Landtag Brandenburg **Drucksache 5/714**

Tätigkeitsbericht

der Landesbeauftragten für den Datenschutz

und für das Recht auf Akteneinsicht

zum 31. Dezember 2009

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht hat dem Landtag und der Landesregierung alle zwei Jahre einen Bericht über ihre Tätigkeit vorzulegen (§ 27 Brandenburgisches Datenschutzgesetz; § 11 Akteneinsichts- und Informationszugangsgesetz). Dieser Bericht schließt an den am 11. März 2008 vorgelegten Tätigkeitsbericht 2006/2007 an und deckt den Zeitraum vom 1. Januar 2008 bis zum 31. Dezember 2009 ab.

Der Tätigkeitsbericht kann auch aus unserem Internetangebot unter http://www.lda.brandenburg.de abgerufen werden.

Datum des Eingangs: 23.03.2010 / Ausgegeben: 30.03.2010

Impressum

Herausgeber: Die Landesbeauftragte für den Datenschutz und
für das Recht auf Akteneinsicht Brandenburg
Stahnsdorfer Damm 77
14532 Kleinmachnow

Telefon: 033203 356-0
Fax: 033203 356-49

E-Mail: Poststelle@LDA.Brandenburg.de
Internet: http://www.lda.brandenburg.de

Fingerprint: 0DD70C8A 65508B73 2A53EFEE AC857D66

Druck: Brandenburgische Universitätsdruckerei und Verlagsgesellschaft Potsdam mbH

Inhaltsverzeichnis

Seite

Verzeichnis der öffentlichen Stellen 12

Einleitung 14

Teil A
Datenschutz

1 Brennpunkte des Datenschutzes 17

1.1 Umfrage zum Stand des Datenschutzes und der IT-Sicherheit in der Kommunalverwaltung 17
1.2 Datenschutz im Internet beginnt an den Schulen 21
1.2.1 Das Projekt „Datenschutz für Schüler und Lehrer“ 21
1.2.2 Welche Daten und Fotos darf die Schule auf ihrer Homepage veröffentlichen? 23
1.2.3 Urheberrecht – wer hat die Rechte an den Werken von Schülern und Lehrern? 24
1.2.4 Spick mich – dürfen Schüler ihre Lehrer im Internet bewerten? 25
1.2.5 Welche Grenzen hat die Nutzung schulischer Rechner? 26
1.3 Zugang zu Informantendaten 27
1.3.1 Brandenburgisches Datenschutzgesetz 28
1.3.2 Ordnungswidrigkeitenverfahren 29
1.3.3 Abgabenrecht 29
1.3.4 Sozialrecht und Jugendhilfe 30
1.3.5 Schweigepflicht im Gesundheitswesen 30
1.3.6 Ergebnis 31

2 Technisch-organisatorische Entwicklungen 32

2.1 Virtualisierung – ein anhaltender Trend 32
2.2 Cloud Computing – Rechnen in der Wolke auf eigene Gefahr? 33
2.3 Tracking Tools – Ich kenn’ dich besser als du denkst! 35
2.4 BlackBerry – Smartphones in der öffentlichen Verwaltung 37
2.5 Telearbeit am häuslichen Arbeitsplatz 39
2.6 Wartung und Fernwartung 41
2.7 Serviceportal der Landesverwaltung 43
2.7.1 E-Payment 45
2.7.2 Identitätsmanagement 46
2.7.3 Virtuelles Bauamt 48

3 Medien und Telekommunikation 50

3.1 Datenschutzgerechte Nachweise zur Befreiung von Rundfunkgebühren 50
3.2 Vorratsdatenspeicherung in der elektronischen Kommunikation – ein Status quo 51
3.3 Internetsperren – ein geeignetes Mittel im Kampf gegen Kinderpornografie? 53
3.4 Wie sich der Bund vor Viren und Würmern schützen will 54

4 Inneres 56

4.1 Polizei- und Ordnungsbehörden 56
4.1.1 Der Datenaustausch zwischen Polizei und Staatsanwaltschaft funktioniert nicht! 56
4.1.2 Überprüfung von Stellenbewerbern 58
4.1.3 Bußgeldverfahren bei Verkehrsverstößen mit im Ausland zugelassenen Fahrzeugen 61
4.1.4 Überflüssige Mitteilungen der Bußgeldstellen über Fahrverbote und Fahrerlaubnisentziehungen an die Wohnortpolizei 62
4.1.5 „Runter vom Gas“ verärgert Briefempfänger 64
4.2 Verfassungsschutz 65
IT-Sicherheitskonzept beim Verfassungsschutz 65
4.3 Ausländer 66
Datenübermittlung der Ausländerbehörde an die Sozialbehörde 66
4.4 Melderecht 69
4.4.1 Änderungen im Melderecht 69
4.4.2 Prüfung des Verfahrens zur Beantragung von Reisepässen 70
4.4.3 Unberechtigte Zugriffe auf die Online-Melderegisterauskunft 73
4.5 Datenverarbeitung, Statistik, Wahlen 75
4.5.1 Vorbereitungen zur Volkszählung 2011 75
4.5.2 IT-Sicherheitskonzepte der Ministerien – eine Bestandsaufnahme 76
4.5.3 IT-Sicherheitsmanagement in der Landesverwaltung 78
4.5.4 Neuer Brandenburgischer IT-Dienstleister 79
4.5.5 Die elektronische Akte in der Landesverwaltung – EL.DOK BB nimmt Fahrt auf 83
4.5.6 IP-Telefonie im LVN 3.0 85
4.6 Personaldaten 86
4.6.1 Novellierung des Landesbeamtengesetzes 86
4.6.2 Der Personalrat darf nicht alles wissen! 88

4.6.3 Personalinformationssystem PERIS 89
4.6.4 Gesundheitsdaten Angehöriger für Sozialauswahl? 92
4.6.5 Kontrolle von E-Mail und Internet am Arbeitsplatz 93
4.6.6 Veröffentlichung von Mitarbeiterdaten im Internet 94
4.7 Kommunales 95
4.7.1 Wie oft duschen Sie? – Datenerhebung eines Abwasserbetriebes 95
4.7.2 Mobiler Bürgerservice 97

5 Justiz 98

5.1 Brandenburgisches Dolmetschergesetz 98
5.2 Untersuchungshaftvollzugsgesetz 99
5.3 Datenverarbeitung im Justizvollzug 101
5.4 Justizzentrum Potsdam 102
5.5 Optimierung der Führungsaufsicht über entlassene Strafgefangene 103

6 Bildung, Jugend und Sport 105

6.1 Novellierung der Datenschutzverordnung Schulwesen zur Umsetzung des Brandenburgischen Schulgesetzes 105
6.2 Sprachstandsfeststellung vor der Einschulung 107
6.3 Gegensprechanlage mit Überwachungsmöglichkeit 108
6.4 Tagespflegestatistik – keine Auskunftspflicht für Tagespflegepersonen 109

7 Arbeit, Soziales, Frauen und Familie 110

7.1 Zum Umgang mit persönlichen Daten der Empfänger von Arbeitslosengeld II 110
7.1.1 Vorlage von Kontoauszügen 110
7.1.2 Mehrbedarf für kostenaufwändige Ernährung 110
7.1.3 Speicherung von Gesundheitsdaten 111
7.1.4 Datenerhebung beim potenziellen Arbeitgeber 111
7.1.5 Datenerhebung beim Vermieter 111
7.1.6 Daten auf dem Flur 112
7.1.7 Datenerhebung bei Selbstständigen 112
7.1.8 Datenzugriff im Verfahren A2LL 112
7.2 Sozialdatenschutz im Verfahren zur Feststellung einer Behinderung 114
7.3 Kontendatenabruf durch Sozialleistungsträger 115
7.4 Prüfung des Verfahrens Open/Prosoz 116
7.4.1 Erstellung eines IT-Sicherheitskonzepts 117

