränderungen bzw. Vermerke oder Verfügungen ergab eine Nutzung der Gefangenenpersonalakten für dienstlich zulässige Zwecke.

Im Gegensatz dazu zeigte sich erneut ein alt bekanntes Problem hinsichtlich der Aktenvernichtung im Wege der Auftragsdatenverarbeitung. Zum Grundsätzlichen der Auftragsdatenverarbeitung im Justizvollzug hatte sich der Landesbeauftragte bereits im VIII. Tätigkeitsbericht (Ziff. 22.2) geäußert. In Kenntnis dieser Ausführungen und der Lösungsvorschläge aus dem Justizministerium im Rahmen der Stellungnahme der Landesregierung zum VIII. Tätigkeitsbericht war der Landesbeauftragte davon ausgegangen, dass diese Thematik befriedigend geregelt werden würde. Aber es verblieb wohl weitgehend bei der gewählten Entsorgungsform durch Auftragsverarbeitung und - wie schon zu Ziff. 19.1 festgestellt - lag dem Landesbeauftragten auch bezüglich der geprüften Justizvollzugsanstalt keine offizielle Information zu einer Auftragsdatenverarbeitung vor. Da jedoch ein nicht-öffentlicher Auftragnehmer beteiligt war, auf den die Vorschriften des DSG-LSA nicht anwendbar sind, hätte der Landesbeauftragte über eine entsprechende Beauftragung gem. § 8 Abs. 6 Satz 2 DSG-LSA unterrichtet werden müssen; dies war versäumt worden. Zwar gab es den Hinweis, dass das Landgericht, in dessen Bezirk die kontrollierte Justizvollzugsanstalt ansässig ist, den Entsorgungsvertrag abgeschlossen hatte, aber weitergehende Informationen wurden nicht erteilt. Es konnten daher weder die konkreten Vertragsbedingungen nachvollzogen werden, noch konnte der Landesbeauftragte klären, wie sich der Auftraggeber von der Einhaltung der beim Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen überzeugt hat (siehe § 8 Abs. 2 Satz 4 DSG-LSA).
Bis zum Ende des aktuellen Berichtszeitraums wurde die Unterrichtung nach § 8 Abs. 6 Satz 2 DSG-LSA nicht nachgeholt.
Die Ausgestaltung des Auftragsverhältnisses aufgrund der Vielzahl beteiligter Stellen wird noch zu klären sein.
Zum 2. Quartal 2009 übersandte das Justizministerium schließlich ein Schreiben, in dem mitgeteilt wurde, dass das Landgericht eine schriftliche Vereinbarung mit den anderen Behörden hinsichtlich der Vergabe von Auftragsdatenverarbeitungen schließen wolle. Das Justizministerium teilte jedoch mit keiner Silbe mit, auf welcher Rechtsgrundlage ein solches Verfahren zulässig sein soll. Ob eine Vereinbarung ausreicht, die eigene Verantwortlichkeit der vom Landgericht „betreuten“ Stellen auf das Landgericht zu

verlagern, erscheint keineswegs selbstverständlich, da eine differenzierte ausdrückliche Regelung besteht. So darf zwar nach § 8 Abs. 2 Satz 3 DSG-LSA auch eine Fachaufsichtsbehörde einen Auftrag erteilen. Allerdings ist ein Landgericht nicht Fachaufsichtsbehörde gegenüber einer Justizvollzugsanstalt.
In Bezug auf die Anfrage, wie sich das Landgericht als verantwortliche Stelle über die beim Auftraggeber getroffenen technisch organisatorischen Maßnahmen überzeugt habe, wurde mitgeteilt, das Landgericht habe sich auf eine Zertifizierung eines privaten Zertifizierungsunternehmens nach DIN EN ISO 9001:2000 bezüglich des Auftragnehmers verlassen. Dieses Verfahren entspricht nicht dem eindeutigen Wortlaut des Gesetzes.

Ein weiteres Manko war leider auch bei der geprüften Justizvollzugsanstalt die Erstellung des - bis zum Kontrolltermin nicht vorhandenen - Verfahrensverzeichnisses.
Unabhängig von der gesetzlichen Pflicht, ein Verfahrensverzeichnis zu führen, sollten die dafür notwendige Feststellungen zum Verfahrensverzeichnis nicht als verzichtbarer Aufwand angesehen werden, da sie insbesondere auch der Eigenkontrolle dienen (siehe Ziff. 19.1). Bedauerlicherweise entstand der Eindruck mangelnder Ernsthaftigkeit hinsichtlich der Erstellung dieser Unterlagen. Zwar wurden nach den Kontrollhinweisen des Landesbeauftragten einige Feststellungen zum Verfahrensverzeichnis übersandt. Diese waren jedoch so unzureichend, dass die darin zu findenden Bezüge u. a. auf hessische Vorschriften und hessische EDV-Einrichtungen eher als amüsante Erscheinung am Rande betrachtet werden konnten.
Schließlich wurden Ende Januar 2009 etliche erneuerte Festlegungen zum Verfahrensverzeichnis übersandt, bei denen auf den ersten Blick schon festzustellen war, dass z. B. keine Rechtsgrundlagen für die Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten aufgeführt worden waren. Zudem waren die technisch-organisatorischen Maßnahmen nach § 6 DSG-LSA vielfach nicht ausreichend beschrieben.
Insgesamt steht die zusammenfassende Auswertung mit den zuständigen Stellen der Justiz noch aus und wird ggf. Gegenstand des nächsten Tätigkeitsberichts sein.

23.3. Jugendstrafvollzugsgesetz

Wie im VIII. Tätigkeitsbericht (Ziff. 22.3) darlegt, hatte das Bundesverfassungsgericht festgestellt, dass die inhaltliche Ausgestaltung des Jugendstrafvollzugs besonderen verfassungsrechtlichen Anforderungen unterliegt. Der Gesetzgeber durfte speziell „*die Frage, inwieweit Besonderheiten, die einfachgesetzlich im Erziehungsgedanken des Jugendgerichtsgesetzes zum Ausdruck gebracht sind, einer Ordnung des Jugendstrafvollzugs nach den Regeln des Erwachsenenstrafvollzugs entgegenstehen,... nicht den Gerichten zur Beantwortung ... überlassen, sondern musste sie selbst beantworten*“.

Zu dem ihm im Mai 2007 vorgelegten Entwurf hatte der Landesbeauftragte eine datenschutzfreundliche Fassung des neuen Jugendstrafvollzugsgesetzes (JStVollzG LSA) angemahnt.

So regte er an, angesichts des vielfach betonten Erziehungsziels, zwischen Personen im geschlossenen Vollzug, im offenen Vollzug und entlassenen Gefangenen bei der Erhebung, Verarbeitung und Nutzung von deren Daten zu unterscheiden.
Soweit eine Zusammenarbeit der Jugendanstalt mit externen Dritten erforderlich werde, sollte vorgesehen werden, diese Personen, soweit ihnen Daten Betroffener zur Kenntnis gelangen können, nach dem Verpflichtungsgesetz zur Verschwiegenheit zu verpflichten. Zwar regelt das letztlich erlassene JStVollzG LSA vom 7. Dezember 2007 (GVBl. LSA S. 368) die Verschwiegenheitspflicht dieses Personenkreises. Die vorgeschlagene ausdrückliche Regelung wurde jedoch nicht aufgenommen. Auch wenn die bestehende Regelung im „Gesetz über die förmliche Verpflichtung nichtbeamteter Personen (Verpflichtungsgesetz)“ lediglich als Soll-Vorschrift ausgestaltet ist, hofft der Landesbeauftragte, dass alle relevanten Personen entsprechend verpflichtet werden.
Die schon im Gesetzentwurf vorhandene Festlegung, welche die Teilnahme anderer Gefangener am Zugangsgespräch auch ausnahmsweise nicht zulässt, hatte er ausdrücklich begrüßt. Die Teilnahme würde anderen Gefangenen nämlich unnötig personenbezogene Informationen des Neuzugangs verschaffen können, die diesem zum Nachteil im Vollzugsalltag gereichen könnten. Die Regelung verhindert damit vor allem auch, dass eine Gesprächsteilnahme anderer Gefangener per Einwilligung des Neuen herbeigeführt werden kann. Es wird damit gesetzlich zudem berücksichtigt, dass z. B. aufgrund von Sprachbarrieren eine wirksame Einwilligung häufig nicht zustande kommen dürfte.

Der Landesbeauftragte hatte darauf gedrungen, dass die Pflicht, Gesprächsteilnehmer auf eine Überwachung ihres Telefongesprächs mit einem Gefangenen hinzuweisen, der Anstalt und nicht dem Gefangenen auferlegt sein sollte. Seine Gründe hierfür hatte er bereits im vergangenen Tätigkeitsbericht (vgl. dort Ziff. 22.2) dargelegt.

Die Erforderlichkeit einer Regelung zur Erfassung biometrischer Merkmale bei jugendlichen Gefangenen war dem Landesbeauftragten nicht nachvollziehbar begründet, da die sonstigen Merkmale und körperlichen Kennzeichen zur Identifizierung ausreichend erscheinen. Die behauptete hohe Fluktuation von Gefangenen trifft nach hiesiger Kenntnis zumindest auf die einzige Jugendanstalt in Sachsen-Anhalt nicht zu. Die in der Begründung genannte „einfache Handhabung“ ist als Hinweis auf „Verwaltungsbequemlichkeit“ für sich allein nicht geeignet, einen weitergehenden Grundrechtseingriff zu begründen, der zudem verfassungsrechtlich keineswegs geringfügig ist. Das Bundesverfassungsgericht hat zuletzt in einer Entscheidung vom 4. Februar 2009 (AnwBl. 2009, 303) deutlich gemacht, dass *„der bloße Umstand, dass Verwaltungsabläufe sich ohne eingriffsvermeidende Rücksichtnahmen einfacher gestalten,* „im beurteilten Fall*“ noch weniger als in anderen, weniger sensiblen Bereichen geeignet* ist*, den Verzicht auf solche Rücksichtnahmen* (hinsichtlich der Menschenwürde des Betroffenen) *zu rechtfertigen.“*
Zweifel bestehen zudem nach wie vor an der Erforderlichkeit einer Speicherung dieser Daten in kriminalpolizeilichen Sammlungen.
Auch die Regelungen zur Löschung der erhobenen biometrischen Daten nach (spätestens) zwei Jahren sind nicht ausreichend begründet worden. Da

die Gefangenenpersonalakte bei Verlegung von Gefangenen mitgereicht wird, ist nicht nachzuvollziehen, warum die Daten bei der bisherigen Justizvollzugsanstalt über einen längeren Zeitraum weiter gespeichert bleiben müssen - zumal in der neuen Justizvollzugsanstalt eine erneute Erhebung/ Speicherung durchgeführt werden dürfte.
Hinsichtlich eines aus dem Strafvollzug entlassenen Gefangenen ist die gesetzlich nun eingeräumte Speicherdauer noch weniger erklärbar. Aus der Begründung des Gesetzentwurfs ließ sich kein hinreichender Anhaltspunkt zur Erforderlichkeit entnehmen. Dass sich aus den zur weiteren Speicherung vorgesehenen Daten der ehemaligen Gefangenen deren mögliche Gefährlichkeit ergeben und einschätzen lassen soll (so aber die Gesetzesbegründung zu § 74, dem heutigen § 75 JStVollzG LSA), ist kaum realistisch, da diese Daten ausschließlich das „Äußere“ der Gefangenen betreffen.
Der Landesbeauftragte wird bei künftigen Kontrollen prüfen, ob eine Ermessenausübung erfolgte oder ob undifferenziert für zwei Jahre gespeichert wurde.

Mit Blick auf die in § 6 DSG-LSA geforderte Revisionsfähigkeit von Datenhaltungen bzw. auf das Gefangenenpersonalakten-Geheimnis hatte der Landesbeauftragte angeregt, auch vor dem Hintergrund seiner Kontrollerfahrungen, eine Regelung zum Protokollieren/Dokumentieren des Einzelfall-Zugriffs auf die Gefangenenpersonalakte durch solche Personen, welche nicht regelmäßig mit der Führung der Gefangenenpersonalakte betraut sind, ins JStVollzG LSA aufzunehmen. Auch wenn dies nicht aufgegriffen wurde, geht er davon aus, dass eine entsprechende Verfahrensweise im Vollzugsalltag beachtet werden wird.

Ohne seine Kritik im Übrigen einschränken zu wollen, hat der Landesbeauftragte die weitgehend eigenständige Regelung im JStVollzG LSA zum Datenschutz positiv vermerkt. Dies bewirkt nicht nur eine bessere Handhabbarkeit für die Anwendung in der täglichen Vollzugspraxis. Da Wesentliches, wie z. B. Zweckbindungs- oder Löschungsregelungen sinnvoll nicht durch Verweis auf das DSG-LSA normiert werden können, bietet sich eine eigenständige Formulierung datenschutzrechtlicher Bestimmungen geradezu an und erhöht durch das Vermeiden zahlreicher Verweise die Verständlichkeit des Gesetzes. Die eigenständige Regelung genügt daher vorliegend auch eher dem verfassungsrechtlichen Grundsatz der Normenklarheit (das Bundesverfassungsgericht hatte sich bereits kritisch zu langen Verweisungsketten geäußert (BVerfG NJW 2004, 2213)).

Ein stets wiederkehrendes Thema bei Regelungsvorhaben zum Umgang mit personenbezogenen Daten ist die Festlegung zur zulässigen Speicherdauer erhobener Daten. Grundsätzlich darf nur im Rahmen des Erforderlichen gespeichert werden, dann ist sofort zu löschen. Mit dem nunmehr verabschiedeten Gesetz wurde die im Strafvollzugsgesetz des Bundes bestehende Löschfrist von 2 auf 5 Jahre verlängert. Ein verfassungsrechtlich tragender Grund für die Verlängerung ist nicht ersichtlich und auch nicht dargelegt worden. Insbesondere ist die in der Begründung zum Gesetzentwurf herangezogene Darstellung, dass die kürzere Frist zu vermeidbarem Verwaltungsaufwand geführt habe, weder sachverhaltlich nachvollziehbar belegt worden, noch kann ein vermeidbarer Verwaltungsaufwand für sich alleine eine Inten-

sivierung eines Grundrechtseingriffs rechtfertigen. Hier ist gleichfalls auf die Eingangs dieser Ziffer erwähnte Rechtsprechung des Bundesverfassungsgericht hinzuweisen.

Leider wurden nur wenige Anregungen des Landesbeauftragten übernommen. Unerfreulich ist ebenfalls, dass in der Verwaltungsvorschrift die gesetzlichen Regelungen, welche den Umgang mit personenbezogenen Daten betreffen, nicht für die Anwendung in der Vollzugspraxis umgesetzt wurden. Der dem Landesbeauftragten bekannt gegebene Vorentwurf einer Verwaltungsvorschrift zum Jugendstrafvollzug war diesbezüglich deutlich praxisgerechter gewesen. Der Landesbeauftragte hofft, dass es insoweit noch zu Ergänzungen kommt.

23.4. Mobilfunkblocker im Justizvollzug

Da datenschutzrechtliche Schutznormen u. U. indirekt berührt sein könnten, äußerte sich der Landesbeauftragte zu dem ihm vom Justizministerium zur Stellungnahme übersandten Entwurf eines Gesetzes zur Verhinderung von Mobilfunkverkehr und unerlaubter Telekommunikation durch Gefangene (Mobilfunkverhinderungsgesetz - MFunkVG - LT-Drs. 5/1940).

So erschien es ihm denkbar, dass durch den Entwurf ein Gesetz geschaffen wird, das eine nicht erfüllbare Forderung aufstellt (§ 2 Abs. 2 MFunkVG). Damit würde sich der Gesetzgeber in ungute Nähe zu den „unglücklichen“ Regelungen begeben, die einst für den Bereich des Insolvenzrechts eine Verpflichtung vorsahen, das Kopieren im Internet bekannt gemachter Insolvenzdaten zu verhindern - dies war und ist technisch unmöglich.
Trotz der in der Entwurfsbegründung dargelegten Absicht, die Störgeräte genau einmessen zu wollen, um eine über die Justizvollzugsanstalt-Gelände hinausgreifende Störung zu vermeiden, scheinen dem Landesbeauftragte hieran Zweifel angebracht. Denn auf eine - von Baden-Württemberg angeregte - entsprechende bundesweite Regelung im Telekommunikationsrecht wurde nach bisherigem Kenntnisstand bislang u. a. deshalb verzichtet, weil es nicht möglich ist, eine ausreichende „Trennschärfe“ zu gewährleisten, um den Telekommunikations-Verkehr außerhalb der jeweiligen Justizvollzugsanstalt nicht zu beeinträchtigen.
Naheliegend ist darum auch, dass der Entwurf inhaltlich einen Regelungsgegenstand betreffen könnte, der die ausschließliche Gesetzgebungszuständigkeit des Bundes berührt.
Im Gesetzestext fiel auf, dass eine Regelung nur den Gefangenen den Besitz und Betrieb von Mobiltelefonen untersagt. Die Grundrechte der Bediensteten werden jedoch hinsichtlich des Betriebs von Mobiltelefonen in gleicher Weise berührt werden. Eine Regelung, welche vorsieht, dass in Abteilungen für den offenen Vollzug Ausnahmen möglich sein sollen, erschien dem Landesbeauftragten zu unbestimmt. Eine Vorgabe, unter welchen sachlichen bzw. vollzuglichen Voraussetzungen die Nutzung von Mobiltelefonen zugelassen werden könnte, sollte im Gesetz fixiert werden. Allerdings dürfte es schon gar nicht möglich sein, eine einzelne Abteilung aus einer Justizvollzugsanstalt mobilfunktechnisch „herauszutrennen“.

Der Gesetzentwurf soll, zwecks Auffindens von Mobilfunkgeräten in der Justizvollzugsanstalt, auch zur Nutzung von Instrumenten ermächtigen, die funktional einem IMSI-Catcher entsprechen. Zwar fordert der Gesetzentwurf, dass diese Detektionsgeräte keinen Mobilfunkverkehr außerhalb der Justizvollzugsanstalt beeinträchtigen dürfen. Andernfalls könnte es in der Tat zu Eingriffen in die Rechte Dritter kommen. Aber auch hier ist die Frage der technischen Realisierbarkeit der - ansonsten zutreffenden - gesetzlichen Forderung nicht geklärt.

23.5. Nicht anonymisierte Speicherung von Entscheidungen nach Verkündung/Rechtskraft

Bei Kontrollen in Gerichten wird vom Landesbeauftragten immer wieder nachgefragt, wie es das richterliche Personal mit sog. Kammersammlungen hält. Auch im Berichtszeitraum war dies der Fall. Die Antworten sind regelmäßig wenig aufschlussreich.
Erörtert, nicht jedoch durch Einsicht in die Speichertechnik geprüft, wurde auch diese, schon mit anderen Gerichten diskutierte, zusätzliche und nicht anonymisierte Speicherung von Entscheidungen in weiteren Verzeichnissen der gerichtlichen EDV, die nach Abschluss eines Verfahrens durch die Richterinnen und Richter u. U. selbst vorgenommen wird.
Dies ist rechtlich bedenklich, denn die personenbezogenen Daten von Verfahrensbeteiligten dürften für andere Verfahren an den richterlichen EDV-Arbeitsplätzen in der Regel nicht mehr gebraucht werden. Ihre Speicherung ist damit datenschutzrechtlich nicht erforderlich. Die Daten sind dann gem. § 16 Abs. 2 DSG-LSA zu löschen. Eine (Kammer-)Sammlung von similes könnte auch ohne Personenbezug angelegt werden.
Der Landesbeauftragte hat in den kontrollierten Gerichten angeregt, durch Nachfragen zu klären, ob derartige Sammlungen vorgehalten werden. Falls diese personenbezogen geführt werden sollten, wäre eine datenschutzgerechte Verfahrensweise zu wählen, d. h. die personalisierten Datensätze von Entscheidungssammlungen wären zu anonymisieren oder zu löschen.

24. Telekommunikations- und Medienrecht

24.1. Vorratsdatenspeicherung

Das Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wurde am 9. November 2007 vom Bundestag verabschiedet (BGBl. I S. 3198) und ist größtenteils zum 1. Januar 2008 in Kraft getreten (vgl. Ziff. 19.2). Damit wurde unter anderem die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, in nationales Recht umgesetzt (vgl. VIII. Tätigkeitsbericht, Ziff. 23.1).

Das Gesetz verpflichtet die Anbieter öffentlich zugänglicher Telekommunikationsdienste, umfangreiche Verkehrsdaten für **sechs Monate auf Vorrat** für die Strafverfolgungsbehörden zu speichern (§§ 113a, b TKG). Damit wird das

gesamte Telekommunikationsverhalten aller Bürgerinnen und Bürger erfasst, ohne dass ein konkreter Verdacht vorliegt.

Seit 1. Januar 2008 müssen Anbieter von öffentlich zugänglichen Telefondiensten folgende Verkehrsdaten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses
2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone, bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht die Zeitpunkte der Versendung und des Empfangs der Nachricht
3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst
4. im Fall mobiler Telefondienste ferner:
   a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss
   b) die internationale Kennung des anrufenden und des angerufenen Endgerätes
   c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen
   d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle.

Anbieter von Mobilfunknetzen für die Öffentlichkeit sind verpflichtet, zu den Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografische Lage der jeweiligen Funkzelle sowie deren Hauptstrahlrichtung ergibt.

Im Fall von Internet-Telefondiensten müssen seit 1. Januar 2009 auch die Internetprotokoll-Adresse (IP-Adresse) des anrufenden und des angerufenen Anschlusses gespeichert werden.

Seit 1. Januar 2009 müssen Anbieter von Diensten der elektronischen Post (E-Mail) folgende Verkehrsdaten speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die IP-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht
2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die IP-Adresse der absendenden Telekommunikationsanlage
3. bei Zugriff auf das elektronische Postfach dessen Kennung und die IP-Adresse des Abrufenden
4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Ebenfalls seit 1. Januar 2009 müssen Anbieter von Internetzugangsdiensten folgende Verkehrsdaten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene IP-Adresse
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt
3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen IP-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen nicht gespeichert werden. Die Verkehrsdaten können von den Strafverfolgungsbehörden unter den Voraussetzungen des § 100g StPO zur Verfolgung schwerer Straftaten (Katalogstraftaten i. S. d. § 100a StPO) abgerufen werden.

Irland und die Slowakei hatten gegen die Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 vor dem Europäischen Gerichtshof geklagt, weil sie als eine Binnenmarktregelung zustande kam. Nach Ansicht der beiden Länder dient die Vorratsdatenspeicherung jedoch der Bekämpfung schwerer Verbrechen und hätte deshalb als EU-Rahmenbeschluss vom zuständigen EU-Ministerrat verabschiedet werden müssen. Dessen ungeachtet stellte der Europäische Gerichtshof am 10. Februar 2009 fest, dass die Richtlinie zu Recht auf der Grundlage des EG-Vertrags erlassen worden ist, da sie in überwiegendem Maß das Funktionieren des Binnenmarkts betrifft (Az. C-301/06, MMR 2009, 44). Er stellte außerdem klar, dass sich die Klage allein auf die Wahl der Rechtsgrundlage bezieht und nicht auf eine eventuelle Verletzung der Grundrechte als Folge von mit der Richtlinie verbundenen Eingriffen in das Recht auf Privatsphäre.

Gegen die §§ 113a und 113b des Telekommunikationsgesetzes (TKG) in der Fassung des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG wurden Ende 2007 bzw. Anfang 2008 beim Bundesverfassungsgericht mehrere Verfassungsbeschwerden, darunter eine Sammelbeschwerde, eingelegt, weil eine systematische, verdachtslose Speicherung personenbezogener Daten auf Vorrat mit den Grundrechten des Grundgesetzes offensichtlich unvereinbar sei.

Daraufhin erließ das Bundesverfassungsgericht eine einstweilige Anordnung Beschluss vom 11. März 2008 (1 BvR 256/08, MMR 2008, 303), in der festgelegt wurde, dass Anbieter von Telekommunikationsdiensten die verlangten Daten zwar zu erheben und zu speichern haben. Die Daten sind jedoch nur dann an die Strafverfolgungsbehörde zu übermitteln, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat im Sinne des § 100a Abs. 2 Strafprozessordnung (StPO) ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre (§ 100a Abs. 1 StPO). In den übrigen Fällen des § 100g Abs. 1 StPO ist von einer Übermittlung der Daten einstweilen abzusehen.
Allerdings wurde die Aussetzung des Vollzugs von § 113a TKG, der die Speicherungspflicht für die Verkehrsdaten regelt, abgelehnt, da das Bundesverfassungsgericht in der Vorratsdatenspeicherung keinen so schwerwie-

genden und irreparablen Nachteil sah, der eine solche Aussetzung rechtfertigen könnte.

Mit den Beschlüssen vom 1. September 2008, 28. Oktober 2008 und 22. April 2009 wurde durch das Bundesverfassungsgericht die einstweilige Anordnung vom 11. März 2008 für die Dauer von 6 Monaten, längstens jedoch bis zur Entscheidung über die Verfassungsbeschwerde, wiederholt. Der Zugriff auf die Vorratsdaten zur Gefahrenabwehr wurde für die Polizei und Geheimdienste eingeschränkt. Das Bundesverfassungsgericht begründet die weiteren Einschränkungen mit der Schaffung neuer Abrufnormen in Bayern und Thüringen, die den „vorsorglichen“ Zugriff auf Verbindungs- und Standortdaten durch die Polizei erlauben.

Anzumerken ist noch, dass mit der Änderung des Bundeskriminalamtsgesetzes (s. o. Ziff. 18.3) das Bundeskriminalamt die Befugnis zum Abruf von auf Vorrat gespeicherten Verkehrsdaten zur Abwehr einer dringenden Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr hat.

24.2. Zehnter Rundfunkänderungsstaatsvertrag

Mit dem Zehnten Rundfunkänderungsstaatsvertrag (GVBl. LSA 2008 S. 248), der zum 1. September 2008 in Kraft getreten ist, wurde auch der Rundfunkgebührenstaatsvertrag (RGebStV) geändert. Dieser enthielt seit dem Inkrafttreten des Achten Rundfunkänderungsstaatsvertrags am 1. April 2005 datenschutzrechtlich bedenkliche Regelungen in Bezug auf die Befreiung von der Rundfunkgebührenpflicht (§ 6 Abs. 2 RGebStV) und die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 8 Abs. 4 RGebStV). Aufgrund dessen wurden im Rahmen einer Arbeitsgruppe, die sich aus Vertretern der Rundfunkanstalten, Vertretern der Rundfunkdatenschutzbeauftragten, Vertretern der Rundfunkreferenten der Länder und Vertretern der Datenschutzbeauftragten des Bundes und der Länder zusammensetzte, bereits im Jahr 2006 Änderungsvorschläge erarbeitet, die nunmehr im Zehnten Rundfunkänderungsstaatsvertrag umgesetzt wurden (vgl. VII. Tätigkeitsbericht, Ziff. 23.5).

Im Achten Rundfunkänderungsstaatsvertrag wurde in Folge der Neuregelung der Gebührenbefreiung festgelegt, dass die Anträge zur Befreiung von der Rundfunkgebührenpflicht nicht mehr bei den Sozialämtern, sondern direkt bei der zuständigen Landesrundfunkanstalt bzw. der durch diese beauftragten Gebühreneinzugszentrale (GEZ) zu stellen sind. Zusammen mit der Antragstellung waren die Voraussetzungen für die Befreiung durch Vorlage der entsprechenden Sozialleistungsbescheide im Original oder in beglaubigter Kopie nachzuweisen. Durch diese Regelung erhielt die GEZ eine Vielzahl sensibler personenbezogener Daten der Antragsteller und u. U. auch deren Angehöriger, die sie für die Befreiung von der Rundfunkgebührenpflicht nicht benötigte. Die Änderung in § 6 Abs. 2 RGebStV ermöglicht nun auch die Vorlage einer entsprechenden Bestätigung des Leistungsträgers im Original, so dass die GEZ nur noch die für sie notwendigen Daten erhält, um über die Gebührenbefreiung zu entscheiden.

Mit § 8 Abs. 4 RGebStV wurde im Rahmen des Achten Rundfunkänderungsstaatsvertrag eine Regelung geschaffen, die den öffentlich-rechtlichen Rundfunkanstalten bzw. der GEZ das Erheben, Verarbeiten und Nutzen personenbezogener Daten gem. § 28 BDSG - und damit einer Vorschrift, die für den nicht-öffentlichen Bereich konzipiert ist - erlaubt. Die Befugnisse des § 28 BDSG stehen nach § 27 Abs. 1 BDSG den nicht-öffentlichen Stellen sowie solchen öffentlichen Stellen zu, die als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Die öffentlich-rechtlichen Rundfunkanstalten stehen jedoch hinsichtlich des Gebühreneinzugs in keinem Wettbewerb zu anderen Rundfunkveranstaltern, so dass diese Regelung systemwidrig war. Mit der Änderung des § 8 Abs. 4 RGebStV wurde nunmehr die Erhebung personenbezogener Daten bei nicht-öffentlichen Stellen bezüglich Art, Umfang, Dauer und Zweckbestimmung der Datenverarbeitung abschließend geregelt. Allerdings wird damit dem Grundsatz der Datensparsamkeit und Datenvermeidung noch nicht hinreichend entsprochen.

24.3. Änderungen im Urheberrecht

Am 1. September 2008 ist das Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (BGBl. I S. 1191) in Kraft getreten (vgl. VIII. Tätigkeitsbericht, Ziff. 23.4). Damit wurde mit einiger Verspätung die Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 in nationales Recht umgesetzt. Das Gesetz umfasst u. a. Änderungen im Patent-, Gebrauchsmuster-, Marken-, Urheberrechts-, Geschmacksmuster- und Sortenschutzgesetz.

Zu den wichtigsten Neuerungen im Urheberrecht zählt der zivilrechtliche Auskunftsanspruch gegen Dritte, die an Rechtsverletzungen unbeteiligt waren, wie z. B. Internetprovider. Damit soll es einfacher werden, die Identität von möglichen Rechtsverletzern, etwa in Tauschbörsen, aufzudecken. Kann die Auskunft nur unter Verwendung von Verkehrsdaten erteilt werden, z. B. unter Angabe der zu einer IP-Adresse gespeicherten Nutzerdaten, ist eine vorherige richterliche Anordnung erforderlich. Voraussetzung für diesen Auskunftsanspruch ist ein Verstoß gegen das Urheberrecht in gewerblichem Ausmaß.

Seit Inkrafttreten des Gesetzes gab und gibt es eine Reihe von Gerichtsentscheidungen, die sich mit der Frage beschäftigten, wann eine Rechtsverletzung in gewerblichem Ausmaß vorliegt (vgl. MMR 2008, 787, Geißler, Jüngel).
So urteilte insbesondere das Landgericht Köln mehrfach (u. a. mit Beschluss vom 2. September 2008 - Az. 28 AR 4/08), dass eine Verletzung des Urheberrechts in gewerblichem Ausmaß bereits dann vorliegt, wenn ein einzelnes Musikalbum zum Download angeboten wird. Entscheidend sei dabei nicht die Anzahl der veröffentlichten Musikstücke, sondern die Schwere der Verletzung, die sich beispielsweise daraus ergebe, dass es sich um ein erst kürzlich veröffentlichtes, stark nachgefragtes Musikalbum bzw. um eines der meistverkauften Musikalben handele.

Allerdings gibt es auch andere Gerichtsentscheidungen wie den Beschluss des Landgerichtes Frankenthal vom 15. September 2008 (Az. 6 O 325/08).

Die Entscheidung orientierte sich offensichtlich an den von deutschen Generalstaatsanwaltschaften erarbeiteten Leitlinien, nach denen Anschlussinhaber nur noch ermittelt werden sollen, wenn sie mehr als 3000 Musik- oder mehr als 200 Filmdateien über Tauschbörsen zum Download angeboten haben.
Das Oberlandesgericht Zweibrücken entschied in zweiter Instanz (Beschluss vom 27. Oktober 2008, Az. 3 W 184/08) zwar ebenfalls, dass es sich im vorliegenden Fall nicht um eine Urheberrechtsverletzung in gewerblichem Ausmaß handelte. Allerdings stellte das Gericht fest, dass das gewerbliche Ausmaß einer Rechtsverletzung nicht von der Anzahl der Down- und Uploads abhängt, sondern eher von der Bekanntheit und der Neuheit eines Produktes. Da es sich im vorliegenden Fall um ein drei Monate altes Computerspiel handelte und keine Umstände zu erkennen waren, die eine besondere Schwere der Rechtsverletzung begründen könnten, lag nach Ansicht des Gerichtes kein gewerbliches Ausmaß vor.

Da zur Realisierung des Auskunftsanspruchs in das vom Grundgesetz geschützte Fernmeldegeheimnis eingegriffen wird, müssen die Voraussetzungen für einen solchen Eingriff klar geregelt werden. Außerdem muss die Verhältnismäßigkeit gewahrt werden, d. h. die Schwere der Rechtsverletzung muss einen solchen Grundrechtseingriff rechtfertigen. Aus diesen Gründen ist der Gesetzgeber gefordert, normenklare Regelungen zu schaffen, die eine einheitliche Rechtsprechung ermöglichen.

24.4. Änderungen im Telemediengesetz

Am 14. Januar 2009 verabschiedete die Bundesregierung den Entwurf eines (Artikel-)Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BT-Drs. 16/11967). Artikel 1 dieses Gesetzes umfasst die Novellierung des BSI-Gesetzes, mit der dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erweiterte Befugnisse zur Abwehr von Angriffen auf die IT-Infrastruktur des Bundes erteilt werden sollen (vgl. Ziff. 0). Verwunderlich ist, dass unter der Überschrift „Stärkung der Sicherheit in der Informationstechnik des Bundes“ in Artikel 3 auch das Telemediengesetz (TMG) geändert werden soll.

Der Gesetzentwurf sieht vor, an § 15 TMG einen Absatz 9 anzufügen, der es Diensteanbietern erlaubt, Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen ihrer für Zwecke ihres Dienstes genutzten technischen Einrichtungen zu erheben und zu verwenden. Begründet wird diese neue Regelung damit, dass das TMG bisher keine dem § 100 Abs. 1 Telekommunikationsgesetz entsprechende Bestimmung enthält. Wie Telekommunikationsdiensteanbieter bräuchten auch Telemedienanbieter eine entsprechende Ermächtigung, um beispielsweise Angriffe abwehren zu können. Zur Erkennung und Abwehr solcher Angriffe gegen Webseiten und andere Telemedien sei die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich.

In ihrer Entschließung vom 18. Februar 2009 **(Anlage 26)** wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unter anderem auch gegen diese weit auslegbare Gesetzesbegründung, die öffent-

lichen und privaten Anbietern von Telemedien pauschal die Möglichkeit einer umfassenden Protokollierung des Surfverhaltens ihrer Nutzer bietet.

Im Zuge der Beratungen im Bundestag wurde diese kritische Regelung nicht weiterverfolgt (BT-Drs. 16/13259).

24.5. Sperrung von Internetseiten zur Bekämpfung von Kinderpornographie

Die Bundesregierung hat am 22. April 2009 auf Vorlage des Bundesministers für Wirtschaft und Technologie den Entwurf für ein Gesetz zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen beschlossen (BT-Drs. 16/12850).

Die neuen Regelungen enthalten Änderungsvorschläge zum Telemediengesetz und zum Telekommunikationsgesetz und beschränken sich auf Zugangserschwerungen zu kinderpornographischen Inhalten.

Auf der Basis von **Sperrlisten** des Bundeskriminalamts (BKA) werden alle großen privaten Internetzugangsanbieter verpflichtet, den Zugang zu kinderpornographischen Inhalten im Internet durch geeignete technische Maßnahmen zu erschweren. Provider mit weniger als 10 000 Kunden und staatliche Einrichtungen werden von dieser Verpflichtung ausgenommen. Im Umkehrschluss bedeutet dies, dass für Kunden kleinerer Provider, für Mitarbeiter von staatlichen Einrichtungen, für Studenten an Hochschulen etc. der Zugang zu Kinderpornographie im Internet nicht erschwert wird. Einer der Gründe dafür ist laut Gesetzesbegründung, den Kreis derer zu beschränken, die Zugriff auf die Sperrliste erhalten. In anderen Ländern sind solche Sperrlisten bereits im Internet veröffentlicht worden.

Nutzern, die in der Sperrliste aufgeführte Seiten aufrufen, wird eine Stoppmeldung angezeigt, die sie über die Sperrung der Seite, die Gründe der Sperrung und eine Kontaktmöglichkeit zum BKA informiert.
Im Gegensatz zum Arbeitsentwurf vom 25. März 2009 schränkt der vorliegende Gesetzentwurf das Grundrecht des Fernmeldegeheimnisses ein, da die Provider personenbezogene Daten - nämlich die IP-Adresse - erheben und speichern und diese den Strafverfolgungsbehörden auf deren Anordnung übermitteln dürfen.
Die Kritik an dem geplanten Gesetz bezieht sich unter anderem darauf, dass die DNS-Sperren leicht umgangen werden können, indem im Browser die IP-Adresse der betreffenden Seite direkt eingegeben wird bzw. an Stelle des provider-eigenen DNS-Servers ein anderer frei verfügbarer DNS-Server eingetragen wird, der keine Sperrung von Seiten vornimmt.
Laut Presseberichten werden Seiten mit kinderpornographischem Inhalt zum großen Teil auf europäischen (auch deutschen!) und Servern bereit gestellt, also in Ländern, in denen Kinderpornographie strafrechtlich verfolgt wird. Es stellt sich deshalb die Frage, wieso die Strafverfolgungsbehörden nicht die Betreiber dieser Server zur Verantwortung ziehen und die kinderpornographischen Inhalte löschen lassen. Auf diese Weise würde der Zugang zu den Seiten nicht nur erschwert, sondern die Seiten wären im Internet nicht mehr verfügbar.

Außerdem ist nach Aussagen von Experten das World Wide Web nicht der normale Verbreitungsweg für kinderpornographische Inhalte. Stattdessen findet der Austausch über geschlossene Nutzergruppen und Netzwerke, über Peer-to-peer-Verbindungen bis hin zum per Chat und SMS koordinierten Postversand statt.

Ein weiterer Kritikpunkt ist die Tatsache, dass eine einzige Stelle - nämlich das BKA - entscheidet, welche Seiten in die Sperrliste eingetragen werden. Da hierfür kein richterlicher Beschluss erforderlich ist und die Sperrliste geheim gehalten wird, ist keine Kontrolle möglich, ob tatsächlich nur Seiten mit kinderpornographischem Inhalt aufgelistet sind. Es ist zu befürchten, dass immer neue Begehrlichkeiten geweckt werden, eine solche Sperrliste auch gegen Urheberrechtsverstöße, Glücksspiel, gewaltverherrlichende Darstellungen etc. einzusetzen und somit ein Instrument der Zensur zu schaffen.

Aus datenschutzrechtlicher Sicht scheint es bedenklich, unter dem Vorwand der Bekämpfung von Kinderpornographie in das verfassungsrechtlich geschützte Fernmeldegeheimnis der Internetnutzer einzugreifen, indem die IP-Adressen von den Providern gespeichert und an Strafverfolgungsbehörden übermittelt werden. Die Urheber der kinderpornographischen Inhalte werden durch die Einführung dieser DNS-Sperren nicht belangt. Statt die Inhalte zu löschen und die Anbieter zu verfolgen, wird jeder Internetnutzer „kriminalisiert“, der - absichtlich oder nicht - eine in der Sperrliste enthaltene Seite aufruft und auf die sogenannte Stoppseite umgeleitet wird.

Infolge der starken öffentlichen Kritik legten die Koalitionsfraktionen einen neu gefassten Entwurf für ein eigenständiges, nur den Bereich von Kinderpornographieangeboten betreffendes „Zugangserschwerungsgesetz“ vor, das der Bundestag am 18. Juni 2009 beschloss. Danach gilt das Prinzip „Löschen vor Sperren“, bei der Sperrung anfallende Nutzungsdaten werden nicht an die Strafverfolgungsbehörden weitergeleitet; ein beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit - insofern fachfremd - bestelltes Kontrollgremium soll die Sperrlisten beim BKA kontrollieren (BT-Drs. 16/13411).