7.4.2 Verschlüsselung sensitiver Daten....117
7.4.3 Sicherung der Arbeitsplatzcomputer....117
7.4.4 Passwortgestaltung....118
7.4.5 Protokollierung von Nutzerzugriffen....118
7.5 ELENA-Verfahren....119

8 Wirtschaft....120

Umsetzung der europäischen Dienstleistungsrichtlinie....120

9 Umwelt, Gesundheit und Verbraucherschutz....122

9.1 Novellierung des Krankenhausgesetzes....122
9.2 Kinder- und Jugendgesundheitsdienstverordnung....123
9.2.1 Verordnung....124
9.2.2 Fragebögen....124
9.2.3 Handbuch....125
9.2.3.1 Untersuchungen von Dreijährigen....125
9.2.3.2 Betreuungscontrolling....126
9.2.3.3 Vorgehen nach der Meldung einer Nichtteilnahme an Früherkennungsuntersuchungen....127
9.3 Kontrolle der Zentralen Stelle Einladungs- und Rückmeldewesen....128
9.4 Babybegrüßungsdienste....130
9.5 Weitergabe von Daten Krankenversicherter an Lieferanten....132

10 Finanzen....133

10.1 Neues Finanzmanagement in der Landesverwaltung....133
10.1.1 Datenschutzrechtliche Anforderungen bei der Einführung des gemeinsamen Verfahrens....133
10.1.2 Erarbeitung und Umsetzung des Sicherheitskonzepts....135
10.1.3 Kontrolle der SAP-Leitstelle im Ministerium der Finanzen....137

11 Landtag....139

Auskünfte und Akteneinsicht für Mitglieder des Landtags....139

Teil B
Akteneinsicht und Informationszugang

1 Brennpunkt der Akteneinsicht: Veröffentlichung der Empfänger von Agrarsubventionen 141

1.1 Ausgangslage 141
1.2 Transparenzinitiative der Europäischen Kommission 141
1.3 Agrar- und Fischereifonds-Informationen-Gesetz 142
1.4 Gerichtsverfahren 142
1.5 Ergebnis 144

2 Entwicklung des Informationszugangsrechts in Brandenburg 145

2.1 Verbraucherinformationsgesetz 145
2.2 Zunehmende Rechtszersplitterung 146
2.3 Defizite im Akteneinsichts- und Informationszugangsgesetz 148

3 Einsicht in Verträge zwischen öffentlichen und privaten Stellen 149

4 Eigenbetriebe unterliegen dem Recht auf Akteneinsicht 151

5 Tierversuche – ein streng geschütztes Unternehmensgeheimnis 151

6 Genehmigung für die Landung von Wasserflugzeugen 153

Teil C
Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle 156

2 Zusammenarbeit mit dem Landtag 157

3 Kooperation mit den behördlichen Datenschutzbeauftragten 159

4 Zusammenarbeit mit anderen Datenschutzbehörden 159

5 Arbeitskreis Medien 160

6 Informationsfreiheitsbeauftragte.....161

7 Öffentlichkeitsarbeit.....162

7.1 Internationales Symposium zum Umweltinformationszugang 162
7.2 Veranstaltungen der Landesbeauftragten.....163
7.3 Bürgersprechstunden 164
7.4 Fortbildungsangebote.....165
7.5 Neue Publikationen der Landesbeauftragten.....166

Anlagen

1 Auszug aus dem Geschäftsverteilungsplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) 169

2 Aktenplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA) 173

3 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder 174

3.1 78. Konferenz vom 8. bis 9. Oktober 2009 in Berlin 174
3.1.1 Datenschutzdefizite in Europa auch nach Stockholmer Programm 174
3.1.2 Aktueller Handlungsbedarf beim Datenschutz - Förderung der Datenschutzkultur 175
3.1.3 Krankenhausinformationssysteme datenschutzgerecht gestalten! 177
3.1.4 Staatsvertrag zum IT-Planungsrat - Datenschutz darf nicht auf der Strecke bleiben 177
3.1.5 „Reality-TV“ - keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen 178
3.1.6 Kein Ausverkauf von europäischen Finanzdaten an die USA! 179
3.2 Entschließung zwischen der 77. und 78. Konferenz vom 16. April 2009 180
Datenschutz beim vorgesehenen Bürgerportal unzureichend 180
3.3 77. Konferenz vom 26. bis 27. März 2009 in Berlin 182
3.3.1 Die polizeiliche Datenverarbeitung in INPOL hat keine Rechtsgrundlage 182
3.3.2 Defizite beim Datenschutz jetzt beseitigen! 183
3.3.3 Eckpunkte für ein Gesetz zum Beschäftigtendatenschutz 184
3.3.4 Auskunftsanspruch der Steuerpflichtigen im Besteuerungsverfahren gewährleisten! 185
3.4 Entschließung zwischen der 76. und 77. Konferenz vom 18. Februar 2009 186
Stärkung der IT-Sicherheit - aber nicht zu Lasten des Datenschutzes! 186
3.5 76. Konferenz vom 6. bis 7. November 2008 in Bonn 188
3.5.1 Gegen Blankettbefugnisse für die Software-Industrie 188

3.5.2 Elektronische Steuererklärung sicher und datenschutzgerecht gestalten 189
3.5.3 Steuerungsprogramme der gesetzlichen Krankenkassen datenschutzkonform gestalten 190
3.5.4 Adress- und Datenhandel nur mit Einwilligung der Betroffenen 191
3.5.5 Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen 192
3.5.6 Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren 193
3.5.7 Datenschutzgerechter Zugang zu Geoinformationen 195
3.5.8 Besserer Datenschutz bei der Umsetzung der „Schwedischen Initiative“ zur Vereinfachung des polizeilichen Datenaustausches zwischen den EU-Mitgliedstaaten geboten 196
3.5.9 Angemessener Datenschutz bei der polizeilichen und justiziellen Zusammenarbeit in der EU dringend erforderlich 197
3.5.10 Mehr Transparenz durch Informationspflichten bei Datenschutzpannen 199
3.6 Entschließung zwischen der 75. und 76. Konferenz vom 16. September 2008 200
Entschlossenes Handeln ist das Gebot der Stunde 200
3.7 75. Konferenz vom 3. bis 4. April 2008 in Berlin 202
3.7.1 Medienkompetenz und Datenschutzbewusstsein in der jungen „online-Generation“ 202
3.7.2 Keine Daten der Sicherheitsbehörden an Arbeitgeber zur Überprüfung von Arbeitnehmerinnen und Arbeitnehmern 203
3.7.3 Datenschutzförderndes Identitätsmanagement statt Personenkennzeichen 204
3.7.4 Unzureichender Datenschutz beim deutsch-amerikanischen Abkommen über die Zusammenarbeit der Sicherheitsbehörden 206
3.7.5 Keine Vorratsspeicherung von Flugpassagierdaten 207
3.7.6 Mehr Augenmaß bei der Novellierung des BKA-Gesetzes 208
3.7.7 Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten 210
3.7.8 Berliner Erklärung: Herausforderungen für den Datenschutz zu Beginn des 21. Jahrhunderts 212

4 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland 214

4.1 19. Sitzung am 16. Dezember 2009 in Hamburg 214
„Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen!“.....214
4.2 18. Sitzung am 23./24. Juni 2009 in Magdeburg.....214
4.2.1 „Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern“.....214
4.2.2 „Informationszugang für Bürgerinnen und Bürger verbessern!“ 215
4.3 Entschließung zwischen der 17. und 18. Sitzung vom 26. Januar 2009 216
„Keine weitere Einschränkung der Transparenz bei Finanzaufsichtsbehörden“ 216
4.4 17. Sitzung am 3./4. Dezember 2008 in Schwerin 217
„Die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich unterzeichnen und ratifizieren!“ 217
4.5 Entschließung zwischen der 16. und 17. Sitzung vom 30. Juni 2008.....218
„Die Europäische Union braucht nicht weniger, sondern mehr Transparenz“.....218
4.6 16. Sitzung am 11. Juni 2008 in Saarbrücken 219
„Transparenz in der Finanzverwaltung“ 219

5 Übersicht aller Orientierungshilfen der Datenschutzbeauftragten 220

6 Abkürzungsverzeichnis 222

7 Stichwortverzeichnis.....226

Verzeichnis der öffentlichen Stellen **Gliederungspunkt**

Amt für Statistik Berlin-Brandenburg ..... A 4.5.1
A 6.4

Brandenburgischer IT-Dienstleister ..... A 4.5.3
A 4.5.4
A 4.5.6

Gebühreneinzugszentrale ..... A 3.1

Generalstaatsanwaltschaft ..... A 4.1.1

Landesamt für Verbraucherschutz, Landwirtschaft und Flurneuordnung ..... B 2.1

Landesgesundheitsamt Brandenburg ..... A 9.3

Landesinstitut für Schule und Medien Berlin-Brandenburg ..... A 1.2.1

Landtag ..... A 11

Ministerium der Finanzen ..... A 4.6.4

Ministerium der Justiz ..... A 5.1
A 5.2
A 5.5
A 9.2.1

Ministerium des Innern ..... A 1.2.1
A 4.5.1
A 4.5.5
A 4.6.1
A 4.6.3

Ministerium für Bildung, Jugend und Sport ..... A 1.2.1
A 6.1
A 6.2
A 6.4
A 9.2.3.1

Ministerium für Umwelt, Gesundheit und Verbraucherschutz (Gesundheit) ..... A 9.1
A 9.2.1
A 9.2.3
A 9.3

Ministerium für Umwelt, Gesundheit und Verbraucherschutz (Verbraucherschutz) ..... B 2.1

Polizei ..... A 5.5

Rundfunk Berlin-Brandenburg ..... A 3.1

Staatliches Schulamt ..... A 6.1
A 6.2

Staatsanwaltschaft ..... A 5.4
A 5.5

Verfassungsschutz ..... A 4.2

Zentraldienst der Polizei ..... A 4.1.1

Zentrale Bußgeldstelle der Brandenburgischen Polizei ..... A 4.1.4
A 4.1.5

Einleitung

Sowohl Unternehmen als auch öffentliche Stellen wiesen im Berichtszeitraum teilweise erhebliche Defizite bei der Einhaltung des Datenschutzes auf. Vielfach wurde auf erforderliche Schutzmaßnahmen für den sicheren Einsatz moderner Technologien bei der Datenverarbeitung verzichtet. Resultat dieser Versäumnisse waren die gravierenden Datenpannen in den beiden zurückliegenden Jahren: In großem Maßstab gelangten die Daten von Telefonkunden, Kontodaten sowie teils sehr persönliche Informationen aus sozialen Netzwerken in falsche Hände. Die in der Öffentlichkeit zu Recht heftig diskutierten Skandale lediglich als fahrlässige, organisatorische Missstände zu betrachten, würde der Realität allerdings nicht gerecht. Dies beweisen die bekannt gewordenen Überwachungsmaßnahmen, mit denen insbesondere Arbeitnehmer – zum Teil mit Hilfe eigens hierfür beauftragter Detekteien – bewusst und in rechtswidriger Weise ausgekundschaftet, ihre Gesundheitsdaten erhoben und die Verbindungsdaten ihrer Telefonate ausgewertet wurden. Zwar standen zunächst die Datenschutzverstöße von Unternehmen im Mittelpunkt, doch gerieten auch Versäumnisse öffentlicher Stellen bald in das Zentrum der Aufmerksamkeit. So gelangten beispielsweise Daten Arbeitssuchender rechtswidrig an Dritte, kamen tragbare Computer der Verwaltungen abhanden und waren Meldedaten brandenburgischer Bürgerinnen und Bürger öffentlich zugänglich.

Personenbezogene Daten werden von vielen Unternehmen als lukrative Waren gehandelt, gleichzeitig die Daten der Arbeitnehmer in zunehmendem Maße für Zwecke der Überwachung verwendet. Der Bund und die Länder richten zentrale Datenbanken ein. Beispielsweise sollen durch das Verfahren ELENA die Lohn- und Gehaltsdaten aller Beschäftigten und in dem geplanten Bundesmelderegister die Informationen aus den Melderegistern zentral zusammengeführt und verarbeitet werden. Wie jede Datenbank bergen auch diese ein Sicherheits- bzw. Missbrauchsrisiko und bedürfen deshalb sorgfältiger Schutzvorkehrungen.

Sowohl in der Wirtschaft als auch in Politik und Verwaltung ist das Bewusstsein für den Datenschutz nicht ausreichend ausgeprägt. Teilweise fehlt die Bereitschaft, auch einen Preis dafür zu zahlen – sei es in finanzieller Hinsicht oder durch die Einschränkung der eigenen Möglichkeiten zur Kontrolle und Steuerung. Das Bundesverfassungsgericht zeigt in seinen jüngsten Entscheidungen deutlich die datenschutzrechtlichen Grenzen staatlichen Handelns auf. Bei-

spielsweise sei an dieser Stelle auf die Entscheidungen zur automatisierten Erfassung von Kennzeichen sowie zur Videoüberwachung im Straßenverkehr oder auf die Beschlüsse zur Vorratsdatenspeicherung verwiesen.[1] Welche Bedeutung die Grundsätze der Transparenz und Nachvollziehbarkeit für den Datenschutz haben, zeigen die Entscheidungen zur Stärkung des Auskunftsanspruchs Steuerpflichtiger gegenüber dem Finanzamt sowie zum Einsatz von Wahlcomputern.[2] Ein Vierteljahrhundert, nachdem das Bundesverfassungsgericht mit dem Volkszählungsurteil feststellte, dass sich der Datenschutz – das „Recht auf informationelle Selbstbestimmung" – aus dem Grundgesetz ableitet, befasste es sich im Rahmen einer Beschwerde gegen die Vorschriften im Verfassungsschutzgesetz von Nordrhein-Westfalen mit der dort vorgesehenen Online-Durchsuchung. Im Ergebnis entwickelte es einen Anspruch auf die Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme aus dem allgemeinen Persönlichkeitsrecht.[3] Mit seinen Entscheidungen hat das Bundesverfassungsgericht den Grundrechtscharakter des Datenschutzes weiter gestärkt und die Schranken moderner Datenverarbeitung aufgezeigt. Parlamente und Verwaltungen sind aufgefordert, die Balance zwischen technologischer Machbarkeit und individuellen Grundrechten stärker als bisher zu halten.

Auch in brandenburgischen Verwaltungen besteht noch ein hoher Bedarf, das Grundrecht auf Datenschutz im Sinne dieser Balance umzusetzen. Meine Umfrage in der Kommunalverwaltung des Landes hat gezeigt, dass insbesondere die Sicherheit von IT-Verfahren, mit denen personenbezogene Daten verarbeitet werden, oft nur unzureichend gewährleistet ist. Gerade öffentliche Stellen, denen ihre Daten anzuvertrauen die Bürgerinnen und Bürger meist verpflichtet sind, tragen auf diesem Gebiet eine besondere Verantwortung. Ich betrachte es als meine wichtigste Aufgabe, die öffentlichen Stellen des Landes Brandenburg zusammen mit meinen Mitarbeiterinnen und Mitarbeitern soweit wie möglich dabei zu unterstützen, dieser Verpflichtung gerecht zu werden.