24.6. Musterdienstanweisung zur Nutzung von E-Mail und Internet am Arbeitsplatz

Bereits im Jahr 2001 wurde durch das Ministerium des Innern eine Musterdienstanweisung über die Bereitstellung und Nutzung von Internet-Zugängen erlassen, die die ausnahmsweise private Nutzung von E-Mail und Internet am Arbeitsplatz erlaubt. Durch das hohe Spamaufkommen wurde es im Dezember 2005 erforderlich, auch im Landesinformationszentrum eine zentrale Spamfilterung aller eingehenden E-Mails durchzuführen. Das Ministerium des Innern informierte die Mitglieder des Koordinierungsausschusses Informationstechnik über diese Maßnahme und wies darauf hin, dass die Ressorts sowie deren nachgeordnete Bereiche bei Gestattung privater E-Mail-Nutzung eine Einwilligung ihrer Mitarbeiter in diese Spamfilterung einholen müssen. Gleichzeitig wurde die Überarbeitung der o. g. Musterdienstanweisung in Aussicht gestellt (vgl. VIII. Tätigkeitsbericht, Ziff. 23.5).

Im Rahmen dieser fast 3 Jahre dauernden Überarbeitung gab es zahlreiche Kontakte zwischen dem Landesbeauftragten und dem zuständigen Referat im Ministerium des Innern. Der Landesbeauftragte unterbreitete Lösungsvorschläge, die von einer gänzlichen Untersagung der privaten E-Mail- und Internetnutzung bis zur ergänzenden Einwilligung der Mitarbeiter in die zentrale Spamfilterung reichten. Allerdings hat der Landesbeauftragte wiederholt darauf hingewiesen, dass nur durch die Untersagung der privaten Nutzung der dienstlichen E-Mail-Adresse tatsächlich Rechtssicherheit geschaffen wird.

Die Frage der Rechtssicherheit bezieht sich dabei nicht nur auf die Möglichkeit, dass durch die zentrale Spam-Filterung u. U. auch erwünschte E-Mails unterdrückt werden können (vgl. §§ 206 Abs. 2 Nr. 2 StGB, 303a Abs. 2 StGB). Vielmehr stellt sich die Frage, ob durch die Einwilligung des Mitarbeiters in die Protokollierung seiner privaten E-Mail-Nutzung und in die Einsichtnahme in seine E-Mail-Kommunikation bei Abwesenheit tatsächlich das Fernmeldegeheimnis für den an der Kommunikation beteiligten Dritten eingeschränkt werden kann. Dieser hat nicht darin eingewilligt, dass der Inhalt seiner E-Mail-Kommunikation im Bedarfsfall von anderen Personen zur Kenntnis genommen werden kann. Außerdem unterliegen schon die näheren Umstände der E-Mail-Kommunikation – wer, wann mit wem kommuniziert hat – dem Fernmeldegeheimnis, so dass durch die Protokollierung in dieses eingegriffen wird.

Aus den o. g. Gründen hat der Landesbeauftragte wiederholt empfohlen, die ausnahmsweise private Nutzung des Internets weiterhin zu gestatten, die private E-Mail-Kommunikation aber nur mittels Web-Mail zu erlauben, d. h. die private Nutzung der dienstlichen E-Mail-Adresse zu untersagen. Diese Empfehlung entspricht auch der vom Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeiteten „Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz“.

Zur Frage der Rechtssicherheit äußert sich auch ein Gutachten vom 21. November 2007, welches die Firma T-Systems zur Bewertung der bestehenden Antispam-Strategie des Landes Sachsen-Anhalt und dem Vergleich möglicher zukünftiger Lösungsvarianten erarbeitet hat. Darin wird festgestellt, dass unabhängig von der technischen Lösung gesetzeskonforme organisatorische Regelungen zu treffen sind, da der an der E-Mail-Kommunikation beteiligte Dienstleister nur solche Lösungen implementieren darf, die er rechtssicher umsetzen kann. Die Gutachter kommen zu dem Ergebnis, dass eine wichtige diesbezügliche Regelung das nachweislich ausgesprochene Verbot der privaten E-Mail-Nutzung ist.

Getreu dem Motto „Was lange währt, wird endlich gut.“ erhielt der Landesbeauftragte ein Schreiben des Ministeriums des Innern vom 17. Juli 2008, in dem ihm ein überarbeiteter Entwurf einer Vorlage für die Staatssekretärskonferenz sowie eine geänderte Musterdienstanweisung als Anlage zugesendet wurden. Darin wurde nun erfreulicherweise seine wiederholt geäußerte Empfehlung berücksichtigt und die private Nutzung der dienstlichen E-Mail-Adresse untersagt.

Leider musste der Landesbeauftragte nach mehreren telefonischen Rückfragen am 24. Oktober 2008 feststellen, dass bei der unendlichen Geschichte dieser Musterdienstanweisung auch das Sprichwort „Man soll den Tag nicht vor dem Abend loben." seine Berechtigung erfuhr. Er wurde nämlich durch das Ministerium des Innern darüber informiert, dass die Staatssekretärskonferenz die Musterdienstanweisung bereits am 8. September 2008 zur Kenntnis genommen hatte, allerdings mit wesentlichen Änderungen. So wurde die im Entwurf enthaltene Regelung, privaten E-Mail-Verkehr nur über Webmail-Dienste abzuwickeln, dahingehend geändert, dass der private E-Mail-Verkehr möglichst über Webmail-Dienste abzuwickeln sei. Die Festlegung, dass die dienstliche E-Mail-Adresse ausschließlich für die dienstliche Kommunikation zu verwenden und eine Verwendung für private Zwecke untersagt ist, wurde gestrichen.

Durch diese Änderungen wurde zum einen das Ziel, Rechtssicherheit bei der E-Mail-Kommunikation zu schaffen, ad absurdum geführt, da davon auszugehen ist, dass Beschäftigte der Landesverwaltung ihre dienstliche E-Mail-Adresse weiterhin für private Zwecke nutzen werden und es somit zu Problemen bei der Wahrung des Fernmeldegeheimnisses kommen kann.

Zum anderen führen die Änderungen im Vergleich zur bisherigen Musterdienstanweisung auch noch zu einer „Verschlimmbesserung", da weitere Änderungen erforderlich gewesen wären. Im Punkt „Protokollierung und Kontrolle" wird festgelegt, dass im Zusammenhang mit der dienstlich zulässigen Nutzung der E-Mail-Systeme Verbindungsdaten protokolliert werden. Dadurch erhält der Mitarbeiter den Eindruck, dass bei der privaten Nutzung keine Protokollierung erfolgt, was nicht den Tatsachen entspricht, da eine Unterscheidung zwischen dienstlicher und privater E-Mail nicht möglich ist. In der Einwilligungserklärung ist nur von der Protokollierung der ausnahmsweisen privaten Internetnutzung die Rede. Somit entsteht für den Mitarbeiter wiederum der Eindruck, dass eine Protokollierung der privaten E-Mail-Kommunikation nicht stattfindet.

Mit Schreiben vom 23. Januar 2009 teilte das Ministerium des Innern mit, dass die Musterdienstanweisung nochmals überarbeitet wird und eine umfassende Einverständniserklärung der Bediensteten vorgesehen ist. Der Landesbeauftragte erwartete, dass die Überarbeitung diesmal zeitnah erfolgte. Diese lag auch im Juni 2009 immer noch nicht vor.

24.7. SPAM-Filterung von E-Mails

Das Thema SPAM etabliert sich als Dauerthema im Tätigkeitsbericht. Im VIII. Tätigkeitsbericht (Ziff. 23.5) wurde auf die Notwendigkeit einer Einwilligung zur SPAM-Filterung hingewiesen, sofern die private E-Mail-Nutzung am Arbeitsplatz gestattet ist. Grund ist die Verpflichtung des Arbeitgebers zur Wahrung des Fernmeldegeheimnisses, da er in diesem Falle Telekommunikationsdiensteanbieter nach dem Telekommunikationsgesetz (TKG) ist.

Auf Hinweis eines Petenten wurde der E-Mail-Server einer Universität bezüglich des Umfangs dort gespeicherter Protokoll-Dateien ohne Beanstandun-

gen kontrolliert. Dabei fiel eine interessante Möglichkeit der Vorabkontrolle von E-Mails auf, deren Nutzung anderen öffentlichen Stellen aus rechtlicher und technischer Sicht nahegelegt werden kann. Um nicht in Konflikt mit bspw. § 206 Abs. 2 Nr. 2 StGB (Unterdrückung von E-Mails) oder § 303a Abs. 2 StGB (Datenveränderung oder -unterdrückung) zu geraten, indem Sendungen dem ordnungsgemäßen Verkehr entzogen werden, wurden Umschlags- und Inhalts-Daten ankommender E-Mails bereits überprüft, noch bevor die E-Mail vollständig übertragen wurde, d. h. bevor sie in den Verfügungsbereich der öffentlichen Stelle gelangte. Wurde ein Hinderungsgrund (Virus, Black List) erkannt, wurde die Verbindung der E-Mail-Einlieferung einfach ohne abschließende Empfangsbestätigung abgebrochen, so dass ein einliefernder Server von einer fehlerhaften Übertragung ausgehen muss. Damit ist die E-Mail nicht in den Verfügungsbereich der Universität gelangt. Probleme durch den späteren Einsatz von Antivirensoftware oder ggf. auch SPAM-Filtern können ausgeschlossen werden, ohne dass die Nutzer vorab um Erlaubnis zur inhaltlichen Prüfung gefragt werden müssten. Die Löschung von E-Mails oder E-Mail-Teilen beispielsweise im Rahmen einer Virenprüfung ist nicht zulässig, da eine Quarantäne-Lösung im Vergleich das weniger einschneidende Mittel ist. Auch die Einrichtung eines Quarantäne-Bereichs mit potentiellem Zugriff auf Schadsoftware ist mit oben genannter Lösung entbehrlich.

In Kombination mit Überprüfungen der Adressen von Absendern und Empfängern sowie Greylisting und Pre-Whitelisting konnten so gute Resultate bei der SPAM-Filterung erzielt werden.
Beim Greylisting erfolgt eine Verzögerung der Mailannahme und es wird eine Kombination von Absender, Empfänger und einlieferndem Rechner ausgewertet. Wenn diese in Ordnung ist, wird diese Kombination zeitlich begrenzt freigeschaltet. Beim Pre-Whitelisting werden Antworten auf E-Mails, die von innen nach außen gingen, wenn sie innerhalb einer Frist eintreffen, akzeptiert.

25. Verfassungsschutz

25.1. Änderung des Verfassungsschutzgesetzes

In seinem letzten Tätigkeitsbericht (VIII. Tätigkeitsbericht, Ziff. 24.4) hat der Landesbeauftragte bereits über die Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt (VerfSchG-LSA) berichtet. Es handelte sich um das im Februar 2006 in Kraft getretene Gesetz zur Änderung verfassungsrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes (GVBl. LSA S. 12). Durch das Zweite Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt soll nun eine weitere Änderung der Vorschriften über den Verfassungsschutz erfolgen (LT-Drs. 5/1468neu).

Eine wesentliche Änderung betrifft in § 8 den Schutz des unantastbaren Kernbereichs privater Lebensgestaltung. Damit reagiert der Gesetzgeber auf die Feststellungen zum **Kernbereichsschutz**, die das Bundesverfassungsgericht in seiner Entscheidung zum Großen Lauschangriff vom 3. März 2004 (VII. Tätigkeitsbericht, Ziff. 18.2) traf. Mit der Regelung zum Kernbereichs-

schutz holt der Gesetzgeber nun nach, was der Landesbeauftragte bereits im Rahmen der Beratungen zum vorhergehenden Änderungsgesetz angemahnt hatte. Gegen die Regelung zum Kernbereichsschutz, wie sie von der Landesregierung ursprünglich vorgesehen war, hat der Landesbeauftragte Bedenken geäußert. Die Formulierung ließ den Schluss zu, dass eine Abwägung der Interessen der von der Abhörmaßnahme Betroffenen mit denen des Staates zulässig sei. Der Landesbeauftragte wies in seiner Stellungnahme gegenüber dem Ministerium des Innern des Landes Sachsen-Anhalt darauf hin: „Für eine Interessenabwägung ist hier kein Raum. Das Bundesverfassungsgericht hat in seiner Entscheidung vom 3. März 2004 insoweit ausgeführt: ‚Selbst überwiegende Interessen der Allgemeinheit können einen Eingriff in diesen absolut geschützten Kernbereich privater Lebensgestaltung nicht rechtfertigen ...'. Vor diesem Hintergrund erscheint die gewählte Formulierung nicht verfassungsgemäß." In dem überarbeiteten Entwurf des Änderungsgesetzes fanden die Anregungen des Landesbeauftragten Eingang.

Anders war es bei den Bedenken, die der Landesbeauftragten zu den §§ 10, 11 und 17a VerfSchG-LSA-Entwurf vorbrachte.

„§ 10 VerfSchG-LSA
Abs. 1
Bereits in meiner Stellungnahme zum Gesetz zur Änderung verfassungsschutzrechtlicher Vorschriften und zur Stärkung des Verfassungsschutzes vom 3. März 2005 habe ich darauf hingewiesen, dass die Ausweitung der Befugnis zum Speichern, Verändern und Nutzen von Daten Minderjähriger nach Vollendung des 14. Lebensjahres und vor Vollendung des 16. Lebensjahres vom Grundsatz her rechtlichen Bedenken begegnet. An meiner Auffassung, dass diese Regelung den Grundsatz der Verhältnismäßigkeit nicht wahrt, halte ich fest. ...

§ 11 VerfSchG-LSA
Abs. 3
Hinsichtlich der 15jährigen Löschfrist [betreffend Bestrebungen gegen die freiheitliche Grundordnung u. a. – zuvor 10 Jahre] habe ich bereits in meiner vorstehend näher bezeichneten Stellungnahme vom 3. März 2005 Bedenken vorgetragen. Diese wurden bis heute nicht ausgeräumt. Die Festsetzung dieser Löschfrist erscheint mangels tragfähiger Begründung nach wie vor unverhältnismäßig (...).

§ 17a VerfSchG-LSA
Abs. 2
Mit der Neufassung des Abs. 2 wird die Eingriffsschwelle für Auskunftsverlangen durch die Verfassungsschutzbehörde herabgesetzt. Das betrifft Auskünfte bei Luftfahrtunternehmen genauso wie Kreditinstitute, Finanzdienstleistungsunternehmen, Postdienstleister, Telekommunikationsdiensteanbieter und Telemediendiensteanbieter. ..."

Absatz 6 sieht darüber hinaus vor, dass die Verfassungsschutzbehörde erst zum 31. Dezember 2009 Maßnahmen mittels des IMSI-Catchers evaluiert. Es erscheint nicht eingängig, dass das VerfSchG-LSA nach Einführung neuer Kompetenzen aber vor deren Ende 2008 vorgesehener Evaluierung be-

reits erneut geändert wird. Nach erfolgter Evaluierung wird sich ggf. neuer Änderungsbedarf aufzeigen. Um die Erfahrungen hinsichtlich der erweiterten Kompetenzen angemessen und zeitnah in die Ausgestaltung der Normen einfließen zu lassen, wäre eine Änderung nach Evaluation sinnvoll gewesen.

Hinsichtlich der vorgetragenen Bedenken zu § 10 VerfSchG-LSA hat sich die Landesregierung in der Begründung darauf zurückgezogen, dass mit dem Zweiten Gesetz zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt die Befugnisse gar nicht erweitert wurden. „Es wurde lediglich auf die bisherige Benennung des Speichermediums [Akten] personenbezogener Daten verzichtet, um im Gleichklang mit § 9 VerfSchG-LSA – Entwurf – die Arbeitsweise der Verfassungsschutzbehörde im Bereich der Speicherung, Veränderung und Nutzung personenbezogener Daten an die Anforderungen an eine dem heutigen Stand der Technik entsprechende Datenverarbeitung anzupassen (LT-Drs. 5/1468, S. 17). An den Voraussetzungen zur Speicherbefugnis wird im Vergleich zur geltenden Rechtslage nichts geändert (...).“ Zutreffend ist, dass die entsprechende Speicherbefugnis mit dem jetzigen Gesetzentwurf nicht geändert werden soll. Aber bereits beim vorhergehenden Änderungsgesetz hat der Landesbeauftragte diese Regelung als unverhältnismäßig angesehen. Nur weil seine damaligen Einwendungen nicht berücksichtigt wurden, wird die Regelung im Verfassungsschutzgesetz deshalb nicht verfassungsgemäß. Der Landesbeauftragte sieht es als seine Aufgabe an, auch auf bedenkliche Regelungen in der bestehenden Rechtslage hinzuweisen.

Soweit es die Bedenken zu § 11 VerfSchG-LSA betrifft, gilt das bereits zu § 10 VerfSchG-LSA Erläuterte analog. Auch hier wird einer inhaltlichen konstruktiven Diskussion durch den Entwurfsverfasser ausgewichen. „An den Voraussetzungen zur Speicherbefugnis wird im Vergleich zur geltenden Rechtslage nichts geändert ....“ (LT-Drs. 5/1468 neu, S. 17). Auch hier hat der Landesbeauftragte bereits beim ersten Änderungsgesetz seine Bedenken vorgetragen. Diese fanden im Rahmen der Rechtsetzung keine Berücksichtigung. Die bedenkliche Regelung wurde geltendes Recht. Im Rahmen des zweiten Änderungsgesetzes weist der Landesbeauftragte auf seine Bedenken erneut hin.

In Bezug auf die zu § 17a Abs. 2 VerfSchG-LSA vorgetragenen Bedenken hat sich der Entwurfsverfasser inhaltlich geäußert und insoweit u. a. ausgeführt: „Die Auffassung des Landesbeauftragten für den Datenschutz, wonach die im Entwurf gewählte Formulierung ‚erhebliche Gefährdung’ eine **niedrigere Eingriffsschwelle** als ‚schwerwiegende Gefahren’ darstellen dürfte, ist zutreffend. Hintergrund dieser Regelung ist, dass nach der Gesetzesbegründung zu § 8a Abs. 2 BVerfSchG im Rahmen des Terrorismusbekämpfungsergänzungsgesetzes die Befugnisse zwar auch für die Aufgaben nach § 3 Abs. 1 Nr. 1 BVerfSchG eingeräumt werden (Inlandsextremismus), aber insoweit auf volksverhetzende und militante Bestrebungen beschränkt werden (siehe BT-Drs. 16/2921, S. 15). Mit dem Landesgesetzentwurf sollen aber gerade z. B. Finanzermittlungen schon bei rechtsextremistischen Bestrebungen ermöglicht werden, welche mit der im Bundesrecht verankerten Regelung (ohne dass noch die o. a. Voraussetzungen hinzutreten) nicht möglich sind.“ (LT-Drs. 5/1468 neu, S. 18). “Eine umfassende Aufklärung rechtsext-

remistischer Finanzierungsquellen soll mit der entsprechenden Änderung in § 17a VerfSchG-LSA - Entwurf - erreicht werden.“ (LT-Drs. 5/1468 neu, S. 19). Aus Sicht des Landesbeauftragten hätte eine entsprechende Regelung begrenzt auf den Rechtsextremismus zur Zielverwirklichung ausgereicht.

Soweit es § 17a Abs. 6 VerfSchG-LSA betrifft, scheint der Landesbeauftragte willentlich missverstanden worden zu sein. Wie dem Auszug aus seiner Stellungnahme zu entnehmen ist, war es das Interesse des Landesbeauftragten, eine erneute Änderung des Verfassungsschutzgesetzes aufzuschieben, bis die zum 31. Dezember 2008 vorgesehene Evaluierung der Änderungen aus dem ersten Änderungsgesetz vorliegt und ausgewertet werden konnte. Stattdessen verschiebt der Entwurfsverfasser die Evaluierung um ein Jahr und rechtfertigt dies mit den Erwägungen des Landesbeauftragten. „Den Erwägungen des Landesbeauftragten für den Datenschutz folgend, soll nunmehr die Evaluierung um ein Jahr verschoben werden. Das Außerkrafttreten ist dementsprechend ebenfalls um ein Jahr zu verschieben.“ (LT-Drs. 5/1468 neu vom 9. September 2008, S. 20) Dass seine Ausführungen so misszudeuten waren, dass sie genau die gegenteilige der beabsichtigten Reaktion bewirken, hält der Landesbeauftragten nicht für eine der ernsthaften Diskussion angemessene Antwort auf seine Anregung.
Im Übrigen steht der Landesbeauftragte mit der Auffassung, dass eine Evaluierung unter Einbeziehung externen Sachverstandes sinnvoll und notwendig ist, nicht allein. Auch die Parlamentarische Kontrollkommission des Bundestages hat im Rahmen des Berichtes zu ihrer Tätigkeit im Jahr 2008 nochmals ausdrücklich auf die Erforderlichkeit einer Evaluierung der Antiterror-Befugnisse durch einen externen Sachverständigen hingewiesen.

25.2. Dokumentenmanagement beim Verfassungsschutz

Im Rahmen der Beratungen des Arbeitskreises Sicherheit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wurden auch die elektronische Vorgangsbearbeitung und die Einführung von Dokumentenmanagementsystemen bei den Verfassungsschutzbehörden thematisiert. Eine Abfrage bei den Verfassungsschutzbehörden ergab, dass einige Länder an der Einführung verschiedener Systeme arbeiten.

Auch die Verfassungsschutzbehörde des Landes Sachsen-Anhalt teilte mit, dass eine analysefähige Amtsdatei und ein Dokumentenmanagementsystem getestet würden. Nach einer Evaluierung sollen die entsprechenden Systeme in den regulären Betrieb übergehen. Es bestand für den Landesbeauftragten kein Grund zu der Annahme, dass sich der Testbetrieb auf personenbezogene Daten erstrecken könnte, deren Speicherung, Verarbeitung und Nutzung in solchen Systemen nicht zulässig ist.

Eine erneute Anfrage bei der Verfassungsschutzbehörde im Januar 2009 ergab, dass sich das Dokumentenmanagementsystem nach wie vor im Testbetrieb befindet. Der Wirkbetrieb solle erst nach Beendigung des aktuellen Gesetzgebungsverfahrens zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt (siehe Ziff. 25.1) aufgenommen werden. Der Entwurf eines Verfahrensverzeichnisses für das Dokumentenmana-

gementsystem werde derzeit in Bezug auf die vorgesehene Gesetzesänderung überarbeitet.

Hinsichtlich der analysefähigen Amtsdatei wurde dem Landesbeauftragten im Januar 2009 der Entwurf eines Verfahrensverzeichnisses übersandt. Dessen Prüfung dauerte noch an, als Mitte Februar 2009 im Rahmen der Beratungen im Landtag zur Änderung des Gesetzes über den Verfassungsschutz im Land Sachsen-Anhalt bekannt wurde, dass die Verfassungsschutzbehörde **personenbezogene Daten Minderjähriger vor Vollendung des 14. Lebensjahres** elektronisch speichern soll. Die Angelegenheit fand umgehend ein breites Echo in der Presse.

Noch im Februar 2009, nur wenige Tage nach dem Bekanntwerden des vermeintlich rechtswidrigen Handelns, stattete der Landesbeauftragte der Verfassungsschutzbehörde einen ersten Besuch ab. Er informierte sich vor Ort über die Art und den Umfang der elektronischen Verarbeitung personenbezogener Daten. Im Nachgang zu diesem Besuch wandte sich der Landesbeauftragte dann schriftlich mit der Bitte an den Innenminister, Fragen zum Stand der Bewertung der Angelegenheit durch das Ministerium des Innern selbst zu beantworten. Insbesondere bat er auch um Auskunft darüber, zu welcher Einschätzung der eingeschaltete behördliche Datenschutzbeauftragte des Ministeriums des Innern gekommen sei.

Die seitens des behördlichen Datenschutzbeauftragten gewonnenen Feststellungen und Bewertungen legte dieser in einem ausführlichen Vermerk nieder, der dem Landesbeauftragten zur Verfügung gestellt wurde. Nach Auswertung dieser Unterlagen und weiterem Schriftwechsel mit dem Ministerium des Innern fand ein Gespräch zwischen der Verfassungsschutzbehörde und dem Landesbeauftragten statt, in dessen Verlauf die streitigen Systeme vorgeführt und vorläufige Einschätzungen ausgetauscht wurden.
Zum Redaktionsschluss dieses Tätigkeitsberichtes hatte der Landesbeauftragte seine Prüfung und Bewertung noch nicht abgeschlossen. Er wird die Angelegenheit weiter verfolgen.

25.3. GIAZ - Teil II

In seinem vorherigen Tätigkeitsbericht (VIII. Tätigkeitsbericht, Ziff. 24.2) hat der Landesbeauftragte die grundsätzliche Bewertung des GIAZ aus datenschutzrechtlicher Sicht vorgestellt und seine Bedenken gegenüber dieser Einrichtung, die in erster Linie der Beachtung des verfassungsrechtlichen Trennungsgebots gelten, deutlich gemacht. Diese Bedenken bestehen fort, weil keine Änderung hinsichtlich der Strukturen vorgenommen wurde. Auch auf Bundesebene gibt es Einrichtungen, deren Organisation nur schwerlich mit dem Trennungsgebot in Einklang zu bringen sein dürfte. So gibt es das dem GIAZ vergleichbare GTAZ (Gemeinsames Terrorismusabwehrzentrum), das GIZ (Gemeinsames Internetzentrum) und Überlegungen zur Schaffung eines Service- und Kompetenzzentrums in Sachen Telekommunikationsüberwachung beim Bundesverwaltungsamt in Köln.

In diesem Tätigkeitsbericht soll das GIAZ aber nicht noch einmal als Ganzes beleuchtet werden, sondern eine spezielle Aufgabe des GIAZ. Anlässlich der

Kontrolle einer Ausländerbehörde im Juni 2007 stellte der Landesbeauftragte fest, dass die Ausländerbehörden vor der Erteilung eines Aufenthaltstitels eine Anfrage an das GIAZ richten. Von dort wird dann mitgeteilt, ob gegen die Maßnahme Bedenken bestehen.

Infolge dieser Feststellung sowie im Anschluss an einem Besuch im GIAZ wandte sich der Landesbeauftragte an das Ministerium des Innern als Fachaufsichtsbehörde für die Ausländerbehörden. Er bat mitzuteilen, aufgrund welcher Regelungen die Ausländerbehörden verpflichtet seien, entsprechende Anfragen an das GIAZ zu stellen. Seitens des Ministeriums des Innern des Landes Sachsen-Anhalt wurde im Juli 2007 die entsprechende Erlasslage durch die Übersendung von fünf Erlassen in Kopie dargestellt. Erläuternd wurde mitgeteilt, dass die Erlasslage „... angesichts der mit Inkrafttreten des Gesetzes zur Umsetzung aufenthalts- und asylrechtlicher Richtlinien der Europäischen Union einhergehenden Rechtsänderungen in nächster Zeit einer Prüfung unterzogen und ggf. der aktuellen Rechtslage angepasst“ werden soll. Im Ergebnis der Prüfung der Unterlagen war festzustellen, dass eine Überarbeitung der Regelungen zu den Anfragen an das GIAZ aus datenschutzrechtlicher Sicht geboten erscheint.

Nach einem Jahr - im September 2008 - fragte der Landesbeauftragte beim Ministerium des Innern nach, ob die entsprechende Erlasslage nunmehr überarbeitet wurde. Einer daraufhin im Oktober 2008 erteilten Auskunft war zu entnehmen, dass die Überarbeitung derzeit erfolgen würde. Die veränderte Erlasslage existiere momentan nur im Entwurfsstadium und müsse zunächst hausintern abgestimmt werden. Im November 2008 teilte der Landesbeauftragte seine Auffassung dem Innenminister schriftlich mit. Der Landesbeauftragte führte u. a. aus:
„Den Informationsbesuch beim GIAZ habe ich u. a. dazu genutzt, Feststellungen, die meine Mitarbeiter bei Kontrollen der Ausländer- und Einbürgerungsbehörden getroffen haben, zu überprüfen. Im Rahmen dieser Kontrollen musste festgestellt werden, dass die Ausländerbehörden ihre Anfragen an die zuständigen Behörden der Polizei nach § 73 Abs. 2 Aufenthaltsgesetz ausschließlich an das Landeskriminalamt richten, welches die Anfragen intern dem GIAZ zur Bearbeitung zuweist. Eine entsprechende Erlasslage Ihres Hauses aus dem Jahre 2005 verpflichtet die Ausländerbehörden, die bis dahin jeweils bei den örtlichen Polizeibehörden zu stellenden Anfragen, zukünftig an das Landeskriminalamt zu richten, wo sie - wie bereits erwähnt - im GIAZ bearbeitet werden.
Die bestehende Erlasslage erscheint mir unter datenschutzrechtlichen Gesichtspunkten zu weitgehend und überarbeitungsbedürftig. Der Erlass Ihres Hauses vom 23. Dezember 2005 definiert als Aufgabe des GIAZ ‚Erkenntnisse zum islamistischen Extremismus und Terrorismus zu gewinnen und zu analysieren’. Nicht jede, wahrscheinlich eher ein ganz geringer Anteil, ausländerbehördlicher Anfragen i. S. d. § 73 Abs. 2 Aufenthaltsgesetz haben aber einen islamistisch-terroristischen Hintergrund. Die Bearbeitung der Anfragen durch das GIAZ kann jedoch den Eindruck erwecken, dass grundsätzlich entsprechende Zusammenhänge gesehen werden.
Wie mir aufgrund telefonisch erteilter Informationen bekannt ist, befasst sich Ihr Haus bereits mit einer Änderung der bestehenden Erlasslage.“

Im Dezember 2008 teilte das Ministerium des Innern auf das Schreiben des Landesbeauftragten mit, dass eine Änderung der Erlasslage erfolgen werde, bei deren Erarbeitung auf die angebotene Unterstützung gern zurückgegriffen würde. Schon nach den Allgemeinen Verwaltungsvorschriften zu § 73 Abs. 2 Aufenthaltsgesetz sind Behörden der Polizei von den beteiligten Landeskriminalämtern nur einzubinden, soweit dies im Einzelfall erforderlich ist. Eine generelle Befassung des GIAZ mit den Anfragen der Ausländerbehörden ist vor dem Hintergrund dieser die gesetzlichen und verfassungsrechtlichen Vorgaben berücksichtigenden Arbeitsanweisung aus Sicht des Landesbeauftragten nicht sachgerecht. Deshalb erklärte das Ministerium des Innern auch weiterführend, dass für das Jahr 2009 angedacht sei, die Anfragen der Ausländerbehörden in einer anderen Abteilung des Landeskriminalamtes bearbeiten zu lassen und das GIAZ nur noch in ausgewählten Fällen zu beteiligen.

Der Landesbeauftragte hat die Absichtserklärung des Ministeriums des Innern des Landes Sachsen-Anhalt zur Kenntnis genommen und wird die Umsetzung beobachten und begleiten.

26. Verkehr

26.1. Online-Anbindung der Fahrerlaubnisbehörden an das Kraftfahrt-Bundesamt

Der Landesbeauftragte hat sich zuletzt in seinem IV. Tätigkeitsbericht (Ziff. 27.1) mit dem ab 1. Januar 1999 in Kraft getretenen Straßenverkehrsgesetz (StVG) kritisch auseinandergesetzt. Die Kritik betraf zum einen die Schaffung eines Zentralen Fahrerlaubnisregisters (ZFER) beim Kraftfahrt-Bundesamt (KBA) gem. § 48 Abs. 2 StVG, einem „Mammutregister“ für ca. 53 Millionen Fahrerlaubnisinhaber. Zum anderen beurteilte er kritisch die so geschaffene „Doppelspeicherung“ von Fahrerlaubnisdaten, denn gem. § 48 Abs. 1 StVG führen neben dem KBA im ZFER auch die ca. 650 in Deutschland bestehenden Fahrerlaubnisbehörden (FEB) der Landkreise und kreisfreien Städte ebenfalls diese Fahrerlaubnisdaten in ihren örtlichen Fahrerlaubnisregistern.
Der Bundesgesetzgeber hatte damals in § 65 Abs. 10 Satz 2 StVG eine Frist zur Auflösung der örtlichen Fahrerlaubnisregister bis 31. Dezember 2005 festgelegt und damit zumindest zeitlich diese Doppelspeicherung begrenzt. Durch die Speicherung der Personalien und der Fahrerlaubnisdaten, aber nicht der Anschrift der Fahrerlaubnisinhaber mit Kartenführerschein im ZFER wurde ein neues bundesweites „Melderegister“ vermieden.

In den nachfolgenden Jahren wurden nur die Fahrerlaubnisdaten von Betroffenen an das KBA übermittelt, die einen **neuen** Führerschein **(Kartenführerschein)** erhielten. Alle anderen Fahrerlaubnisinhaber sind bisher nicht im ZFER erfasst. Solange aber nicht alle Fahrerlaubnisinhaber ihren alten Führerschein in einen Kartenführerschein umgetauscht haben, bestehen die örtlichen Fahrerlaubnisregister mit diesen „alten“ Fahrerlaubnisdaten fort. Da ein Zwangsumtausch nicht vorgesehen ist, wird dieser Zustand noch lange Zeit anhalten. Von den Fahrerlaubnisinhabern in Deutschland besitzt erst ca. die Hälfte einen Kartenführerschein und ist somit im Bestand des ZFER erfasst.

Nach § 51 StVG haben die FEB dem KBA unverzüglich die zu speichernden oder zu einer Änderung oder Löschung einer Eintragung führenden Fahrerlaubnisdaten mitzuteilen. Dabei wird offen gelassen, in welcher Weise diese Mitteilungen zu erfolgen haben.
Weder für den direkten Zugriff der FEB auf den Datenbestand des ZFER per File-Transfer oder im sog. „Online-Dialog-Verfahren“ noch für die vom KBA durchgeführte Protokollierung dieser Zugriffe bestehen entsprechende Rechtsgrundlagen. Das hat der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bei seiner Kontrolle des KBA im Jahr 2008 festgestellt.

Die wenigen Papierunterlagen bei der Beantragung einer allgemeinen Fahrerlaubnis und deren Erteilung werden zur Fahrerlaubnisakte genommen. Diese wird aber in Sachsen-Anhalt in der Regel nach 5 Jahren vernichtet, falls keine weiteren Tatsachen und Entscheidungen der Fahrerlaubnisbehörde zur Befähigung und Eignung des Fahrerlaubnisinhabers aktenkundig gemacht worden sind.
Bei der Vernichtung einer Fahrerlaubnisakte nach dieser 5-Jahresfrist oder einem eventuellen Führerscheinverlust nach dieser Frist besteht der **einzige** Nachweis für den Bestand und den Umfang der Fahrerlaubnis, d. h. des rechtmäßigen Besitzes einer Fahrerlaubnis für den Betroffenen, zukünftig nur noch in einem beim KBA im ZFER gespeicherten Datensatz. Die automatisierte Speicherung dieser Fahrerlaubnisinhaber mit Kartenführerschein erfolgt nämlich nicht mehr dezentral bei den Fahrerlaubnisbehörden, sondern **zentral** beim KBA im ZFER, an das die jeweilige örtliche Fahrerlaubnisbehörde nur noch die Erteilung, Änderung oder Löschung der Fahrerlaubnis mitteilt.

Da abzusehen war, dass auch zum 31. Dezember 2005 noch nicht alle Daten in das ZFER übernommen sein würden, hatte der Bundesgesetzgeber in § 65 Abs. 10 Satz 2 StVG die Frist zur Auflösung der örtlichen Fahrerlaubnisregister um ein weiteres Jahr bis zum 31. Dezember 2006 verlängert. Aber auch diese Frist hat sich im Nachhinein als zu kurz erwiesen.
Auf Initiative der Länder hat der Bundesgesetzgeber mit einem Gesetz zur Änderung des Straßenverkehrsgesetzes vom 3. Februar 2009 (BGBl. I S. 150) die Übergangsfrist für die Führung der örtlichen Fahrerlaubnisregister bis zum 31. Dezember 2012 verlängert.

Vor einer endgültigen Löschung der Fahrerlaubnisdaten in den örtlichen Fahrerlaubnisregistern der FEB muss sichergestellt werden, dass die örtlich zu löschenden Fahrerlaubnisdaten vollständig und richtig im ZFER übernommen worden sind. Hierzu werden die Bestände der örtlichen Fahrerlaubnisregister mit dem des ZFER seit 2002 abgeglichen. Datenlöschungen in den örtlichen Fahrerlaubnisregistern dürfen danach erst dann erfolgen, wenn festgestellte fehlende Datensätze im Rahmen des jährlich durchzuführenden sog. „Datenabgleich 1“ zum ZFER nachgemeldet bzw. fehlerhafte Eintragungen im Rahmen des einmalig durchzuführenden sog. „Datenabgleich 2“ berichtigt worden sind. Grundlage für diese Datenabgleiche zwischen den örtlichen Fahrerlaubnisregistern und dem ZFER bildet § 59 Abs. 3 StVG. Vor seiner Auflösung muss also der gesamte Datenbestand des örtlichen Fahrerlaubnisregisters vom KBA in das ZFER übernommen worden sein und

zugleich müssen die Daten von den FEB im automatisierten Verfahren aus dem ZFER abgerufen werden können. Dementsprechend muss ein datenschutzgerechtes Online-Dialog-Verfahren zum ZFER für Anfragen und Auskünfte und Mitteilungen eingerichtet werden.

Ein weiteres grundsätzliches Problem besteht in der bereits bestehenden Praxis des Zugriffs der FEB auf das ZFER. Durch die vorgesehene zentrale Speicherung im ZFER wird den zur Mitteilung an das ZFER verpflichteten FEB nicht mehr nur der lesende Zugriff auf die Fahrerlaubnisdaten ermöglicht, sondern auch die Speicherung neuer Fahrerlaubnisdaten sowie deren Änderung und Löschung, d. h. neben dem lesenden Zugriff ist bereits auch der **schreibende** Zugriff für die FEB möglich. Das StVG und auch die Fahrerlaubnisverordnung (FeV) enthalten bisher jedoch keine Regelungen, die diesem Umstand Rechnung tragen.

Bereits die 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. Oktober 2007 fasste einen Beschluss zur Notwendigkeit einer sicheren Gestaltung der elektronischen Kommunikation der FEB mit dem KBA und der rechtsverbindlichen Speicherung der Fahrerlaubnisdaten im ZFER. Die Datenschutzbeauftragten des Bundes und der Länder forderten, dass bei der Online-Anbindung aller FEB an das ZFER die erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um eine integere, authentische, revisionsfähige und transparente Verarbeitung der Fahrerlaubnisdaten auf Dauer zu gewährleisten.
Bislang ist auch die Frage ungelöst, inwieweit die FEB oder das KBA die Verantwortung für die Richtigkeit der dort gespeicherten Fahrerlaubnisdaten tragen. Weiterhin ungeklärt sind die datenschutzrechtlichen Kontrollbefugnisse vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Landesbeauftragten. Auch hierzu fehlen sowohl im StVG als auch in der FeV entsprechende Vorschriften.
Grundsätzlich erfordert die Schaffung von Zentralregistern, auf die mehrere Stellen lesenden und schreibenden Zugriff haben, wie es bereits Praxis beim Zugriff der FEB auf das ZFER ist, eindeutige und umfassende Festlegungen hinsichtlich der Verantwortlichkeiten sowie der zu ergreifenden organisatorischen und technischen Maßnahmen. Hierzu gehören vor allem auch klare Regelungen, wie die Authentizität und Integrität der Fahrerlaubnisdatensätze auf Dauer im ZFER sichergestellt werden können, denn gerade die Daten zur allgemeinen Fahrerlaubnis müssen Jahrzehnte lang, wenn nicht sogar oft lebenslänglich für den Betroffenen sicher im ZFER gespeichert werden. Letztendlich sind auch Regeln zur Revisionsfähigkeit im ZFER selbst notwendig.

Der zuvor genannte Beschluss der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder basierte auf einem **Gutachten** (vom 19. Oktober 2007), welches durch eine Arbeitsgruppe des Arbeitskreises Verkehr erarbeitet wurde. An dieser Arbeitsgruppe war auch der Landesbeauftragte beteiligt. Beschluss und Gutachten wurden dem Ministerium für Landesentwicklung und Verkehr zugeleitet.
Im Ergebnis der Bemühungen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3./4. April 2008 in Berlin kam es zu einem ersten Gespräch des Bundesbeauftragten für den Datenschutz und

die Informationsfreiheit und Vertretern des Arbeitskreises Verkehr mit dem zuständigen Bundesministerium für Verkehr, Bau und Stadtentwicklung. Im Ergebnis dieses Gesprächs wurden aber keine wesentlichen Fortschritte in Bezug auf die Umsetzung der datenschutzrechtlichen Vorschläge und Handlungsempfehlungen erreicht. Insbesondere sah das Bundesministerium für Verkehr, Bau und Stadtentwicklung hier die Länder als erstes in der Pflicht.
Aus diesem Grund wandte sich der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit als Vorsitzender des Arbeitskreises Verkehr an den Verkehrsminister des Landes Sachsen-Anhalt als damaligen Vorsitzenden der Verkehrsministerkonferenz, um ein Meinungsbild der Länder zu den im Gutachten vorgeschlagenen Gesetzesänderungen im StVG zu erhalten. In seiner Antwort verwies der Vorsitzende der Verkehrsministerkonferenz auf die Gesetzgebungskompetenz des Bundes und sah daher keine Möglichkeit, die im Gutachten und den Beschluss der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgeschlagenen Änderungen des StVG und der FeV selbst zu initiieren, verschloss sich aber nicht einer inhaltlichen Diskussion im Bund-Länder-Fachausschuss Fahrerlaubnis-/Fahrlehrerrecht (BLFA-FE/FL).

Es bleibt zu hoffen, dass sich der BLFA-FE/FL weiter dieses Themas annimmt. Durch Verlängerung der Übergangsfrist für die Führung der örtlichen Fahrerlaubnisregister bis zum 31. Dezember 2012 sollte ausreichend Zeit und Gelegenheit sein, die rechtlichen Voraussetzungen im StVG und der FeV für eine datenschutzrechte Lösung zur Online-Anbindung der FEB an das KBA und der nur noch zentralen Speicherung von Fahrerlaubnisdaten im ZFER zu schaffen.
Allerdings hat der Landesbeauftragte bisher vom Ministerium für Landesentwicklung und Verkehr kein eigenes Meinungsbild zum übersandten Beschluss der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie zum Gutachten erhalten.

26.2. Verkehrsüberwachung mittels Videoaufzeichnung

Ein besorgter Bürger, dem von der Zentralen Bußgeldstelle im Technischen Polizeiamt des Landes (ZBS) ein Anhörungsbogen im Bußgeldverfahren wegen einer Geschwindigkeitsüberschreitung auf einer Autobahn zugestellt worden war, hatte sich an den Landesbeauftragten mit der Frage gewandt, ob in Sachsen-Anhalt eine Geschwindigkeitsmessung durch Videoerfassung mittels sog. „Kennzeichenscanning“ von LKW-Mautbrücken aus erfolge. Eine telefonische Nachfrage bei der ZBS hätte dies bestätigt.
Die daraufhin erfolgte Nachfrage des Landesbeauftragten ergab, dass es sich seitens eines Mitarbeiters der ZBS um eine Fehlinformation gehandelt hatte. Die Videoaufzeichnungen erfolgten aus Kraftfahrzeugen der Polizei heraus, die hierzu auf den jeweiligen Autobahnbrücken abgestellt wurden. Da diese verdachtsunabhängige Videoaufzeichnung über einen längeren Zeitraum von **allen** Verkehrsteilnehmern erfolgte, scheinbar auch von denen, für die kein Anfangsverdacht für eine Verkehrsordnungswidrigkeit vorlag (wie z. B. ein Geschwindigkeitsverstoß, Verstoß gegen die Gurtanlegepflicht; die Einhaltung des Sicherheitsabstands oder gegen das Handynutzungsverbot) und eine Auswertung dieser Videoaufzeichnungen erst im Nachhinein erfolgte, war diese Verfahrensweise der Polizei datenschutzrechtlich bedenklich.

Die so von der ZBS geschilderte Durchführung dieser Verkehrsüberwachungsmaßnahme (als Beweismittel wurde im Anhörungsbogen des Bußgeldverfahrens eine Video-Band-Aufzeichnung angegeben) veranlasste den Landesbeauftragten, das Ministerium des Innern zur Klärung des Sachverhalts aufzufordern und dessen rechtliche Beurteilung einzuholen.

Im SOG LSA findet sich für diese Videoaufzeichnung ohne Vorliegen eines Anfangsverdachts zur Verkehrsüberwachung durch die Polizei keine Rechtsgrundlage.
Den besorgten Bürger konnte der Landesbeauftragte beruhigen, in Sachsen-Anhalt erfolgt kein „Kennzeichenscanning“ (vgl. auch Ziff. 18.12).

Bei der Verkehrsüberwachung erfolgt die Videoaufzeichnung mittels des sog. Verkehrs-Kontroll-Systems (VKS). Allerdings hatte die Untersuchung der Praxis dieser Videoaufzeichnungen mit dem VKS durch das Ministerium des Innern ergeben, dass diese Videoaufzeichnungen zum Teil auch im **Dauerbetrieb** erfolgten. Diese Aufzeichnungsweise war datenschutzrechtlich unzulässig. Dieser Meinung war auch das Ministerium des Innern in seiner Stellungnahme.
Mit einem Erlass hat es die Polizeibehörden angewiesen, den Einsatz der Geräte nur im rechtlich zulässigen Umfang vorzunehmen. Danach ist die Videoaufzeichnung von Unverdächtigen im Dauerbetrieb nicht statthaft. Erst bei Vorliegen eines Anfangsverdachts im Messfeld darf der den Verkehrsablauf beobachtende Polizeibeamte die Videoaufzeichnung starten und muss diese dann auch nach der Beweisaufnahme wieder beenden.

26.3. Datenschutz im Verkehrsordnungswidrigkeitenverfahren

Mit dem Auto eines Bürgers war eine Verkehrsordnungswidrigkeit begangen worden, ein Rotlichtverstoß. Das wurde durch zwei Polizisten beobachtet, die in einer Zeugenaussage auch den Fahrer vage beschreiben konnten. In der folgenden Anhörung im Bußgeldverfahren bestritt der beschuldigte Fahrzeughalter den Verstoß. Er sei am Tattag verreist gewesen.
Daraufhin forderte die Bußgeldstelle vom Einwohnermeldeamt am Wohnsitz des beschuldigten Fahrzeughalters unter Hinweis auf § 2b Abs. 2 des Gesetzes über Personalausweise (PersAuswG) eine Kopie des Lichtbildes des Betroffenen an. Zu diesem Zweck versandte sie einen zur Fotoanforderung regelmäßig verwandten Standardbrief, in dem es allerdings hieß: „Bei der Aufnahme des Verstoßes ist ein Foto des/der Betroffenen gefertigt worden.“ Das stimmte natürlich im vorliegenden Fall nicht. Hier beging die Bußgeldstelle den ersten datenschutzrelevanten Fehler. Zunächst hätte sie gegenüber dem Einwohnermeldeamt natürlich nicht behaupten dürfen, sie habe zu Vergleichszwecken ein Tatortfoto vorliegen.
Das war jedoch nur verwaltungstechnisch ungeschickt, da der genannte § 2b PersAuswG den Personalausweisbehörden bei Vorliegen der entsprechenden Voraussetzungen die Übermittlung von Daten aus dem Personalausweisregister auch dann erlaubt, wenn kein Vergleichsfoto vorliegt.
Allerdings, und da sieht der Landesbeauftragte das wesentliche Problem, ist eine der in § 2b Abs. 2 PersAuswG für die Übermittlung genannten Voraussetzungen, dass die ersuchende Behörde, also die Bußgeldstelle, ohne Kenntnis der Daten nicht in der Lage wäre, eine ihr obliegende Aufgabe zu

erfüllen. Genau dort hätte die Bußgeldstelle ansetzen müssen: Der Beschuldigte gab an, am Tattag verreist gewesen zu sein. Die Bußgeldstelle hätte ihm zunächst Gelegenheit geben müssen, das nachzuweisen, was als Mittel zur Ermittlung des Sachverhaltes für den Betroffenen wesentlich weniger eingreifend und damit datenschutzgerechter gewesen wäre.
Allerdings, so muss der Vollständigkeit halber auch berichtet werden, forderte die Bußgeldstelle den Betroffenen kurz danach tatsächlich auf, entsprechende Abwesenheitsnachweise zu erbringen. Diese Nachweise blieb er kommentarlos schuldig.

Dann forderte die Bußgeldstelle einen der polizeilichen Zeugen auf anzugeben, ob er auf dem übersandten (Personalausweis-)Foto den Täter erkennen könne. Auch das ging datenschutzrechtlich schief. Das Foto wurde mit der gesamten Ermittlungsakte der Dienststelle des Zeugen zugesandt. Das war sach- und fachlich nicht erforderlich und stellte eine unzulässige Datenübermittlung dar. Ein ziviler Zeuge hätte die Akte schließlich auch nicht komplett erhalten.
Im Übrigen lief das Verfahren der Täter-(wieder-)erkennung durch die Lichtbildvorlage ebenfalls eher unglücklich. Dem Zeugen wurde ausschließlich das Foto des Beschuldigten „zur Auswahl“ vorgelegt. In Ziff. 18 der Richtlinien für das Strafverfahren und das Bußgeldverfahren ist aber vorgesehen, dem Zeugen bei Gegenüberstellungen Fotos einer Reihe anderer Personen gleichen Geschlechts, ähnlichen Alters und ähnlicher Erscheinung vorzulegen, und zwar in einer Form, die nicht erkennen lässt, wer der Beschuldigte ist (Wahlgegenüberstellung). Hierbei handelt es sich jedoch eher um ein Problem der Beweiserhebung und -würdigung, weniger um eine datenschutzrechtliche Frage.

Das Verfahren gegen den Fahrzeughalter vor dem Amtsgericht ist übrigens aus Ermessensgründen eingestellt worden.

26.4. Datenschutz im Kfz-Zulassungsrecht

Ein Bürger hatte wegen diverser Ungereimtheiten ein Auskunftsersuchen bei einer Zulassungsbehörde eines Landkreises über seine dort gespeicherten Daten und deren Herkunft gestellt. Da keine seiner Fragen seiner Meinung nach beantwortet wurden, bat er den Landesbeauftragten um Hilfe in dieser Angelegenheit, auch um gegebenenfalls Schadensersatzansprüche geltend zu machen.
Gegen ihn war ein Fahrverbot verhängt und sein Fahrzeug auf Grund einer angeblichen Veräußerungsanzeige durch die Zulassungsbehörde beim zuständigen Finanzamt abgemeldet worden. Da er täglich auf sein Fahrzeug angewiesen sei, resultiere daraus ein für ihn erheblicher wirtschaftlicher Verlust.
Die Zulassungsbehörde hatte ihm gem. § 27 Abs. 3 StVZO den Betrieb seines Fahrzeuges im öffentlichen Verkehr untersagt, kurze Zeit später aber die Anordnung wieder aufgehoben, mit der Begründung einer Fehlinformation durch das zuständige Gewerbeamt.

Der Landesbeauftragte musste zur Aufklärung des Sachverhaltes alle an diesem Vorgang beteiligten Stellen befragen, um Klarheit in das vermeintli-

che Durcheinander zu bringen. Er konnte die vom Petenten beklagte unzureichende Beantwortung von Fragen durch die Zulassungsbehörde weitestgehend aufklären.
Die datenschutzrechtlichen Defizite beruhten zum Teil auf Fehlern bei der automatisierten Verarbeitung in der Zulassungsbehörde und im Gewerbeamt der Verwaltungsgemeinschaft. Weiterhin wurde festgestellt, dass das Verwaltungshandeln nicht ordnungsgemäß in den Akten dokumentiert wurde. Dies betraf insbesondere fehlende Vermerke über Anfragen bzw. Auskünfte in beiden Behörden.
Die vom Petenten vermuteten Datenschutzverletzungen waren zum Teil unbegründet. Die durchgeführten Maßnahmen der Zulassungsbehörde gem. § 32 Abs. 1 Straßenverkehrsgesetz waren datenschutzrechtlich nicht zu beanstanden.
Auch die Datenübermittlung des Gewerbeamtes der Verwaltungsgemeinschaft an die Zulassungsbehörde auf deren Anfrage erfolgte gem. § 14 Abs. 6 Gewerbeordnung und war ebenfalls datenschutzrechtlich zulässig.

Allerdings hatte es nie eine Veräußerungsanzeige seitens des Petenten gegeben. Durch eine falsche Programmeinstellung in der Zulassungsbehörde wurde gleichzeitig mit der Bescheiderstellung zur Untersagung des Betriebes eines Fahrzeuges im öffentlichen Verkehr gem. § 27 Abs. 3 StVZO an den Petenten **automatisch** durch das Programm eine Mitteilung an das zuständige Finanzamt ausgelöst.
Dadurch wurde im Bescheid des Finanzamtes nur das Datum der Datenübermittlung übernommen und in den am Ende des Formulars befindlichen Standardtext, in dem von einer „Veräußerungsanzeige“ die Rede ist, eingefügt.
Das Gesetz zum Schutz personenbezogener Daten der Bürger (DSG-LSA) sieht für solche Fälle eine verschuldensunabhängige Haftung der öffentlichen Stelle gem. § 18 Abs. 1 DSG-LSA vor. Damit besteht für einen Betroffenen die Möglichkeit, auf zivilrechtlichem Weg einen wirtschaftlichen Schaden gegenüber der den Schaden verursachenden öffentlichen Stelle geltend zu machen.

Der Petent hat diesen zivilrechtlichen Weg beschritten, er klagte auf Schadenersatz. Das Verfahren endete mit einem Vergleich.

26.5. Videoüberwachung in Straßenbahnen

Nach Mitteilungen in der Presse zur Videoüberwachung in kommunalen Straßenbahnen befasste sich der Landesbeauftragte erneut mit dieser Angelegenheit (vgl. V. Tätigkeitsbericht, Ziff. 22.1).

Zunächst musste der Verkehrs-AG ihre Pflicht dargestellt werden, den Landesbeauftragten u. a. mit Erteilung von Auskünften nach § 23 Abs. 1 Nr. 1 DSG-LSA zu unterstützen. Der Adressat des DSG-LSA, die öffentlichen Stellen, sind in § 3 Abs. 1 Satz 1 DSG-LSA gesetzlich definiert (Legaldefinition). Danach ist nicht nur die Stadt als Gebietskörperschaft, sondern auch ihre Vereinigung ungeachtet ihrer Rechtsform (die Verkehrs-AG) öffentliche Stelle im Sinne des DSG-LSA. Der Grundsatz, dass das DSG-LSA nur auf öffentlich-rechtlich organisierte Stellen Anwendung findet, ist teilweise durch-

brochen. Dies gilt einmal für nicht-öffentliche Stellen, die hoheitliche Aufgaben wahrnehmen (Beliehene). Im Weiteren gilt es insbesondere für die von Trägern öffentlicher Aufgaben gebildeten Vereinigungen, wobei deren Rechtsform unerheblich ist. Anliegen der Vorschrift ist, die öffentliche Hand bei der Erledigung öffentlicher Aufgaben in privater Rechtsform den strengeren Datenschutzvorschriften für den öffentlichen Bereich zu unterstellen, um die sog. „Flucht in das Privatrecht“ zu begrenzen.
Da eine Straßenverkehrsgesellschaft am tatsächlichen bzw. möglichen Wettbewerb teilnimmt, ist sie allerdings als Wettbewerbsunternehmen im Sinne des § 3 Abs. 2 Nr. 1 DSG-LSA zu qualifizieren. Danach findet u. a. § 23 DSG-LSA Anwendung. Im Übrigen aber gelten die Vorschriften des BDSG.

Inhaltlich bedurften die Erforderlichkeit und Verhältnismäßigkeit der Videobeobachtung in den Straßenbahnen auf der Grundlage des § 3 Abs. 2 DSG-LSA i. V. m. § 6b BDSG der detaillierten Erörterung. Grundsätzlich ist sie im Rahmen der Ausübung des Hausrechtes zu Präventionszwecken zulässig. Jedoch sind die Grundsätze der Datensparsamkeit und Datenvermeidung zu beachten. Beispielsweise wären Aussagen zum Verhältnis des Rückgangs von Straftaten in überwachten und nicht überwachten Straßenbahnen nötig. Auch wäre das frühere, inzwischen reduzierte Schadensvolumen zu bewerten. Fraglich erschien zudem, ob das verfassungsrechtlich schützenswerte Persönlichkeitsrecht aller beobachteten Fahrgäste hinreichend Berücksichtigung gefunden hat. Dieses umfasst auch den Anspruch, sich in der Öffentlichkeit unbeobachtet zu bewegen. Hierzu war den Darstellungen der Verkehrs-AG nicht genügend zu entnehmen. Von einer freiwilligen Einwilligung in die Beobachtung konnte angesichts des Beförderungsbedarfs jedenfalls nicht ausgegangen werden.

Immerhin hatte die Verkehrs-AG den Zugang zu den Aufzeichnungen beschränkt (verschlossenes Aufzeichnungsgerät) und die Löschung nach 48 Betriebsstunden ohne Auslesung vorgesehen. Der Landesbeauftragte wies aber darauf hin, dass eine unbegrenzte Ausweitung der Überwachung unzulässig wäre. Unter kritischer Würdigung der zugrunde liegenden Vorfallszahlen und Schadensvolumina hielt er eine regelmäßige Überprüfung der Notwendigkeit des Überwachungsumfanges und ggf. eine weitere Reduzierung für geboten.

Anlage 1

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 8. Juni 2007

Telekommunikationsüberwachung und heimliche Ermittlungsmaßnahmen dürfen Grundrechte nicht aushebeln

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wendet sich mit Nachdruck gegen die von Bundesregierung und Bundesratsgremien geplante Einführung der Vorratsspeicherung von Telekommunikationsverkehrsdaten und die Verschärfungen verdeckter Ermittlungsmaßnahmen, vor allem durch Telekommunikationsüberwachung:

Die Datenschutzbeauftragten haben am 8./9. März 2007 auf ihrer Konferenz in Erfurt einen ersten Gesetzentwurf als verfassungswidrig beanstandet. Insbesondere haben sie vor heimlichen Online-Durchsuchungen und der Vorratsdatenspeicherung gewarnt. Damit würde tief in die Privatsphäre eingegriffen und das Kommunikationsverhalten der gesamten Bevölkerung - ob via Telefon oder Internet - pauschal und anlasslos erfasst.

Die einhellige Kritik der Datenschutzbeauftragten und ihre Aufforderung, stattdessen verhältnismäßige Eingriffsregelungen zu schaffen, wurden von der Bundesregierung nicht beachtet. In ihrem Gesetzentwurf vom 27. April 2007 wird demgegenüber der Schutz der Zeugnisverweigerungsberechtigten verringert, Benachrichtigungspflichten gegenüber betroffenen Personen werden aufgeweicht, Voraussetzungen für die Erhebung von Standortdaten in Echtzeit und für den Einsatz des IMSI-Catchers erheblich ausgeweitet und die Verwendungszwecke für die auf Vorrat gespeicherten Daten über die europarechtlichen Vorgaben hinaus auch auf leichte Straftaten, auf Zwecke der Gefahrenabwehr und sogar der Nachrichtendienste erstreckt.

Die nun im Bundesratsverfahren erhobenen zusätzlichen Forderungen zeugen von mangelndem Respekt vor den Freiheitsrechten der Bürgerinnen und Bürger. Dies zeigen folgende Beispiele: Die ohnehin überzogene Speicherdauer aller Verkehrsdaten wird von 6 auf 12 Monate verlängert. Die Überwachungsintensität erhöht sich durch eine Verschärfung der Prüfpflichten der Telekommunikationsunternehmen - bis zum Erfordernis des Ablichtens und Aufbewahrens von Identitätsnachweisen aller Personen, die Prepaid-Produkte nutzen wollen. Die Sicherheitsbehörden erhalten Auskunft über Personen, die bestimmte dynamische IP-Adressen nutzen. Ausschüsse des Bundesrates wollen die Nutzung dieser Daten sogar zur zivilrechtlichen Durchsetzung der Rechte an geistigem Eigentum gestatten und bewegen sich damit weit jenseits des durch die EG-Richtlinie zur Vorratsspeicherung abgesteckten Rahmens, die Nutzung auf die Verfolgung schwerer Straftaten zu beschränken. Weiterhin ist eine Ausdehnung der Auswertung von Funkzellendaten von Mobiltelefonen mit dem Ziel der Ermittlung des Aufenthaltes von möglichen Zeuginnen und Zeugen geplant. Daten, die Beweiserhebungs- oder -verwertungsverboten unterliegen, sollen nicht unmittelbar gelöscht, sondern nur gesperrt werden.

Ganz nebenbei will der Innenausschuss des Bundesrats eine Rechtsgrundlage für die heimliche Online-Durchsuchung von Internet-Computern schaffen. Allein die Zulassung

dieser Maßnahme würde rechtsstaatlichen Grundsätzen eklatant widersprechen und das Vertrauen in die Sicherheit der Informationstechnik massiv beschädigen.

Das Bundesverfassungsgericht hat in letzter Zeit eine Reihe von Sicherheitsgesetzen mit heimlichen Erhebungsmaßnahmen aufgehoben. Auch europäische Gerichte haben Sicherheitsmaßnahmen für rechtswidrig erklärt. Eine Entscheidung des Europäischen Gerichtshofs über die Verpflichtung zur Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten sollte abgewartet werden ebenso wie die Entscheidung des Bundesverfassungsgerichtes zur nordrhein-westfälischen Regelung, die dem Verfassungsschutz die Online-Durchsuchung erlaubt.

Die Forderungen im Gesetzgebungsverfahren zeugen von einem überzogenen Sicherheitsdenken. Sie führen dazu, dass die Freiheitsrechte der Bevölkerung untergraben werden. Sicherheit in der Informationsgesellschaft ist nicht mit überbordenden Überwachungsregelungen zu erreichen, sondern nur durch maßvolle Eingriffsbefugnisse mit effektiven grundrechtssichernden Verfahrensregelungen und durch deren besonnene Anwendung. Die betroffenen Grundrechte verkörpern einen zu hohen Wert, als dass sie kurzfristigen Sicherheitsüberlegungen geopfert werden dürfen.

Anlage 2

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring: Nachbesserung bei Auskunfteienregelungen gefordert

Die fortschreitende technologische Entwicklung führt zu immer weitreichenderer Erfassung und Verknüpfung von persönlichen Daten und ermöglicht deren Auswertung für Kontroll- und Präventionszwecke. In der Privatwirtschaft ist daher ein engmaschiges Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien entstanden, die durch Profilbildung das Verhalten eines jeden Menschen ohne dessen Wissen und Wollen abbilden und bewerten können.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass das Bundesministerium des Innern endlich damit begonnen hat, die gesetzlichen Regelungen zu den Auskunfteien zu überarbeiten und neue Regelungen zum Scoring zu schaffen.

Die vorgesehenen Regelungen zu den Auskunfteien verschlechtern die Rechtsposition der Betroffenen. Sie tragen dem sich ständig weiter entwickelnden Auskunfteimarkt und den dadurch hervorgerufenen Bedrohungen für das Recht auf informationelle Selbstbestimmung nicht hinreichend Rechnung. Ziel einer gesetzlichen Regelung muss es sein, den rasant wachsenden, branchenübergreifenden Datenaustausch zu beschränken. Es kann nicht hingenommen werden, dass Auskunfteidienste nur einseitig das Informationsinteresse der angeschlossenen Unternehmen bedienen. Sie müssen auch in stärkerem Maße die schutzwürdigen Belange der betroffenen Bürgerinnen und Bürgern berücksichtigen. Mit der im Entwurf vorgesehenen Möglichkeit, die Auskunftstätigkeit auf jegliche rechtliche und wirtschaftliche Risiken zu erstrecken, wäre zu befürchten, dass letztlich bei allen vertraglichen Beziehungen - also auch bei Versicherungs- und Arbeitsverträgen - vorab Auskunfteien eingeschaltet werden. Damit würden die allgemeinen Vertragsrisiken im Wirtschaftsleben in nicht mehr angemessener Weise einseitig auf die Kundinnen und Kunden verlagert.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber auf, die Situation der Verbraucherinnen und Verbraucher deutlich zu verbessern und mit dem Gesetzesvorhaben einen fairen Ausgleich zwischen den Interessen der Wirtschaft und der betroffenen Verbraucherinnen und Verbraucher zu schaffen. Die Konferenz hält es für dringend erforderlich, die Auskunfteitätigkeit auf kreditorische Risiken zu begrenzen. Zudem fordert die Konferenz, Auskunfteidienste branchenspezifisch zu begrenzen.

Der vorgelegte Referentenentwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes sieht beim Scoring nun Ansätze für ein transparenteres Verfahren für die Betroffenen vor. Es muss jedoch darauf geachtet werden, dass dieser Ansatz auch vorbehaltlos umgesetzt wird. Das Scoring, bei dem mittels einer mathematisch-statistischen Formel das zukünftige vertragstreue Verhalten eines Menschen durch einen Zahlenwert ausgedrückt wird, dringt seit Jahren in immer mehr Bereiche des Wirtschaftslebens vor. Den Betroffenen wurde jedoch bisher das Wissen darüber, wie sich

der Scorewert zusammensetzt, vorenthalten. Diese Praxis soll der Gesetzentwurf beenden. Die Betroffenen sollen Auskunft darüber erhalten, welche Daten mit welcher Gewichtung in den jeweiligen Scorewert eingeflossen sind. Die vorgeschlagenen Regelungen gehen jedoch noch nicht weit genug. Unbedingt zu streichen ist etwa eine im Entwurf enthaltene Regelung, wonach die Auskunft mit der Begründung verweigert werden kann, es würden Geschäftsgeheimnisse offenbart.

Anlage 3

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007

Zentrale Steuerdatei droht zum Datenmoloch zu werden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es für inakzeptabel, dass die Bundesregierung mit dem Jahressteuergesetz 2008 im Schnelldurchgang ohne ausführliche parlamentarische Beratung die beim Bundeszentralamt für Steuern aufzubauende zentrale Steuerdatei um zusätzliche - teilweise sensible - Daten anreichern will. Zugleich droht die Steueridentifikationsnummer (Steuer-ID) bereits vor ihrer endgültigen Einführung zu einem allgemeinen Personenkennzeichen zu werden.

Der Gesetzentwurf sieht die Ablösung des Lohnsteuerkartenverfahrens durch ein elektronisches Abrufverfahren (ElsterLohn II) ab 2011 vor. Bereits am 9. November 2007 soll das Gesetz abschließend im Bundestag beraten werden. Geplant ist unter anderem, die in Zusammenhang mit der seit dem 1. Juli 2007 vergebenen Steuer-ID errichtete Datenbank um weitere Daten zu ergänzen, etwa um die Religionszugehörigkeit, Ehepartner/Ehepartnerinnen/Kinder und deren Steuer-ID, dazu Angaben über Steuerklassen. Hierbei werden auch zahlreiche Datensätze auf Vorrat aufgenommen, da auch Personen betroffen sind, die (noch) keine Arbeitnehmer/Arbeitnehmerinnen sind.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert vom Bundestag und Bundesrat, dieses Vorhaben der Umstellung auf ein elektronisches Verfahren mit dem Jahressteuergesetz 2008 nicht zu beschließen. Folgende Punkte sind datenschutzrechtlich kritisch:

- Der durch die Vergabe der Steueridentifikationsnummer an alle Steuerpflichtigen und damit für alle Einwohnerinnen und Einwohner der Bundesrepublik entstehende Datenpool erhält eine neue Dimension. Zwar sind die Lohnsteuerabzugsmerkmale auch bisher auf der Lohnsteuerkarte vermerkt. Die Speicherung dieser Daten in einer zentralen Datenbank würde aber erhebliche datenschutzrechtliche Fragen aufwerfen. In den zentralen Datenbestand würden die Daten aller Personen mit Lohnsteuerkarten einfließen, also auch von solchen Personen, die sich nicht in einem lohnsteuerpflichtigen Beschäftigungsverhältnis befinden. Es ist zweifelhaft, ob die Aufnahme dieses Personenkreises dem Erforderlichkeitsgrundsatz entspricht. Nützlichkeitserwägungen sind für eine Datenhaltung auf Vorrat in keinem Fall ausreichend.

- Die Daten würden bundesweit annähernd vier Millionen Arbeitgebern zur Verfügung stehen. Als einzige Sicherung ist dabei vorgesehen, dass nur ein autorisierter Arbeitgeber die Lohnsteuerabzugsmerkmale abrufen kann. Klärungsbedürftig ist allerdings, wie dies sichergestellt werden kann. Zwar ist ein Authentifizierungsverfahren für den Arbeitgeber vorgesehen. Die Frage ist jedoch, ob damit tatsächlich eine rechtswidrige Informationsbeschaffung Dritter auszuschließen ist. Zumindest sollten die Daten aus der zentralen Datenbank nur unter Mitwirkung der Betroffenen abgerufen werden können.

- Die gesetzlich vorgeschriebene Evaluierung des Verfahrens (§ 87a Abs. 6 AO) ist noch nicht erfolgt. Gleichzeitig existieren bereits jetzt Bestrebungen, die Kommunikationsplattform "Elster" für Nutzungen durch andere Verwaltungszweige zu öffnen (OpenElster). Dies aber bedeutete, dass damit die Steuer-ID auch für die Identitätsfeststellung bei steuerfremden Anwendungen herangezogen werden könnte, ohne damit der strikten Zweckbindung nach § 139b Abs. 5 Abgabenordnung zu rein steuerlichen Zwecken Rechnung zu tragen. Diese Zweckbindung kann nach § 139b Abs. 2 AO auch nicht durch die jeweilige Einwilligung der betroffenen Bürgerinnen und Bürger überwunden werden. Mit OpenElster sollen diese Vorkehrungen offenbar aufgeweicht werden, bevor die Steuer-ID überhaupt eingeführt wurde. Allein dies macht deutlich, dass jede Erweiterung des zentralen Datenbestandes kritisch hinterfragt werden muss.

Schließlich ist zu befürchten, dass die vorgesehene Erweiterung der Datenbank beim BZSt nicht den Schlusspunkt darstellt. Die im neuen Datenpool gespeicherten Daten wären auch für Sozialleistungsträger und Strafverfolgungsbehörden interessant. Es gibt zahlreiche Beispiele, dass Daten, die zunächst nur für einen engen Zweck gespeichert werden dürfen, später für viele andere Zwecke verwendet werden: Die für steuerliche Zwecke erhobenen Daten über Freistellungsaufträge werden mit den ebenfalls beim BZSt gespeicherten Daten der Empfänger von BaföG- und anderen Sozialleistungen abgeglichen. Die Mautdaten, die zunächst nur zur Mautberechnung erhoben wurden, sollen zukünftig auch zur Strafverfolgung verwendet werden. Der zunächst ausschließlich zur Terrorismusbekämpfung und der Bekämpfung der organisierten Kriminalität eingeführte Kontendatenabruf steht heute auch Finanzämtern und anderen Behörden wie z. B. der Bundesagentur für Arbeit über das BZSt offen. Das BZSt enthält so einen einzigartigen aktuellen Datenpool aller Bundesbürgerinnen und -bürger, der wesentliche Meldedaten, Bankkontenstammdaten und Steuerdaten zentral verknüpfen kann.

Anlage 4

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007

Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Bei dem geforderten heimlichen Zugriff auf informationstechnische Systeme geht es nicht nur um "Online-Durchsicht" als einmalige Durchsuchung und die damit verbundene Übertragung von Festplatteninhalten an die Strafverfolgungs- oder Sicherheitsbehörden, sondern auch um die anhaltende Überwachung, um das Ausspähen von Passworten und die Protokollierung aller elektronischen Aktivitäten. Auch sollen andere Kommunikations- und Datenverarbeitungssysteme, wie Computernetze, Mobiltelefone, PDA usw. in die heimliche Durchsuchung einbezogen werden. Dabei ist die Feststellung des Computers einer Zielperson technisch ohne Zusatzinformationen nicht ohne weiteres möglich. Die Gefahr ist daher sehr groß, dass von einer solchen Maßnahme eine Vielzahl von - auch unverdächtigen - Nutzerinnen und Nutzern betroffen sein werden.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Darüber hinaus wird eingeräumt, dass sich mit Hilfe der entsprechenden Software die auf den Festplatten gespeicherten Inhalte manipulieren ließen, was die Beweiseignung der gewonnenen Erkenntnisse und damit - jedenfalls bei der Verfolgung von Straftaten - die Geeignetheit der Online-Durchsuchung in Frage stellt.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden. So begründen z. B. die drohende Aufweichung der Zweckbindung der Mautdaten und die Entwicklung der Telekommunikationsüberwachung die Befürchtung, dass Online-Durch-suchungen entsprechend dem technischen Fortschritt als Standardmaßnahme künftig auch bei Gefahren und Straftaten von geringerer Bedeutung eingesetzt werden. Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

Sie halten es für zwingend notwendig, dass das Urteil des Bundesverfassungsgerichts in dem Verfahren gegen die Online-Durchsuchung im Verfassungsschutzgesetz Nordrhein-Westfalens abgewartet wird.

Anlage 5

Entschließung der 74. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. bis 26. Oktober 2007

Zuverlässigkeitsüberprüfungen bei Großveranstaltungen

Anlässlich der Fußball-WM 2006 wurden im Rahmen der Akkreditierung umfassende Zuverlässigkeitsüberprüfungen nach einem auf Verwaltungsebene festgelegten Verfahren durchgeführt. Dabei wurde auf die Datenbestände der Polizei- und Verfassungsschutzbehörden des Bundes und der Länder zurückgegriffen. Dieses gesetzlich nicht vorgesehene Verfahren soll nunmehr beliebigen weiteren Veranstaltungen als Vorbild dienen.

Solche Zuverlässigkeitsüberprüfungen greifen in das Grundrecht auf informationelle Selbstbestimmung ein. Grundrechtseingriffe dürfen nicht unter Umgehung gesetzlicher Vorschriften durchgeführt werden, die Voraussetzungen und Begrenzungen solcher Verfahren regeln. Die Sicherheitsüberprüfungsgesetze des Bundes und der Länder sind für die Durchführung von allgemeinen Zuverlässigkeitsprüfungen, z. B. anlässlich von Veranstaltungen, nicht einschlägig. Eine generelle rechtliche Grundlage für Zuverlässigkeitsüberprüfungen besteht außerhalb der spezialgesetzlichen Bestimmungen nicht.

Einwilligungen können - auch wenn die Betroffenen über die Umstände informiert wurden - diese Maßnahme alleine nicht legitimieren. Dies nicht nur deshalb, weil Betroffene oft Nachteile befürchten müssen, wenn sie die Einwilligung verweigern und insoweit eine echte Freiwilligkeit fehlt. Viele Regelungen zu Überprüfungsverfahren verlangen - zusätzlich - zu den materiellen und verfahrensrechtlichen Regelungen die Mitwirkung der betroffenen Personen in Form einer schriftlichen Erklärung bei der Einleitung einer solchen Überprüfung. Außerdem sollen die Vorschriften ein transparentes Verfahren gewährleisten, in dem u. a. die Rechte Betroffener geregelt sind, so etwa das Recht auf Auskunft oder Anhörung vor negativer Entscheidung. Diese flankierenden Schutzmechanismen sind bei Überprüfungsverfahren unerlässlich.

Anlage 6

75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder
am 3. und 4. April 2008 in Berlin

Berliner Erklärung:
Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts

Regelungen insbesondere zum großen Lauschangriff, zur Telekommunikationsüberwachung, zur Rasterfahndung, zur Online-Durchsuchung, zur automatischen Auswertung von Kfz-Kennzeichen und zur Vorratsspeicherung von Telekommunikationsdaten haben die verfassungsrechtlich zwingende Balance zwischen Sicherheitsbefugnissen der staatlichen Behörden und persönlicher Freiheit der Bürgerinnen und Bürger missachtet. Das Bundesverfassungsgericht hat mit einer Reihe von grundlegenden Entscheidungen diese Balance wieder hergestellt und damit auch den Forderungen der Datenschutzbeauftragten des Bundes und der Länder größtenteils Rechnung getragen.

Die Herausforderungen für den Datenschutz gehen aber weit über die genannten Bereiche hinaus. Datenverarbeitungssysteme dringen immer stärker in alle Lebensbereiche ein und beeinflussen den Alltag. Das Internet ist zum Massenmedium geworden. Vielfältig sind dabei die Möglichkeiten, das persönliche Verhalten zu registrieren und zu bewerten. Der nächste Quantensprung der Informationstechnik steht unmittelbar bevor: Die Verknüpfung von Informationstechnik mit Körperfunktionen, insbesondere bei der automatisierten Messung medizinischer Parameter und bei der Kompensation organischer Beeinträchtigungen. Die Miniaturisierung von IT-Systemen geht so weit, dass demnächst einzelne Komponenten nicht mehr mit bloßem Auge wahrgenommen werden können (Nanotechnologie).

Das Handeln staatlicher und nicht-öffentlicher Stellen ist verstärkt darauf gerichtet, viele Daten ohne klare Zweckbestimmung zu sammeln, um sie anschließend vielfältig auszuwerten, beispielsweise um versteckte Risiken aufzudecken oder um persönliches Verhalten unbemerkt zu beeinflussen. Geht es der Wirtschaft etwa darum, durch Scoringverfahren die Kundinnen und Kunden vorab einzuschätzen, gewinnt die immer exzessivere Registrierung und automatisierte Beobachtung für staatliche Stellen an Bedeutung. In beiden Bereichen wird ganz normales Verhalten registriert, unabhängig von konkreten Gefahren oder Verdachtsmomenten. Auch diejenigen, die sich nichts haben zu schulden kommen lassen, werden einem verstärkten Kontroll- und Anpassungsdruck ausgesetzt, der Einschüchterungseffekte zur Folge haben wird.

Der Schutz der Grundrechte, nicht zuletzt des Datenschutzes, dient in einer demokratischen Gesellschaft auch dem Gemeinwohl und ist zunächst Aufgabe jeglicher Staatsgewalt. Darüber hinaus ist er eine gesamtgesellschaftliche Aufgabe. Schließlich ist jede Bürgerin und jeder Bürger auch zur Eigenverantwortung aufgerufen. Hilfen zum informationellen Selbstschutz müssen zur Verfügung gestellt werden, die es den Betroffenen ermöglichen, eine Erfassung ihres Verhaltens zu vermeiden und selbst darüber zu entscheiden, ob und wem gegenüber sie Daten offenbaren. Von zunehmender Bedeutung sind auch Projekte, die das Datenschutzbewusstsein fördern, um vor allem jüngere Menschen von einem fahrlässigen Umgang mit ihren persönlichen Daten abzuhalten.

Alle diese Maßnahmen tragen zur Entwicklung einer neuen Datenschutzkultur bei. Voraussetzung dafür ist auch, dass nicht länger versucht wird, die verfassungsrechtlichen Grenzen und Spielräume auszureizen. Stattdessen muss dem Gebot der Datenvermeidung und -sparsamkeit Rechnung getragen werden.