---

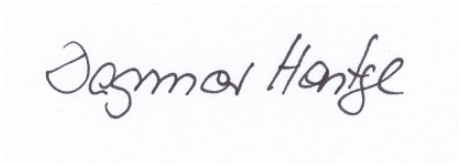
1 Urteile des Bundesverfassungsgerichts vom 11. März 2008 (Kennzeichenerfassung, 1 BvR 2074/05, 1BvR 1254/07) sowie vom 11. August 2009 (Videoüberwachung, 2 BvR 941/08) sowie Beschlüsse des Bundesverfassungsgerichts zur Vorratsdatenspeicherung vom 11. März und 28. Oktober 2008 (1 BvR 256/08)

2 Beschluss des Bundesverfassungsgerichts vom 10. März 2008 (Auskunftsanspruch, 1 BvR 2388/03) sowie Urteil des Bundesverfassungsgerichts vom 3. März 2009 (Wahlcomputer, 2 BvC 3/07, 2BvC 4/07)

3 Urteil des Bundesverfassungsgerichts vom 27. Februar 2008 (Online-Durchsuchung, 1 BvR 370/07)

Dieser Bericht informiert über meine Tätigkeit auf den Gebieten des Datenschutzes und der Informationsfreiheit in den Jahren 2008 und 2009. Allen Leserinnen und Lesern wünsche ich eine interessante Lektüre.

Kleinmachnow, den 22. März 2010



Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

Teil A

Datenschutz

1 Brennpunkte des Datenschutzes

1.1 Umfrage zum Stand des Datenschutzes und der IT-Sicherheit in der Kommunalverwaltung

Der zunehmende Einsatz von Informationstechnik in der Verwaltung und der wachsende Automatisierungsgrad der Verwaltungsprozesse stellen hohe Anforderungen an Datenschutz und IT-Sicherheit. Die im Berichtszeitraum durchgeführte Umfrage gibt erstmals einen landesweiten Überblick über den Stand der Umsetzung des Brandenburgischen Datenschutzgesetzes in der Kommunalverwaltung des Landes.

Die Landesbeauftragte hat im Zeitraum vom 5. Mai bis 9. Oktober 2009 eine Umfrage zum Thema Datenschutz und IT-Sicherheit in der Kommunalverwaltung des Landes Brandenburg durchgeführt. Deren Ziel war es, den Bedarf an Unterstützung im Bereich des Datenschutzes und der IT-Sicherheit im Flächenland Brandenburg zu ermitteln und daraus Empfehlungen und mögliche Unterstützungsleistungen, z. B. Beratungs- und Schulungsangebote, abzuleiten. Die Ergebnisse der Umfrage sollten von vornherein nicht als Grundlage für zusätzliche Kontrollen und Aufsichtsmaßnahmen genutzt werden. Der Ansatz einer allgemeinen Umfrage zur Erhebung des Ist-Zustandes des Datenschutzes und der IT-Sicherheit ermöglichte einen höheren Informationsgewinn als eine stichprobenartige Prüfung nur einzelner Kommunen.

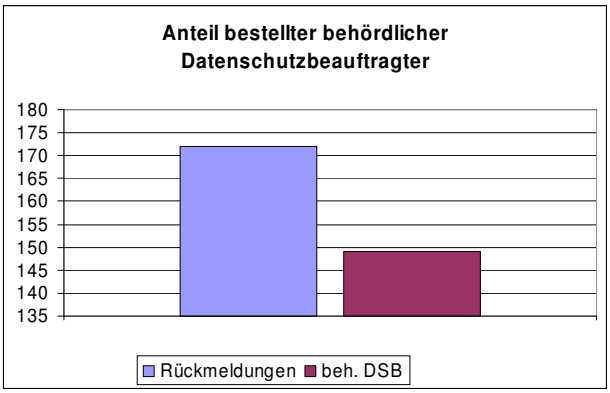
Die Erhebung enthielt Fragen zum Personaleinsatz hinsichtlich des behördlichen Datenschutz- und des IT-Sicherheitsbeauftragten, zur organisatorischen Umsetzung des Datenschutzes und der IT-Sicherheit, zur Verfahrensbeschreibung und zu technischen Aspekten der IT-Sicherheit, Fragen zur IT-Infrastruktur sowie zu der gewünschten Unterstützung seitens der Landesbeauftragten. Von den 216 befragten Kommunen des Landes Brandenburg haben bis zum Stichtag ca. 80% geantwortet.

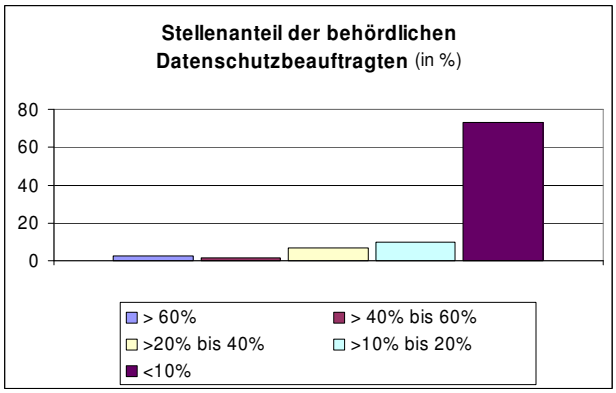
Unsicherheit bei der Beantwortung des versandten Fragebogens löste der Städte- und Gemeindebund Brandenburg e. V. aus. Er gab den Kommunen die Empfehlung, Teile des Fragebogens nicht zu beantworten, da diese nach seiner Auffassung nicht der Aufsichtsfunktion der Landesbeauftragten unter-

lägen. Dies erfolgte ohne vorherige Rücksprache mit uns. Die Landesbeauftragte legte daraufhin allen Kommunen ihre Rechtsposition ausführlich dar und wies insbesondere auf die Auskunfts- und Unterstützungspflicht nach § 26 Brandenburgisches Datenschutzgesetz (BbgDSG) hin. Im Ergebnis führten die Aktivitäten des Städte- und Gemeindebundes sowohl zu einer erheblichen Verzögerung der Umfrage als auch zu teils inkonsistenten (weil unvollständigen) Antworten der Kommunen.

Nachfolgend werden die wichtigsten Resultate der Auswertung unserer Umfrage dargestellt. Ausführlichere Informationen – auch angepasst an die Größe der jeweiligen Verwaltung – stehen auf der Website der Landesbeauftragten zur Verfügung. Die im Folgenden genannten Anteile vom Hundert beziehen sich auf die Gesamtheit der bei uns eingegangenen Antworten.

Die Betrachtung der Umfrageergebnisse zeigt ein sehr differenziertes Bild bei der Wertigkeit und Umsetzung des Datenschutzes in den einzelnen Kommunalverwaltungen. So haben zwar ca. 80% der Kommunen einen behördlichen Datenschutzbeauftragten berufen, jedoch wendet dieser auch in fast 80% aller Fälle nur höchstens 10% der regelmäßigen Arbeitszeit für diese Aufgabe auf.

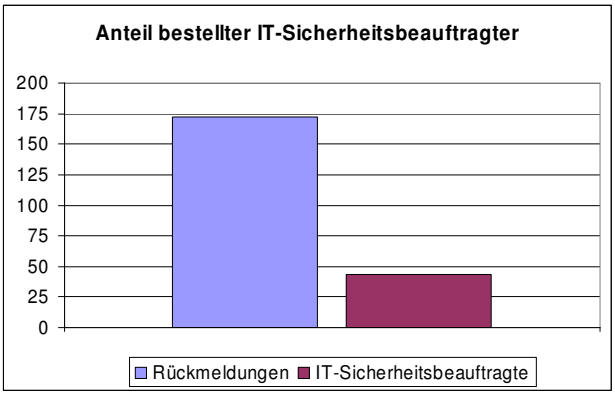


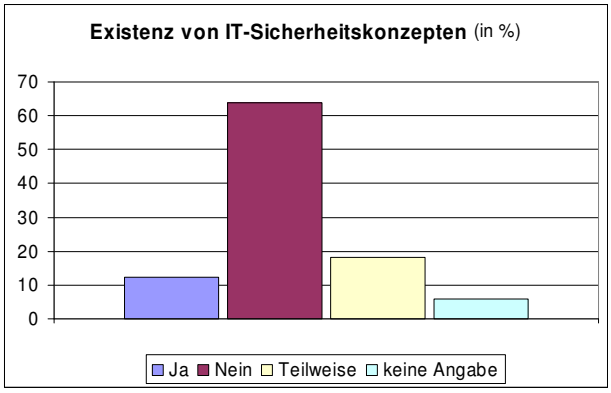


Zwar ist der Arbeitsaufwand eines behördlichen Datenschutzbeauftragten in einer kreisfreien Stadt oder einem Landkreis nicht mit dem eines Kollegen in einer Gemeinde- oder Amtsverwaltung mit 20 Mitarbeitern vergleichbar. Angesichts seines umfangreichen Aufgabenspektrums ist jedoch zu bezweifeln, ob der genannte Stellenanteil ausreicht. Im Rahmen seiner Tätigkeit soll der behördliche Datenschutzbeauftragte auf die Einhaltung der Datenschutzvorschriften hinwirken, die Daten verarbeitende Stelle bei der Umsetzung der nach § 7 Abs. 3 BbgDSG und nach den §§ 8, 10, 11, 11a, und 26 BbgDSG erforderlichen Maßnahmen beraten und unterstützen sowie die Vorabkontrolle nach § 10a BbgDSG vornehmen. Einen Schwerpunkt der Arbeit des behördlichen Datenschutzbeauftragten nimmt die Schulung der Mitarbeiter ein. Die Verarbeitung von personenbezogenen Daten in den Fachverfahren der Verwaltung erfordert schließlich ein hohes Maß an Sensibilität der Beschäftig-

ten für die Einhaltung der gesetzlichen Vorgaben. Zu beachten sind Fragen der Zulässigkeit der Datenerhebung, der Datensparsamkeit, der Erforderlichkeit und Zweckbindung. Die Analyse der Risiken für die Betroffenen, die z. B. bei Verlust der Daten oder ihrer Kenntnisnahme durch Unbefugte entstehen können, ist Voraussetzung für die Festlegung geeigneter Maßnahmen zum Datenschutz. Ein Schulungsangebot des behördlichen Datenschutzbeauftragten, das diese Kriterien berücksichtigt, bildet die Grundlage für die Umsetzung des Brandenburgischen Datenschutzgesetzes in der Kommunalverwaltung.

Auch bezüglich des IT-Sicherheitsbeauftragten sind die Ergebnisse unserer Umfrage kritisch zu betrachten. Das Brandenburgische Datenschutzgesetz fordert diese Funktion zwar nicht explizit. Der Inhaber wirkt aber im Rahmen eines IT-Sicherheitsmanagements in der Verwaltung koordinierend und steuernd. Nur 25% der Kommunen besetzen zurzeit diese Position. Entsprechend zeigen sich auch die Ergebnisse bei der Realisierung von IT-Sicherheitskonzepten in der Verwaltung: Nur 12% der Kommunen gaben in der Umfrage an, ein IT-Sicherheitskonzept erstellt zu haben, 18% erfüllten diese Aufgabe teilweise. Bei mehr als 60% der Verwaltungen liegt kein IT-Sicherheitskonzept vor, welches die Gefahren, Risiken und vor allem Maßnahmen zur Wahrung der IT-Sicherheit beschreibt.

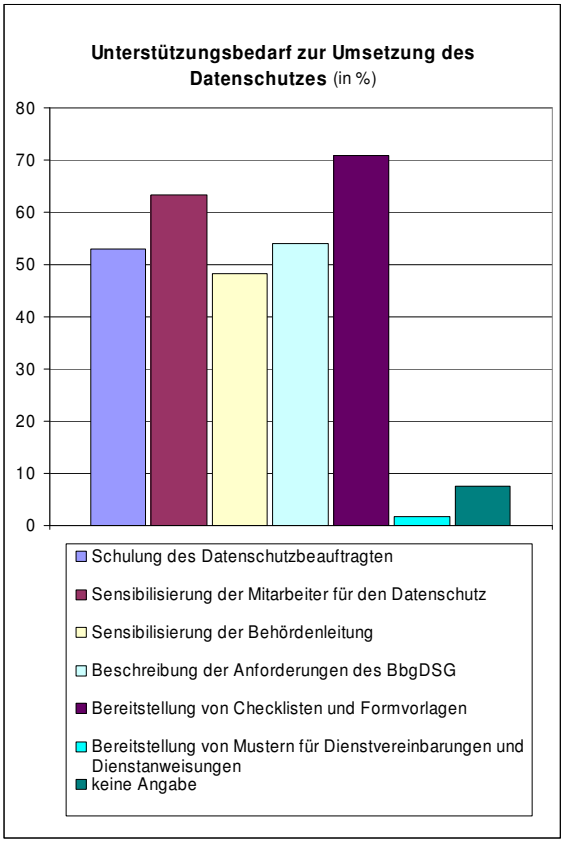


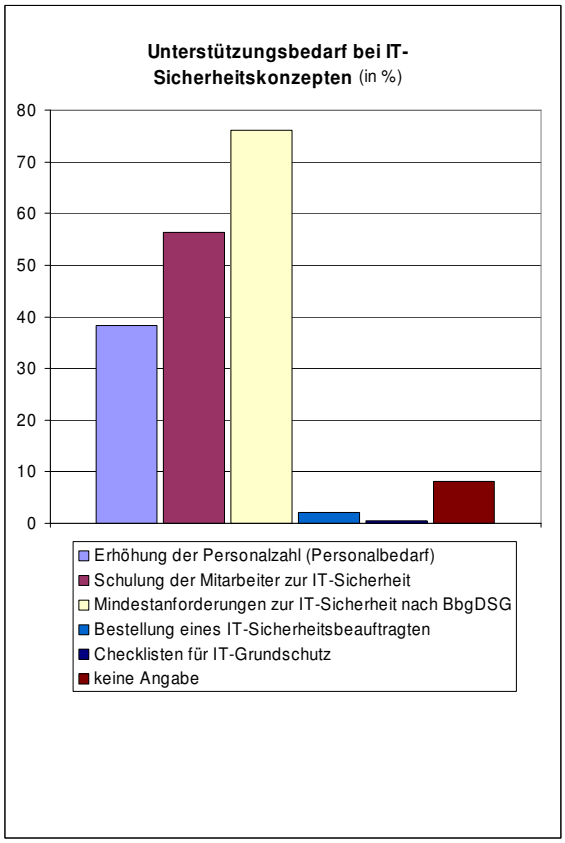


In einer Vielzahl von Kommunen fehlen nach eigenen Aussagen qualifiziertes Personal sowie zeitliche und finanzielle Ressourcen zur Umsetzung der Anforderungen an Datenschutz und IT-Sicherheit. Um dem entgegenzuwirken, wünscht der Großteil der Kommunen die Bereitstellung von Checklisten sowie eine genaue Beschreibung der Mindestanforderungen an ein IT-Sicherheitskonzept. Weiterhin werden häufig Schulungsangebote zum Datenschutz und zur IT-Sicherheit erbeten.

Ein grundlegendes Problem, nicht nur in der Kommunalverwaltung, ist die Sensibilisierung der Mitarbeiter, insbesondere der Behördenleitung. Ohne ein entsprechendes Bewusstsein für die Bedeutung des Datenschutzes und der

IT-Sicherheit lässt sich kein gesetzeskonformes Datenschutzniveau erreichen.





Die auf Basis der gesetzlichen Anforderungen durchgeführte Umfrage zeigt die bestehenden Mängel bei der Umsetzung des Brandenburgischen Datenschutzgesetzes auf. Die existierenden Vollzugsdefizite in vielen Bereichen der Kommunalverwaltung sind Ausdruck für die bestehende Unsicherheit bezüglich der Belange des Datenschutzes, aber auch der zunehmenden Aufgabenfülle der Verwaltung bei gleichzeitig knappen Ressourcen. Die Einführung neuer E-Government-Projekte stellt die Kommunen vor neue Herausforderungen. Nur die datenschutzgerechte und sichere Verarbeitung der personenbezogenen Daten auf Basis einer IT-Sicherheitskonzeption kann das Vertrauen der Bürger in die Verwaltung dauerhaft stärken. Dabei ist eine enge Zusammenarbeit zwischen der Landesverwaltung als Initiator vieler E-Government-Projekte und den Kommunen zwingend notwendig, um einheitliche Standards zu gewährleisten.