Anlage 7

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“

1. Die Nutzung moderner Informationssysteme ist auch mit Risiken verbunden. Diese begründen ein besonderes Schutzbedürfnis der Bürgerinnen und Bürger. Dieses verlangt aber nicht nur rechtliche Vorkehrungen und Sicherungen, sondern auch Aufklärung und Information darüber, mit welchen Risiken die Nutzung dieser Informationssysteme verbunden sind. Dies gilt vor allem für die junge „online-Generation“, die in der Altersgruppe der 14- bis 19-Jährigen zu 96 % regelmäßig das Internet nutzt und zwar im Durchschnitt länger als zweieinhalb Stunden täglich.

2. Die Datenschutzbeauftragten des Bundes und der Länder sehen es daher als wichtige Aufgabe an, Kinder und Jugendliche für einen sorgsamen und verantwortungsbewussten Umgang mit den eigenen Daten und den Daten anderer zu sensibilisieren. Diese Aufgabe obliegt gesellschaftlichen Einrichtungen ebenso wie staatlichen Organen.

   Die Erfahrungen, die anlässlich des 2. Europäischen Datenschutztages am 28. Januar 2008 gemacht wurden, stützen dies. Zu dem Motto "Datenschutz macht Schule" wurde von den Datenschutzbeauftragten des Bundes und der Länder eine Vielzahl von Veranstaltungen und Schulbesuchen organisiert. Eltern, Lehrkräfte, Schülerinnen und Schüler, aber auch Studierende hatten dabei die Möglichkeit, sich z. B. bei Podiumsdiskussionen, Rollenspielen und Workshops über datenschutzrelevante Fragen bei der Nutzung moderner Medien zu informieren. Die dabei gewonnenen Erfahrungen lassen nicht nur einen enormen Informationsbedarf, sondern auch ein großes Informationsinteresse erkennen, und zwar bei allen Beteiligten, bei den Jugendlichen ebenso wie bei ihren Eltern und den Lehrkräften.

   Bei den Informationsangeboten, die derzeit den Schulen angeboten werden, um die Medienkompetenz junger Menschen zu verbessern, spielt das Thema „Datenschutz“ aber nur eine untergeordnete Rolle. Es beschränkt sich überwiegend auf Fragen der Datensicherheit und wird zudem häufig von Fragen des Jugendmedienschutzes und des Verbraucherschutzes überlagert.

3. Die Datenschutzbeauftragten des Bundes und der Länder halten es daher für notwendig, dass die für die schulische Bildung zuständigen Ministerinnen und Minister der Landesregierungen bei der Förderung der Medienkompetenz von Kindern und Jugendlichen – schon im Grundschulalter - deren Datenschutzbewusstsein stärken. Der Datenschutz muss bei den Angeboten und Projekten zur Förderung der Medienkompetenz eine größere Rolle spielen. Die bisherigen Ansätze reichen bei weitem nicht aus. Gerade bei jungen Menschen muss das Bewusstsein über den Datenschutz als Bürgerrecht und Bestandteil unserer demokratischen Ordnung stärker gefördert werden.

Anlage 8

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

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 Sicher-

heitsbehörden 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.

Anlage 9

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Mehr Augenmaß bei der Novellierung des BKA-Gesetzes

Der vom Bundesministerium des Innern erarbeitete Referentenentwurf eines Gesetzes zur Abwehr des internationalen Terrorismus durch das Bundeskriminalamt hat zum Ziel, das Bundeskriminalamt mit umfassenden polizeilichen Befugnissen zur Verhütung von terroristischen Straftaten und zur Abwehr von Gefahren für die öffentliche Sicherheit in diesem Zusammenhang auszustatten. Insbesondere sind Befugnisse zur Durchsuchung, Rasterfahndung, Wohnraumüberwachung und Telekommunikationsüberwachung vorgesehen. Außerdem will das Bundesinnenministerium eine Befugnis zum heimlichen Zugriff auf informationstechnische Systeme („Online-Durchsuchung") in das BKA-Gesetz aufnehmen.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dagegen aus, dass dem Bundeskriminalamt nach dem Gesetzentwurf mehr Befugnisse eingeräumt werden sollen, als einzelnen Landespolizeien zur Erfüllung ihrer eigenen Gefahrenabwehraufgaben zustehen. Sie halten es daher für geboten, im weiteren Gesetzgebungsverfahren die Befugnisse des BKA auf die zur Aufgabenerfüllung zwingend notwendigen Kompetenzen zu beschränken.

Die bisherige informationelle Gewaltenteilung zwischen den Polizeien der Länder und dem BKA diente auch dem Datenschutz. Die Konferenz fordert deshalb eine klare, d. h. hinreichend trennscharfe Abgrenzung der spezifischen Befugnisse des Bundeskriminalamts einerseits zu denen der Landespolizeien und Verfassungsschutzbehörden andererseits.

Dem Referentenentwurf zufolge soll die Aufgabenwahrnehmung durch das Bundeskriminalamt die Zuständigkeit der Landespolizeibehörden auf dem Gebiet der Gefahrenabwehr unberührt lassen. Dies führt zu erheblichen datenschutzrechtlichen Problemen, da nach geltendem Recht auch die Länder bei Abwehr einer durch den internationalen Terrorismus begründeten Gefahr parallele Abwehrmaßnahmen ergreifen können. Angesichts der Weite der für das Bundeskriminalamt vorgesehenen und den Landespolizeibehörden bereits eingeräumten Datenerhebungs- und Datenverarbeitungsbefugnisse steht zu befürchten, dass es zu sich überlappenden und in der Summe schwerwiegenderen Eingriffen in das informationelle Selbstbestimmungsrecht Betroffener durch das Bundeskriminalamt und die Landespolizeibehörden kommen wird.

Ebenso stellt sich die grundsätzliche Frage der Abgrenzung von Polizei und Verfassungsschutz. In den vergangenen Jahren sind die Polizeigesetze des Bundes und der Länder zunehmend mit Befugnissen zur verdeckten Datenerhebung (z. B. heimliche Video- und Sprachaufzeichnungen, präventive Telekommunikationsüberwachung) ausgestattet worden. Zudem wurden die Eingriffsbefugnisse immer weiter ins Vorfeld von Straftaten und Gefahren erstreckt. Damit überschneiden sich die polizeilichen Ermittlungsbefugnisse zunehmend mit denen des Verfassungsschutzes.

Das Bundesverfassungsgericht hat in seinem Urteil zur „Online-Durchsuchung“ vom 27.02.2008 den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung zu gewährleisten. Diese Vorgabe des Gerichts gilt nicht nur für eine etwaige gesetzliche Regelung zur „Online-Durchsuchung“, sondern für alle Eingriffsmaßnahmen. Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber deshalb auf, im Rahmen der Novellierung des BKA-Gesetzes den Schutz des Kernbereichs privater Lebensgestaltung für alle Eingriffsmaßnahmen zu regeln.

Anlage 10

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Keine Vorratsspeicherung von Flugpassagierdaten

Die EU-Kommission hat den Entwurf eines Rahmenbeschlusses des Rates zur Speicherung von Flugpassagierdaten und zu deren Weitergabe an Drittstaaten vorgelegt. Künftig sollen die Fluggesellschaften bei Flügen aus der EU und in die EU zu jedem Fluggast insgesamt 19 Datenelemente, bei unbegleiteten Minderjährigen sechs weitere Datenelemente, an eine von dem jeweiligen Mitgliedstaat bestimmte „Zentralstelle" übermitteln. Die Daten sollen bei den Zentralstellen anlass- und verdachtsunabhängig insgesamt 13 Jahre lang personenbezogen gespeichert werden und zur Durchführung von Risikoanalysen dienen. Unter im Einzelnen noch unklaren Voraussetzungen sollen die Daten an Strafverfolgungsbehörden von Nicht-EU-Staaten (z. B. die USA), übermittelt werden dürfen. Neben Grunddaten zur Person, über Reiseverlauf, Buchungs- oder Zahlungsmodalitäten und Sitzplatzinformationen sollen auch andere persönliche Angaben gespeichert werden. Unklar ist, welche Daten unter „allgemeine Hinweise" gespeichert werden dürfen. Denkbar wäre, dass beispielsweise besondere Essenswünsche erfasst werden.

Mit der beabsichtigten Vorratsspeicherung und der Datenübermittlung wird die EU es auswärtigen Staaten ermöglichen, Bewegungsbilder auch von EU-Bürgerinnen und –Bürgern zu erstellen. In Zukunft besteht die Gefahr, dass Menschen Angst haben werden, durch ihre Reisegewohnheiten aufzufallen.

Die in dem Rahmenbeschluss vorgesehene Vorratsdatenspeicherung von Daten sämtlicher Fluggäste, die EU-Grenzen überschreiten, verstößt nicht nur gegen Art. 8 der Europäischen Menschenrechtskonvention und die Europaratskonvention 108, sondern ist auch mit dem im Grundgesetz verankerten Recht auf informationelle Selbstbestimmung nicht vereinbar. Grundrechtseingriffe „ins Blaue hinein", also Maßnahmen ohne Nähe zu einer abzuwehrenden Gefahr sind unzulässig.

Der Vorschlag für den Rahmenbeschluss erfolgte, ohne den Nutzen der erst jüngst in nationales Recht umgesetzten Richtlinie 2004/82/EG[1], die bereits alle Beförderungsunternehmen verpflichtet, die Daten von Reisenden an die Grenzkontrollbehörden zu übermitteln, auszuwerten. Hinzu kommt, dass der Vorschlag kaum datenschutzrechtliche Sicherungen enthält. Er bezieht sich nur auf eine bisher nicht bestehende und im Entwurf mit Mängeln behaftete EU-Datenschutzregelung. Diese Mängel wirken sich dadurch besonders schwerwiegend aus, dass in den Drittstaaten ein angemessenes Datenschutzniveau nicht immer gewährleistet ist und eine Änderung dieser Situation auch in Zukunft nicht zu erwarten ist.
Die EU-Kommission hat nicht dargelegt, dass vergleichbare Maßnahmen in den USA, in Kanada oder in Großbritannien einen realen, ernst zu nehmenden Beitrag zur Erhöhung der Sicherheit geleistet hätten. Sie hat die kritischen Stellungnahmen der nationalen

[1] RL 2004/82 EG v. 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

und des Europäischen Datenschutzbeauftragten sowie der Art. 29-Datenschutzgruppe nicht berücksichtigt.

Die Konferenz fordert die Bundesregierung auf, den Entwurf abzulehnen. Sie teilt die vom Bundesrat geäußerten Bedenken an der verfassungsrechtlichen Zulässigkeit der Speicherung der Passagierdaten.

Anlage 11

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beobachtet mit Sorge, dass die Datenschutzrechte der Bürgerinnen und Bürger im Rahmen der internationalen Zusammenarbeit der Sicherheitsbehörden immer häufiger auf der Strecke bleiben. Aktuelles Beispiel ist das am 11.3.2008 paraphierte deutsch-amerikanische Regierungsabkommen über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität. Die Konferenz fordert Bundestag und Bundesrat auf, dem Abkommen solange nicht zuzustimmen, bis ein angemessener Datenschutz gewährleistet ist.

Mit dem Abkommen wurde ein gegenseitiger Online-Zugriff auf Fundstellendatensätze von daktyloskopischen Daten und DNA-Profilen im hit/no-hit-Verfahren nach dem Muster des Prümer Vertrages vereinbart. Zudem wurden dessen Regelungen über den Austausch personenbezogener Daten zur Verhinderung terroristischer Straftaten weitgehend übernommen. Eine Übertragung des als Bedingung für diese umfangreichen Zugriffs- und Übermittlungsbefugnisse im Prümer Vertrag geschaffenen Datenschutzregimes erfolgte jedoch nicht.

Die Voraussetzungen, unter denen ein Datenaustausch erlaubt ist, sind nicht klar definiert. Der Datenaustausch soll allgemein zur Bekämpfung von Terrorismus und schwerer Kriminalität möglich sein. Welche Straftaten darunter konkret zu verstehen sind, wird nicht definiert. Es erfolgt hier lediglich der Verweis auf das jeweilige nationale Recht. Damit trifft nach dem Abkommen die USA einseitig eine Entscheidung über die Relevanz der abgerufenen Daten.

Bevor in so großem Umfang zusätzliche Datenübermittlungen erlaubt werden, muss zunächst geklärt werden, warum die bisherigen Datenübermittlungsbefugnisse für die internationale Polizeizusammenarbeit mit den USA nicht ausreichen.

Für die weitere Verarbeitung aus Deutschland stammender Daten in den USA bestehen für die Betroffenen praktisch keine Datenschutzrechte. Das Abkommen selbst räumt den Betroffenen keine eigenen Rechte ein, sondern verweist auch hierzu auf die Voraussetzungen im Recht der jeweiligen Vertragspartei. In den USA werden aber Datenschutzrechte, wie sie in der Europäischen Union allen Menschen zustehen, ausschließlich Bürgerinnen und Bürgern der Vereinigten Staaten von Amerika und dort wohnenden Ausländerinnen und Ausländern gewährt. Anderen Personen stehen Rechtsansprüche auf Auskunft über die Verarbeitung der eigenen Daten, Löschung unzulässig erhobener oder nicht mehr erforderlicher Daten oder Berichtigung unrichtiger Daten nicht zu. Außerdem besteht in den USA keine unabhängige Datenschutzkontrolle. Vor diesem Hintergrund sind die im Abkommen enthaltenen weiten Öffnungsklauseln für die weitere Verwendung der ausgetauschten Daten sowie der Verzicht auf Höchstspeicherfristen aus datenschutzrechtlicher Sicht nicht akzeptabel.

Anlage 12

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die Übermittlung polizeilicher und nachrichtendienstlicher Erkenntnisse an Arbeitgeber zur Überprüfung von Bewerberinnen und Bewerbern, Beschäftigten und Fremdpersonal (z. B. Reinigungskräfte) außerhalb gesetzlicher Grundlagen. In zunehmendem Maß bitten Arbeitgeber die Betroffenen, in eine Anfrage des Arbeitgebers bei der Polizei oder dem Verfassungsschutz zu etwaigen dort vorliegenden Erkenntnissen zu ihrer Person einzuwilligen. In anderen Fällen sollen die Betroffenen eine solche Auskunft („fremdbestimmte Selbstauskunft“) selbst einholen und ihrem Arbeitgeber vorlegen. Eine solche „Einwilligung des Betroffenen“ ist regelmäßig keine wirksame Einwilligung. Die Betroffenen sehen sich oftmals dem faktischen Druck des Wohlverhaltens zum Zwecke des Erhalts und der Sicherung des Arbeitsplatzes ausgesetzt.

Die gesetzliche Grundentscheidung, in einem „Führungszeugnis“ dem Arbeitgeber nur ganz bestimmte justizielle Informationen zu einer Person verfügbar zu machen, wird dadurch unterlaufen. Es stellt einen Dammbruch dar, wenn jeder Arbeitgeber durch weitere Informationen direkt oder indirekt an dem Wissen der Sicherheitsbehörden und Nachrichtendienste teilhaben kann. Die Übermittlung dieser Informationen an Arbeitgeber kann auch den vom Bundesarbeitsgericht zum „Fragerecht des Arbeitgebers“ getroffenen Wertentscheidungen widersprechen. Danach darf der Arbeitgeber die Arbeitnehmerinnen und Arbeitnehmer bei der Einstellung nach Vorstrafen und laufenden Ermittlungsverfahren fragen, wenn und soweit die Art des zu besetzenden Arbeitsplatzes dies erfordert.

Polizei und Nachrichtendienste speichern – neben den in ein „Führungszeugnis“ aufzunehmenden Daten – auch personenbezogene Daten, die in das Bundeszentralregister gar nicht erst eingetragen werden oder Arbeitgebern in einem „Führungszeugnis“ nicht übermittelt werden dürfen. Es stellt eine grundsätzlich unzulässige Durchbrechung des Zweckbindungsgrundsatzes dar, wenn ein Arbeitgeber diese Daten – über den Umweg über die Polizei oder einen Nachrichtendienst – für Zwecke der Personalverwaltung erhält. Dabei ist besonders zu beachten, dass polizeiliche oder nachrichtendienstliche Daten nicht zwingend gesicherte Erkenntnisse sein müssen, sondern oftmals lediglich Verdachtsmomente sind. Die Folgen von Missdeutungen liegen auf der Hand.

Anlage 13

Entschließung der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen

Elektronische Identitäten sind der Schlüssel zur Teilnahme an der digitalen Welt. Die Möglichkeiten der pseudonymen Nutzung, die Gewährleistung von Datensparsamkeit und -sicherheit und der Schutz vor Identitätsdiebstahl und Profilbildung sind wichtige Grundpfeiler moderner Informations- und Kommunikationstechnologien. Darauf hat die Bundesregierung zu Recht anlässlich des Zweiten Nationalen IT-Gipfels im Dezember 2007 (Hannoversche Erklärung) hingewiesen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass der gesetzliche Rahmen für die anonyme oder pseudonyme Nutzung elektronischer Verfahren bereits seit langem vorhanden ist. Beispielsweise hat jeder Diensteanbieter die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist (§ 13 Abs. 6 Telemediengesetz).

Bisher werden jedoch anonyme oder pseudonyme Nutzungsmöglichkeiten nur sehr selten angeboten. Vielmehr speichern Wirtschaft und Verwaltung immer mehr digitale Daten mit direktem Personenbezug. Erschlossen werden diese Datenbestände in der Regel über einheitliche Identifizierungsnummern. Mit der lebenslang geltenden, bundeseinheitlichen Steuer-Identifikationsnummer (Steuer-ID) oder der mit der Planung der Gesundheitskarte zusammenhängenden, ebenfalls lebenslang geltenden Krankenversichertennummer werden derzeit solche Merkmale eingeführt. Auch mit der flächendeckenden Einführung des ePersonalausweises wird jeder Bürgerin und jedem Bürger eine elektronische Identität zugewiesen, mit der sie bzw. er sich künftig auch gegenüber eGovernment-Portalen der Verwaltung oder eCommerce-Angeboten der Wirtschaft identifizieren soll.

Einheitliche Personenkennzeichen bergen erhebliche Risiken für das Recht auf informationelle Selbstbestimmung. So könnte sich aus der Steuer-ID ein Personenkennzeichen entwickeln, über das alle möglichen Datenbestände personenbezogen verknüpft und umfassende Persönlichkeitsprofile erstellt werden. Angesichts der stetig verbesserten technischen Möglichkeiten, zunächst verteilt gespeicherte Daten anwendungsübergreifend zu verknüpfen, wachsen entsprechende Begehrlichkeiten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die effektive Nutzung von Informationstechnik und hohe Datenschutzstandards keinen Widerspruch bilden. Ein datenschutzförderndes Identitätsmanagement kann den Einzelnen vor unangemessener Überwachung und Verknüpfung seiner Daten schützen und zugleich eine moderne und effektive Datenverarbeitung ermöglichen. Entsprechende EU-Projekte wie PRIME (Privacy and Identity Management for Europe) und FIDIS (Future of Identity in the Information Society) werden im Rahmen des 6. Europäischen Forschungsprogramms „Technologien für die Informationsgesellschaft“ gefördert.

Identitätsmanagement sollte auf der anonymen oder pseudonymen Nutzung von elektronischen Verfahren und der dezentralen Haltung von Identifikationsdaten unter möglichst weitgehender Kontrolle der betroffenen Bürgerinnen und Bürger basieren. Datenschutzfördernde Identitätsmanagementsysteme schließen Verknüpfungen nicht aus, wenn die Nutzenden es wünschen oder wenn dies gesetzlich vorgesehen ist. Sie verhindern jedoch, dass unkontrolliert der Bezug zwischen einer elektronischen Identität und einer Person hergestellt werden kann. Unter bestimmten, klar definierten Bedingungen kann mit Hilfe von Identitätsmanagementsystemen sichergestellt werden, dass ein Pseudonym bei Bedarf bezogen auf einen bestimmten Zweck (z. B. Besteuerung) einer Person zugeordnet werden kann.

Identitätsmanagementsysteme werden nur dann die Akzeptanz der Nutzerinnen und Nutzer finden, wenn sie einfach bedienbar sind, ihre Funktionsweise für alle Beteiligten transparent ist, möglichst alle Komponenten standardisiert sind und die Technik von unabhängigen Dritten jederzeit vollständig nachprüfbar ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung daher auf, den Absichtserklärungen des IT-Gipfels Taten folgen zu lassen und den Einsatz datenschutzfördernder Identitätsmanagementsysteme voranzutreiben. Sowohl die öffentliche Verwaltung als auch die Wirtschaft sollte die Einführung solcher datenschutzfördernder Systeme unterstützen.

Anlage 14

Beschluss der 75. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 3. und 4. April 2008 in Berlin

Informationssystem „IMI“

Vor dem Hintergrund, dass die Europäische Kommission für europaweite Verwaltungsvorgänge den Einsatz interoperabler E-Government-Dienste vorantreibt und das Binnenmarkt-Informationssystem IMI insoweit als Ausgangspunkt für eine neue Kommunikationsinfrastruktur verstanden werden muss, unterstützt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder nachdrücklich die Stellungnahme des Europäischen Datenschutzbeauftragten vom 22. Februar 2008 zur IMI-Entscheidung der Europäischen Kommission.
Das IMI-System muss auf eine tragfähige Rechtsgrundlage gestellt werden. Am ehesten kommt hierfür die Verabschiedung eines eigenständigen Rechtsakts durch den Rat und das Europäische Parlament in Betracht. In diesem müssen neben der präzisen Beschreibung von Funktionen, Rechten und Pflichten der IMI-Akteurinnen und Akteure und IMI-Nutzerinnen und -Nutzer die Datenverarbeitungsbedingungen des Systems, insbesondere im Hinblick auf die Verteilung der datenschutzrechtlichen Verantwortlichkeiten, die Erforderlichkeit und Transparenz der Datenverarbeitung, die Betroffenenrechte, die Speicherdauer, die Sicherheitsmaßnahmen und die Datenschutzkontrolle verbindlich festgelegt werden.

Anlage 15

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. September 2008

Entschlossenes Handeln ist das Gebot der Stunde

Nie haben sich in der jüngeren Geschichte die Skandale um den Missbrauch privater Daten in der Wirtschaft so gehäuft wie heute und damit deutlich gemacht, dass nicht nur im Verhältnis Bürger-Staat das Grundrecht auf informationelle Selbstbestimmung bedroht ist. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat wiederholt - zuletzt in ihrer Berliner Erklärung vom 4. April dieses Jahres - auf diese Gefahren hingewiesen, die von massenhaften Datensammlungen privater Unternehmen und ihrer unkontrollierten Nutzung ausgehen. Sie hat auch deshalb den Gesetzgeber zu einer grundlegenden Modernisierung und Verbesserung des Datenschutzrechts aufgefordert und eine neue Datenschutzkultur angemahnt.

Dass jetzt endlich im politischen und gesellschaftlichen Raum die Problematik erkannt und diskutiert wird, ist zu begrüßen. Dabei kann und darf es aber nicht bleiben, nur entschlossenes Handeln kann die Bürgerinnen und Bürger vor weiterem Missbrauch ihrer persönlichen Daten schützen und das verlorene Vertrauen wiederherstellen.

Das vom Grundgesetz garantierte Recht eines Jeden, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu entscheiden, muss endlich die ihm gebührende Beachtung finden Die Weitergabe von persönlichen Angaben zu Werbezwecken darf nur mit ausdrücklicher Einwilligung der Betroffenen zulässig sein. Daten sind mit einem Vermerk über ihre Quelle zu kennzeichnen. Der Abschluss von Verträgen darf nicht von der Einwilligung in die Datenübermittlung zu Werbezwecken abhängig gemacht werden. Verstöße gegen den Datenschutz dürfen nicht ohne Konsequenzen bleiben, sondern müssen strikt geahndet werden. Deshalb müssen die bestehenden Lücken in den Bußgeld- und Strafbestimmungen geschlossen und der Bußgeld- und Strafrahmen für Datenschutzverstöße deutlich erhöht werden. Diese Sofortmaßnahmen, die bereits Gegenstand des Spitzentreffens im Bundesministerium des Innern am 4. September 2008 waren, können vom Deutschen Bundestag noch in den bereits vorliegenden Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes aufgenommen werden.

Gesetzgeberische Maßnahmen allein helfen aber nicht weiter, wenn ihre Einhaltung nicht ausreichend kontrolliert und Verstöße nicht sanktioniert werden können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, die Datenschutzaufsichtsbehörden endlich organisatorisch, personell und finanziell in die Lage zu versetzen, ihren Beratungs- und Kontrollaufgaben flächendeckend, unabhängig und wirkungsvoll nachkommen zu können, und entsprechend der EU-Datenschutzrichtlinie mit wirksamen Einwirkungsbefugnissen auszustatten, die sie bisher nicht haben.

Außerdem müssen Konzepte zur grundlegenden Modernisierung des Datenschutzes entwickelt und umgesetzt werden. Wichtige Themen sollten dabei noch in dieser Legislaturperiode angegangen werden:

- Verbesserung der Protokollierung des Datenzugriffs in automatisierten Verfahren
- Stärkung der datenschutzrechtlichen Auskunftsrechte
- Pflicht zur Information der betroffenen Personen und der Aufsichtsbehörden bei Datenpannen und missbräuchlicher Datennutzung
- Gewinnabschöpfung aus unbefugtem Datenhandel
- Einführung eines gesetzlich geregelten Datenschutzaudits, mit dem unabhängig und qualifiziert die Datenschutzkonformität von Verfahren und Produkten bestätigt wird
- Stärkung der betrieblichen Datenschutzbeauftragten als Organ der Selbstkontrolle
- Spezialisierung der Strafverfolgungsbehörden
- Anerkennung von Datenschutzbestimmungen als verbraucherschützende Normen

Nur wenn jetzt den Ankündigungen Taten folgen und entschlossen gehandelt wird, können die Bürgerinnen und Bürger künftig vor Datenmissbrauch und Verletzung ihres Grundrechts auf informationelle Selbstbestimmung besser als in der Vergangenheit geschützt werden.

Anlage 16

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Adress- und Datenhandel nur mit Einwilligung der Betroffenen

Der auf dem „Datenschutzgipfel“ im September 2008 gefundene Konsens, den Adress- und Datenhandel zukünftig nur auf der Grundlage einer Einwilligung zuzulassen, ist in Politik und Gesellschaft auf breite Zustimmung gestoßen. Nur eine solche Lösung respektiert das informationelle Selbstbestimmungsrecht und damit die Wahlfreiheit der Verbraucherinnen und Verbraucher. Wer davon jetzt abrücken will, verkennt die auf Grund der jüngsten Datenskandale ans Licht gekommenen Missstände, deren Ursache nicht nur in der kriminellen Energie Einzelner zu suchen ist. Um die Daten der Betroffenen tatsächlich wirksam schützen zu können, muss die Wahlmöglichkeit der Menschen von Maßnahmen flankiert werden, die die Herkunft der Daten jederzeit nachvollziehbar machten.

Die von der Werbewirtschaft gegen die Einwilligungslösung ins Feld geführten Argumente sind nicht überzeugend. Die behaupteten negativen Folgen für den Wirtschaftsstandort sind nicht zu belegen. Unabhängig davon gilt: Es gibt keine schutzwürdigen Interessen für die Beibehaltung von Geschäftsmodellen, die darauf beruhen, hinter dem Rücken und ohne Information der Betroffenen mit deren Daten Handel zu treiben. Die Einführung des Einwilligungsprinzips würde im Gegenteil zielgenaueres und wirksameres Direktmarketing erlauben. Die Bundesregierung sollte sich deshalb nicht von ihrer Absicht abbringen lassen, die beim „Datenschutzgipfel“ gegebenen Zusagen zur schnellen Verbesserung des Datenschutzes einzulösen. Sie würde es sonst versäumen, die notwendigen Lehren aus den jüngsten Skandalen zu ziehen. Der Referentenentwurf des Bundesinnenministeriums zur Änderung des Bundesdatenschutzgesetzes im Bereich des Adress- und Datenhandels (Stand: 22.10.2008) zieht mit der Einwilligungslösung – bei aller Verbesserungswürdigkeit im Detail – die einzig richtige und notwendige Konsequenz aus den zahlreichen Datenskandalen und darf nicht verwässert werden.

Anlage 17

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Mehr Transparenz durch Informationspflichten bei Datenschutzpannen

In den letzten Monaten hat eine Reihe von gravierenden Datenschutzverstößen die Aufmerksamkeit der Öffentlichkeit und der Medien gefunden. In vielen dieser Fälle lag der Verlust oder Missbrauch personenbezogener Daten längere Zeit zurück und war der verantwortlichen Stelle bekannt, ohne dass die Betroffenen oder die zuständige Datenschutzaufsichtsbehörde hierüber informiert worden wären. Dadurch wurde ihnen die Möglichkeit genommen, Sicherheitsmaßnahmen zu ergreifen und mögliche Schäden zu begrenzen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder bekräftigt deswegen die Forderung, alle verantwortlichen Stellen - grundsätzlich auch alle öffentlichen Stellen - gesetzlich zu verpflichten, bei Verlust, Diebstahl oder Missbrauch personenbezogener Daten unverzüglich die hiervon betroffenen Bürgerinnen und Bürger und die zuständigen Aufsichts- oder Kontrollbehörden sowie gegebenenfalls auch die Öffentlichkeit zu unterrichten. Dies entspricht ihrer datenschutzrechtlichen Verantwortung und ermöglicht es den Betroffenen, negative Konsequenzen solcher Datenschutzpannen abzuwenden oder einzugrenzen. Hinter diesem Interesse hat der Wunsch der entsprechenden Stellen zurückzustehen, solche Vorkommnisse geheim zu halten, um keinen Imageschaden oder keine wirtschaftlichen Nachteile zu erleiden.

Etliche Staaten haben bereits entsprechende Regelungen. Eine solche Informationspflicht würde die Transparenz erhöhen und das Vertrauen der Betroffenen in eine korrekte Datenverarbeitung stärken. Darüber hinaus würde sie einen wichtigen Anstoß geben, mehr für Datenschutz und Datensicherheit zu tun.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deswegen, entsprechende umfassende Informationspflichten für Unternehmen und öffentliche Stellen im Bundesdatenschutzgesetz und den Landesdatenschutzgesetzen zu schaffen. Die übrigen aus Anlass der Datenschutzskandale in einer Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 16.09.2008 erläuterten Forderungen zur Novellierung des Bundesdatenschutzgesetzes werden bekräftigt.

Anlage 18

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren

Die Bundesregierung hat am 25.06.2008 den Gesetzentwurf über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) beschlossen (BT-Drs. 16/10492). Danach haben Beschäftigte die monatliche Übermittlung ihrer Einkommensdaten an die Zentrale Speicherstelle zu dulden, obwohl zurzeit nicht verlässlich abgeschätzt werden kann, in welchem Umfang die Speicherung der Daten tatsächlich erforderlich ist. Ein großer Anteil der Betroffenen wird die dem Anwendungsbereich des ELENA-Verfahrens unterfallenden Sozialleistungen niemals oder erst zu einem erheblich späteren Zeitpunkt geltend machen. Es steht somit bereits jetzt zu vermuten, dass eine große Zahl der übermittelten Daten von der Zentralen Speicherstelle wieder zu löschen sein wird, ohne jemals für irgendein Verfahren genutzt worden zu sein.

Die Datenschutzbeauftragten des Bundes und der Länder haben deshalb wiederholt verfassungsrechtliche Bedenken unter dem Gesichtspunkt der Verhältnismäßigkeit und speziell der Erforderlichkeit geltend gemacht und eine substantiierte Begründung gefordert. Diese ist nicht erfolgt. Bisher bestehen lediglich höchst vage Erwartungen auf langfristige Effizienzsteigerungen insbesondere der Arbeitsverwaltung. Angesichts dieser Unklarheiten verbleiben erhebliche Zweifel an der Verfassungsmäßigkeit des Gesetzes. Hinzu kommt, dass derartige umfangreiche Datensammlungen Begehrlichkeiten wecken, die Daten für andere Zwecke zu verwenden.

Für den Fall, dass diese verfassungsrechtlichen Bedenken ausgeräumt werden können, sind unter dem Gesichtspunkt des *technisch-organisatorischen Datenschutzes* noch folgende Verbesserungen durch den Gesetz- bzw. Verordnungsgeber erforderlich:

- Es muss sichergestellt werden, (z. B. durch die Einrichtung eines Verwaltungsausschusses der Zentralen Speicherstelle), dass unter Mitwirkung von Datenschutzbeauftragten gemeinsame Grundsätze zur Wahrung des Datenschutzes und der technischen Sicherheit berücksichtigt werden.

- Für die Zentrale Speicherstelle muss ein Datenschutzbeauftragter eingesetzt werden, der dazu verpflichtet ist, regelmäßig an den Verwaltungsausschuss zu berichten.

- Schlüssel zur Ver- und Entschlüsselung der bei der Zentralen Speicherstelle gespeicherten Daten dürfen nicht in der Verfügungsgewalt der Zentralen Speicherstelle liegen. Die Ver- und Entschlüsselungskomponente muss von einer unabhängigen Treuhänderstelle verantwortet werden.

- Mittelfristig ist ein Verfahren anzustreben, das die technische Verfügungsmöglichkeit über die individuellen Daten den Betroffenen überträgt.

- Das im Rahmen der ELENA-Modellvorhaben erarbeitete differenzierte Löschungskonzept muss weiterentwickelt und umgesetzt werden.

- Für abrufende Stellen sind starke Authentisierungsverfahren vorzuschreiben, die dem Stand der Technik entsprechen und den Forderungen der Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 11. Oktober 2006 zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren genügen.

- Für die technischen Komponenten muss eine Zertifizierung durch eine unabhängige Prüfung vorgeschrieben werden.

Anlage 19

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potential an volkswirtschaftlichem Nutzen und ist geeignet, vielen E-Government- und E-Commerce-Anwendungen die erforderliche Infrastruktur zur Verfügung zu stellen. Als einen ersten Schritt regelt das europäische Recht mit der so genannten INSPIRE-Richtlinie, die bis Mai 2009 in nationales Recht umgesetzt werden muss, die Bereitstellung von amtlichen Geodaten nach einheitlichen Standards für europaweite behördliche, kommerzielle und private Nutzungen.

Durch diese neue Infrastruktur werden georeferenzierbare Angaben auf Grund der Erschließungsmöglichkeit über Wohnanschriften oder Eigentümer- bzw. Standortdaten als personenbezogene Daten zur Verfügung gestellt. Diesem Umstand müssen die gesetzlichen Regelungen gerecht werden und angemessene Datenschutzregelungen enthalten.

Bei der Bereitstellung amtlicher Geodaten ist sowohl nach der europäischen Richtlinie als auch nach deutschem Verfassungsrecht der Schutz personenbezogener Daten angemessen zu gewährleisten. Der Entwurf der Bundesregierung zur Umsetzung dieser Richtlinie in einem Geodatenzugangsgesetz (BT-Drs. 16/10530) sieht eine entsprechende Anwendung der Schutzvorschriften des Umweltinformationsgesetzes vor. Im Gegensatz zum einzelfallbezogenen Zugang nach den Umweltinformationsgesetzen birgt der im Entwurf eines Geodatenzugangsgesetzes vorgesehene massenhafte Abruf solcher Daten aber ein höheres datenschutzrechtliches Gefährdungspotenzial. Der Verweis auf das Umweltinformationsgesetz ist nach Ansicht der Konferenzen der Datenschutz- und der Informationsfreiheitsbeauftragten des Bundes und der Länder deshalb nicht interessengerecht. Ein Geodatenzugangsgesetz muss einen differenzierenden Ausgleich zwischen Informations- und Schutzinteressen für die spezielle Problematik der Geobasis- und der Geofachdaten vornehmen. Es ist insbesondere zu berücksichtigen, dass nach der INSPIRE-Richtlinie die Zugangsmöglichkeit eingeschränkt werden soll, wenn der Zugang nachteilige Auswirkungen auf die Vertraulichkeit personenbezogener Daten haben kann.

Anlage 20

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Elektronische Steuererklärung sicher und datenschutzgerecht gestalten

Mit dem Steuerbürokratieabbaugesetz (BR-Drs. 547/08) sollen u. a. verfahrenstechnische Regelungen für die elektronische Übermittlung von Steuererklärungen durch Steuerpflichtige festgelegt werden. Zu diesem Zweck soll § 150 Abgabenordnung (AO) durch Abs. 7 Satz 1 dahingehend ergänzt werden, dass bei Einführung einer Verpflichtung zur elektronischen Abgabe die übermittelten Steuerdaten mit einer qualifizierten Signatur nach dem Signaturgesetz zu versehen sind.

Die Konferenz sieht es kritisch, dass § 150 Abs. 7 Satz 2 Nr. 6 und 7 AO auch vorsieht, zur Erleichterung und Vereinfachung des automatisierten Besteuerungsverfahrens anstelle der qualifizierten elektronischen Signatur ein so genanntes anderes sicheres Verfahren im Benehmen mit dem Bundesinnenministerium zuzulassen oder sogar auf beide Verfahren vollständig zu verzichten. In der Gesetzesbegründung wird darauf verwiesen, dass neben der qualifizierten elektronischen Signatur künftig auch eine Übermittlung der Daten unter Nutzung der Möglichkeiten des neuen elektronischen Personalausweises möglich sein soll.
Bereits in ihrer Entschließung zur sachgemäßen Nutzung von Authentisierungs- und Signaturverfahren vom 11. Oktober 2006 hat die Konferenz gefordert, Nutzenden die Möglichkeit zu eröffnen, die elektronische Kommunikation mit der Verwaltung durch eine qualifizierte elektronische Signatur abzusichern. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt daher die vorgesehene Regelung in der AO zur Nutzung der qualifizierten elektronischen Signatur, da dieses Verfahren geeignet ist, die Authentizität und Integrität eines elektronisch übermittelten Dokuments sicherzustellen, und somit die handschriftliche Unterschrift ersetzen kann.

Die Datenschutzbeauftragten des Bundes und der Länder erklären hierzu:

1) Das Verfahren der qualifizierten elektronischen Signatur nach dem Signaturgesetz ist im Hinblick auf die Authentizität und Integrität elektronisch übermittelter Dokumente derzeit alternativlos.

2) Für die Bewertung anderer Verfahren sollte unmittelbar auf die Fachkenntnis unabhängiger Gutachter abgestellt werden. Als Gutachter für die Beurteilung der technischen Sicherheit kämen etwa die Bundesnetzagentur oder das BSI in Frage.

3) Steuerpflichtige müssen auch im elektronischen Besteuerungsverfahren die Möglichkeit haben, die elektronische Kommunikation mit der Finanzverwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

Anlage 21

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten

Mit der Gesundheitsreform soll über die Einführung von Wettbewerbsmechanismen die Qualität und Effizienz der gesetzlichen Krankenkassen verbessert werden. Die Kassen sind daher bemüht und auch vom Gesetzgeber gehalten, Versicherten ein Versorgungsmanagement anzubieten. Von zentraler Bedeutung sind dabei Patientenschulungsmaßnahmen und strukturierte Behandlungsprogramme für chronisch kranke Versicherte, die jedoch lediglich Angebotscharakter haben dürfen. Ihre Teilnahme soll nach dem Willen des Gesetzgebers freiwillig sein und eine eingehende Unterrichtung voraussetzen. Diese Vorgaben werden von einzelnen Krankenkassen nicht beachtet, wenn sie versuchen, die Versicherten in ihrem Gesundheitsverhalten zu steuern und sie in bestimmte Maßnahmen und Programme zu drängen.
Um Teilnehmerinnen und Teilnehmer zu gewinnen und um Maßnahmen durchzuführen, bedienen sich die Kassen vielfach privater Dienstleister und offenbaren diesen teils höchst sensible Gesundheitsdaten ihrer Versicherten. Dies ist datenschutzrechtlich nach dem Sozialgesetzbuch unzulässig, wenn die Übermittlung ohne Kenntnis und vorherige Einwilligung der jeweiligen Versicherten erfolgt.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält die Einhaltung insbesondere der folgenden Eckpunkte bei gesundheitlichen Steuerungsprogrammen der Krankenkassen für unerlässlich:

- Die Krankenkassen dürfen Versichertendaten nur dann zur Auswahl von Personen für besondere Gesundheitsmaßnahmen verwenden, wenn dies gesetzlich ausdrücklich vorgesehen ist. Es muss sich um valide und erforderliche Daten handeln. Mit der Auswahl darf kein privater Dienstleister beauftragt werden.

- Die erstmalige Kontaktaufnahme mit potenziell für eine Gesundheitsmaßnahme in Betracht kommenden Versicherten muss durch die Krankenkasse selbst erfolgen, auch wenn ein privater Dienstleister mit der späteren Durchführung der Gesundheitsmaßnahme beauftragt worden ist.

- Die Versicherten sind vor Übermittlung ihrer Daten umfassend zu informieren. Die Information muss auch den Umstand umfassen, dass ein privates Unternehmen mit der Durchführung betraut werden soll. Soweit die Versicherten ausdrücklich in die Teilnahme eingewilligt haben, dürfen die für die Durchführung der Maßnahme erforderlichen Daten an den Dienstleister übermittelt werden.

- Wenn Versicherte - zu welchem Zeitpunkt auch immer - eindeutig zum Ausdruck bringen, nicht an einer Maßnahme teilnehmen zu wollen oder nicht an weitergehenden Informationen, einer konkreten Anwerbung oder einer fortgesetzten Betreuung interessiert zu sein, ist dies zu respektieren. Weitere Maßnahmen (auch telefonische Überredungsversuche) sind zu unterlassen.

Anlage 22

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Auftrag des Bundesministeriums der Justiz die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung (§§ 100g, 100h StPO alte Fassung) evaluiert. Die Studie geht zu Recht davon aus, dass Verkehrsdaten ein hohes Überwachungspotential in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Der Studie zufolge ist die Zahl der Verkehrsdatenabfragen erheblich und kontinuierlich von 10.200 (2002) auf 40.000 Abfragen (2005) angestiegen. Zudem erfasst die Maßnahme regelmäßig auch eine Vielzahl unbescholtener Bürgerinnen und Bürger.

Das Bundesministerium der Justiz hat die Studie erst im Februar dieses Jahres und somit nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlicht. Das Gutachten liefert Erkenntnisse, deren Berücksichtigung im Gesetz vom 21. Dezember 2007 erforderlich gewesen wäre. Die Datenschutzbeauftragten des Bundes und der Länder sehen sich durch die Studie in ihrer schon früher geäußerten Kritik (vgl. ihre Entschließung vom 8./9. März 2007) bestätigt. Sie fordern den Gesetzgeber auf, die gesetzliche Regelung unter folgenden Aspekten nun zügig nachzubessern:

- Die Straftatenschwelle für Verkehrsdatenabfragen sollte insbesondere im Hinblick auf die inzwischen eingeführte Vorratsdatenspeicherung auf schwere Straftaten angehoben werden. Ein bedeutsamer Anteil der überprüften Verfahren war allenfalls der mittleren Kriminalität zuzuordnen.

- Die gesetzliche Höchstdauer der Maßnahme sollte von drei auf zwei Monate reduziert werden. Das Gutachten hat gezeigt, dass die praktischen Bedürfnisse, wie sie sich in den Aktendaten und Befragungsergebnissen äußern, dadurch vollständig abgedeckt würden.

- Für die Verkehrsdatenabfrage sollten (nach dem Vorbild der Regelungen für die akustische Wohnraumüberwachung) qualifizierte Begründungspflichten in der StPO vorgesehen werden. Dabei sollten auch die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen gesetzlich geregelt werden (z. B. Beweisverwertungsverbote). Wesentliche Kritikpunkte der Studie waren insbesondere die lediglich formelhafte Wiedergabe des Gesetzestextes sowie die häufig wörtliche Übernahme der staatsanwaltschaftlichen Anträge in den Begründungen.

- Zur Vermeidung von Rechtsunsicherheit und zur Stärkung des Richtervorbehalts sollte in den Fällen staatsanwaltschaftlicher Eilanordnung die Verwertbarkeit der erlangten Daten davon abhängig gemacht werden, dass ein Gericht rückwirkend die

formelle und materielle Rechtmäßigkeit der Maßnahme feststellt. Dem Gutachten zufolge besteht insbesondere bei den Telekommunikationsunternehmen Unsicherheit, inwieweit sie zur Herausgabe der Verkehrsdaten verpflichtet sind, wenn eine staatsanwaltschaftliche Eilanordnung nicht innerhalb der gesetzlichen Frist richterlich bestätigt wird.

- Der tatsächliche Nutzen der Vorratsdatenspeicherung für die Strafverfolgung und damit die Erforderlichkeit der Maßnahme müssen in Frage gestellt werden. Bereits bei der früheren Höchstspeicherdauer von 3 Monaten waren nach der Studie 98 % der Abfragen erfolgreich.

Auch in der praktischen Anwendung der Regelungen zur Verkehrsdatenabfrage hat die Studie Defizite deutlich gemacht. Die Datenschutzbeauftragten des Bundes und der Länder appellieren daher auch an die Strafverfolgungsbehörden und Gerichte, aus dem Gutachten Konsequenzen zu ziehen. Besonderes Augenmerk ist vor allem auf die Prüfung der Angemessenheit der Maßnahme zu richten. Dies muss auch in substantiierten Begründungen zum Ausdruck kommen. Die gesetzlich festgeschriebenen, dem Grundrechtsschutz dienenden Benachrichtigungs-, Löschungs- und Dokumentationspflichten müssen - trotz hoher Belastungen in der Praxis - unbedingt eingehalten werden. Der Richtervorbehalt muss seine grundrechtssichernde Funktion effizient erfüllen können. Die Justizverwaltungen sind in der Verantwortung, hierfür ausreichende personelle Ressourcen zur Verfügung zu stellen.

Eine Fortführung der wissenschaftlichen Evaluation der Verkehrsdatenabfrage ist - unter den neuen rechtlichen Rahmenbedingungen und aufgrund der Weiterentwicklung der Technik - unerlässlich. Insbesondere sollten dabei Notwendigkeit und Nutzen der Verkehrsdatenabfrage - auch im Vergleich zu anderen möglichen Maßnahmen - mit Blick auf den Verhältnismäßigkeitsgrundsatz auf den Prüfstand gestellt werden.

Anlage 23

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich

Auf europäischer Ebene ist eine Vielzahl von Vorhaben beschlossen bzw. initiiert worden, die in ihrer Gesamtheit zu erheblichen Eingriffen in die Persönlichkeitsrechte führt:

- Die Telekommunikationsunternehmen in den Mitgliedstaaten der EU sind verpflichtet, die bei der Nutzung öffentlich zugänglicher Telekommunikationsdienste anfallenden Verkehrsdaten über das Kommunikationsverhalten der Einzelnen für die Sicherheitsbehörden ohne konkreten Anlass auf Vorrat zu speichern.

- Die Pässe der Bürgerinnen und Bürger der EU-Mitgliedstaaten werden mit biometrischen Merkmalen ausgestattet.

- Fluggastdaten (PNR) werden in die USA übermittelt, um sie den dortigen Behörden zur Verfügung zu stellen. Die Nutzung von Fluggastdaten zu Strafverfolgungszwecken wird auch in der Europäischen Union vorbereitet.

- Der Vertrag von Prüm, der in den Rechtsrahmen der Union überführt wird, ermöglicht den Polizei- und Strafverfolgungsbehörden der Mitgliedstaaten einen gegenseitigen Zugriff auf Fingerabdruck-, DNA- und Kfz-Daten.

- Es soll ein Europäisches Strafregisterinformationssystem geschaffen werden, mit dem Informationen über strafrechtliche Verurteilungen zwischen den Mitgliedstaaten ausgetauscht werden können.

- Das Schengener Informationssystem wird weiter ausgebaut, u. a. durch die Speicherung von biometrischen Merkmalen. Zudem wird der Kreis der Nutzer erweitert um das Europäische Polizeiamt EUROPOL und die Einheit für justizielle Zusammenarbeit in der EU (EUROJUST).

- Ein Europäisches Visa-Informationssystem (VIS) wird eingeführt, um den Austausch von Visa-Daten zwischen den Mitgliedstaaten zu erleichtern. Auch für EUROPOL, die Sicherheitsbehörden und die Nachrichtendienste soll dieser Datenbestand zugänglich sein.

- Das europäische Verfahren EURODAC, in dem die Fingerabdrücke von Asylbewerberinnen und Asylbewerbern gespeichert sind, soll auch von der Polizei und den Strafverfolgungsbehörden genutzt werden können.

- Der Aufgabenbereich von EUROPOL soll über die Bekämpfung der Organisierten Kriminalität hinaus auch auf andere Formen der schweren Kriminalität erweitert werden. Außerdem soll EUROPOL erstmals die Befugnis erhalten, Daten auch von privaten Stellen entgegenzunehmen und Zugriff auf alle polizeilich relevanten Datenbanken in der EU bekommen.

- Der Informationsaustausch zwischen den Strafverfolgungsbehörden der EU wird entsprechend dem Rahmenbeschluss des Rates vom 18. Dezember 2006 („Schwedische Initiative“) ausgebaut. Danach soll der Austausch verfügbarer Daten innerhalb der EU zu den gleichen Bedingungen erfolgen wie nach nationalem Recht.

Neben diesen Vorhaben gibt es zudem Abkommen auf bilateraler Ebene zwischen EU-Mitgliedstaaten und Drittstaaten, wie z. B. das Abkommen der Bundesrepublik Deutschland mit den Vereinigten Staaten für einen erweiterten Informationsaustausch zwischen den Sicherheitsbehörden.

Der Aufbau zentraler Datenbestände und der Ausbau der grenzüberschreitenden Datenübermittlung greifen erheblich in das Grundrecht auf informationelle Selbstbestimmung ein und führen dadurch zu Gefahren für jede Einzelne und jeden Einzelnen. Diese werden noch gesteigert durch die angestrebte Verknüpfbarkeit der bestehenden und geplanten Datenbanken.

Umso wichtiger ist deshalb ein hoher und gleichwertiger Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Europa. Dies wurde von den Datenschutzbeauftragten auf nationaler und europäischer Ebene mehrfach angemahnt. Der hierzu im Oktober 2005 vorgelegte Rahmenbeschluss-Vorschlag genügt diesen Anforderungen nicht (siehe dazu die Entschließung der 71. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. März 2006 „Mehr Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in Strafsachen“). Zur Wahrung des erforderlichen Gleichgewichts zwischen Freiheit und Sicherheit sollten die Parlamente und Regierungen ihre Einflussmöglichkeiten bei europäischen Vorhaben stärker nutzen und dabei auch datenschutzrechtliche Aspekte einbringen. Wie notwendig ein angemessener Datenschutz ist, hat sich beim Verfahren der Aufnahme Verdächtiger in die so genannte EU-Terrorliste gezeigt, das durch den Europäischen Gerichtshof für rechtswidrig erklärt wurde.

Die Datenschutzbeauftragten fordern deshalb:

- Bei jeder neuen Initiative ist das Verhältnismäßigkeitsprinzip zu wahren und deren Auswirkung auf das bestehende System von Eingriffsmaßnahmen zu berücksichtigen.

- Im Hinblick auf den Kumulationseffekt sind die verschiedenen europäischen Initiativen zudem grundrechtskonform aufeinander abzustimmen. Redundanzen und Überschneidungen müssen verhindert werden.

  - Ein Rechtsakt muss unverzüglich beschlossen werden, der über den Rahmenbeschlussvorschlag hinaus einen hohen und gleichwertigen Datenschutzstandard bei der Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit verbindlich vorschreibt. Die gesamte nationale und grenzüberschreitende Informationsverarbeitung in diesem Bereich muss davon erfasst sein, um ein einheitliches Datenschutzniveau in den EU-Mitgliedstaaten zu gewährleisten.

- Ein unabhängiges, beratendes Datenschutzgremium sowie eine unabhängige und umfassende datenschutzrechtliche Kontrolle müssen für die polizeiliche und justizielle Zusammenarbeit eingerichtet bzw. gewährleistet werden.

Anlage 24

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten

Der Rahmenbeschluss des Rates zur Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten (sog. „Schwedische Initiative“) vom 18.12.2006 verpflichtet diese, an die grenzüberschreitende Übermittlung personenbezogener Daten innerhalb der EU keine höheren Anforderungen zu stellen, als auf nationaler Ebene für den Datenaustausch zwischen Polizei- und Strafverfolgungsbehörden gelten. Seine Umsetzung wird zu einem deutlichen Anstieg und zur Beschleunigung des Informationsaustausches und damit zu einer weiteren Intensivierung der polizeilichen und justiziellen Zusammenarbeit in Strafsachen auf EU-Ebene führen. Das erstrebte Ziel, nämlich die Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts setzt aber auch voraus, dass in den Mitgliedstaaten ein möglichst gleichwertiger Datenschutz auf hohem Niveau besteht. Dies ist bislang nicht erfüllt. Es besteht nach wie vor der aus datenschutzrechtlicher Sicht unhaltbare Zustand, dass die auf EU-Ebene ausgetauschten polizeilichen Informationen in den jeweiligen EU-Mitgliedstaaten unterschiedlichen Datenschutzregelungen hinsichtlich ihrer Verwendung unterworfen sind. Zudem gelten keine einheitlichen Rechte auf Auskunft, Berichtigung und Löschung der Datenverarbeitung für die Betroffenen in den Empfängerstaaten.

Vor diesem Hintergrund fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, den bei der innerstaatlichen Umsetzung der „Schwedischen Initiative“ verbleibenden Spielraum zu nutzen und die Befugnisse zum Informationsaustausch mit den Strafverfolgungsbehörden der EU-Mitgliedstaaten für die nationalen Polizei- und Strafverfolgungsbehörden normenklar und unter Beachtung des Grundsatzes der Verhältnismäßigkeit gesetzlich zu regeln. Dazu zählen insbesondere:

- Ausschluss der gesonderten Erhebung der angefragten Daten durch die Strafverfolgungsbehörden allein um diese zu übermitteln,

- Eindeutige inhaltliche Anforderungen, die an ein Ersuchen um Datenübermittlung zu stellen sind, um Überschussinformationen zu vermeiden,
- *Regelung enger Voraussetzungen für sog. Spontanübermittlungen, um für den Empfänger nutzlose und damit nicht erforderliche Übermittlungen auszuschließen,*

  - Nutzung des Spielraums bei der Ausgestaltung der Verweigerungsgründe, um unverhältnismäßige Datenübermittlungen zu verhindern,

  - normenklare Abgrenzung der Befugnis zur Übermittlung von Daten zu präventiven Zwecken gegenüber der justiziellen Rechtshilfe,

  - vollständige Umsetzung der Datenschutzbestimmungen in Art. 8 des Rahmenbeschlusses und begrenzende Regelungen zur Weiterübermittlung an Drittstaaten,

- normenklare Bestimmung welche Behörden als zuständige Strafverfolgungsbehörden im Sinne des Rahmenbeschlusses gelten und welche Informationen nur durch Ergreifen von Zwangsmaßnahmen im Sinne des Rahmenbeschlusses verfügbar sind,

- normenklare Bestimmung, welche Informationen nicht vom Rahmenbeschluss erfasst werden, weil sie für die Strafverfolgungsbehörden nur durch das Ergreifen von Zwangsmaßnahmen verfügbar sind.

Anlage 25

Entschließung der 76. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 6. und 7. November 2008 in Bonn

Gegen Blankettbefugnisse für die Software-Industrie

Gegenwärtig wird auf europäischer Ebene über Änderungen der Richtlinie zum Datenschutz in der elektronischen Kommunikation (2002/58/EG) beraten. Dabei geht es auch um die Frage, ob in Zukunft einzelfallunabhängig Verkehrsdaten zur Gewährleistung der Netz- und Informationssicherheit, also etwa zur Verfolgung von Hackerangriffen, verarbeitet werden dürfen.

Bereits auf der Grundlage der geltenden Richtlinie erlaubt § 100 Telekommunikationsgesetz den Telekommunikationsdiensteanbietern eine zielgerichtete, einzelfallbezogene Datenverarbeitung zur Fehlerbeseitigung und Missbrauchsbekämpfung. Diese Regelung hat sich in der Praxis bewährt. Es ist daher nicht erforderlich, zur Gewährleistung der Netz- und Informationssicherheit einzelfallunabhängig personenbezogene Verkehrsdaten zu speichern. Die Anbieter von Telekommunikationsdiensten sind aufgefordert, ihre Systeme so sicher zu gestalten, dass Angriffe von vornherein erfolglos bleiben.

Obwohl die Europäische Kommission eine Änderung der bisherigen Rechtslage nicht für erforderlich hält, schlagen mehrere Mitgliedstaaten bei den gegenwärtigen Beratungen im Rat vor, entsprechend den Vorstellungen der Software-Industrie (Business Software Alliance) eine generelle Ermächtigung in die Richtlinie aufzunehmen, wonach *„jede natürliche oder juristische Person mit einem berechtigten Interesse“* berechtigt sein soll, Verkehrsdaten zu verarbeiten, um „technische Maßnahmen zur Gewährleistung der Sicherheit eines öffentlichen Telekommunikationsdienstes, eines öffentlichen oder privaten Telekommunikationsnetzes, eines Dienstes der Informationsgesellschaft oder von Endgeräten zu deren Nutzung“ zu ergreifen. Damit wäre nicht nur der jeweilige Diensteanbieter, der Maßnahmen zum Schutz des eigenen Angebots treffen will, zur einzelfallunabhängigen Speicherung von Verkehrsdaten berechtigt, sondern praktisch jeder mit einem wirtschaftlichen Verarbeitungsinteresse, insbesondere auch die Hersteller von Sicherheitssoftware.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder lehnt eine solche zeitlich unbegrenzte und inhaltlich unbestimmte Blankett-Ermächtigung als inakzeptabel ab. Der Hinweis auf die „Informationssicherheit“ rechtfertigt es nicht, dass Verkehrsdaten nahezu uferlos auch von Dritten verarbeitet werden. Die Bundesregierung wird aufgefordert, einer derartigen Aufweichung des Telekommunikationsgeheimnisses im Rat ihre Zustimmung zu verweigern.

Anlage 26

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 18. Februar 2009

Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes!

Das Bundeskabinett hat am 14. Januar 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

1. 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),
2. die vorgesehene Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen werden (§ 5 Abs. 4) und
3. 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 27

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

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 28

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

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 29

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

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. März 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. Dezember 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 30

Entschließung der 77. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. März 2009 in Berlin

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. Dezember 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 31

Entschließung der Konferenz der Datenschutzschutzbeauftragten des Bundes und der Länder vom 16. April 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 Bürgerinnen 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 32

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 08./09. November 2007 in Hamburg

Anwendbarkeit des Bundesdatenschutzgesetzes auf Rechtsanwälte

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung in ihrer Stellungnahme zum 21. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit erklärt hat, dass die Erhebung und Verwendung personenbezogener - auch mandatsbezogener - Daten durch Rechtsanwälte den Vorschriften des Bundesdatenschutzgesetzes unterliegt und dass die Aufsichtsbehörden der Länder zuständig sind, die Datenschutzkontrolle durchzuführen.
Der Düsseldorfer Kreis sieht darin die Bestätigung seiner Auffassung, dass das Bundesdatenschutzgesetz (BDSG) - auch hinsichtlich mandatsbezogener Daten - auf Rechtsanwälte anwendbar ist. In der Bundesrechtsanwaltsordnung (BRAO) befinden sich aus datenschutzrechtlicher Hinsicht nur punktuelle Regelungen (§ 43a Abs. 2 BRAO Schweigepflicht, § 50 BRAO Handakten). Die Vorschriften des BDSG treten gemäß § 1 Abs. 3 BDSG lediglich insoweit zurück, als bereichsspezifische Datenschutzvorschriften bestehen. Durch das anwaltliche Berufsgeheimnis werden die Informationsrechte der Aufsichtsbehörden nach § 38 BDSG in Verbindung mit § 24 Abs. 6 und 2 BDSG nicht eingeschränkt.

Anlage 33

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 08./09. November 2007 in Hamburg

Gesetzesinitiative der Bundesregierung zu Auskunfteien und Scoring

Im modernen Wirtschaftsleben kommt Auskunfteien eine ständig wachsende Bedeutung zu. Diese sammeln eine Vielzahl von persönlichen Daten auch über Privatpersonen, um sie Dritten insbesondere für die Beurteilung der Kreditwürdigkeit ihrer Geschäftspartner gegen Entgelt zur Verfügung zu stellen.
Während in der Vergangenheit vor allem Kreditinstitute, der Versandhandel und Telekommunikationsunternehmen Auskünfte abgefragt haben, werden Informationen zur Beurteilung der Kreditwürdigkeit zunehmend auch von Vermietern, Versicherungen und sonstigen Unternehmen eingeholt. Von den Auskunfteien wird dabei vielfach ein so genannter Scorewert übermittelt. Hierbei handelt es sich um einen Wert, der auf der Grundlage eines mathematisch-statistischen Verfahrens aus den bei der Auskunftei vorhandenen Angaben errechnet wird und eine Aussage über die Wahrscheinlichkeit des künftigen Zahlungsverhaltens der Betroffenen und damit über ihre Kreditwürdigkeit enthält.
Der Aufbau und die Erweiterung der zentralen Datenbestände über Betroffene bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen sowie der zunehmende Einsatz von Scoring-Verfahren gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Betroffenen.
Vor diesem Hintergrund begrüßt der Düsseldorfer Kreis im Grundsatz den vom Bundesministerium des Innern vorgelegten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, mit dem die Rechte der Betroffenen gestärkt und insbesondere auch die Transparenz beim Einsatz von Scoring-Verfahren verbessert werden sollen.
Nach Auffassung des Düsseldorfer Kreises bedarf der vorliegende Gesetzentwurf allerdings einer grundlegenden Überarbeitung, um das Ziel der Stärkung der Rechte der Betroffenen auch tatsächlich zu erreichen.
Dabei muss insbesondere sichergestellt werden, dass die bei Auskunfteien gesammelten Daten die Erstellung umfassender Persönlichkeitsprofile von Betroffenen nicht zulassen. Darüber hinaus ist gesetzlich eindeutig zu regeln, dass die Einholung einer Bonitätsauskunft auch in Zukunft an das Vorliegen eines finanziellen Ausfallrisikos geknüpft bleibt. Die im Entwurf derzeit vorgesehene Regelung, wonach jedes rechtliche oder wirtschaftliche Interesse einschließlich der Vermeidung allgemeiner Vertragsrisiken ein berechtigtes Interesse darstellen kann, würde die Rechte der Betroffenen unverhältnismäßig beeinträchtigen.
Des Weiteren muss eindeutig klargestellt werden, dass nur vertragsrelevante Daten in die Berechnung eines Scorewerts einbezogen werden dürfen. Im Übrigen dürfen die Auskunftsrechte der Betroffenen nicht durch die pauschale Berufung auf ein Geschäftsgeheimnis vereitelt werden.

Anlage 34

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Keine fortlaufenden Bonitätsauskünfte an den Versandhandel

Auskunfteien dürfen Bonitätsauskünfte gemäß § 29 Absatz 2 Nr. 1a BDSG grundsätzlich nur erteilen, wenn der Dritte, dem die Daten übermittelt werden sollen, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat.
Besteht zwischen diesem Dritten (also dem anfragenden Unternehmen) und dem Betroffenen ein Dauerschuldverhältnis, aufgrund dessen das anfragende Unternehmen während der gesamten Dauer des Bestehens ein finanzielles Ausfallrisiko trägt (z. B. Ratenzahlungskredit, Girokonto, Energielieferungs-, Telekommunikationsvertrag), so dürfen Bonitätsauskünfte nicht nur zu dem Zeitpunkt erteilt werden, zu dem der Betroffene ein solches Vertragsverhältnis beantragt hat, sondern während der gesamten Laufzeit des Vertragsverhältnisses und bis zur Erfüllung sämtlicher Pflichten des Betroffenen.

Ein Versandhandelsgeschäft stellt als solches kein Dauerschuldverhältnis dar. Die aufgrund der bisherigen Erfahrungen mit den Kunden möglicherweise bestehende Wahrscheinlichkeit und darauf gegründete Erwartung, dass der Kunde nach der ersten Bestellung wiederholt bestellen wird, und die zur Erleichterung der Bestellvorgänge möglicherweise erfolgte Einrichtung eines "Kundenkontos" rechtfertigten es nicht, ein Versandhandelsgeschäft mit einem Dauerschuldverhältnis gleichzusetzen.

Ein berechtigtes Interesse seitens des Versandhandels gem. § 29 BDSG ist demnach nur gegeben, wenn aufgrund eines konkreten Bestellvorgangs ein finanzielles Ausfallrisiko vorliegt.

Nach Vertragsschluss sind Bonitätsauskünfte an Versandhändler dann nicht zu beanstanden, wenn ein Ratenzahlungskredit vereinbart wurde oder noch ein offener Saldo besteht. In allen anderen Fällen ist das Rechtsgeschäft nach Abwicklung des einzelnen Kaufgeschäftes für den Versandhandel abgeschlossen, ein berechtigtes Interesse an Bonitätsauskünften ist dann nicht mehr zu belegen. Damit sind Nachmeldungen oder sonstige Beauskunftungen in dieser Konstellation rechtlich unzulässig.

Hinweis:
Die Vertreter des Versandhandels und der Auskunfteien haben sich bereit erklärt, ihre Verfahren entsprechend den vorgenannten gesetzlichen Anforderungen bis spätestens Ende September 2008 umzustellen.

Anlage 35

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Internet-Portale zur Bewertung von Einzelpersonen

1. Die Datenschutzaufsichtsbehörden weisen darauf hin, dass es sich bei Beurteilungen und Bewertungen von Lehrerinnen und Lehrern sowie von vergleichbaren Einzelpersonen in Internet-Portalen vielfach um sensible Informationen und subjektive Werturteile über Betroffene handelt, die in das Portal eingestellt werden, ohne dass die Urheber erkennbar sind und die jederzeit von jedermann abgerufen werden können.

2. Anbieter entsprechender Portale haben die Vorschriften des Bundesdatenschutzgesetzes über die geschäftsmäßige Verarbeitung personenbezogener Daten einzuhalten.

3. Bei der danach gesetzlich vorgeschriebenen Abwägung ist den schutzwürdigen Interessen der bewerteten Personen Rechnung zu tragen. Das Recht auf freie Meinungsäußerung rechtfertigt es nicht, das Recht der Bewerteten auf informationelle Selbstbestimmung generell als nachrangig einzustufen.

Anlage 36

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 17./18. April 2008 in Wiesbaden

Datenschutzkonforme Gestaltung sozialer Netzwerke

Der datenschutzgerechten Gestaltung sozialer Netzwerke im Internet kommt eine zentrale Bedeutung zu. Die Aufsichtsbehörden rufen in diesem Zusammenhang in Erinnerung, dass Anbieter in Deutschland zur Einhaltung des Regulierungsrahmens zum Datenschutz verpflichtet sind.

Insbesondere sind folgende rechtliche Rahmenbedingungen einzuhalten:

- Anbieter sozialer Netzwerke müssen ihre Nutzer umfassend gemäß den gesetzlichen Vorschriften über die Verarbeitung ihrer personenbezogenen Daten und ihre Wahl- und Gestaltungsmöglichkeiten unterrichten. Das betrifft auch Risiken für die Privatsphäre, die mit der Veröffentlichung von Daten in Nutzerprofilen verbunden sind. Darüber hinaus haben die Anbieter ihre Nutzer aufzuklären, wie diese mit personenbezogenen Daten Dritter zu verfahren haben.

- Die Aufsichtsbehörden weisen darauf hin, dass nach den Bestimmungen des Telemediengesetzes (TMG) eine Verwendung von personenbezogenen Nutzungsdaten für Werbezwecke nur zulässig ist, soweit die Betroffenen wirksam darin eingewilligt haben. Bei Werbemaßnahmen aufgrund von Profildaten müssen die Betroffenen nach den Bestimmungen des Bundesdatenschutzgesetzes (BDSG) mindestens eine Widerspruchsmöglichkeit haben. Die Aufsichtsbehörden empfehlen, dass die Anbieter die Nutzer selbst darüber entscheiden lassen, ob - und wenn ja, welche - Profil- oder Nutzungsdaten zur zielgerichteten Werbung durch den Anbieter genutzt werden.

- Die Aufsichtsbehörden erinnern weiterhin daran, dass eine Speicherung von personenbezogenen Nutzungsdaten über das Ende der Verbindung hinaus ohne Einwilligung der Nutzer nur gestattet ist, soweit die Daten zu Abrechnungszwecken gegenüber dem Nutzer erforderlich sind.

- Für eine vorauseilende Speicherung von Daten über die Nutzung sozialer Netzwerke (wie auch anderer Internet-Dienste) für eventuelle zukünftige Strafverfolgung besteht keine Rechtsgrundlage. Sie wird insbesondere auch nicht durch die Regelungen zur Vorratsdatenspeicherung vorgeschrieben.

- Schließlich weisen die Aufsichtsbehörden darauf hin, dass das TMG die Anbieter dazu verpflichtet, das Handeln in sozialen Netzwerken anonym oder unter Pseudonym zu ermöglichen. Dies gilt unabhängig von der Frage, ob ein Nutzer sich gegenüber dem Anbieter des sozialen Netzwerks mit seinen Echtdaten identifizieren muss.

- Die Anbieter sind verpflichtet, die erforderlichen technisch-organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Sie müssen ins-

besondere einen systematischen oder massenhaften Export oder Download von Profildaten aus dem sozialen Netzwerk verhindern.

- Bei der datenschutzfreundlichen Gestaltung von sozialen Netzwerken kommt den Standardeinstellungen - z. B. für die Verfügbarkeit von Profildaten für Dritte - eine zentrale Bedeutung zu. Die Aufsichtsbehörden fordern die Anbieter sozialer Netzwerke auf, datenschutzfreundliche Standardeinstellungen für ihre Dienste zu wählen, durch die die Privatsphäre der Nutzer möglichst umfassend geschützt wird. Diese Standardeinstellungen müssen besonders restriktiv gefasst werden, wenn sich das Portal an Kinder richtet. Der Zugriff durch Suchmaschinen darf jedenfalls nur vorgesehen werden, soweit der Nutzer ausdrücklich eingewilligt hat.

- Der Nutzer muss die Möglichkeit erhalten, sein Profil auf einfache Weise selbst zu löschen. Schließlich sollten die Anbieter sozialer Netzwerkdienste die Einführung von Verfallsdaten oder zumindest automatische Sperrungen erwägen, die von den Nutzern selbst festgelegt werden können.

Anlage 37

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden

Novellierung des Bundesdatenschutzgesetzes in den Bereichen Adressenhandel, Werbung und Datenschutzaudit

Der Düsseldorfer Kreis begrüßt, dass die Bundesregierung durch eine Novellierung des Bundesdatenschutzgesetzes aus den jüngst bekannt gewordenen Datenschutzverstößen im Bereich der Privatwirtschaft Konsequenzen ziehen möchte. Die uneingeschränkte Streichung des Listenprivilegs und die Pflicht zur Einholung einer Einwilligung des Betroffenen bei der Übermittlung an Dritte oder bei der Nutzung für Werbezwecke für Dritte sind erforderlich, um das informationelle Selbstbestimmungsrecht der Bürgerinnen und Bürger zu stärken. Hiervon wird künftig auch die Wirtschaft profitieren. Die geplanten Änderungen ermöglichen es, Werbung zielgerichteter und ohne Streuverluste vorzunehmen und unerwünschte Belästigungen zu vermeiden, so dass das Verbrauchervertrauen in die Datenverarbeitung der Wirtschaft gestärkt wird. Die vorgesehenen Regelungen zur Klarstellung, wann eine wirksame Einwilligung in die Werbenutzung vorliegt, und dass diese nicht mit wichtigen vertraglichen Gegenleistungen gekoppelt werden darf, verbessern die Transparenz und die Freiwilligkeit für den Betroffenen.

Darüber hinaus hat die beim Datenschutzgipfel am 4. September 2008 eingesetzte Länderarbeitsgruppe weitere Vorschläge zur Verbesserung des Bundesdatenschutzgesetzes unterbreitet, die jedoch bisher nicht berücksichtigt wurden.

Die derzeit geplanten Vorschriften genügen nicht, um künftig im Bereich der privaten Wirtschaft ein ausreichendes Datenschutzniveau zu verwirklichen. Hierzu bedarf es zum einen einer angemessenen Ausstattung der Datenschutzaufsichtsbehörden. Es bedarf zum anderen gemäß den europarechtlichen Vorgaben wirksamer Einwirkungsbefugnisse. Hierzu gehört neben adäquaten Kontroll- und Sanktionsmitteln die Möglichkeit, bei schwerwiegenden Datenschutzverstößen die Erhebung und Verwendung personenbezogener Daten zu untersagen. Auch die Stellung der betrieblichen Datenschutzbeauftragten sollte gestärkt werden.

Die bisherigen Vorschläge des Bundesministeriums des Innern zur Einführung eines Datenschutzaudits sind nicht geeignet, den Datenschutz in der Wirtschaft zu verbessern.

Anlage 38

Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 13./14. November 2008 in Wiesbaden

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.

Anlage 39

ERKLÄRUNG
der Europäischen Datenschutzkonferenz über die Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung vom 11. Mai 2007

Die Europäische Union hat verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung und des Kampfes gegen den Terrorismus in der Europäischen Union eingeleitet. In diesem Zusammenhang ist der Austausch von Informationen zur Strafverfolgung in Übereinstimmung mit dem Verfügbarkeitsgrundsatz („principle of availability“) eine Schlüsselfrage.

Angesichts dieser Entwicklungen rief die Europäische Datenschutzkonferenz die Mitgliedstaaten der Europäischen Union sowie die Kommission, den Rat und das Europäische Parlament dazu auf, tragfähige und harmonisierte Maßnahmen zur Sicherung des Datenschutzes einzuführen.

Die verschiedenen Ausprägungen, in denen dieses Prinzip der „Verfügbarkeit“ explizit oder implizit zur Entwicklung von Strategien und Rechtsakten zur Verbesserung der Effizienz bei der Strafverfolgung genutzt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effizienz von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen.

Die Konferenz hat den folgenden Gemeinsamen Standpunkt über die Anwendung des Verfügbarkeitsgrundsatzes bei der Strafverfolgung angenommen. Dieser Gemeinsame Standpunkt enthält eine Checkliste für die Beurteilung eines jeden Vorschlags, dessen Grundlage die Verfügbarkeit von personenbezogenen Daten ist.

Dieses Dokument und die Checkliste sind insbesondere an alle EU-Institutionen und die nationalen Parlamente adressiert, als ein konstruktiver Beitrag zur Achtung und Stärkung der bürgerlichen Freiheiten der in der EU lebenden Bürger bei der Ausweitung der Möglichkeiten zur Nutzung von Informationen durch Strafverfolgungsbehörden.

Gemeinsamer Standpunkt der Europäischen Datenschutzkonferenz über die Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

Angenommen am 11. Mai 2007

Erläuternde Zusammenfassung

Im Zusammenhang mit dem Kampf gegen Terrorismus und zur Verbesserung der inneren Sicherheit hat die Europäische Union verschiedene Initiativen zur Verbesserung der Effizienz der Strafverfolgung in der Europäischen Union eingeleitet und dabei das Verfügbarkeitsprinzip als ein Leitprinzip für den Austausch von Informationen zur Strafverfolgung bei der Zusammenarbeit in der dritten Säule angewandt.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip explizit oder implizit zur Verbesserung der Effizienz der Strafverfolgung angewandt wird, macht auch die Einführung eines umfassenden Rahmens zur Beurteilung der datenschutzrechtlichen Aspekte im Zusammenhang mit der Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags zur Verfügung gestellt, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität von Strafverfolgung nutzt. Ein solcher Rahmen soll somit dazu beitragen, eine ausgewogene Beurteilung der Wechselwirkung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten vorzunehmen, wie er in der Charta der Grundrechte der Europäischen Union verankert ist.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Anwendung des Verfügbarkeitsprinzips im folgenden Gemeinsamen Standpunkt und der Checkliste entwickelt. Diese Checkliste kann zur Beurteilung eines jeden Vorschlags genutzt werden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung nutzt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese Checkliste bei der Entwicklung, Beurteilung und Annahme eines jeden Vorschlags zu nutzen, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

Gemeinsamer Standpunkt zur Anwendung des Verfügbarkeitsprinzips bei der Strafverfolgung

1. Einführung

Im Zusammenhang mit der Bekämpfung von Terrorismus und der Verbesserung der internationalen Sicherheit, leitete die Europäische Union verschiedene Initiativen ein, um die Effektivität der Strafverfolgung in der Europäischen Union zu verbessern. Artikel 29 EUV zielt darauf ab, den Bürgern ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts zu verschaffen. Dieser Raum der Freiheit, der Sicherheit und des Rechts entwickelt sich schrittweise und führt zur Abschaffung der Grenzen zwischen den Mitgliedstaaten bezüglich der Informationen zur Strafverfolgung. Jedoch sind die Durchsetzungsbefugnisse der Mitgliedstaaten noch immer an diese nationalen Grenzen gebunden.

In diesem Zusammenhang ist der Austausch von Strafverfolgungs-Informationen unter Anwendung des Verfügbarkeitsprinzips zu einer Schlüsselfrage bei der Zusammenarbeit innerhalb der dritten Säule geworden: - als wichtiges Instrument bei der Verwirklichung eines freien Flusses von Strafverfolgungs-Informationen, der nicht durch Binnengrenzen behindert wird, - durch Gewährleistung von Sicherheit für den Bürger im Wege der Vereinfachung des Kampfes gegen grenzüberschreitende Straftaten, - durch Achtung des Schutzes der Grundrechte und -freiheiten des Bürgers, insbesondere des Rechts auf Privatsphäre und Datenschutz.

Diese drei Ziele müssen in ausgewogener Weise erreicht werden. Dies liegt mit Blick auf den besonderen Charakter der Strafverfolgung und in Anbetracht der Tendenz zur zunehmenden Nutzung personenbezogener Daten für proaktive Nachforschungen der Polizei nicht auf der Hand. Ein Leitsatz bei der Strafverfolgung scheint zu sein: wenn Daten gebraucht werden, sollten sie genutzt werden. Oder noch deutlicher: wenn Daten verfügbar sind, können sie genutzt werden.

Dieses Thema demonstriert deutlich die enge Wechselbeziehung zwischen öffentlicher Sicherheit und dem Grundrecht auf den Schutz personenbezogener Daten, wie es in der Charta der Grundrechte der Europäischen Union verankert ist.

Ein wichtiger Bestandteil in dieser Wechselbeziehung ist gegenseitiges Vertrauen. Gegenseitiges Vertrauen (und gegenseitige Anerkennung) ist eine entscheidende Bedingung für den Austausch von Strafverfolgungs-Informationen. Regierungen und Regierungsbehörden sind zum wirksamen Austausch mit (Behörden in) anderen Mitgliedstaaten nur bereit, wenn sichergestellt ist, dass diese anderen Mitgliedstaaten die Informationen im Einklang mit angemessenen rechtlichen Bestimmungen nutzen, aus Gründen des Datenschutzes und der Sicherheit.
Bereits verabschiedete EU-Rechtsakte und neuere Initiativen beschränken sich nicht darauf, den Austausch solcher personenbezogener Daten zwischen Strafverfolgungsbehörden zu fördern, die bereits von den Behörden verarbeitet werden. Einige konzentrieren sich auch auf die Nutzung solcher personenbezogener Daten zum Zwecke der Strafverfolgung, die von privaten und öffentlichen Stellen oder in europäischen Datenbanken verarbeitet werden. Wenn es Hinweise darauf gibt, dass diese für die Zwecke der Strafverfolgung benötigt werden, werden sie (so vorgeschlagen) den Strafverfolgungsbehörden zugänglich gemacht.