Die Landesbeauftragte beabsichtigt, den Kommunalverwaltungen die gewünschte Unterstützung zu gewähren und dabei mit dem Brandenburgischen IT-Dienstleister, der TUIV-AG (Kommunale Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg) sowie dem Netzwerk SeSamBB (Security and Safety made in Berlin-Brandenburg e. V.) zu kooperieren. Die betroffenen Kommunen sind jedoch zunächst gehalten, ihre

eigene Verantwortung zur Umsetzung des Datenschutzes wahrzunehmen. Synergieeffekte durch verwaltungsübergreifende Kooperationen sowie externe Unterstützung können insbesondere kleinen Verwaltungen helfen, fehlende Ressourcen zu kompensieren.

Durch die Auswertung der Umfrage konnten wir die Defizite der Umsetzung des Brandenburgischen Datenschutzgesetzes sowie den vorhandenen Unterstützungsbedarf in den Verwaltungen der brandenburgischen Kommunen konkret feststellen. Wir betrachten dies als einen ersten Schritt zur Verbesserung des Datenschutzes in der Kommunalverwaltung. Den Erfolg des Weiteren Prozesses werden wir mittels einer Folgeumfrage überprüfen und gegebenenfalls stichprobenartig kontrollieren.

1.2 Datenschutz im Internet beginnt an den Schulen

Der Umgang mit den neuen Medien ist ein unverzichtbarer Teil der Lebenswirklichkeit von Schülern aller Altersstufen geworden. Beschleunigt wurde diese Entwicklung nicht zuletzt durch die enorme Beliebtheit sozialer Netzwerke im Internet. Auch in unserer täglichen Arbeit hat sich das Thema zum Dauerbrenner entwickelt. Eltern, Lehrer und Schüler wenden sich regelmäßig an uns und erkundigen sich nach ihren Rechten und Pflichten.

1.2.1 Das Projekt „Datenschutz für Schüler und Lehrer“

Die Entwicklung einer Medienkompetenz brandenburgischer Schüler haben wir während des Berichtszeitraums zu einem Schwerpunkt unserer Tätigkeit gemacht. In Zusammenarbeit mit dem Ministerium des Innern hat die Landesbeauftragte das Projekt "Datenschutz für Schüler und Lehrer" erarbeitet.[4] Es besteht aus Modulen zu Themen wie Internetnutzung, Mobilfunk, Gewinnspiele und Kundenkarten, Arbeitsweise von Auskunfteien, Datenschutz bei Bewerbungsgesprächen, bei der Strafverfolgung oder beim Arzt und nicht zuletzt zu dem wichtigen Thema der Datensicherheit. Diese Bausteine stehen für den Unterricht zur Verfügung, um die Schüler für die Wahrung ihrer Persönlichkeitsrechte zu sensibilisieren. Insbesondere informieren wir im Rahmen dieses Projekts darüber, welche Gefahren sich ergeben, wenn Schüler ihre persönlichen Daten unkontrolliert über Internet oder Mobilfunk verbreiten und natürlich, wie sie diese Gefahren selbstständig reduzieren können. Sowohl rechtliche als auch technische Aspekte werden aufgezeigt.

Das Projekt haben wir anlässlich des Zweiten Europäischen Datenschutztages am 28. Januar 2008 der Öffentlichkeit vorgestellt. Auf einer zentralen

4 vgl. Tätigkeitsbericht 2006/2007, A 6.3

Podiumsdiskussion in Potsdam erörterte die Landesbeauftragte mit den Schülern die Frage „Was bedeutet Datenschutz für Jugendliche heute?“ Zeitgleich besuchten ihre Mitarbeiter zwei Schulen, um dort ebenfalls Inhalte des Projekts vorzustellen. Im Berichtszeitraum haben wir solche Veranstaltungen in Gymnasien in Eberswalde, Senftenberg, Potsdam und Frankfurt (Oder), im Oberstufenzentrum in Teltow sowie in einer Gesamtschule in Brandenburg an der Havel durchgeführt. In Kooperation mit der Universität Potsdam veranstalteten wir im Juli 2009 in deren Räumlichkeiten einen Projekttag zum Datenschutz. Die Schüler zweier Gymnasien aus Potsdam und Michendorf haben unsere Einladung zu der Veranstaltung angenommen und sich engagiert in die Diskussion eingebracht.

Sämtliche dieser Veranstaltungen haben uns gezeigt, dass viele Schüler ihre persönlichen Daten in sozialen Netzwerken, auf Bewertungsportalen, im Chat oder auch auf der eigenen Website preisgeben, in der Regel ohne sich über die Folgen ihres Handelns im Klaren zu sein. Den erstaunlich geringen Kenntnissen über Möglichkeiten zur Sicherung ihrer Privatsphäre steht aber ein großes Interesse der Kinder und Jugendlichen an Fragen des Datenschutzes auf dem Gebiet der neuen Medien gegenüber. Dies bestärkt uns in der Auffassung, dass die Vermittlung datenschutzrelevanter Medienkompetenz an den Schulen auch weiterhin erforderlich ist.

Um Multiplikatoren für unser Anliegen zu gewinnen, haben wir uns mit dem Ministerium für Bildung, Jugend und Sport sowie mit dem Landesinstitut für Schule und Medien Berlin-Brandenburg in Verbindung gesetzt. Außerdem regten wir an, die Stärkung der Medienkompetenz in die Lehrpläne aufzunehmen. Die anfangs große Resonanz und Bereitschaft zur Zusammenarbeit ließ im Laufe der Zeit leider erheblich nach.

Im Rahmen unserer Besuche an Schulen und der dort geführten Diskussionen haben wir gelernt, dass datenschutzrechtliche Themenstellungen in diesem Zusammenhang nicht isoliert behandelt werden können. Das Persönlichkeitsrecht umfasst neben dem Recht auf informationelle Selbstbestimmung (Datenschutz) noch andere Ansprüche wie zum Beispiel das Recht am eigenen Bild, das Urheberrecht oder den Schutz der persönlichen Ehre in der Öffentlichkeit. Die Fragen, welche Schüler, Eltern und Lehrer an uns richten, unterscheiden diese Rechte oft nicht. Wir nehmen dies zum Anlass, unsere Antworten an ausgewählten Beispielen darzustellen.

Ausführlichere Hinweise zur Nutzung des Internets an Schulen bieten wir in einem gesonderten Faltblatt[5] an. Außerdem enthält ein Rundschreiben des

[5] siehe http://www.lda.brandenburg.de → Informationsmaterial → Faltblätter → Schulen, Internet und Datenschutz – Tipps für Schüler, Eltern und Lehrer

Ministeriums für Bildung, Jugend und Sport[6] wichtige Einzelheiten zu diesem Thema.

1.2.2 Welche Daten und Fotos darf die Schule auf ihrer Homepage veröffentlichen?

Schulen stellen ihre Aktivitäten im Internet häufig recht umfangreich dar. Neben dem eigentlichen Unterrichtsprogramm finden sich auf deren Websites Informationen zu Wettbewerben, Projekttagen und Ähnliches. Diese Darstellungen enthalten oft auch Namen der Lehrkräfte oder der Schüler sowie Foto- und Filmaufnahmen, auf denen Personen zu sehen sind.

Die Veröffentlichung der Namen von Schülern auf der Homepage der Schule stellt eine Datenübermittlung an Dritte dar und geht über den Zweck des Erziehungs- und Bildungsauftrages der Schule hinaus. Sie ist zur Aufgabenerfüllung der Schule nicht erforderlich und deshalb nur mit schriftlicher Einwilligung der Betroffenen oder – im Falle minderjähriger Schüler – ihrer Eltern zulässig. Die Schule ist verpflichtet, in diesem Zusammenhang auf die mit einer solchen Veröffentlichung verbundenen Risiken hinzuweisen. Die Betroffenen können ihre Einwilligung jederzeit widerrufen. In diesem Fall ist die Schule verpflichtet, die Daten auf der Website zu löschen.

Anders sieht die Rechtslage im Hinblick auf die Veröffentlichung von Namen und Funktion der Lehrkräfte aus. Diese Angaben genießen nicht den weitgehenden Schutz des Rechts auf informationelle Selbstbestimmung durch die Betroffenen, da es hier um den Bezug zu ihrer dienstlichen Tätigkeit geht.[7] Die Namen der Eltern oder Schüler, die ihre Schule nach außen vertreten, sowie ihre Funktionsbezeichnungen (z. B. Schulelternsprecher oder Schülersprecher) dürfen auf der Homepage veröffentlicht werden. Die Betroffenen sollten vor der Veröffentlichung in jedem Fall informiert werden. Rechtsgrundlagen sind das Brandenburgische Schulgesetz und die Datenschutzverordnung Schulwesen.

Die Antwort auf die Frage, inwieweit Foto- und Filmaufnahmen von Schülern, Eltern oder Lehrkräften veröffentlicht werden dürfen, richtet sich nach dem so genannten Recht am eigenen Bild gemäß § 22 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Fotografie (Kunsturheberrechtsgesetz). Dieses gilt selbstverständlich auch im Internet. Eine Abbildung einzelner Personen – gleich, ob Schüler, Eltern oder Lehrer – ist ohne deren Einverständnis nicht zulässig. Die Einverständniserklärung muss schriftlich erfolgen und die Aufnahme, Verwendung und Veröffentlichung der Aufnah-

---

6 Regelungen für die rechtssichere Nutzung des Internets an Schulen – Rundschreiben 4/03 des Ministeriums für Bildung, Jugend und Sport vom 12. Mai 2003 (Amtsblatt des MBJS 2003 S. 158)

7 vgl. auch A 4.6.6

men für Zwecke der schulischen Öffentlichkeitsarbeit umfassen. Die Verwendung der Bilder sollte möglichst konkret bezeichnet werden. Der kunsturheberrechtliche Schutz greift nicht, wenn es sich lediglich um Übersichtsaufnahmen handelt, die keine Identifizierung der abgebildeten Personen erlaubt. Dies kann beispielsweise durch eine geringe Auflösung digitaler Fotografien erreicht werden.

Der Betrieb der Homepage macht die Schule zum Anbieter eines Telemediendienstes. Sie muss deshalb die Bestimmungen des Telemediengesetzes und des Rundfunkstaatsvertrages beachten. Hierzu zählen beispielsweise die Impressumspflicht, eine Datenschutzerklärung, die Vorschriften zur Protokollierung sowie die Verantwortung für externe Verweise.

1.2.3 Urheberrecht – wer hat die Rechte an den Werken von Schülern und Lehrern?

Das Urheberrecht ist ein Persönlichkeitsrecht des Urhebers und schützt dessen geistige Werke. Die Anwendung dieses komplexen Rechtsgebiets an den Schulen richtet sich vor allem nach zwei Aspekten: Wer ist Urheber des Werks und welchem Zweck dient seine Nutzung? Grundsätzlich gilt, dass die Nutzung eines Werks ohne Zustimmung des Urhebers nur in dem Maße zulässig ist, wie dies für den vorgesehenen schulischen Zweck erforderlich ist. Die urheberrechtlich relevanten Werke Schulangehöriger, die zu solchen Zwecken entstanden sind, unterliegen somit geringeren Einschränkungen als beispielsweise Werke Schulfremder, deren Veröffentlichung auch über den schulischen Rahmen hinaus vorgesehen ist.

Die Nutzungsrechte von Werken, die Schüler im Rahmen des Unterrichts geschaffen haben (z. B. Aufsätze, Plakate oder die Aufführung eines Musikstücks), liegen zu weiten Teilen bei der Schule. Gegen die Darstellung dieser Werke im schulischen Rahmen, also beispielsweise im Unterricht oder im Rahmen einer Ausstellung in den Räumen der Schule ist nichts einzuwenden. Für eine weiter gehende Veröffentlichung über den schulischen Bereich hinaus bedarf es jedoch ihres Einverständnisses. Ähnliches gilt für urheberrechtlich relevante Werke von Lehrkräften, die diese in Erledigung ihrer Dienstaufgaben geschaffen haben (z. B. Arbeitsmaterialien, Theaterstücke oder Versuchsaufbauten). Das Urheberrecht räumt den Schulen außerdem in bestimmten Grenzen eine privilegierte Nutzung von Werken Dritter für Unterrichtszwecke ein.

Das Urheberrecht gilt unabhängig von dem für die Veröffentlichung vorgesehenen Medium. Bei der Beurteilung des Zwecks der Veröffentlichung ist zu beachten, dass die Publikation auf einer öffentlich zugänglichen Seite im

Internet – im Gegensatz zu einem schulinternen Netz – immer bedeutet, dass für die Verwendung die entsprechenden Nutzungsrechte einzuholen sind.

1.2.4 Spick mich – dürfen Schüler ihre Lehrer im Internet bewerten?

Frei zugängliche Bewertungsportale im Internet sind in den letzten Jahren in Mode gekommen. So bewerten Gäste die von ihnen besuchten Hotels, Studenten ihre Professoren, Patienten die behandelnden Ärzte oder eben – auf dem Portal www.spickmich.de – Schüler ihre Lehrer. Registrierte Nutzer konnten dort ihre Bewertungen entsprechend den Schulnoten eins bis sechs abgeben. Sie waren dabei an vorgegebene Kriterien gebunden wie beispielsweise „cool und witzig“, „beliebt“ oder „guter Unterricht“. Die Gesamtnote ergab sich aus dem Durchschnitt der anonym abgegebenen Bewertungen. Die Eingabe eines Freitextes war nicht möglich, allerdings konnten die Nutzer auf einer bestimmten Seite angebliche Zitate des Lehrers eintragen. Eine betroffene Lehrerin klagte gegen das Portal, da sie sich in ihren Rechten verletzt sah. In dem viel diskutierten Fall hatten die Gerichte zwei Grundrechte gegeneinander abzuwägen: die Meinungsfreiheit der Schüler und das Persönlichkeitsrecht der Lehrerin, aus dem auch das Recht auf informationelle Selbstbestimmung abgeleitet wird.

Die Kritik an dem Bewertungsportal konzentrierte sich auf die Frage, ob dessen weltweite Abrufbarkeit im Internet zulässig war. Datenschutzrechtlich gesehen habe es sich um eine Datenübermittlung an Dritte gehandelt, die ohne Einwilligung des Betroffenen unter anderem dann zulässig ist, wenn die Empfänger der Daten ein berechtigtes Interesse an der Kenntnisnahme haben und kein Grund zur Annahme eines schutzwürdigen Interesses der Betroffenen besteht. Ein berechtigtes Interesse könne nur in Einzelfällen und allenfalls auf Seiten von Schulangehörigen bejaht werden.

Die Klage der Lehrerin blieb in allen Instanzen ohne Erfolg.[8] Die Gerichte befanden, die Bewertungen stellten Meinungsäußerungen dar, die die berufliche Tätigkeit der Lehrerin betreffen und seien deshalb nicht in gleichem Maße geschützt wie deren Privatsphäre. Eine konkrete Beeinträchtigung habe die Klägerin zudem nicht geltend gemacht. Außerdem seien die Äußerungen weder schmähend noch beleidigend. Auch ihre anonyme Abgabe mache sie nicht unzulässig. Die Meinungsfreiheit umfasse grundsätzlich das Recht, das Verbreitungsmedium frei zu bestimmen. Die Zulässigkeit der Datenübermittlung könne nur aufgrund einer Gesamtabwägung zwischen dem Persönlichkeitsschutz des Betroffenen und dem Recht auf Kommunikationsfreiheit im jeweiligen Einzelfall beurteilt werden. Im Streitfall ist die

[8] vgl. Urteile des Landgerichts Köln vom 30. Januar 2008 (28 O 319/07), des Oberlandesgerichts Köln vom 3. Juli 2008 (15 U 43/08) sowie des Bundesgerichtshofs vom 23. Juni 2009 (VI ZR 196/08)

Übermittlung der Daten nicht von vornherein unzulässig, da sie nur eine geringe Aussagekraft bzw. Eingriffsqualität haben und der Zugang zum Portal beschränkt ist.