Die verschiedenen Ausprägungen, in denen dieses Verfügbarkeitsprinzip bei der Entwicklung von Strategien und Rechtsinstrumenten zur Verbesserung der Effektivität der Strafverfolgung implizit oder explizit angewandt wird, macht die Schaffung eines umfassenden Rahmens für die Beurteilung datenschutzrechtlicher Aspekte in Bezug auf die Nutzung dieses Prinzips erforderlich. Durch die Schaffung eines solchen Rahmens wird eine Anleitung zur Beurteilung eines jeden Vorschlags gegeben, der das Vorhandensein personenbezogener Daten als Möglichkeit zur Verbesserung der Effektivität der Strafverfolgung nutzt.

Die Europäische Datenschutzkonferenz, die Notwendigkeit der Schaffung eines solchen Rahmens betonend, hat einige Bedingungen und Leitlinien für die Beurteilung der Nutzung des Verfügbarkeitsprinzips entwickelt. Die Europäische Datenschutzkonferenz fordert die Kommission, den Rat und das Europäische Parlament dringend dazu auf, diese bei der Entwicklung, Beurteilung und Annahme jeglichen Vorschlags anzuwenden, der die Verfügbarkeit personenbezogener Daten als Einstieg zur Verbesserung der Strafverfolgung oder der Zusammenarbeit zwischen Strafverfolgungsbehörden nutzt.

2. Anwendungsbereich des Verfügbarkeitsprinzips

Die Strategie der Europäischen Union, wie sie im Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht beschrieben wird, zielt darauf, dass mit Wirkung vom 1. Januar 2008 der Austausch von Strafverfolgungs-Informationen durch den Verfügbarkeitsgrundsatz bestimmt wird.

In Verfolgung dieser Strategie legte die Kommission am 12. Oktober 2005 ihren Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit vor. Dieser Vorschlag statuiert eine Verpflichtung der Mitgliedstaaten, Zugang zu bestimmten Daten zu ermöglichen, die für ihre Behörden verfügbar sind oder diese zu beschaffen (vgl. Erwägung 6).

Der Verfügbarkeitsgrundsatz, wie er im Haager Programm und dem vorgeschlagenen Rahmenbeschluss zur Anwendung kommt, bedeutet, dass in der gesamten Europäischen Union in einem Mitgliedstaat ein Polizist, der Informationen zur Erfüllung seiner Pflichten benötigt, in der Lage sein sollte, diese von einem anderen Mitgliedstaat zu erhalten und dass die Strafverfolgungsbehörde in dem anderen Staat, die über diese Information verfügt, sie zum genannten Zweck zugänglich machen wird. Der vorgeschlagene Rahmenbeschluss begrenzt den Verfügbarkeitsgrundsatz, indem er feststellt, dass er keine Verpflichtung auferlegt, Informationen zum alleinigen Zweck der Zurverfügungstellung zu sammeln oder zu speichern (Artikel 2 (1)).

Die Weitergabe verfügbarer Informationen wie personenbezogener Daten ist bereits in bestehender EU-Gesetzgebung sowie in multilateralen Übereinkommen vorgesehen. Neuere Vorschläge zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden enthalten das Verfügbarkeitsprinzip ebenfalls als Leitsatz. Jedoch wird in all diesen Rechtsinstrumenten und Vorschlägen die Verfügbarkeit personenbezogener Daten in unterschiedlicher Art und Weise ausgelegt, was zu unterschiedlichen Konsequenzen führt. Diese Unterschiede machen die weitere Untersuchung des Anwendungsbereichs dieses Prinzips erforderlich.

Eines der ersten Beispiele für den Austausch personenbezogener Daten als besonde-

rem Bestandteil effektiver Zusammenarbeit zwischen europäischen Strafverfolgungsbehörden ist vielleicht das Übereinkommen vom 19. Juni 1990 zur Durchführung des Schengener Übereinkommens vom 14. Juni 1985. Die Verarbeitung personenbezogener Daten besonderer Personenkategorien und deren Zurverfügungstellung – unter Nutzung eines zentralen Informationssystems – für verschiedene Behörden in den Staaten, die das Schengener Übereinkommen umgesetzt haben, wird als notwendige, ausgleichende Maßnahme zur Schaffung eines hohen Sicherheitsstandards in einem Raum des freien Personenverkehrs angesehen.

Ein weiterer Schritt zur Verbesserung der Zusammenarbeit zwischen Strafverfolgungsbehörden fand durch das Europol-Übereinkommen und die Eurojust Entscheidung statt. Zwei Europäische Ämter wurden geschaffen, deren besondere Aufgabe es unter anderem war, den Austausch von Strafverfolgungs-Informationen zu erleichtern.

Diese Formen der Zusammenarbeit können charakterisiert werden als Zusammenarbeit durch Äußerung der Absicht zur Zusammenarbeit ohne besondere Verpflichtung dazu.

Neuere Beispiele der Zurverfügungstellung personenbezogener Daten für Strafverfolgungsbehörden sind der Rahmenbeschluss über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union und der Vertrag von Prüm vom 27. Mai 2005. Diese beiden Rechtsinstrumente führen einen neuen Aspekt in die Zusammenarbeit bei der Strafverfolgung ein: Mitgliedstaaten sind grundsätzlich verpflichtet, personenbezogene Daten zur Verfügung zu stellen. Die Benutzung von Formulierungen wie: „sollen auf Ersuchen“ (Rahmenbeschluss) und „gestatten Zugriff ... und das Recht zum Abruf“(z. B. Artikel 3 (1) Vertrag von Prüm) zeigen deutlich den verpflichtenden Charakter der Zurverfügungstellung von Daten.

Der Vertrag von Prüm führt darüber hinaus eine Verpflichtung zur Erstellung bestimmter Dateien ein, um die Verhütung und Verfolgung von Straftaten zu erleichtern. Die Vertragsparteien müssen zum Beispiel die Verfügbarkeit von Fundstellendatensätzen von Fingerabdrücken garantieren (Artikel 8).

Der bestehende, mehr oder minder freiwillige Austausch von Informationen wird auf diesen Gebieten nicht nur durch eine Verpflichtung zur Zurverfügungstellung von Informationen ersetzt, sondern auch durch die Verpflichtung, für bestimmte Kategorien personenbezogener Daten eine Infrastruktur zu schaffen, die anderen Strafverfolgungsbehörden den Zugriff darauf ermöglicht.

Eine solche Verpflichtung zur Zurverfügungstellung von Informationen beschränkt sich nicht notwendig auf Strafverfolgungsbehörden. Zum Beispiel wird in Erwägung 19 der Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze gewonnen oder verarbeitet werden und zur Änderung der Richtlinie 2002/58/EG ausdrücklich erwähnt, dass „*es notwendig ist, dass vorhandene Daten zugänglich gemacht werden*“. Auf europäischer Ebene wird abgesichert, dass bestimmte Kategorien von Daten, die durch private Stellen verarbeitet werden, für die Strafverfolgung zugänglich gemacht werden sollen.

Das Verfügbarkeitsprinzip ist ebenfalls ein wichtiges Thema der Mitteilung der Kommission an den Rat und das Europäische Parlament vom 24. November 2005 über die

Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen. Die Weitergabe verfügbarer Informationen durch die Verbindung von Datenbanken ist ein Schlüsselelement bei den Zukunftsplanungen in der Europäischen Union. Andere Initiativen wie die neue Rechtsgrundlage des Schengener Informationssystems der zweiten Generation und die Schaffung des Visa-Informationssystems beinhalten ebenfalls Aspekte des Verfügbarkeitsprinzips. Personenbezogene Daten, die für einen bestimmten Zweck verarbeitet wurden, werden für andere Zwecke wie etwa Strafverfolgung zugänglich gemacht.

Im Hinblick auf diese Bandbreite der Erscheinungsformen des Verfügbarkeitsprinzips als Schlüsselelement bei der Verbesserung der Strafverfolgung und der Auswirkung auf das Grundrecht auf den Schutz personenbezogener Daten, betont die Europäische Datenschutzkonferenz die Notwendigkeit, die Nutzung des Verfügbarkeitsprinzips in umfassender Weise in den Kontext zu setzen. Jegliche Harmonisierung der Verarbeitung personenbezogener Daten durch die Einführung von Verpflichtungen zur Vorratsspeicherung personenbezogener Daten oder von Verpflichtungen zur Erstellung spezifischer Datenbestände und die Absicht oder die Verpflichtung, diese personenbezogenen Daten für Strafverfolgungsbehörden oder für mit der Strafverfolgung in Zusammenhang stehende europäische oder internationale Einrichtungen verfügbar zu machen, sollte als Umsetzung des Verfügbarkeitsprinzips angesehen werden.

Unter Zugrundelegung dieses Anwendungsbereiches hat die Europäische Datenschutzkonferenz seine Auswirkungen im Hinblick auf anwendbare Datenschutzbestimmungen untersucht.

3. Anwendbares Recht

Zusätzlich zum Recht auf die Achtung des Privat- und Familienlebens, das durch Artikel 8 der EMRK garantiert und durch Artikel 7 der Charta der Grundrechte der Europäischen Union nochmals bestätigt wird, ist das neue Grundrecht auf Datenschutz in Artikel 8 der Charta verankert.

Die EMRK erlaubt den Eingriff in den Schutzbereich des Rechts auf Privatleben, wenn er zur Wahrung der im zweiten Absatz des Artikel 8 bezeichneten Interessen notwendig und durch diese Interessen gerechtfertigt ist; ein solcher Eingriff muss dem Verhältnismäßigkeitsgrundsatz entsprechen. Artikel 8 der Charta der Grundrechte weitet dies aus, indem er festlegt, dass personenbezogene Daten nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen legitimen Grundlage verarbeitet werden müssen. Diese legitime Grundlage muss ebenfalls dem Verhältnismäßigkeitsgrundsatz entsprechen.

Das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten von 1981 (Konvention 108) enthält spezifischere Grundsätze für den Datenschutz, die auch innerhalb der dritten Säule anwendbar sind. Es gibt auch eine Empfehlung (Nr. R(87) 15) mit spezifischen Datenschutzvorschriften für die Verwendung personenbezogener Daten bei der Polizei, die 1987 vom Ministerkomitee der Mitgliedstaaten zur Regelung der Verwendung personenbezogener Daten bei der Polizei verabschiedet wurde.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sieht eine harmonisierte Datenschutzordnung in der Europäischen Union vor. Obwohl Maßnahmen, die in Titel V und VI des Vertrages über die Europäische Union bezeichnet sind, außerhalb des Anwendungsbereichs dieser Richtlinie liegen, wenden Mitgliedstaaten die allgemeinen Datenschutz-Grundsätze auf Maßnahmen der Strafverfolgung an.

Die Verordnung 45/2001 des Europäischen Parlaments und des Rates vom 18. September 2000 sieht Regeln für den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr vor. Die Grundsätze dieser Verordnung werden zur Definition der Datenschutz-Ordnung genutzt, die auf die Verarbeitung personenbezogener Daten in Europäischen Datenbanken wie dem Visa-Informationssystem und dem Schengener Informationssystem der zweiten Generation anwendbar ist.

Das Europol-Übereinkommen und die Eurojust-Entscheidung enthalten für diese Organisationen spezifische Datenschutzregelungen, die auf den allgemeinen Datenschutz-Prinzipien beruhen, wie sie in der Konvention 108 und der Empfehlung Nr. R(87) 15 definiert werden, die oben genannt wurden.
Für Datenverarbeitung durch private und öffentliche Stellen sowie durch die Europäischen Institutionen und in Europäischen Datenbanken enthält das anwendbare EU-Recht einen Grundsatz über die Rechtmäßigkeit der Verarbeitung personenbezogener Daten: Daten sollten für ausdrückliche und legitime Ziele gesammelt werden und nicht in einer Art und Weise weiterverarbeitet werden, die mit diesen Zielen unvereinbar ist. Eine Ausnahme oder Beschränkung ist nur dann erlaubt, wenn diese gesetzlich vorgesehen ist und eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten darstellt. Die in diesen Rechtsinstrumenten genutzte Definition der Datenverarbeitung umfasst die Bekanntgabe durch Weitergabe, Verbreitung oder sonstige Zurverfügungstellung.

In den Situationen, in denen das Verfügbarkeitsprinzip angewendet wird, um ursprünglich zu anderen Zwecken als der Strafverfolgung verarbeitete Daten für die Strafverfolgung zu nutzen, muss die Ausnahme vom Grundsatz der Zweckbestimmung alle Bedingungen für das Eingreifen dieser Ausnahme erfüllen.

4. Umsetzung des Verfügbarkeitsprinzips

Die Effektivität der Strafverfolgung wird von der Informationslage der Strafverfolgungsbehörden abhängen, von der Möglichkeit, innerhalb der Grenzen des Rechts Informationen zu sammeln, von der Qualität und dem Nutzen dieser Daten und der Fähigkeit zur Weitergabe dieser Daten an andere Strafverfolgungsbehörden. Die verschiedenen Arten der Zusammenarbeit bei der Strafverfolgung in der Europäischen Union, wie sie in Kapitel 2 beschrieben wurden, umfassen all diese Gesichtspunkte.

Bezüglich aller Initiativen zum Austausch personenbezogener Daten zwischen Strafverfolgungsbehörden in der Europäischen Union und dem Austausch mit Drittstaaten und -stellen, hat die Europäischen Datenschutzkonferenz bereits erklärt, dass „*In Anbetracht der Verpflichtung der Union zur Achtung der Menschenrechte und der Grundfreiheiten, Initiativen zur Verbesserung der Strafverfolgung in der EU, wie der Verfügbarkeits-*

grundsatz, nur auf Grundlage eines angemessenen Systems von Vorkehrungen zum Datenschutz eingeführt werden sollten, das einen hohen und gleichwertigen Standard beim Datenschutz gewährleistet."

Diesbezüglich begrüßt die Europäische Datenschutzkonferenz den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Ein harmonisierter und hoher Standard des Datenschutzes im Bereich der Strafverfolgung, wie er von einem Rahmenbeschluss des Rates gewährleistet werden sollte, wird nun als unabdingbare Voraussetzung für die Strafverfolgung in der Europäischen Union bezeichnet.

Es sollte jedoch betont werden, dass ein solcher harmonisierter Datenschutz-Rahmen an sich noch kein umfassendes Instrument zur Beurteilung der Umsetzung des Verfügbarkeitsprinzips in all seinen in Kapitel 2 beschriebenen Erscheinungsformen darstellt. Dieser Rahmen ist nur dann anwendbar, wenn personenbezogene Daten bereits von Strafverfolgungsbehörden verarbeitet werden. Darüber hinaus wird der Entwurf des Rahmenbeschlusses im Rat weiter diskutiert.

Da die Bandbreite der Nutzung des Verfügbarkeitsprinzips zur Anwendung verschiedener Rechtsinstrumente führt, sollte ein umfassender Rahmen zur Beurteilung der Nutzung dieses Prinzips sämtliche Gesichtspunkte der Nutzung des Verfügbarkeitsprinzips abdecken. Ein solcher Rahmen sollte in einem gesonderten Instrument bestehen, das nachträglich auch auf bestehendes Recht angewendet wird.

5. Ein umfassender Rahmen zur Beurteilung der Nutzung des Verfügbarkeitsprinzips.

Strafverfolgung ist von Informationen abhängig. Grundsätzlich werden zweierlei Informationsquellen genutzt: Informationen, die bereits von Strafverfolgungsbehörden verarbeitet werden und Informationen, die von anderen verarbeitet werden. Diese Unterscheidung ist in gewisser Weise künstlich, weil Daten, die von Strafverfolgungsbehörden verarbeitet werden, von privaten oder öffentlichen Stellen erlangt worden sein können.

Wenn personenbezogene Daten durch private oder öffentliche Stellen verarbeitet werden, sind die in der Richtlinie 95/46/EG definierten Datenschutzgrundsätze maßgeblich. Wenn diese Daten entweder von Europäischen Organen oder in Europäischen Datenbanken verarbeitet werden, sind die Grundsätze der Verordnung 45/2001 und/oder die für diese Dateien einschlägigen spezifischen Regeln anwendbar.

Wie bereits dargelegt, stellt die Nutzung dieser Daten zum Zwecke der Strafverfolgung in der Regel eine Ausnahme vom Grundsatz der Zweckbindung dar, die nur erlaubt ist, wenn dies gesetzlich vorgesehen ist und es um eine notwendige Maßnahme zum Schutz der nationalen und öffentlichen Sicherheit oder zur Verhütung, Aufklärung, Entdeckung und Verfolgung von Straftaten geht.

In dem Falle, dass die Daten bereits von Strafverfolgungsbehörden verarbeitet werden, wird der (Entwurf des) Rahmenbeschluss des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen für den notwendigen rechtlichen Datenschutz-Rahmen bei der Verarbeitung und dem Austausch von Informationen zwischen Strafverfolgungsbehörden sorgen. Es könnten jedoch neue Initiativen für die Verarbeitung dieser Daten vorgelegt werden, die auf dem Verfügbarkeitsprinzip basieren.

Zur Beurteilung, ob eine Ausnahme notwendig ist und den formellen Bedingungen entspricht, oder bei der Beurteilung neuer Initiativen zur Bereitstellung von Daten zur Strafverfolgung, wird es notwendig sein, die verschiedenen Bedingungen in den Blick zu nehmen, die die einschlägigen Datenschutzvorschriften enthalten.

Die erste Bedingung bezieht sich auf die Anforderung, dass jede Maßnahme gesetzlich vorgesehen sein soll. Dieses Gesetz muss strengen Anforderungen entsprechen, so muss es klar, einfach und präzise sein: es soll transparent und für jedermann leicht verständlich sein. Nach der Rechtsprechung des Gerichtshofes erfordert der Grundsatz der Rechtssicherheit, dass Gesetze klar und präzise sein müssen und ihre Anwendung für den Einzelnen vorhersehbar. Darüber hinaus müssen die Gesetze immer Begründung und Zweck sowie die Bedingungen für die Verarbeitung festlegen und ein angemessenes und effektives Kontrollsystem festsetzen.

Die zweite Bedingung, die erfüllt werden muss, ist, dass jede Maßnahme erforderlich und verhältnismäßig sein muss. Insbesondere die Beurteilung dieses Aspekts erfordert einen umfassenden Ansatz. Ein solcher Ansatz sollte die folgenden Beurteilungs-Schritte enthalten:

> **A. Evaluation bereits bestehender rechtlicher Maßnahmen,** die die Verarbeitung inklusive des Austauschs von Daten erlauben. Sind diese Maßnahmen nicht ausreichend oder sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv? Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag zur Verbrechensbekämpfung leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird. Wenn jedoch die Evaluation ergibt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme gerechtfertigt ist.
>
> Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt werden:
>
> **B. Verhältnismäßigkeit**
>
> Effektive Durchsetzung, aber mit minimalen Eingriffen in die Privatsphäre. Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:
>
> - Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.
> - Eine weniger eingreifende Maßnahme kann nicht zum gleichen Ergebnis führen.
> - Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz ge-

rechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 (2) der Rahmentscheidung zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.

- Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

Die dritte Bedingung bezieht sich auf die Kategorien der zu verarbeitenden Daten und auf weitere besondere Bedingungen. Verschiedene Arten von Daten sind betroffen: von Daten zur Identifikation (genutzt sowohl zur Identifikation des Betroffenen als auch zu dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z. B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z. B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss zwischen diesen Daten unterscheiden und zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für empfindliche Daten; durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen. Sie sollte Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für besondere Arten von Verbrechen unterscheidet. Zum Beispiel sollten Personen, die von einer Anklage freigesprochen wurden oder gegen die keine Beschuldigungen erhoben werden, klar von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten klar von Daten über Verdächtige unterschieden werden. Eine solche Unterscheidung könnte mit der Unterscheidung zwischen verschiedenen Kategorien von Personen verbunden sein, wie sie sich in Artikel 4 (3) des Kommissionsvorschlags für den Entwurf eines Rahmenbeschlusses des Rates zum Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen findet.

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Auswirkungen der Nutzung von Daten auf die Strafverfolgung sollten

ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätzlichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung erfordert zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifikation anhand der Nutzung

solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung riesiger Mengen von Daten geschieht, wie beim neuen Schengener Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Operationen bei der Verarbeitung, die besondere Gefahren darstellen können (z. B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Stand der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

Die vierte Bedingung bezieht sich auf den Zugang zu diesen Daten.

Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein. Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungsmaßnahme begrenzt sein und die Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein. Empfänger-Behörden müssen klar identifiziert sein. Wenn direkter Zugang zu Daten vorgeschlagen wird, sind die Nutzung eines Index oder von hit/no hit-Systemen und eine ausreichende Zugangskontrolle erforderlich.
Die fünfte Bedingung bezieht sich auf Kontrolle und Aufsicht.

Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungsvorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Tätigkeiten inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden. Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.

6. Schlussfolgerung

Die Europäische Datenschutzkonferenz erkennt an, dass Informationen und personen-

bezogene Daten für eine effektive Strafverfolgung entscheidend sind. Sie wiederholt jedoch, dass jegliche Maßnahme unter Nutzung des Verfügbarkeitsprinzips verhältnismäßig sein und die Grundrechte des Einzelnen achten sollte. Dieser Gemeinsame Standpunkt und die Checkliste richten sich insbesondere an die EU-Organe, als ein konstruktiver Beitrag zu gegenwärtigen Initiativen. Sie stellen die Bedingungen dar, die erfüllt werden müssen, um einen hohen Datenschutz-Standard auf dem Gebiet der Strafverfolgung aufrecht zu erhalten. Die Europäische Datenschutzkonferenz ist natürlich bereit, weiter dazu beizutragen, dass der Vorgang der Verbesserung der Strafverfolgung sich im Einklang mit der Achtung von Grundrechten befindet.

Checkliste zur Beurteilung jeglicher Maßnahme zur Umsetzung des Verfügbarkeitsprinzips bei der Strafverfolgung

I. Recht und Evaluation

Jede Maßnahme muss gesetzlich vorgesehen sein. Das Gesetz muss strengen Anforderungen entsprechen. So muss es klar sein und Verlässlichkeit und Vorhersehbarkeit schaffen. Darüber hinaus muss Gesetzgebung immer:

- Begründung und
- Zweck festlegen, sowie
- die Bedingungen für die Verarbeitung.
- Ein angemessenes und effektives System zur unabhängigen Kontrolle einsetzen.

II. Bedarf und Verhältnismäßigkeit

Die Maßnahme sollte eine notwendige Sicherheitsvorkehrung darstellen.

A. Evaluation bereits bestehender rechtlicher Maßnahmen, die die Verarbeitung inklusive des Austauschs von Daten erlauben.

- Sind diese Maßnahmen nicht ausreichend?
  Wenn eine rechtliche Maßnahme tatsächlich genutzt wird, anscheinend aber keinen ausreichenden und effektiven Beitrag im Kampf gegen Straftaten leistet, kann dies ein Anzeichen dafür sein, dass eine andere Maßnahme benötigt wird.
- Sind ihre Umsetzung und die Folgemaßnahmen nicht effektiv?
  Wenn die Evaluation zeigt, dass bereits bestehende Möglichkeiten nicht ausreichend genutzt werden, kann dies erhebliche Zweifel darüber wecken, ob die vorgeschlagene neue Maßnahme eine gerechtfertigte Ausnahme vom Grundsatz der Zweckbegrenzung ist.
- Für den Fall, dass diese Beurteilung anzeigt, dass die rechtliche Maßnahme gerechtfertigt sein könnte, sollten die folgenden Bedingungen erfüllt sein:

B. Verhältnismäßigkeit

- Die Maßnahme sollte darauf zugeschnitten sein, folgendes zu erreichen:
  - Effektive Durchsetzung,
  - Minimale Eingriffe in die Privatsphäre.
- Dies bedeutet einen Verhältnismäßigkeitstest mit den folgenden Bestandteilen:
  - Die Maßnahme muss geeignet sein, was bedeutet, dass ihr Beitrag zur Strafverfolgung klar aufgezeigt werden muss.
  - Sie darf nicht gegen das Erforderlichkeitsgebot verstoßen, was bedeutet, dass eine weniger eingreifende Maßnahme nicht zum gleichen Ergebnis führen kann.
  - Ein Gleichgewicht muss bestehen: wo ein Eingriff in den Datenschutz gerechtfertigt sein kann, um Terrorismus und andere schwere Straftaten zu bekämpfen (wie in Artikel 2 (2) des Rahmenbeschlusses zur Einführung des Europäischen Haftbefehls genannt), bedeutet dies nicht, dass die Daten auch zum Kampf gegen geringfügige Vergehen zur Verfügung stehen.
- Das Rechtsinstrument sollte Gegenstand einer verbindlichen Evaluation sein.

III. Besondere Bedingungen

Verschiedene Arten von Daten sind betroffen: von Daten zur Identifizierung (genutzt zur

Identifizierung des Betroffenen und dessen Kontaktierung) sowie allgemein und spezifisch kennzeichnenden Daten (z. B. Intelligenz) bis zu Arten, die aufgrund ihrer Biometrie dechiffriert werden (z. B. Fingerabdrücke und digitale Darstellung der DNA) und empfindlichen Daten (wie in Artikel 8 der Richtlinie 95/46 genannt). Gleichermaßen sind verschiedene Arten von Personen betroffen: Verdächtige, Nicht-Verdächtige, Zeugen, verurteilte oder freigesprochene Personen. Die folgenden Punkte sollten berücksichtigt werden:

A. Gesetzgebung muss:

- Zwischen diesen Daten unterscheiden,
- Besondere zusätzliche Schutzvorkehrungen für die Verarbeitung solcher Daten gewährleisten, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, insbesondere für die Nutzung empfindlicher Daten durch die Einführung einer gleitenden Skala von Sicherungsmaßnahmen, bei der die Eigenschaften der Daten bestimmte Sonderbedingungen und Begrenzungen ihrer Nutzung festlegen.
- Maßstäbe für eine klare Unterscheidung personenbezogener Daten enthalten, indem sie zwischen Kategorien personenbezogener Daten und deren Verfügbarkeit für spezifische Arten von Verbrechen unterscheidet. (Zum Beispiel sollten Personen, die von einem Vorwurf freigesprochen wurden oder gegen die keine Vorwürfe erhoben werden, deutlich von verurteilten Personen unterschieden werden. Daten über Nicht-Verdächtige und Zeugen sollten deutlich von Daten über Verdächtige unterschieden werden.)

B. Spezifische Maßnahmen zur Beurteilung der Qualität von Daten müssen eingeführt werden, um den höchstmöglichen Qualitätsstandard der Daten zu garantieren, bevor diese verfügbar gemacht werden. Im Hinblick auf die Auswirkungen der Nutzung von Daten auf die Strafverfolgung sollten ausreichende technische und organisatorische Maßnahmen zur Hand sein, um die Qualität der Daten zu garantieren. Für den Fall, dass solche Garantien nicht gewährleistet werden können, muss dies vermerkt werden und die Nutzung solcher Daten muss auf spezifische Strafverfolgungsmaßnahmen mit zusätzlichen Sicherheitsvorkehrungen beschränkt bleiben. Eine Verpflichtung, den Empfänger personenbezogener Daten über jede Änderung bei diesen Daten zu informieren, muss verbindlich sein.

C. Die Nutzung biometrischer Daten bei der Strafverfolgung verlangt zusätzliche Sicherheitsvorkehrungen. Insbesondere die Identifizierung anhand der Nutzung solcher Daten, die manchmal unter Verwendung von Vorrichtungen zur Verarbeitung umfangreicher Mengen von Daten geschieht, wie beim neuen Schengen-Informationssystem, muss begleitet sein von Verfahren, die dem Individuum die Möglichkeit bieten, das Ergebnis des Abgleichs überprüfen zu lassen.

D. Besondere Verfahren bei der Verarbeitung, die besondere Gefahren darstellen können (z. B. Ausforschungsaufträge, themenbezogene Datensuche, spezielle Überwachungstechniken) erfordern zusätzliche Sicherheitsvorkehrungen für die Nutzung dieser Daten und die Überwachung der Nutzung solcher Operationen.

E. Es wird wichtig sein, mit technischen und organisatorischen Maßnahmen und Verfahren abzusichern, dass die Empfänger personenbezogener Daten mit den nötigen Informationen versorgt werden, um die Daten für die Zwecke nutzen zu können, für die sie ausgetauscht wurden und um diese auf aktuellem Stand zu halten.

F. Wenn eine Initiative oder ein Vorschlag die Wahl zwischen der Verarbeitung personenbezogener Daten auf zentralisierter oder dezentralisierter Ebene trifft, kann diese Wahl nicht nur aufgrund praktischer Erwägungen getroffen werden. Eine solche Wahl muss auch die Notwendigkeit berücksichtigen, den höchstmöglichen Standard der Datenqualität und des Datenschutz-Niveaus zu garantieren. Wenn eine dezentralisierte Verarbeitung die besten Sicherheitsvorkehrungen gewährleistet, sollte eine zentralisierte Verarbeitung keine Option sein.

IV. Zugang der Strafverfolgungsbehörden zu personenbezogenen Daten

- Routinemäßiger Zugang zu personenbezogenen Daten muss verboten sein.
- Zugang sollte auf bestimmte Fälle oder eine bestimmte Strafverfolgungs-Aufgabe begrenzt sein.
- Kontrolle der Nutzung dieses Zugangs muss ausreichend sichergestellt sein.
- Wenn direkter Zugang zu Daten vorgeschlagen wird, ist die Nutzung eines Index oder von hit/no hit -Systemen und eine ausreichende Zugangskontrolle erforderlich.
- Die Empfänger-Behörden müssen klar identifiziert sein.

V. Kontrolle und Aufsicht

- Über die gewöhnlichen Zuständigkeiten von Strafverfolgungsbehörden, Organen der Rechtspflege und Datenschutzkontrollinstanzen für die Kontrolle von und die Aufsicht über solche Datenverarbeitungs-Vorgänge, die besondere Risiken für die Rechte und Freiheiten des Betroffenen darstellen können, hinaus sollten zusätzliche maßgeschneiderte Kontroll- und Aufsichtsmaßnahmen für alle operationellen Vorgänge inklusive der Nutzung und des Missbrauchs personenbezogener Daten eingeführt werden.
- Besondere Vorschriften werden benötigt, die den Schwierigkeiten vorbeugen, die sich aus dem Austausch von Daten zwischen Mitgliedstaaten ergeben. Da diese Daten in verschiedenen Zuständigkeitsbereichen zugänglich sind, muss sichergestellt werden, dass Kontrolle und Aufsicht in allen betroffenen Zuständigkeitsbereichen wirksam sind.

Anlage 40

Erklärung der Europäischen Datenschutzkonferenz von Zypern, angenommen am 11. Mai 2007

Im Rat der Europäischen Union ist ein Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten bei der Verarbeitung im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen Gegenstand von Beratungen.

Die Schaffung eines harmonisierten und hohen Standards für den Datenschutz bei polizeilichen und justiziellen Maßnahmen in der Union ist in der Tat ein entscheidender Bestandteil der Achtung und des Schutzes von Grundrechten, wie des Rechts auf den Schutz personenbezogener Daten, bei der Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts.

Die Initiativen in der Europäischen Union zur Verbesserung der Bekämpfung von schweren Straftaten und Terrorismus haben das Ziel gemeinsam, nationale Grenzen innerhalb der Union zunehmend unwichtiger werden zu lassen, wenn es um die Bedingungen für den Austausch von Daten zwischen zuständigen Behörden geht. Daten für die Strafverfolgung sollen auf verschiedenen Wegen zugänglich gemacht werden, inklusive der Möglichkeit des direkten Zugriffs auf nationale Datenbestände.

Diese Initiativen zeigen deutlich, dass die Verpflichtung der Union zur Hilfe beim Kampf gegen schwere Straftaten und Terrorismus nicht auf die Schaffung der Bedingungen für den Informationsaustausch zwischen den Mitgliedstaaten beschränkt ist; klar erkennbar haben die Initiativen auch Auswirkungen auf die Datenverarbeitung auf nationaler Ebene, die jedem möglichen Austausch vorangeht. Es ist klar, dass jede Entwicklung auf diesem Gebiet abgewogen werden muss mit angemessenen und harmonisierten Datenschutzrechten und -verpflichtungen, wobei das gegenseitige Vertrauen in diese ein entscheidender Bestandteil ist.

Innerhalb der Europäischen Union unterscheidet sich die Datenschutz-Gesetzgebung für Maßnahmen der Strafverfolgung sowohl der Natur als auch der Sache nach. Sie gewährleistet somit sicherlich keinen harmonisierten Ansatz zum Datenschutz für Strafverfolgungs-Informationen, für die Rechte des Betroffenen sowie für eine effektive unabhängige Kontrolle.

Im Hinblick auf den zunehmenden Rückgriff auf die Verfügbarkeit („availability“) von Informationen als Konzept zur Verbesserung des Kampfes gegen schwere Straftaten, sowohl auf nationaler Ebene wie zwischen den Mitgliedstaaten, führt das Fehlen eines harmonisierten und hohen Standards für den Datenschutz in der Union zu einer Situation, in der das Grundrecht auf den Schutz personenbezogener Daten nicht mehr ausreichend gewährleistet wird.
Mit Bezugnahme auf ihr Positionspapier zu Strafverfolgung und Informationsaustausch in der EU (April 2005) und an ihre Erklärungen von Krakau (2005), Budapest (2006) und London (2006) erinnernd, ruft die gesamte Europäische Datenschutzkonferenz daher die im Rat der Europäischen Union und im Europäischen Parlament vertretenen Mitgliedstaaten dazu auf, einen solchen harmonisierten und hohen Standard des Datenschutzes in der Europäischen Union zu schaffen.

Die Europäische Datenschutzkonferenz ist sich über die Grundsatz-Diskussion im Rat über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses bewusst: sollte er nur auf Daten anwendbar sein, die zwischen Mitgliedstaaten ausgetauscht werden oder auf jegliche Verarbeitung durch Polizei- und Justizbehörden?

Die Europäische Datenschutzkonferenz weist wiederholt darauf hin, dass Initiativen der Union Auswirkungen auf nationaler Ebene haben und darauf, dass eine Begrenzung des Anwendungsbereiches auf Daten, die zwischen den Mitgliedstaaten ausgetauscht werden oder werden könnten, das Risiko besonderer Unsicherheiten und Unwägbarkeiten über den Anwendungsbereich des vorgeschlagenen Rahmenbeschlusses mit sich bringen würde. Sie **betont, dass nur ein umfassender Anwendungsbereich unter Einschluss aller Arten der Verarbeitung personenbezogener Daten den notwendigen Schutz der Individuen gewährleisten kann.**

Die Europäische Datenschutzkonferenz **betont weiter, dass die von der deutschen Ratspräsidentschaft am 13. März 2007 vorgelegte Fassung des Entwurfs des Rahmenbeschlusses auch bezüglich anderer Datenschutz-Grundsätze keine verlässliche und strenge Datenschutzordnung enthält** und dass sie weder die Stellungnahme der Europäischen Datenschutzkonferenz vom 24. Januar 2006 noch die Stellungnahme des EP vom 18. Mai 2006 einbezogen hat. Während der Entwurf einige Verbesserungen im Hinblick auf die Erreichung eines harmonisierten Rahmens für die Verarbeitung gebracht hat, ist er bislang unbefriedigend bei den Vorkehrungen zur Gewährleistung des Schutzes der Privatsphäre der Bürger. Dies muss besonders gelten, wenn man die bereits bestehende europäische Gesetzgebung zum Datenschutz berücksichtigt, insbesondere den rechtlichen Rahmen, der von den nationalen Gesetzgebern bei der Umsetzung der Richtlinie 95/46/EG geschaffen wurde und der ebenfalls auf die Verarbeitung personenbezogener Daten in dem fraglichen Bereich anwendbar ist. Darüber hinaus wiederholt die Europäische Datenschutzkonferenz, dass es notwendig ist, die auf nationaler Ebene bestehenden Schutzvorkehrungen zum Datenschutz zu erhalten, indem ein bindendes europäisches Instrumentarium verabschiedet wird.

Mit dem Ziel einer tatsächlichen Verbesserung beim Datenschutz in der dritten Säule unterstreicht die Europäische Datenschutzkonferenz die folgenden Grundsätze, die bei dem wichtigen Gesetzgebungsakt Rahmenbeschluss zu beachten sind:

- Zweckbegrenzung: die Notwendigkeit, die gesetzlichen Zwecke genau zu definieren, zu denen die Verarbeitung personenbezogener Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen erlaubt ist, ohne irgendwelche Generalklauseln, die die weitere Verarbeitung „für jegliche andere Zwecke“ erlaubt. Das Prinzip der Zweckbegrenzung ist ein Grundsatz in der EU-Richtlinie und in der Konvention 108.

- Datenkategorien: die Verarbeitung besonderer Kategorien von Daten ist verboten, es sei denn besondere Bedingungen werden erfüllt und besondere Garantien werden in der nationalen Gesetzgebung gegeben (Artikel 8 EU-Richtlinie, Artikel 6 Konvention 108). Darüber hinaus sollen angemessene Sicherheitsvorkehrungen für die Verarbeitung biometrischer und genetischer Daten gewährleistet werden.

- Kategorien von Betroffenen: Es ist ein Erfordernis des Verhältnismäßigkeitsgrundsatzes, Unterscheidungen zwischen den verschiedenen Kategorien von

Personen wieder einzuführen, die von der Verarbeitung für Polizei und Strafverfolgung betroffen sind.

- Regelung der Weitergabe von Daten an Drittstaaten: Es ist ein Erfordernis des Zweckmäßigkeits-Grundsatzes, dass gemeinsame Kriterien definiert und ein Verfahren geschaffen wird, um den Datenschutz-Standard in einem Drittland oder einer internationalen Einrichtung einschätzen zu können, bevor personenbezogene Daten übertragen werden. Dies soll nicht allein dem Ermessen der Mitgliedstaaten überlassen werden. Die Festlegung eines EU-Standards für ein solches Verfahren ist erforderlich, um Harmonisierung in Europa zu erreichen, und das Prinzip der Feststellung eines angemessenen Datenschutzniveaus entspricht der Regelung durch das Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981.

- Benachrichtigung des Betroffenen: Benachrichtigung des Betroffenen soll umfassend sein, einschließlich der Identität der für die Verarbeitung verantwortlichen Stelle, der möglichen Empfänger und der Rechtsgrundlage für die Verarbeitung. Jede Beschränkung soll präzise gefasst und begrenzt sein.

- Auskunftsrecht: Die Regelung zum Auskunftsrecht muss im Einklang mit den Anforderungen der Europäischen Menschenrechtskonvention und der Rechtsprechung stehen. Durch den Ausschluss eines wirksamen Beschwerderechts in einigen Fällen befindet sich der derzeitige Vorschlag nicht im Einklang mit diesen Anforderungen. Darüber hinaus soll die Kontrollinstanz oder das Beschwerdegericht das Recht haben, dem Betroffenen Informationen zu übermitteln, wenn ihm diese ungerechtfertigter Weise vorenthalten wurden. Es sollte weniger Ausnahmen vom Auskunftsrecht geben.

- Anzeige und Vorabkontrolle: Anzeige gegenüber und Vorabkontrolle durch die Kontrollinstanz sollten, soweit angemessen, eine Vorbedingung für die Verarbeitung sein. Die Vorabkontrolle soll von den nationalen Datenschutzkontrollinstanzen vorgenommen werden. Die Möglichkeit von Ausnahmen bei der Veröffentlichung der Anzeige sollte je nach Art der Verarbeitung erwogen werden.

- Kontrollinstanzen: Eine Gemeinsame Kontrollbehörde (JSA) soll als unabhängige Kontrollinstanz konzipiert sein. Der Rahmenbeschluss soll Aussagen über deren Zusammensetzung, Aufgaben und Zuständigkeiten enthalten. Sie soll insbesondere mit der Befugnis zu Beratung, Nachforschung und zum Einschreiten ausgestattet sein.

Die Europäische Datenschutzkonferenz anerkennt auch die Wichtigkeit einer möglichst schnellen Verabschiedung des Rahmenbeschlusses. Jedoch wird der derzeit diskutierte Vorschlag keinen ausreichend harmonisierten und hohen Standard des Datenschutzes gewährleisten. Die grundlegende Bedeutung des Rahmenbeschlusses nicht nur für den Schutz der Rechte der Bürger der Europäischen Union, sondern auch für die Strafverfolgung, rechtfertigt eine Diskussion, die nicht durch einen engen Zeitrahmen gefährdet wird.

Die Europäische Datenschutzkonferenz ruft den Rat daher dazu auf, sich mehr Zeit für die Verhandlungen zur Entwicklung eines Rahmenbeschlusses zu nehmen, der einen

hohen Datenschutz-Standard bietet.

Die Europäische Datenschutzkonferenz ist bereit, weiter zum Verfahren der Verabschiedung eines solchen Rahmenbeschlusses beizutragen und schlägt eine Anhörung der Arbeitsgruppe des Rates vor, um ihre Standpunkte darzulegen.

Anlage 41

Europäische Datenschutzkonferenz vom 17. –18. April in Rom

Erklärung

Die Europäische Union wird in Kürze über verschiedene neue Initiativen zur verbesserten Kontrolle von Reisenden in die Europäische Union und aus der Europäischen Union, diskutieren. Drei von der Kommission vor kurzem verabschiedete Mitteilungen1 haben zum Ziel, eine solche Diskussion über die nächsten Schritte zum Border Management, sowie über die Schaffung eines Europäischen Grenzüberwachungssystems und über die Bewertung von Frontex in Gang zu bringen.

Zusammen mit den Maßnahmen, die bereits eingeführt wurden oder bald eingeführt werden sollen, und die auf eine verbesserte Überwachung von Reisenden für Grenzkontrollen, Visum-Politik und Strafverfolgungsmaßnahmen abzielen, lassen die aktuellen Mitteilungen deutlich eine Entwicklung in Richtung einer vollständigen Kontrolle und Überwachung von Personen – unabhängig von ihrer Nationalität – die in das Schengen-Gebiet einreisen oder ausreisen, erkennen.

Obwohl ein effizientes Border Management für den Schutz der Union gegen mögliche Bedrohungen notwendig ist, so darf dies niemals in unverhältnismäßiger Weise die Rechte und Freiheiten der Reisenden, und vor allem nicht deren Recht auf Privatsphäre verletzen. Die Überwachung der Reisenden muss wohlbegründet sein und darf nur in Ausnahmefällen gestattet werden, und dies auch nur für berechtigte und besondere Zwecke. Jede allgemeine Überwachung stellt nicht hinnehmbare Risiken für die Freiheit der Einzelnen dar.

Ein anderes Thema, das überdacht werden muss, ist das zu Grunde liegende Konzept, Reisenden zu misstrauen, in dem man ausgewählte „vertrauenswürdige“ Reisende von allen anderen Reisenden isoliert, und die letzteren sogar als potentielle Straftäter erachtet. Das wird eine Durchleuchtung vor und am Eingang beinhalten, so wie die Kontrolle der Grenzüberschreitungen und die automatische Verarbeitung spezieller Daten der Reisenden. Dieses Konzept trägt nicht gerade viel dazu bei, den „symbolischen Effekt, die EU als weltoffen darzustellen“2, zu verwirklichen, so wie es die Mitteilung der Kommission erwähnt, und es ist sogar fraglich, ob dies mit den Werten der Europäischen Union im Einklang steht.

Die Konferenz hat bereits die Mitglieder der Europäischen Union und die Kommission, den Rat und das Europäische Parlament dazu aufgerufen, zuerst einmal eine Evaluierung zu fertigen, ob die bereits bestehenden rechtlichen Maßnahmen effektiv umgesetzt und durchgeführt werden.3 Ein neuer Vorschlag sollte nur dann eingebracht werden und wenn klare Hinweise vorliegen, die solche Maßnahmen unterstützen. Allerdings fand bis jetzt keine solche Bewertung über die Effektivität der Umsetzung der bestehenden rechtlichen Maßnahmen statt. Auch wurden keine verlässlichen Hinweise vorgelegt, die die Notwendigkeit neuer Systeme untermauern. Ebenso wenig wurden Beweise erbracht, die es erforderlich erscheinen lassen, die aktuellen Initiativen auf diesem Gebiet zu ergänzen. Die von der Kommission vorgelegten Informationen über die

geplanten Systeme liefern keinen klaren Beweis für ihre Effektivität. In Bezug auf die direkten und indirekten Kosten im Hinblick auf die Freiheiten und die Bürgerrechte – ganz abgesehen von den finanziellen Aspekten - für die Schaffung neuer Systeme wie zum Beispiel das Einreise-Ausreise-System, sollten auch aussagekräftige Beweise vorliegen, dass dieses System die beste Antwort auf das Problem ist, das es in Angriff nehmen soll.

Da dies anscheinend nicht der Fall ist, ruft die Konferenz die Europäische Union auf, die Notwendigkeit und Verhältnismäßigkeit weiterer Maßnahmen im Lichte der oben erwähnten Kommentare sorgfältig zu überdenken, und zwar vor allem in Bezug auf die in den Mitteilungen der Kommission vorgesehenen Vorschläge.

---

1 KOM (2008) 69 endg.
KOM (2008) 68 endg.
KOM (2008) 67 endg.

2 KOM (2008) 69 endg. Seite 6.
3 Erklärung von Larnaka über die Verfügbarkeit, Mai 2007

Anlage 42

29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre - Montreal (Kanada), 26.-28. September 2007 -

Resolution über den dringenden Bedarf an globalen Standards zum Schutz von Passagierdaten, die von Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden

Antragsteller: Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit (Deutschland)

Unterstützt von: Österreichische Datenschutzkommission (Österreich)
Office of the Privacy Commissioner of Canada (Kanada)
Office of the Information and Privacy Commissioner of British Columbia
Office of the Information and Privacy Commissioner of Ontario
European Data Protection Supervisor (Europäische Gemeinschaft)
La Commission Nationale de l'Informatique et des Libertés (Frankreich)
Landesbeauftragte für Datenschutz und die Informationsfreiheit Nordrhein-Westfalen, Deutschland – Regional)
Garante per la protezione dei dati personali (Italien)
College Bescherming Persoonsgegevens (Niederlande)
Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (Rumänien)
Agencia de Protección de Datos (Spanien)
Information Commissioner (Vereinigte Königreich)

Die Konferenz beruft sich auf

- das 2002 auf der 24. Internationalen Konferenz in Cardiff angenommene Kommuniqué;
- die 2003 auf der 25. Internationalen Konferenz in Sydney angenommene Resolution über die Übertragung von Passagierdaten;
- die 2005 auf der 27. Internationalen Konferenz in Montreux verabschiedete Deklaration zum Datenschutz und zum Schutz der Privatsphäre in einer globalisierten Welt;

in denen zum Ausdruck kommt, dass es gilt, zwischen dem legitimen Kampf gegen den Terrorismus und gegen die internationale Kriminalität einerseits und dem Datenschutz und dem Schutz der Privatsphäre andererseits ein Gleichgewicht herzustellen.

Die Konferenz vermerkt, dass

- Regierungsstellen zunehmend den Zugriff zu Passagierdaten suchen, die im Kampf gegen den Terrorismus, gegen illegale Einwanderung und andere Verbrechen verwendet werden sollen, ohne dass genügend Rücksicht auf Persönlichkeitsschutz und die Menschenrechte der Passagiere genommen wird;
- manche Passagierdaten dazu benutzt werden können, Folgerungen über Religionszugehörigkeit, Ethnie und andere äußerst heikle Zusammenhänge zu

ziehen,

- weltweit viele Regierungen ständig mehr Daten von Verkehrsträgern verlangen,
- Verkehrsträger die Passagierdaten aus kommerziellen Gründen erfassen und dann
  aufgefordert werden, sie für Justizvollzugszwecke zur Verfügung zu stellen,
- Verkehrsträger zunehmend viele verschiedene Forderungen zur Übergabe von Daten erfüllen müssen und sich an viele verschiedene Datenübertragungssysteme halten müssen, wodurch unter den Verkehrsträgern wie auch unter den Passagieren Ungewissheit über ihre Rechte und Pflichten entsteht, wodurch die Passagiere nur schwer verstehen, wie ihre Daten genutzt werden, und wodurch auch das Risiko entsteht, dass die Verkehrsträger die Daten unsachgemäß übertragen,
- diese vielen verschiedenen Forderungen und Systeme sowohl für die Verkehrsträger als auch für die Passagiere mit Kosten verbunden sind,
- juristische und technische Übereinstimmung erforderlich ist, damit die Verkehrsträger diese Forderungen erfüllen können,
- manche Verkehrsträger immer noch nicht ihrer Pflicht nachkommen, Passagiere über die Verwendung und Offenlegung ihrer Daten zu unterrichten,
- andere globale Abmachungen zur Erleichterung des internationalen Flugverkehrs getroffen worden sind, und dass dringender Bedarf besteht, globale Lösungen zu treffen, die den internationalen Reiseverkehr erleichtern und dabei das Recht der Passagiere auf Persönlichkeitsschutz respektieren.

Die Konferenz bestätigt erneut, dass

- Datenschutz und Schutz der Privatsphäre - wie in Art. 12 der Allgemeinen Deklaration der Menschenrechte und in anderen Rechtsinstrumenten verankert - Privatpersonen und ihre persönlichen Daten schützen und zusammen mit anderen Rechten in allen Ersuchen zur Übertragung und Nutzung von Passagierdaten für Justizvollzugszwecke berücksichtigt werden müssen,
- die Verarbeitung von Passagierdaten in einem Rahmen stattfinden sollte, der die anerkannten Datenschutzgrundsätze und -standards berücksichtigt,
- in allen Ersuchen staatlicher Behörden für die Nutzung von Passagierdaten Folgendes nachgewiesen werden sollte:
  - sie sind nachweisbar notwendig, um ein spezifisches Problem anzusprechen,
  - sie sind nachweisbar mit Wahrscheinlichkeit geeignet, das Problem anzusprechen,
  - sie entsprechen proportional ihrem Sicherheitswert, und
  - sie greifen nachweisbar weniger in die Privatsphäre ein als alternative Optionen,

  sowie dass all solche Ersuche regelmäßig zu überprüfen sind, um festzustellen, ob die Maßnahmen noch erforderlich sind,
- die Notwendigkeit, unter allen Umständen die Privatsphäre zu schützen, nicht nur für globale Datenschutzkreise, sondern auch für alle eine grundsätzliche Aufgabe bleibt, die um die Wahrung der fundamentalen Rechte und Freiheiten besorgt sind, und
- wenn Regierungsstellen sich nicht bemühen, die Datenschutzbelange richtig zu wägen, die echte Gefahr besteht, dass diese Stellen beginnen könnten, die fundamentalen Rechte und Freiheiten selbst, die sie schließlich schützen wollen, zu unterminieren.

Im Bestreben nach globalen Standards zum Schutz von Passagierdaten, die von

Regierungsstellen zu Justizvollzugs- und Grenzschutzzwecken herangezogen werden, ruft die Konferenz dazu auf,

- dass internationale Organisationen (wie z. B. IATA und ICAO), Regierungsstellen und
  Verkehrsträger mit den Beauftragten für den Datenschutz und für die Privatsphäre
  zusammenarbeiten, um verbindliche globale Lösungen mit angemessenen Datenschutzsicherheiten einzuführen,

- dass Regierungsstellen gewährleisten, dass alle Ersuche für die Nutzung von Passagierdaten
  - nachweisbar notwendig sind, um ein spezifisches Problem anzusprechen,
  - nachweisbar mit Wahrscheinlichkeit geeignet sind, das Problem anzusprechen;
  - ihrem Sicherheitswert proportional entsprechen, und
  - nachweisbar weniger in die Privatsphäre eingreifen als alternative Optionen,

  sowie dass all solche Ersuche regelmäßig überprüft werden sollten, um festzustellen, ob die Maßnahmen noch erforderlich sind,
- dass alle Passagierdaten nutzenden staatlichen Programme für Datenminimalisierung sowie für die ausdrückliche Beschränkung der Nutzung, Offenlegung und Einbehaltung der Daten auf die entsprechenden Programmzwecke sowie für die Richtigkeit der Daten, für das Recht auf Zugriff zu den Daten, für die Korrigierung der Daten und für eine unabhängige Überprüfung sorgen sollten,
- dass alle Lösungen die juristischen, technischen, finanziellen und wirtschaftlichen Belange der Verkehrsträger und der Behörden berücksichtigen müssen,
- dass Regierungsstellen offen und transparent die Zwecke, zu denen die Daten gesammelt und genutzt werden, angeben, und sicher stellen, dass alle Passagiere - ungeachtet ihrer Nationalität oder ihres Herkunftslandes - Zugang zu ihren persönlichen Informationen sowie zu einem angemessenen Rechtshilfemechanismus haben,
- dass Verkehrsträger ihre Passagiere über die Nutzung und Offenlegung ihrer Daten durch Regierungsstellen und Justizvollzugsbehörden, über Flugverbotslisten und ähnliche Überwachungslisten sowie über die Verfügbarkeit von Rechtshilfemaßnahmen im Zusammenhang mit Passagierdaten und damit zusammenhängenden persönlichen Informationen ausreichend unterrichten, und
- dass die Beauftragten für den Datenschutz und den Schutz der Privatsphäre weiterhin zusammenarbeiten, um sachgemäße Datenschutzmaßnahmen zu gewährleisten und auf verbindliche globale Lösungen zu dringen.

Erläuternder Hinweis

Die Regierungen verschiedener Länder haben zunehmend versucht, Passagierdaten als Waffe im Kampf gegen Terrorismus, transnationale Kriminalität und andere Verbrechen zu nutzen. Dadurch sind in Bezug auf die geforderten Datenelemente, die Verwendung der Daten und die Stufe der Sicherheitsmaßnahmen Differenzen aufgetreten.

Das Wesen des internationalen Reiseverkehrs fordert einen globalen Ansatz, und es ist eine globale Lösung dringend erforderlich, um eine angemessene Sicherheitsstufe zu erlangen und das Vertrauen der Passagiere zu gewinnen, während proportionale Maßnahmen unternommen werden, die den notwendigen Datenschutz und den Schutz der

Privatsphäre beinhalten.

Während Bedenken über den Datenschutz und den Schutz der Privatsphäre die vorrangigen Themen darstellen, die bei jeder globalen Lösung zu berücksichtigen sind, bietet sich auch Gelegenheit, andere juristische, technische, finanzielle und wirtschaftliche Fragen von Fluggesellschaften und Passagieren in Betracht zu ziehen.

Globale Standards können die Fairness, Übereinstimmung, juristische Gewissheit und Sicherheit für Passagiere und Verkehrsträger gewährleisten. Es ist klar, dass Verkehrsträger, Justizvollzugsbehörden, internationale Organisationen, zivilgesellschaftliche Gruppen und Datenschutzexperten an der globalen Lösung beteiligt sein müssen. Das Engagement der Datenschutzbeauftragten ist unentbehrlich, wenn Fortschritte erzielt werden sollen. Sie müssen die Führung übernehmen und auf einer solchen Lösung bestehen.

Anlage 43

29. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre - Montreal (Kanada), 26.-28. September 2007 -

Resolution über die Entwicklung internationaler Standards

Antragsteller: Datenschutzbeauftragter von Kanada

Unterstützt durch: Bundesbeauftragter für den Datenschutz, Deutschland
Datenschutzkommission, Belgien
Berliner Beauftragter für Datenschutz und Informationsfreiheit
Ontario Beauftragter für Datenschutz und Informationsfreiheit
Datenschutzbeauftragter, Spanien
Eidgenössische Datenschutzbeauftragte, Schweiz

Die Entwicklung von Standards im Datenschutz für die Anwendung und den Einsatz neuer und bestehender Technologien ist in den letzten Jahren Gegenstand erheblicher Debatten und Diskussionen sowohl innerhalb der internationalen Normungsorganisationen als auch in internationalen Datenschutzkreisen. Solche Standards sind u. a. bereits auf den 25., 26. und 28. internationalen Konferenzen in Sydney/Australien, Breslau/Polen und London/Großbritannien erörtert worden.

Diese Diskussionen spiegeln die zunehmende Erkenntnis in Kreisen des Datenschutzes und des Schutzes der Privatsphäre wider, dass Datenschutzgesetze und Gesetze zum Schutz der Privatsphäre zwar zum Schutz privater Informationen unerlässlich sind, dass sie allein jedoch nicht genügen. Vielmehr sind auch internationale Standards erforderlich, um die Beteiligten bei der Aufstellung und Befolgung gesetzlicher Regelungen zum Datenschutz und zum Schutz der Privatsphäre zu unterstützen.

Die Entwicklung von Datenschutzstandards für die Nutzung und den Einsatz neuer und bestehender Technologien sollte nicht so verstanden werden, dass sie von der zentralen Rolle der einzelnen nationalen Datenschutzbehörden und Kommissionen zum Schutz der Privatsphäre ablenken. Standards sind eine Methode zur Anwendung technischer und organisatorischer Spezifikationen, die gesetzliche Regelungen für die Praxis interpretieren können. Was technische Standards anbelangt, so ist dies bisher ohne aktive Beteiligung der Datenschutzkreise geschehen. Diese Situation muss sich ändern, damit die konsequente Interpretation und Befolgung gewährleistet ist.

Mit der Aufstellung der Arbeitsgruppe 5 (Identitätsmanagement und Datenschutztechnologien) im Unterausschuss 27 (Sicherheit der Informationstechnik) hat die Internationale Organisation für Normung (ISO) ihre Absicht bekundet, die Entwicklung von Datenschutzstandards voranzutreiben. Die Arbeitsgruppe hat dazu aufgerufen, mit der Internationalen Konferenz der Datenschutzbeauftragten (im Folgenden die "Konferenz") zusammenzuarbeiten. Besonders hervorgehoben werden dabei die gemeinsamen Datenschutzinteressen beider Organisationen sowie das Ziel der Arbeitsgruppe,

"Aspekte des Identitätsmanagements, der Biometrik und des Datenschutzes im Zusammenhang mit der Informationstechnologie mit einem internationalen Standardpaket zu harmonisieren".

Wenn auch die Entwicklung datenschutzrelevanter Standards[1] unter der Federführung einer sicherheitsorientierten Gruppe keine Ideallösung für die am Datenschutz und dem Schutz der Privatsphäre Beteiligten darstellt, ist dies nun einmal - zumindest vorläufig - die von der ISO gewählte Struktur. Will man gewährleisten, dass Datenschutzstandards entwickelt werden, ist es unerlässlich, auf diesen Ansatz von Seiten der Normungskreise mit aktiverer Einbindung in den Standardentwicklungsprozess zu reagieren. Es ist auch eine natürliche Erweiterung der Arbeit, die von der Konferenz bereits im Einvernehmen mit dem Datenschutz in anderen Kompetenzbereichen auf internationaler Ebene geleistet wird – zum Beispiel mit der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung und der Asiatisch-Pazifischen Wirtschaftsgemeinschaft –, dass man sich mit Datenschutzfragen befasst, die durch grenzüberschreitende Datenströme entstehen. Vereinfacht ausgedrückt, liegt es im besten Interesse der Konferenz sowie der Normungsexperten, dass die Konferenzmitglieder einen kooperativeren, gemeinschaftlicheren Weg zur Entwicklung von Standards antreten.

Die Konferenz fasst darum folgende Entschlüsse:

1. Die Konferenz unterstützt die Entwicklung effektiver, universal akzeptierter internationaler Datenschutzstandards und wird der ISO dafür ihre Erfahrungen bei der Entwicklung solcher Standards zur Verfügung stellen.
2. Die Konferenz ruft ihre Mitglieder auf, sich über ihre nationalen Normungsorganisationen stärker am Entwicklungsprozess der ISO-Standards zu beteiligen.
3. Angesichts der Tatsache, dass vielen Mitgliedern nur beschränkte Mittel zur Verfügung stehen, ruft die Konferenz ihre Mitglieder auf, in Betracht zu ziehen, wie sie ihre Erfahrungen und Fachkenntnisse am Besten teilen können, um diese Erfahrungen und Fachkenntnisse der ISO zur Verfügung zu stellen.
4. Die Konferenz ruft ihre Mitglieder auf, in Betracht zu ziehen, wie sie ihre Beiträge zum Standardentwicklungsprozess am Besten koordinieren können, damit gewährleistet ist, dass diese Beiträge allen Konferenzmitgliedern zugute kommen.
5. Die Konferenz ruft ihre Mitglieder auf, potentielle Mechanismen zu untersuchen, die zur Zusammenarbeit zwischen ISO und der Konferenz zustande bringen.
6. Die Konferenz ruft ihre Mitglieder auf, die Beteiligung an der Entwicklung von ISO-Standards durch andere Interessierte (wie Akademiker, NGOs, Forschungszentren usw.) aktiv zu fördern und sie aufzufordern, sich über ihre nationalen Normungsorganisationen zu beteiligen.

Anlage 44

Resolution über internationale Zusammenarbeit

Antragsteller: Privacy Commissioner of Canada

Unterstützt von: Information Commissioner, UK
Privacy Commissioner, New Zealand
Information and Privacy Commisssioner, Alberta
Information and Privacy Commissioner, Saskatchewan

Unter Bezugnahme auf die Deklaration von Montreux, in der die Bereitschaft der Datenschutzbeauftragten, die Zusammenarbeit untereinander und mit anderen mit dem Datenschutz befassten Organisationen zu fördern, und in der Regierungen aufgerufen wurden, die Einführung von Rechtsmitteln für den Datenschutz und den Schutz der Privatsphäre einzuführen,

in der Erkenntnis, dass mehrere internationale Organisationen aktiv die Zusammenarbeit im Datenschutz fördern, einschließlich dieser Konferenz, dem Europarat, der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD), der Asiatisch-Pazifischen Wirtschaftsgemeinschaft (APEC), den Asiatisch-Pazifischen Datenschutzbehörden (APPA), dem Iberoamerikanischen Datenschutznetz, dem Verband französischsprachiger Datenschutzbehörden, und der Arbeitsgruppe "Artikel 29 der Europäischen Union",

in Anerkennung der seit der 28. Konferenz in Paris und Brüssel unternommenen Schritte als Teil der Londoner Initiative, praktische Informationen mit dem Ziel auszutauschen, den Datenschutz durch bessere Kommunikation und Durchsetzung effektiver zu gestalten,

im Bewusstsein, dass die sowohl an Volumen als auch an Komplexität zunehmenden globalen Datenströme mit personenbezogenen Informationen in Hinsicht auf den Schutz persönlicher Informationen zu neuen Herausforderungen führen, und

im Bewusstsein, dass eine zunehmende Anzahl an Nationen heute die wichtige Bedeutung des Datenschutzes erkannt hat und schnell dazu übergeht, sich mit dem Schutz personenbezogener Informationen auf eine Weise zu befassen, die ihren jeweiligen juristischen, politischen und kulturellen Realitäten entspricht,

haben die an der 29. Internationalen Konferenz teilnehmenden Beauftragten für den Datenschutz und für die Privatsphäre daher wie folgt beschlossen:

1. Sie erkennen an, dass die Nationen jeweils verschiedene Ansätze entwickelt haben, um personenbezogene Informationen zu schützen und private Rechte zu stärken,

2. Sie unterstützen Datenschutzbeauftragte dabei, ihre gegenwärtigen Bemühungen zur Förderung internationaler Zusammenarbeit fortzusetzen und mit internationalen Organisationen daran zu arbeiten, den Datenschutz weltweit zu stärken,

3. Sie begrüßen, dass der OECD-Rat die Empfehlungen über grenzüberschreitende Zusammenarbeit bei der Durchsetzung von Datenschutzgesetzen angenommen hat, und sie rufen die Regierungen der OECD-Mitgliedstaaten auf, die Empfehlungen zu implementieren,

4. Sie fördern die Beauftragten in ihrem Bestreben, ihre wertvolle Arbeit gemäß der Londoner Initiative fortzusetzen und dabei Instrumente, Rahmenbedingungen und Erfahrungen auszutauschen, um die Wirksamkeit und Effizienz unserer Aktivitäten und Eingriffe auf nationaler und internationaler Ebene auswerten zu können, und

5. Sie unterstützen die Beauftragten in ihren fortlaufenden Bemühungen um die Steigerung des Datenschutzbewusstseins und des Bewusstseins für den Schutz der Privatsphäre durch Initiativen wie z. B. die "Woche des Datenschutzbewusstseins" (APPA) und den "Tag des Datenschutzes" (Europarat).

Anlage 45

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007

Entschließung über die Dringlichkeit des Schutzes der Privatsphäre in einer Welt ohne Grenzen und die Erarbeitung einer gemeinsamen Entschließung zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten

Antragsteller: Die Agencia de Protección de Datos (Spanien) und der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (Schweiz)

Unterstützt von: Der Commission nationale de l'Informatique et des Libertés (Frankreich)
Dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
Dem Garante per la Protezione dei Dati Personali (Italien)
Dem Staatlichen Inspektorat für den Datenschutz der Republik Litauen
Dem Amt für Datenschutz der Republik Tschechien
Der griechischen Datenschutzbehörde
Der niederländischen Datenschutzbehörde
Dem Europäischen Datenschutzbeauftragten Dem Generalinspekteur für den Datenschutz (Polen)
Dem Datenschutzbeauftragten von Irland
Der Nationalen Direktion für den Datenschutz von Argentinien
Der Agence de protection des données de la Principauté d'Andorre
Dem Amt des Informationsbeauftragten (Vereinigtes Königreich)
Der Nationalen Kommission für den Datenschutz (Portugal)
Dem Beauftragten für den Schutz der Privatsphäre von Neuseeland
Dem Datenschutzbeauftragten von Guernsey
Dem Berliner Beauftragten für Datenschutz und Informationsfreiheit
Der Datenschutzbehörde des Baskenlandes (Spanien)
Der Datenschutzbehörde von Katalonien (Spanien) Der Datenschutzbehörde von Madrid (Spanien)

Die Konferenz erinnert daran, dass:

- die auf ihrer 22. Konferenz in Venedig verabschiedete Erklärung;
- die auf ihrer 26. Konferenz in Breslau gefasste Entschließung;
- die auf ihrer 27. Konferenz in Montreux verabschiedete Erklärung;
- die auf ihrer 28. Konferenz vorgestellte Londoner Initiative;
- die auf ihrer 29. Konferenz gefasste Entschließung;

- den universellen Charakter des Rechts auf Datenschutz und auf den Schutz der Privatsphäre stärken wollen und zur Erstellung eines universellen Übereinkommens

zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten aufrufen.

- Insbesondere in der Erklärung von Montreux ruft die Konferenz die Organisation der Vereinten Nationen auf, ein zwingendes Rechtsinstrument auszuarbeiten, in dem das Recht auf Datenschutz und das Recht auf den Schutz der Privatsphäre als durchsetzbare Menschenrechte im Einzelnen festgeschrieben werden. Fernerruft die Konferenz den Europarat auf, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten dieser Organisation, die eine entsprechende Datenschutzgesetzgebung besitzen, aufzufordern, dem Übereinkommen (STE Nr. 108) und seinem Zusatzprotokoll (STE Nr. 181) beizutreten.

- In der Entschließung der 29. Konferenz haben die Datenschutzbeauftragten die Notwendigkeit unterstrichen, die Erarbeitung effizienter, universell anerkannter internationaler Normen zum Schutz der Privatsphäre zu unterstützen, als Mechanismus, um den Parteien zu helfen, die Konformität mit den gesetzlichen Anforderungen im Bereich des Datenschutzes und des Schutzes der Privatsphäre herzustellen und nachzuweisen.

Die Konferenz stellt fest, dass inzwischen ermutigende Anstrengungen gemacht wurden, um diese Ziele zu erreichen und dass insbesondere:

- Die Frage eines universellen Übereinkommens auf dem Arbeitsprogramm der Kommission für internationales Recht der Vereinten Nationen steht;

- Der Europarat den Beitritt von Nichtmitgliedstaaten befürwortet, deren Datenschutzgesetzgebung den Anforderungen des Übereinkommens STE Nr. 108 entspricht, und beschlossen hat, sich für dieses Regelwerk weltweit einzusetzen; so hat er die potenziell universelle Gültigkeit des Übereinkommens STE Nr. 108 betont, insbesondere auf dem Weltgipfel zur Informationsgesellschaft in Tunis im November 2005 und bei den Foren zur Internet-Governance 2006 in Athen und 2007 in Rio;

- Die OECD am 12. Juni 2007 eine Empfehlung zur grenzübergreifenden Zusammenarbeit bei der Anwendung der Rechtsvorschriften zum Schutz der Privatsphäre angenommen hat, die insbesondere darauf abstellt, die nationalen Rahmen zur Anwendung der Gesetze über den Schutz der Privatsphäre zu verbessern, um eine bessere Zusammenarbeit der nationalen Behörden mit den ausländischen Behörden zu ermöglichen, und wirksame internationale Mechanismen zu erarbeiten, um die grenzübergreifende Zusammenarbeit zur Anwendung der Gesetze zum Schutz der Privatsphäre zu erleichtern;

- Die Regionalkonferenzen der Unesco 2005 (Asien-Pazifik) und 2007 (Europa) den prioritären Charakter des Datenschutzes unterstreichen;

- Die Artikel 29-Gruppe der Europäischen Union Initiativen ergriffen hat, um das Verabschiedungsverfahren für zwingende Vorschriften für Unternehmen (BCR) und die Entwicklung vertraglicher Lösungen für den grenzübergreifenden Datenaustausch zu erleichtern.

- Die Staats- und Regierungschefs der „Frankophonie“ sich zum Abschluss ihres 11. Gipfels im September 2006 in Budapest verpflichtet haben, auf nationaler Ebene die Arbeit an den erforderlichen gesetzlichen und verordnungsrechtlichen Regelungen zur Festschreibung des Rechtes der Menschen auf Datenschutz zu intensivieren und

- sich weltweit für die Ausarbeitung eines internationalen Übereinkommen einzusetzen, das die Effektivität des Rechts auf Datenschutz gewährleistet;

- Die APEC im November 2004 Leitprinzipien zum Schutz der Privatsphäre verabschiedet hat, um den Schutz der Privatsphäre zu verstärken und den Informationsfluss aufrechtzuerhalten. Im September 2007 hat die APEC eine Initiative „Privatsphäre“ zur Entwicklung des Umsetzungsrahmens gestartet, um zertifizierte internationale Datenflüsse sicherzustellen, die den Bedürfnissen des Geschäftsverkehrs entsprechen, die Konformitätskosten senken, den Verbrauchern ein wirksames Instrument an die Hand geben, den Regulatoren effizientes Handeln ermöglichen und die Vorschriftenlast verringern;

- Die in Montreal am Rande der 29. Internationalen Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre gegründete Frankophone Vereinigung der Datenschutzbehörden (AFAPDP) in ihren Zielsetzungen die Ausarbeitung eines universellen Übereinkommens und die Bemühungen mit Blick auf den Beitritt von Nichtmitgliedstaaten des Europarats zum Übereinkommen STE Nr. 108 unterstützt;

- Das Iberoamerikanische Datenschutz-Netzwerk (RIPD) zum Abschluss seiner 6. Tagung im Mai 2008 in Kolumbien eine Erklärung angenommen hat, in der die internationalen Konferenzen für den Datenschutz und für die Privatsphäre aufgerufen werden, unabhängig von ihrer geografischen Zugehörigkeit ihre Bemühungen mit dem Ziel der Verabschiedung eines gemeinsamen Rechtsinstruments fortzusetzen;

- Die mittel- und osteuropäischen Datenschutzbehörden (APDCO) auf ihrer jüngsten Tagung im Juni 2008 in Polen ihren Willen bekundet haben, ihre Aktivitäten im Rahmen von APDCO fortzusetzen und zu verstärken und insbesondere gemeinsame Lösungen zu erarbeiten und die neuen Mitglieder bei der Implementierung ihrer Datenschutzgesetzgebung zu unterstützen.

Die Konferenz ist der Ansicht, dass:

- das Recht auf Datenschutz und den Schutz der Privatsphäre ein Grundrecht der Menschen ist, unabhängig von ihrer Staatsangehörigkeit und ihrem Wohnsitz;

- in der sich ausbreitenden Informationsgesellschaft das Recht auf Datenschutz und auf den Schutz der Privatsphäre in einer demokratischen Gesellschaft eine unerlässliche Voraussetzung ist, um die Achtung der Rechte der Personen, den freien Fluss von Informationen und eine offene Marktwirtschaft zu gewährleisten;

- die Globalisierung des Austauschs und der Verarbeitung personenbezogener Daten, die Komplexität der Systeme, die Schäden, die durch eine unangemessene Nutzung immer leistungsfähigerer Technologien entstehen können und der Anstieg der Sicherheitsmaßnahmen eine rasche und angemessene Antwort erfordern, um die Achtung der Grundrechte und -freiheiten, insbesondere des Rechts auf Schutz der Privatsphäre, zu gewährleisten;

- die anhaltenden Disparitäten im Bereich des Datenschutzes und der Achtung der Privatsphäre weltweit, insbesondere wegen des Fehlens von Garantien in mehreren Staaten, dem Austausch personenbezogener Daten und der Schaffung eines effizienten, globalen Datenschutzes schaden;

- die Entwicklung internationaler Regeln, die die Achtung des Datenschutzes und des Schutzes der Privatsphäre einheitlich gewährleisten, eine Priorität darstellt;
- die Anerkennung dieser Rechte die Verabschiedung eines universellen, zwingenden Rechtsinstruments erfordert, das die in den verschiedenen bestehenden Instrumenten festgeschriebenen gemeinsamen Prinzipien des Datenschutzes und der Achtung der Privatsphäre bestätigt, auflistet und ergänzt und die internationale Zusammenarbeit zwischen Datenschutzbehörden verstärkt;

- die Umsetzung der von Organisationen wie der APEC oder der OECD entwickelten Leitlinien, insbesondere derjenigen, die die Annahme eines internationalen Rahmens zur Verbesserung der Achtung des Rechts auf Datenschutz und auf den Schutz der Privatsphäre bei grenzüberschreitenden Datenflüssen betreffen, eine positive Etappe zur Erreichung dieses Ziels darstellt;

- der Beitritt zu zwingenden Instrumenten mit universeller Gültigkeit, wie das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (STE Nr. 108) und sein Zusatzprotokoll über die Kontrollbehörden und den grenzüberschreitenden Datenfluss (STE Nr. 181), die Grundprinzipien des Datenschutzes enthalten, den Austausch von Daten zwischen Parteien erleichtern kann; diese Instrumente sehen in der Tat Mechanismen und eine Plattform für die Zusammenarbeit zwischen den Datenschutzbehörden vor, tragen Sorge dafür, dass diese Behörden bei der Erfüllung ihrer Aufgaben völlig unabhängig sind und fördern die Einrichtung eines angemessenen Datenschutzniveaus;

- die 30. Internationale Datenschutzkonferenz eine geeignete Instanz für die Verabschiedung einer Strategie ist, die speziell auf die Verwirklichung dieser Ziele ausgerichtet ist.

Daher erneuert die Konferenz **ihren Appell**, ein zwingendes, universelles Rechtsinstrument zum Datenschutz und zum Schutz der Privatsphäre auszuarbeiten und **fasst dazu folgende Entschließungen**:

1. Die Konferenz unterstützt die Bemühungen des Europarats, das Grundrecht auf Datenschutz und auf den Schutz der Privatsphäre zu fördern. Die Konferenz fordert daher die Mitgliedstaaten dieser Organisation, die dies noch nicht getan haben, auf, die Ratifizierung des Übereinkommens zum Schutz des Menschen bei der automati-

schen Verarbeitung personenbezogener Daten und ihres Zusatzprotokolls zu prüfen. Die Konferenz fordert die Nichtmitgliedstaaten, die in der Lage sind, es zu tun, auf, zuerwägen, der Einladung des Europarats, dem Übereinkommen STE Nr. 108 und seinem Zusatzprotokoll beizutreten, Folge zu leisten. Mit Blick auf ihre Entschließung über die Errichtung einer Lenkungsgruppe zur Vertretung bei Tagungen internationaler Organisationen hat die Konferenz den Wunsch, auch einen Beitrag zu den Arbeiten des beratenden Ausschusses des Übereinkommens STE Nr. 108 zu leisten.

2. Die Konferenz unterstützt die Initiativen der APEC, der OECD und anderer regionaler Organisationen und internationaler Foren für die Entwicklung wirksamer Mittel zur Förderung besserer internationaler Standards für den Datenschutz und den Schutz der Privatsphäre.

3. **Die Konferenz beauftragt** eine Arbeitsgruppe, die von der den 31. Internationalen Konferenz ausrichtenden Behörde koordiniert wird und sich aus den interessierten nationalen Datenschutzbehörden zusammensetzt, einen **gemeinsamen Vorschlag zur Erstellung internationaler Normen zum Schutz der Privatsphäre und zum Schutz personenbezogener Daten** abzufassen und ihr auf ihrer nichtöffentlichen Sitzung vorzulegen, wobei folgender Kriterien vorgegeben werden:
   - Vornahme einer Bestandsaufnahme der Grundsätze und Rechte im Bereich des Schutzes personenbezogener Daten in den verschiedenen geografischen Gebieten der Welt, wobei besonders auf Gesetzestexte oder andere Texte abzustellen ist, die in den regionalen und internationalen Foren auf weitgehenden Konsens gestoßen sind;
   - Erarbeitung einer Zusammenstellung von Prinzipien und Rechten, die die bestehenden Texte widerspiegelt und ergänzt und dadurch die Erreichung eines Höchstmaßes an internationaler Akzeptanz zur Sicherung eines hohen Schutzniveaus ermöglicht;
   - Beurteilung der Sektoren, in denen diese Rechte und Prinzipien Anwendung finden, einschließlich der Varianten, die den Akzent auf die Harmonisierung ihrer Anwendungsbereiche legen;
   - Bestimmung der grundlegenden Kriterien, die ihre tatsächliche Anwendung gewährleisten, unter Berücksichtigung der Verschiedenheit der Rechtssysteme;
   - Prüfung der Rolle, die die Selbstregulierung spielen muss;
   - Formulierung wesentlicher Garantien für bessere und flexiblere internationale Datentransfers.

Bei dem Verfahren, das zur Abfassung dieses gemeinsamen Vorschlags führt, sollen die öffentlichen und privaten Organisationen und Instanzen zu einer breiten Beteiligung an den Arbeitsgruppen und an Foren und Anhörungen ermutigt werden, um zu einem möglichst umfassenden institutionellen und gesellschaftlichen Konsens zu gelangen. Besondere Aufmerksamkeit sollte den laufenden Arbeiten der Internationalen Organisation für Normung (ISO) und der Kommission für internationales Recht gewidmet werden.

Anlage 46

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007

Entschließung zum Datenschutz in Sozialen Netzwerkdiensten

Antragsteller:
Berliner Beauftragter für Datenschutz und Informationsfreiheit, Deutschland

Unterstützt durch:
Commission Nationale de l'Informatique et des Libertés (CNIL), Frankreich;
Bundesbeauftragter für Datenschutz und Informationsfreiheit, Deutschland;
Garante per la protezione dei dati personali, Italien;
College Bescherming Persoonsgegevens, Niederlande;
Privacy Commissioner, Neuseeland;
Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB), Schweiz

Entschließung

Soziale Netzwerkdienste haben in den letzten Jahre große Beliebtheit erworben. Diese Dienste bieten ihren Teilnehmern Interaktionsmöglichkeiten auf der Basis von selbst generierten persönlichen Profilen, die in einem noch nie da gewesenen Ausmaß die Veröffentlichung persönlicher Informationen zu den betreffenden Personen (und auch anderen Personen) mit sich bringen. Die sozialen Netzwerkdienste bieten zwar ein neues Spektrum von Möglichkeiten für Kommunikation und den Echtzeit-Austausch von Informationen jeder Art, die Nutzung dieser Dienste kann jedoch auch eine Gefährdung der Privatsphäre ihrer Nutzer - und Anderer - mit sich bringen, denn personenbezogene Daten einzelner Personen werden in bisher unbekannter Weise und Menge öffentlich (und global) zugänglich, einschließlich großer Mengen digitaler Fotos und Videos. Der Einzelne läuft Gefahr, die Kontrolle über die Nutzung der Daten durch Andere zu verlieren, wenn sie erst einmal im Netzwerk publiziert sind: Während der Community-Bezug sozialer Netzwerke die Vorstellung erweckt, die Veröffentlichung der eigenen persönlichen Daten laufe in etwa auf das Gleiche hinaus, wie früher das Mitteilen von Information unter Freunden von Angesicht zu Angesicht, können Profildaten tatsächlich für alle Teilnehmer einer Community (deren Zahl in die Millionen gehen kann) verfügbar sein.

Derzeit gibt es wenig Schutz dagegen, dass personenbezogene Daten jeder Art aus Profilen kopiert werden – durch andere Mitglieder des Netzwerks oder durch unbefugte netzwerkfremde Dritte – und zum Aufbau von Persönlichkeitsprofilen verwendet werden oder dass die Daten anderweitig wieder veröffentlicht werden. Es kann sehr schwierig - und manchmal unmöglich - sein zu erreichen, dass Daten, wenn sie einmal publiziert sind, wieder vollständig aus dem Internet entfernt werden. Selbst nach ihrer Löschung auf der ursprünglichen Website (z. B. dem sozialen Netzwerk) können Kopien bei Dritten oder bei den Anbietern der sozialen Netzwerkdienste verbleiben. Personenbezogene Daten aus Nutzerprofilen können auch außerhalb des Netzwerks bekannt werden, wenn sie von Suchmaschinen indexiert werden. Hinzu kommt, dass manche Anbieter sozialer Netzwerkdienste über Applikationsprogrammierschnittstellen Drittanbietern

Nutzerdaten zur Verfügung stellen, die dann unter der Kontrolle dieser Dritten stehen.

Ein Beispiel von Wiederverwendungen, das großes öffentliches Aufsehen erregt hat, ist die Praxis von Personalverantwortlichen, Nutzerprofile von Stellenbewerbern oder Angestellten zu durchsuchen. Presseberichten zufolge gibt bereits heute ein Drittel der Personalverantwortlichen an, bei ihrer Arbeit Daten aus sozialen Netzwerkdiensten zu nutzen, z. B. um die einzelnen Angaben von Bewerbern zu überprüfen und/oder zu ergänzen.

Profilinformationen und Verkehrsdaten werden von Anbietern sozialer Netzwerkdienste auch zur Weiterleitung zielgerichteter Werbung an ihre Nutzer verwendet.

Sehr wahrscheinlich werden in Zukunft noch weitere unerwartete Verwendungen von Informationen in Nutzerprofilen auftreten.

Zu weiteren, bereits jetzt identifizierten spezifischen Risiken für Datenschutz und Datensicherheit zählen erhöhte Risiken durch Identitätsbetrug, der durch die umfangreiche Verfügbarkeit personenbezogener Daten in Nutzerprofilen begünstigt wird, und durch eine mögliche Übernahme von Profilen durch unbefugte Dritte. Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre erinnert daran, dass diese Risiken bereits in dem Dokument “Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten” (”Rom-Memorandum”) der 43. Tagung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommuniktion (3. - 4. März 2008) und in dem ENISA Positionspapier Nr. 1 „Security Issues and Recommendations for Online Social Networks“ (Oktober 2007) analysiert wurden.

Die in der Internationalen Konferenz versammelten Datenschutzbeauftragten sind von der Notwendigkeit überzeugt, dass als Erstes eine intensive Informationskampagne unter Beteiligung aller öffentlichen und privaten Interessengruppen – von Regierungsstellen bis zu Bildungseinrichtungen wie Schulen, von Anbietern sozialer Netzwerkdienste bis zu Verbraucher- und Nutzerverbänden, einschließlich der Datenschutzbeauftragten selbst – durchgeführt werden muss, um den vielfältigen mit der Nutzung sozialer Netzwerkdienste verbundenen Gefahren vorzubeugen.

Empfehlungen

In Anbetracht der besonderen Natur der Dienste und der kurz- und langfristigen Gefahren für die Privatsphäre des Einzelnen richtet die Konferenz folgende Empfehlungen an Nutzer und Anbieter sozialer Netzwerkdienste:

Nutzer sozialer Netzwerkdienste

Organisationen, denen am Wohl der Nutzer sozialer Netzwerke gelegen ist – einschließlich Diensteanbieter, Regierungen und Datenschutzbehörden – sollten mithelfen, die Nutzer über den Schutz ihrer personenbezogenen Daten aufzuklären und die fol-

gende Botschaften zu vermitteln.

1. Veröffentlichung von Daten

Nutzer sozialer Netzwerkdienste sollten sich sorgfältig überlegen, welche persönlichen Daten sie - wenn überhaupt - in einem sozialen Netzwerkprofil publizieren. Sie sollten bedenken, dass sie zu einem späteren Zeitpunkt mit einer Information oder mit Bildern konfrontiert werden könnten, z. B. wenn sie sich um eine Arbeitsstelle bewerben. Insbesondere sollten Minderjährige vermeiden, ihre Privatanschrift oder ihre Telefonnummer mitzuteilen.

Privatpersonen sollten sich überlegen, ob es nicht ratsam wäre, in einem Profil anstelle ihres wirklichen Namens ein Pseudonym zu verwenden. Dabei sollten sie jedoch nicht vergessen, dass auch die Benutzung von Pseudonymen nur einen begrenzten Schutz gewährt, da Dritte in der Lage sein können, ein solches Pseudonym aufzudecken.

2. Die Privatsphäre Anderer

Nutzer sollten auch die Privatsphäre Anderer achten. Sie sollten besonders vorsichtig sein bei der Veröffentlichung personenbezogener Daten Anderer (einschließlich Bildern, oder sogar mit Zusatzinformationen versehenen Bildern) ohne die Einwilligung der betreffenden Personen.

Anbieter sozialer Netzwerkdienste

Anbieter sozialer Netzwerkdienste tragen eine besondere Verantwortung dafür, die Belange von Personen, die soziale Netzwerke nutzen, zu beachten und zu wahren. Sie sollten nicht nur die Regelungen des Datenschutzrechts einhalten, sondern auch die folgenden Empfehlungen umsetzen.

1. Datenschutzvorschriften und -standards

Anbieter, die in verschiedenen Ländern oder sogar weltweit tätig sind, sollten die Datenschutzstandards der Länder einhalten, in denen sie ihre Dienste betreiben. Zu diesem Zweck sollten die Anbieter Datenschutzbehörden konsultieren, wenn und soweit dies notwendig ist.

2. Aufklärung der Nutzer

Anbieter sozialer Netzwerkdienste sollten ihre Nutzer über die Verarbeitung ihrer personenbezogenen Daten transparent und offen informieren. Es sollte auch aufrichtig und verständlich über mögliche Folgen einer Veröffentlichung persönlicher Daten in einem Profil und über verbleibende Sicherheitsrisiken sowie über gesetzliche Zugriffsrechte Dritter (einschließlich z. B. von Strafverfolgungsbehörden) aufgeklärt werden. Eine solche Aufklärung sollte auch Hinweise dazu enthalten, wie Nutzer mit personenbezoge-

nen Daten von Dritten umgehen sollten, die in ihren Profilen enthalten sind.

3. Nutzerkontrolle

Anbieter sollten die Kontrolle der Nutzer über die Verwendung ihrer Profildaten durch andere Community-Mitglieder weiter verbessern. Sie sollten die Einschränkung der Sichtbarkeit ganzer Profile sowie von in Profilen enthaltenen Daten, und in Community-Suchfunktionen ermöglichen.

Die Anbieter sollten auch eine Kontrolle der Nutzer über die Nutzung von Profil- und Verkehrsdaten, z. B. für zielgerichtete Werbung, ermöglichen. Als ein Minimum sollten eine Opt-out-Möglichkeit für allgemeine Profildaten und eine Opt-in-Möglichkeit für sensible Profildaten (z. B. politische Überzeugungen, sexuelle Orientierung) und Verkehrsdaten geboten werden.

4. Datenschutzfreundliche Standardeinstellungen

Darüber hinaus sollten Anbieter datenschutzfreundliche Standardeinstellungen für Nutzerprofilinformationen anbieten. Standardeinstellungen spielen eine Schlüsselrolle beim Schutz des Privatsphäre der Nutzer: Es ist bekannt, dass lediglich eine Minderheit von Nutzern, die sich bei einem Dienst anmelden, irgendwelche Änderungen daran vornimmt.
Diese Einstellungen müssen bei einem sozialen Netzwerkdienst, der sich an Minderjährige wendet, besonders restriktiv sein.

5. Sicherheit

Anbieter sollten die Sicherheit ihrer Informationssysteme weiter verbessern und aufrechterhalten und die Nutzer gegen betrügerische Zugriffe auf ihre Profile schützen, indem sie für die Konzeption, die Entwicklung und den Betrieb ihrer Anwendungen anerkannte Methoden einschließlich unabhängigem Auditing und unabhängiger Zertifizierung verwenden.

6. Auskunftsrechte

Anbieter sollten Personen (gleichgültig ob Mitglieder des sozialen Netzwerkdienstes oder nicht) ein Recht auf Auskunft zu ihren personenbezogenen Daten gewähren und erforderlichenfalls diese Daten berichtigen.

7. Löschung von Nutzerprofilen

Anbieter sollten den Nutzern die Möglichkeit geben, ihre Mitgliedschaft auf einfache Weise zu beenden und ihre Profile sowie alle Inhalte oder Informationen, die sie in dem sozialen Netzwerk publiziert haben, zu löschen.

8. Pseudonyme Nutzung des Dienstes

Anbieter sollten als Option die Möglichkeit der Einrichtung und Verwendung pseudonymer Profile anbieten und zur Nutzung dieser Option ermutigen.

9. Zugriff durch Drittpersonen

Anbieter sollten wirksame Maßnahmen ergreifen, um das Durchsuchen und/oder massenweise Herunterladen (oder „bulk harvesting“) von Profildaten durch Dritte zu verhindern.

10. Indexierbarkeit der Nutzerprofile

Die Anbieter sollten sicherstellten, dass Nutzerdaten von externen Suchmaschinen nur durchsucht werden können, wenn der Nutzer dazu seine ausdrückliche, vorherige und informierte Einwilligung erteilt hat. Die Nichtindexierbarkeit von Profilen durch Suchmaschinen sollte als Standard eingestellt sein.

Anlage 47

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007

Entschließung zum Schutz der Privatsphäre von Kindern im Internet

Antragstellerin: Die Datenschutzbeauftragte von Kanada

Unterstützt durch: Datenschutzbeauftragter, Neuseeland
La Commission Nationale de l'Informatique et des Libertés (Frankreich)
Datenschutzbeauftragter, Irland
Beauftragter für den Datenschutz und Informationsfreiheit, Berlin

Überall in der Welt gehen die Jugendlichen von zu Hause und von der Schule aus sowie über ihre kabellosen Geräte ins Internet. Sie nutzen das Internet zur sozialen Interaktion
– sie tauschen Geschichten, Ideen, Fotos und Videos aus, sie bleiben den Tag über durch SMS-Mitteilungen in Kontakt mit ihren Freunden und sie beteiligen sich an Online-Spielen gemeinsam mit anderen Personen am anderen Ende der Welt.

Dabei werden die Jugendlichen auch mit den Schwierigkeiten und Herausforderungen bezüglich des Schutzes ihrer persönlichen Daten im Internet konfrontiert. Das Fehlen einer Regelung bei zahlreichen Internetdiensten macht die Sache schwierig. Viele der bei Jugendlichen beliebtesten Websites sammeln große Mengen personenbezogener Daten für Verkaufs- und Marketingzwecke.

Mit steigender Anzahl der im Internet angebotenen Anwendungen und Technologien wird die Menge der gesammelten und aufbewahrten personenbezogenen Daten immer größer. Heute sind sich die Jugendlichen oft nicht darüber bewusst, dass ihre Auskünfte, ihre Gewohnheiten und ihre Verhaltensweisen im Internet überwacht werden.

Untersuchungen zeigen, dass die Jugendlichen (wie auch zahlreiche Erwachsene) nur selten die Geheimhaltungserklärungen der von ihnen besuchten Websites lesen, was nicht überrascht, denn die Vertraulichkeitserklärungen zahlreicher Websites sind in einer technischen oder juristischen Fachsprache abgefasst, die für die meisten Leser schwer verständlich ist.

Wenn auch manche Jugendliche die mit ihren Online-Aktivitäten verbundenen Gefahren erkennen, so verfügen sie doch nicht über die Erfahrung, die technischen Kenntnisse oder die nötigen Instrumente, um diese Gefahren zu mindern. Oft kennen sie ihre gesetzlichen Rechte nicht.

Vor fast 20 Jahren hat die Generalversammlung der Vereinten Nationen 1989 ein Übereinkommen über die Rechte des Kindes verabschiedet. In diesem heißt es, dass die Staaten die Rechte des Kindes achten und schützen müssen, einschließlich ihres Rechtes auf den Schutz ihrer Privatsphäre.

Seit dieser Zeit bereiteten den Datenschutzbeauftragten die Verletzungen der Privatsphäre von Kindern im Internet immer mehr Sorgen.

In der am 20. Februar 2008 vom Ministerrat des Europarats angenommenen Erklärung zum Schutz der Würde, Sicherheit und der Privatsphäre von Kindern im Internet zeigt sich dieser von der Notwendigkeit überzeugt, Kinder über die lange Speicherdauer und über die Risiken der von ihnen ins Internet eingestellten Inhalte aufzuklären. Er erklärte darüber hinaus, dass, anders als bei der Strafverfolgung, keine fortbestehenden oder dauerhaft zugänglichen Aufzeichnungen über die von Kindern ins Internet eingestellten Inhalte existieren sollten, die deren Würde, Sicherheit und Privatsphäre angreifen oder ihnen auf andere Art und Weise jetzt oder zu einem späteren Zeitpunkt ihres Lebens schaden können.

Die Datenschutzbeauftragten haben zugleich erkannt, dass ein auf Erziehung ausgerichteter Ansatz, verbunden mit einer Regelung des Datenschutzes, eine der wirksamsten Methoden zur Bewältigung dieses Problems darstellt. So haben mehrere Länder innovative, auf Erziehung angelegte Konzepte umgesetzt, um der Herausforderung zu begegnen, die der Schutz der Privatsphäre von Kindern im Internet darstellt.

Kinder und Jugendliche haben ein Recht darauf, sich online sicher bewegen und positive Erfahrungen machen zu können, bei denen sie die Absichten der Personen, mit denen sie interagieren, kennen und verstehen.

Die auf der 30. internationalen Konferenz versammelten Beauftragten für den Datenschutz und für die Privatsphäre haben beschlossen:

- die Erarbeitung von Ansätzen zu fördern, die auf Erziehung angelegt sind, um die Lage in Bezug auf den Schutz der Privatsphäre im Internet auf nationaler wie auf internationaler Ebene zu verbessern;

- bemüht zu sein, dafür zu sorgen, dass Kinder und Jugendliche in der ganzen Welt Zugang zu einem sicheren Online-Umfeld haben, das ihre Privatsphäre respektiert;

- mit Partnern und Akteuren im eigenen Land und im Ausland zusammenzuarbeiten, in der Erkenntnis, dass die Zusammenarbeit mit den Fachleuten, die das tägliche Leben der Kinder beeinflussen, von entscheidender Bedeutung ist;

- miteinander zu arbeiten, um beispielhafte Praktiken auszutauschen und Aktivitäten zur Erziehung der Öffentlichkeit durchzuführen, um Kinder und Jugendliche stärker zu sensibilisieren hinsichtlich der Gefahren in Bezug auf den Schutz ihrer Privatsphäre, die mit ihren Online-Aktivitäten verbunden sind, und bezüglich der sich ihnen bietenden Möglichkeiten einer aufgeklärten Wahl, um ihre persönlichen Informationen zu kontrollieren;

- bei Erziehenden die Einsicht zu fördern, dass die Sensibilisierung für den Schutz der Privatsphäre einen wesentlichen Aspekt der Kindererziehung darstellt und in ihr Unterrichtsprogramm aufgenommen werden muss;

- zu fordern, dass die Behörden Gesetze erlassen, die die Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern einschränken, einschließlich geeigneter Bestimmungen für den Fall von Verstößen;

- bei Online-Werbung für Kinder oder verhaltensbezogener Werbung geeignete

Einschränkungen bei der Sammlung, Verwendung und Mitteilung personenbezogener Daten von Kindern zu fordern;

- die Betreiber von Websites für Kinder anzuhalten, ihr soziales Bewusstsein unter Beweis zu stellen, indem sie Vertraulichkeitserklärungen und Nutzungsvereinbarungen einführen, die klar, einfach und verständlich sind und indem sie die Nutzer über die Gefahren für den Schutz der Privatsphäre und die Sicherheit sowie über die ihnen auf der Website gebotenen Wahlmöglichkeiten aufklären.

Anlage 48

30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre in Straßburg, Frankreich, 15.-17. Oktober 2007

Entschließung zur Prüfung der Einrichtung eines Internationalen Tages oder einer Woche für den Schutz der Privatsphäre/Datenschutz

Antragsteller: Privacy Commissioner of Australia, Australien
Unterstützt von:
Privacy Commissioner of Canada, Kanada Information and Privacy Commissioner, British Columbia, Kanada Beauftragter für den Schutz personenbezogener Daten, Hongkong Koreanische Agentur für Informationssicherheit, Korea Privacy Commissioner of New Zealand, Neuseeland Information Commissioner, Northern Territory, Australien Privacy Commissioner, Victoria, Australien Datenschutzkommission, Frankreich Bundesbeauftragter für den Datenschutz, Deutschland
Entschließung:

Die 30. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre beschließt:

1. darauf hinzuarbeiten, dass ein Tag oder eine Woche bestimmt wird, an dem/in der alljährlich weltweit der Schutz der Privatsphäre und der Datenschutz gefeiert und gefördert werden,

2. eine Arbeitsgruppe einzusetzen, die einen geeigneten Tag oder eine Woche ermitteln und die damit zusammenhängende Fragen prüfen soll, mit der besonderen Anweisung an die Arbeitsgruppe, Verbindung zu anderen internationalen Akteuren zu suchen, für die die Förderung des Schutzes der Privatsphäre und des Datenschutzes von Interesse ist, und

3. auf der 31. Internationalen Konferenz von der Arbeitsgruppe einen Bericht mit der Empfehlung eines Tages oder einer Woche sowie Anregungen für die effektive Förderung des Datenschutzes und des Schutzes der Privatsphäre zu erhalten.

Erläuternde Hinweise

Die Londoner Initiative

1. Die Erklärung von London hat die Datenschützer aufgefordert, der Öffentlichkeit den Datenschutz näher zu bringen und effektiver zu gestalten. Dies könnte erheblich gefördert werden durch die Einführung eines jährlichen internationalen Tages oder einer Woche für den Schutz der Privatsphäre und den Datenschutz. Eine solche jährliche weltweite Veranstaltung würde umfassende Gelegenheiten zur Kommunikation mit Bürgern und Verbrauchern bieten. Ein Schlüsselthema in jedem Jahr würde zeigen, dass alle Datenschutzbehörden mit einer Stimme sprechen.

2. Es gibt bereits Erfahrungen mit grenzübergreifend koordinierten Initiativen zur Schaffung von Bewusstsein für den Schutz der Privatsphäre. Zwei erwähnenswerte Initiativen sind die Asia Pacific Privacy Awareness Week (Asiatisch-pazifische Woche zur Förderung des Bewusstseins für den Schutz der Privatsphäre) und der Europäische Datenschutztag.

Privacy Awareness Week (Asiatisch-pazifische Woche zur Förderung des Bewusstseins für den Schutz der Privatsphäre)

3. Die asiatisch-pazifischen Datenschutzbehörden (APPA) veranstalten gemeinsam die Privacy Awareness Week (PAW). Diese Veranstaltung wurde 2001 vom Amt für den Schutz der Privatsphäre von Victoria initiiert und hat sich seit 2006 zu einer jährlichen Veranstaltung zur Förderung des Bewusstseins für den Schutz der Privatsphäre über den asiatisch-pazifischen Raum entwickelt. Die PAW hat sich als erfolgreiche Veranstaltung erwiesen, die das Bewusstsein und das Verständnis für den Schutz der Privatsphäre in der Geschäftswelt, bei den Regierungen und bei den Privatpersonen gestärkt hat. Gleichzeitig mit den APPA haben sich auch Reichweite und Profil der PAW erweitert.

4. Die APPA-Mitglieder organisieren eine ganze Woche lang gemeinsame Aktivitäten, wie z. B. einen Datenschutzwettbewerb für Jugendliche, und koordinieren auch eigene regionale Veranstaltungen. Für die Mitglieder der APPA hostet das Amt des Privacy Commissioner von Australien eine PAW-Website (www.privacyawarenessweek.org). Diese Site bietet Informationen über gemeinsame Aktivitäten und Veranstaltungen der APPA und Aktionen in den einzelnen Regionen.

5. Bisher wurde die PAW alljährlich in der letzten Augustwoche abgehalten. Nachdem sich seit Kurzem nun auch die Länder der nördlichen Hemisphäre Kanada und Korea beteiligen, wird die Veranstaltung von 2009 an auf Mai verlegt werden. Diese Jahreszeit ist für alle beteiligten Länder geeignet und die Hauptturlaubszeiten werden vermieden.

Datenschutztag

6. Am 28. Januar 2007 initiierte der Europarat mit Unterstützung der Europäischen Kommission den Datenschutztag und der 28. Januar wurde feierlich zum Datenschutztag erklärt. Zweck des Datenschutztags ist es, die Bürger Europas zu ermutigen, ein größeres Bewusstsein für den Schutz personenbezogener Daten und für ihre Rechte und Verantwortungen zu entwickeln. Der Datenschutztag wird seit Januar 2007 jährlich veranstaltet.

Weitere koordinierte Wochen für den Schutz der Privatsphäre

7. Einige Länder organisieren landesweit gleichartige Veranstaltungen. In den USA, wo es keine zentrale Datenschutzbehörde gibt, wird seit einigen Jahren von einem Berufsfachverband, der American Health Information Management Association, eine wichtige Woche für den Schutz der Gesundheitsdaten veranstaltet. Ihre nächste Woche für den Schutz der Gesundheitsdaten soll vom 12. -18. Februar 2009 stattfinden.[2]

Entschließung der APPA

8. Auf dem 29. APPA Forum am 19. - 20. Juni 2008 in Seoul, Korea, wurde über den Erfolg des PAW-Konzepts diskutiert und es wurde angeregt, dass es sich lohnen würde, die PAW und den Datenschutztag zu einem einzigen koordinierten internationalen Tag für den Schutz der Privatsphäre/Datenschutz zusammenzulegen. Eine weltweite Koordinierung könnte das Profil und die Wirkung beider Veranstaltungen auf kosteneffektive Weise steigern. Die Tagung beschloss, diesen Gedanken auf der 30. Internationalen Konferenz zu unterbreiten.

Erwägungen

9. Mit der Einführung eines einzigen internationalen Tages oder einer Woche für den Schutz der Privatsphäre/Datenschutz ist es notwendig, über eine geeignete Zeit für dieses Ereignis nachzudenken, die in der nördlichen wie der südlichen Hemisphäre günstig ist und Konflikte mit kulturellen Ereignissen, Feiertagen oder anderen wichtigen Tagen minimiert. In Anbetracht der erforderlichen Vorlaufzeit wird nicht damit gerechnet, dass der erste derartige weltweit festgesetzte Tag oder die Woche vor 2010 stattfinden wird.

10. Weitere Überlegungen müssen geprüft werden, einschließlich der Koordinierung und der Verwaltung eines solchen Tages oder einer Woche. Im Einklang mit den Zielen der Erklärungen von Montreux und London wird angeregt, dies auch als eine Gelegenheit zu nutzen, um Brücken zu Akteuren zu bauen, die an der Förderung des Schutzes der Privatsphäre außerhalb der Internationalen Konferenz interessiert sind.

Arbeitsgruppe

11. Es wird vorgeschlagen, dass die Konferenz grundsätzlich dem Gedanken zustimmt, dass eine einzige internationale Veranstaltung zur Förderung des Schutzes der Privatsphäre und des Datenschutzes vorteilhaft für die Förderung des weltweiten Datenschutzbewusstseins sein würde. Es sollte eine Arbeitsgruppe eingerichtet werden, um diese Initiative voranzutreiben, mit dem Ziel, ein geeignetes Datum zu ermitteln und die mit der Koordinierung einer solchen Veranstaltung zusammenhängenden Fragen zu untersuchen.

12. Australien ist bereit, die Koordinierung/den Vorsitz in dieser Arbeitsgruppe zu übernehmen. Es wäre sehr wichtig, dass in der Arbeitsgruppe alle Regionen vertreten sind und es könnte nützlich sein, auch einige internationale und supranationale DSB und Organisationen aufzunehmen.

SACHSEN-ANHALT

Landesbeauftragter für den Datenschutz

Landesbeauftragter
Herr Dr. von Bose

Leitender Beamter der Geschäftsstelle und Stellvertreter
Herr MR Michl

Dienstgebäude:	Berliner Chaussee 9, 39114 Magdeburg
Postanschrift:	Postfach 1947, 39009 Magdeburg
Telefon:	0391 81803-0 oder 0391 567 7797-0
Telefax:	0391 81803-33 oder 0391 567 7797-33
Freecall:	0800 9153190 (Festnetz DTAG in S.-A.)
E-Mail:	poststelle@lfd.sachsen-anhalt.de
Internet:	www.datenschutz.sachsen-anhalt.de

Referat 1

Geschäftsstellenleitung

Landtag,
Justizverwaltung,
Justizvollzug,
Staatsanwaltschaften,
Europäischer und Internationaler Datenschutz

Polizei,
Verfassungsschutz und Nachrichtendienste

Geschäftsstelle:
Haushalts- und Verwaltungsangelegenheiten

Finanzen,
Kommunalrecht,
Ausländer- und Staatsangehörigkeitsrecht

Geschäftsstelle:
Vorzimmer des Landesbeauftragten,
Schreibdienst und Bücherei

Melde-, Pass- und Ausweiswesen, Wahlen, Personenstandswesen

Geschäftsstelle:
Registratur und Schreibdienst

Referat 2

Grundsatzfragen des Datenschutzrechts,
Öffentlicher Dienst,
Hochschulen,
Kammern

Informationszugangsrecht

Sozialwesen,
Verwaltungsverfahrensrecht

Gesundheitswesen, Kinder- und Jugendhilfe, Schulen, Wissenschaft und Forschung, Archivwesen, Personalakten- und Personalvertretungsrecht

Referat 3

Grundsatzfragen der Informationstechnik und der Organisation des Datenschutzes,
eGovernment,
Wirtschaft,
Verkehr

Verwaltungsmodernisierung,
eGovernment,
Betriebssysteme, Datenbanken,
Technische Gutachten

IT der Geschäftsstelle

Telekommunikations- und Mediendienrecht,
Presserecht,
Netze

IT der Geschäftsstelle
Homepage des LfD

Vermessungswesen und Geoinformation,
Statistik,
Handwerk und Gewerbe

Stichwortverzeichnis

A

Abgabenordnung 65, 66, 70, 71, 232, 257, 272
Abrechnungsstelle 94, 180
Abrechnungszwecke 93, 94, 280
Adressfeld 175
Aktenaufbewahrung 158
Amtsärztliche Stellungnahme 92
Arbeitnehmerdatenschutz 22
Arbeitslosengeld II 169
Arbeitspaket 172, 173
Archivierungssysteme 142, 143
Auftragsdatenverarbeitung 31, 160, 197, 198
Auskunftei 277
Auskunfteien 20, 229, 269, 277, 278
Auskunftsanspruch 64, 65, 207, 272
Auskunftsrecht
  im Steuerverfahren 5, 11, 63, 64, 139, 301
Ausländerzentralregister 52
Ausstellung
  Gedenkstätte 49

B

Bedarfsgemeinschaft 172, 173
Beeinflussung von Patienten 178
Behördliche Datenschutzbeauftragte 4, 13, 14, 27, 29, 31, 69, 86, 87, 108, 149, 153, 155, 160, 217, 271
Beratungs- und Auskunftspflicht 188
Berufsanerkennungsrichtlinie 42, 43
Beschwerdestelle Polizei 140
Beteiligungsbericht 116, 117
Bewertungsportal 2, 7, 165
Binnenmarktinformationssystem IMI 38, 42, 43
BlackBerry 106, 107, 108
Bundeselterngeld- und Elternzeitgesetz 185
Bundeskriminalamtgesetz 133
Bundesmeldegesetz 56
Bundesmelderegister 56
Bundespolizeigesetz 62, 136
Bundeszentralregister 128, 246
Bürgerentlastungsgesetz 71
Bürgerportale 47, 48, 274
Bußgeldstelle 222, 223, 224

D

Datenschutzbewusstsein 1, 12, 14, 15, 16, 24, 155, 163, 164, 166, 236, 238, 312, 328

Datenübermittlung 19, 89, 90, 95, 96, 113, 121, 141, 147, 156, 163, 180, 197, 224, 225, 243, 250, 262, 264, 267
durch Polizei an Private 141
De-Mail 7, 47, 274
Deutsche Bundesbank 147
Diebstahl von Laptops 97
Dienstleistungsstatistik 190, 191
DNS-Sperren 209, 210
Dokumentenmanagementsystem 216

E

EFS 103, 104
eGovernment-Initiative der Landesregierung 40
eGovernment-Maßnahmenplan 26, 34, 38
EGVP 42, 102
Eingliederungs- und Vermittlungsleistungen 176
Eingliederungshilfe 92
Eingliederungsmanagement 130, 131
Einsatzprotokolle 93
Einschulungsuntersuchungen 90
Einstellungstests 126, 127
Einwilligung 21, 43, 47, 75, 76, 77, 87, 95, 119, 121, 126, 128, 129, 139, 156, 166, 167, 176, 177, 180, 185, 186, 200, 210, 211, 212, 226, 232, 235, 246, 250, 252, 258, 269, 280, 282, 289, 320, 322
Einwilligungslösung 21, 252
Elektronische Gesundheitskarte 62, 87
Elektronischer Heilberufsausweis 87
elektronischer Personalausweis 54
ElsterLohn II 68, 231
E-Mail 8, 19, 29, 30, 34, 35, 36, 47, 48, 53, 99, 100, 108, 112, 114, 122, 204, 210, 211, 212, 270, 274
E-Mail-Verteiler 108
Erfahrungsaustausch 13, 14, 37
Ermittlungsgruppe Schulweg 146
Ersatzschulverordnung 167
Ersatzzustellung 157
EU-Dienstleistungsrichtlinie 26, 38, 40
Europäische Datenschutzkonferenz 62
Europäischer Datenschutztag 24, 163, 238

F

Familienpaten 185
Fernwartungsverbindung 98
Feuerwehr-Unfallkasse Mitte 181
Firewall 34, 98, 99, 111
Fluggastdaten 60, 61, 261

Flugpassagierdaten 61, 243
Föderalismusreform 80, 118
Forschung
  anonyme 75
  mit Sozialdaten 76
  Sozialdaten 186
Fortbildungsmanagement 120, 121
Früherkennungsuntersuchungen 182, 184

G

Gedenkstätte 48, 49
Gemeinderat 116
Gentest 90
Geodaten 44, 45, 256
Geodateninfrastrukturgesetz 44
Gerichtsvollzieher 157
Gesamtbeurteilungsbogen 166
Gewerbeordnung 96, 225
Gewerbetreibende 97
GIAZ 13, 217, 218, 219
Google Analytics 105, 106
Greylisting 213
Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme III, 2, 134, 135

H

Hasselbachplatz Magdeburg 137, 138, 155
hauptamtliche Mitarbeiter 49
Hilfsmerkmale 189, 190, 191
Homepage des Landesbeauftragten 18, 99, 164, 170
Hospitation 166, 167
Hundegesetz 77, 80

I

ICAO 52, 307
Identitäts- und Zugriffsmanagement-System 33, 35
IMSI-Catcher 150, 203
Ingenieurgesetz 95
INPOL 148
INSPIRE-Richtlinie 44, 45, 256
Integrationsfachdienste 185
Internationale Datenschutzkonferenz 63
IT-Architektur 27, 33, 34, 35
IT-Betriebsstättenverbund 28, 32
IT-Kataster 39
ITN-LSA 32, 36, 37
IT-Querschnittsdienst 31, 32, 33
IT-Ressortplan 26, 39
IT-Sicherheitsmanagement 36, 37

IT-Strategie 15, 25, 26, 27, 28, 31, 33, 34, 37, 39
IuK-Betriebsmodell 31

J

Jugendstrafvollzugsgesetz 199
Justizakten 158
Justizvollzugsanstalt Burg 15, 192, 194, 196, 197
Justizzentrum 15, 16, 152, 153, 154, 155, 156

K

Kennzeichenerfassung 143, 144
Kernbereichsschutz 131, 132, 213, 233
Kerndatensatz 161, 162
Kettenmodell 100
Kinderpornographie 209, 210
Kinderschutzgesetz 15, 182
Kindeswohlgefährdung 181, 184
Klinikum 114, 115
KONSENS 26, 69
Kontaktformular
  im Landesportal 19, 20
Kontenabrufverfahren 65
Kontoauszüge 170, 171, 172
Kraftfahrzeugsteuer 69, 72, 73, 74
Künstlerische Zwecke 139

L

Landesbeamtenrecht 118
Landesleitlinie IT-Sicherheit 27, 36, 37
Landesrechenzentrum 26, 28
Landesrechnungshof 118, 179
Liegenschaftsbuch 115
Logdateien 104
Löschung 52, 59, 64, 74, 85, 113, 114, 127, 129, 136, 138, 146, 153, 157, 165, 173, 174, 189, 191, 194, 195, 200, 213, 220, 221, 226, 245, 264, 318, 321
LUNA 68, 69

M

Mammographie-Screening 88
Maßregelvollzugsgesetz 88
Masterplan Landesportal 39, 40
Medienkompetenz 15, 24, 163, 238
Meldedaten 58, 89, 182, 189, 232
Melderegisterauskunft 57, 58
  Online 58
Mikado 158

Missbrauch personenbezogener Daten 57
Mitarbeiterüberwachung 124
Mobilfunkblocker 202

N

Namens- und Verzeichnisdienst 33, 34, 36
Netzwerk 53, 98, 102, 104, 109, 176, 281, 315, 318, 321
Nicht-öffentlicher Bereich 15, 17, 21, 23, 165, 166, 207, 279, 280, 282, 283
Novellierung 20, 21, 22, 88, 95, 208, 241, 242, 253, 282

O

Octoware 91
Online-Anbindung 219, 221, 222
Online-Dialog-Verfahren 220, 221
Online-Durchsuchung 11, 134, 135, 227, 228, 233, 234, 236, 239, 240, 241, 242
Online-Melderregisterauskunft 58
Opferpension 187
OSCI 2.0 102

P

Patientenunterlagen 94, 95
Personalaktendaten 115, 118, 121, 196, 197
Personaldaten im Internet 126
Personalmanagementsystem 15, 35, 119
Personalservicecenter 129
Personalvertretung 120, 124, 125, 130, 131
Personenstandsgesetz 58
Personenstandswesen 58
PKD 52
PKI 34, 48, 52, 99, 100
Polizeiliche Auskunftssysteme 127
Protokollierung 62, 98, 127, 145, 209, 211, 212, 220, 233, 251, 268
Push-Dienst 106

R

Rezepte, ärztliche 178
Roter Ochse 49
Rückständedatei 72, 73, 74
Rundfunkgebührenpflicht 206

S

Schadenersatz 225
Schalenmodell 100, 101
Schriftgutaufbewahrungsgesetz 158
Schülergericht 156

Schülerstammblatt 160, 161
Schulstatistik 161
Schulträger 161, 167, 168
Schulverwaltungssoftware 162
Schwedische Initiative 59, 264
Scoring 10, 20, 229, 277
Selbständige 174
Sexualstraftäterdatei 142
Sicherheitssoftware für Laptops 97, 98, 111, 266
Signatur 40, 54, 55, 56, 70, 71, 100, 101, 102, 257
SOG LSA 131, 132, 137, 139, 141, 147, 223
Soziale Netzwerke 7, 165
SPAM-Filterung 212, 213
Spielbankgesetz 82, 84
Sprachstandsfeststellung 184
SSID 109
Steuer-Identifikationsnummer 66, 247
Steuerungsprogramme 177, 178, 258
Street-View 45
Studierendendatenbank 112
StUG 50
Suchlauf 15, 122, 123, 124, 158

T

Telearbeit 110, 111
Telefax 95
Telefonnummer 116, 126, 173, 174, 320
Telekommunikationsüberwachung 11, 135, 149, 150, 151, 203, 205, 217, 227, 233, 236, 241, 259
Telemediengesetz 105, 208, 209, 247, 267
Terminsrolle 155, 156
Terror-Camp 151
Terrorliste 60, 262
TIS 120
Tracking-Dienste 106
Trennungsgebot 217

Ü

Übermittlung der
- Bezügedaten eines Geschäftsführers 117
- Daten Gewerbetreibender 97
- Namen von Mandatsträgern 116
- Steuerdaten bei ELSTER 71
- Steuer-Identitätsnummer 67
- Studierendendaten 113
- Zentralregisterauskunft/Bewerbungsverfahren 128

Übermittlung von
- Daten an Auftragsdatenverarbeiter 193
- Daten im Schülergerichtsverfahren 156
- Daten zwischen Bildungsträgern 176

Fluggastdaten	60
Fremdpersonaldaten	147
Patientendaten	180
Personalaktendaten	196
Personalausweisregisterdaten	223
Sozialdaten an Rechnungshöfe	180
Spielerdaten	83

U

Unabhängigkeit	23, 29
Urheberrecht	207

V

Verfahrensverzeichnis	148, 154
Verfassungsschutz	46, 81, 213, 215, 216, 217, 228, 241, 246
Verfassungsschutzgesetz	4, 213, 216
Verhaltenskontrolle	124
Verkehrs-AG	225, 226
Verkehrsdaten	203, 204, 205, 207, 227, 259, 260, 261, 266, 319, 321
Verkehrsordnungswidrigkeit	222, 223
Verkehrsüberwachung	222, 223
Verpflichtungsgesetz	157, 193, 200
Versammlungsgesetz	81, 82
Verschlüsselung	47, 55, 67, 90, 97, 102, 104, 106, 107, 119, 125, 162, 194, 274
Vertrag von Prüm	62, 261, 288
Verwaltungs-PKI	99
Videoaufzeichnung	139, 222, 223
Videoaufzeichnungen	84, 137, 138, 139, 154, 222, 223
Videoüberwachung	11, 15, 82, 83, 84, 85, 88, 136, 137, 138, 152, 153, 225
Visa-Einlader- und Warndatei	51
Vorratsdatenspeicherung	III, 4, 61, 121, 149, 203, 205, 227, 228, 243, 259, 260, 280
Vorratsspeicherung	11, 61, 149, 150, 203, 227, 236, 243, 288, 289
VPN	109, 110

W

Waffenbehörde	86
Web-Mail	47, 211
Webserver	104, 105, 111, 112, 113
Whitelisting	213
WLAN	13, 108, 109

Z

Zensus 2011	188, 189, 190
zentraler IT-Dienstleister	26, 28, 32, 34

Zentrales Fahrerlaubnisregister 219
Zugänglichmachung im Internet 112, 113
Zulassungsbehörde 13, 73, 74, 224, 225
Zusammenarbeit 5, 8, 9, 14, 16, 17, 31, 59, 62, 63, 64, 132, 142, 148, 166, 200, 245, 261, 262, 263, 264, 285, 286, 287, 288, 290, 291, 292, 293, 299, 300, 310, 311, 312, 314, 316, 324
Zuverlässigkeitsüberprüfung 147, 235
Zwangsversteigerung
  Internetbekanntmachung 159, 160