Andere Bewertungsportale im Internet waren nicht Gegenstand des Klageverfahrens vor dem Bundesgerichtshof. Seinem Urteil sind deshalb zur Frage ihrer datenschutzrechtlichen Zulässigkeit nur Anhaltspunkte zu entnehmen. Keinesfalls stellt die Entscheidung einen Freibrief für unbegrenzte Bewertungen dar. Das Recht der Betroffenen auf informationelle Selbstbestimmung ist von allen Portalbetreibern in angemessener Weise zu beachten.

1.2.5 Welche Grenzen hat die Nutzung schulischer Rechner?

Schulen stellen – je nach Ausstattung – Computer zu unterschiedlichen Zwecken und in unterschiedlichem Umfang zur Verfügung. Die Spannbreite reicht vom rein auf den Unterricht beschränkten PC-Einsatz bis hin zum Angebot der privaten Nutzung des Internets.

Regelmäßig richten Schulen Computerarbeitsplätze für Unterrichtszwecke ein. Dieselben Rechner werden darin von mehreren Klassen zur Übung genutzt. Den Schülern sollte in diesen Fällen empfohlen werden, auf die – für die Übungszwecke im Übrigen gar nicht erforderliche – Speicherung persönlicher Angaben auf diesen Rechnern zu verzichten, da alle Schüler gleichermaßen Zugriff darauf haben. Ein gesonderter Passwortschutz ist nicht erforderlich; die Schule sollte gegebenenfalls dennoch gespeicherte Daten regelmäßig löschen. Bei der ausschließlich schulischen Nutzung gelten die allgemeinen Bestimmungen des Schul- und des Datenschutzrechtes.

Erlaubt die Schule auch die private Nutzung des Internets, wird sie zum Anbieter eines Telekommunikationsdienstes und hat die Bestimmungen des Telemediengesetzes zu beachten. Dies gilt auch, wenn die Schule ein Internet-Café für die ausschließlich private Nutzung einrichtet. Zwar sind die gesetzlichen Bestimmungen des Straf- und Jugendschutzrechts ohnehin zu beachten. Danach ist es verboten, pornografische, Gewalt verherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Allerdings kann bereits die Nutzung des Internets an einschränkende Bedingungen geknüpft werden, um eine Gefährdung von vornherein zu vermeiden. Beispielsweise darf die Schule technische Vorkehrungen treffen, um den Zugriff der Schüler auf bestimmte, durch die Schule für unbedenklich befundene Seiten zu begrenzen. Die erlaubten Seiten müssen zuvor ein Zulassungsverfahren durchlaufen, dessen Kriterien allen beteiligten Lehrkräften bekannt sein sollten. Diese relativ strikte, aber auch aufwendige Methode kommt umso eher in Betracht, je niedriger die Klassenstufe ist. Flexibler ist der Einsatz von Filterprogrammen, die Seiten mit bestimmten Inhalten sperren und deren Einstel-

lungen die Schule entsprechend der Altersstufe der Nutzer eigenständig konfigurieren kann. Darüber hinaus kann eine Aufsicht führende Lehrkraft den von den Schülern aufgerufenen Bildschirminhalt am Lehrerarbeitsplatz kontrollieren. Auch eine nachträgliche Kontrolle auf dem Wege der Protokollierung ist möglich.

Der Umfang der erlaubten privaten Nutzung des Internets und deren Bedingungen sollten in einer Nutzungsordnung festgelegt werden, die jeder Anwender zur Kenntnis nehmen muss. Soweit die oben beschriebenen Kontrollmaßnahmen vorgesehen sind, dürfen sie nur mit Einwilligung ergriffen werden. Ohne Zustimmung ist die private Nutzung des Internets nicht möglich.

Das Bewusstsein für den Datenschutz im Internet ist Teil einer Medienkompetenz, die es an den Schulen weiterhin zu stärken gilt. Eine enge Kooperation zwischen Landesregierung, Schulverwaltung und Lehrkräften ist dabei unabdingbar. Die Landesbeauftragte steht allen Beteiligten gern beratend zur Verfügung.

1.3 Zugang zu Informantendaten

„Wer hat mich angeschwärzt?“ – Eine einfache Frage, deren Beantwortung den Behörden oftmals gar nicht so leicht fällt. Was wiegt schwerer: Das Datenschutzrecht des Informanten oder das Informationsrecht des Angezeigten?

Anfragen, wie mit den Daten von Informanten umzugehen ist, erreichen uns in verlässlicher Regelmäßigkeit. Die Grundhaltungen hierzu sind durchaus unterschiedlich. Ein Teil hält Hinweise auf Missstände für unverzichtbar – erst mit deren Hilfe könne die Verwaltung rechtswidrige Zustände entdecken und Abhilfe schaffen. Solche Informationen erhalte die Behörde aber nur, wenn sie den Hinweisgebern Geheimhaltung zusichern kann. Andere vermuten von vornherein Missgunst oder Neid als Motive jener Informanten, die nicht bereit sind, sich zu erkennen zu geben. Ein Beschuldigter müsse sich vor falschen Beschuldigungen schützen können. Für beide Sichtweisen lassen sich Argumente finden; die Grenze zwischen sachlichen Hinweisen an die Verwaltung und reiner Denunziation ist in der Praxis indes fließend.

Darf nun aber eine Behörde die Identität des Informanten gegenüber dem Beschuldigten offenbaren? Dass es sich hierbei im Hinblick auf den Anzeigenden um eine datenschutzrechtliche Frage handelt, liegt auf der Hand. Die Information, um wen es sich bei dem Informanten handelt, bezieht sich allerdings nicht nur auf diesen selbst, sondern stellt auch ein auf die Person des Beschuldigten bezogenes Datum dar. Schließlich geht es um die Frage, aus

welcher Quelle die Beschuldigung stammt. Anders ausgedrückt heißt das: Bestandteil personenbezogener Daten ist immer auch die Information über ihre Herkunft.

Ein berechtigtes Schutzinteresse des Informanten besteht grundsätzlich nicht, wenn ausreichende Anhaltspunkte dafür vorliegen, dass der Informant wider besseres Wissen oder leichtfertig falsch über den Betroffenen informiert hat. Wahrheitswidrige Angaben sind für die Aufgabenerfüllung der Behörde immer kontraproduktiv; der Hinweisgeber macht sich damit gegebenenfalls sogar strafbar. Ein öffentliches Interesse, diese Straftat zu decken, besteht nicht. Außerdem ist die Identität des Anzeigenden im Falle eines strafrechtlichen Verfahrens – beispielsweise wegen falscher Verdächtigung oder Verleumdung – ohnehin offen zu legen.

1.3.1 Brandenburgisches Datenschutzgesetz

Nach § 18 Absatz 1 Brandenburgisches Datenschutzgesetz ist dem von der Datenverarbeitung Betroffenen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen. Diese Auskunftspflicht öffentlicher Stellen erstreckt sich aber nicht nur auf den Inhalt, sondern auch auf die Quelle der Daten. Sie entfällt nur, soweit die Information wegen einer speziellen Rechtsvorschrift oder wegen der überwiegenden berechtigten Interessen eines Dritten (hier also des Informanten) geheim gehalten werden müssen (Absatz 3). Dies wäre der Fall, wenn der Hinweisgeber bei Bekanntwerden seiner Identität beispielsweise Repressalien oder gar die Beeinträchtigung seiner körperlichen Unversehrtheit befürchten müsste. In den meisten Fällen haben Hinweisgeber somit kein Recht, ungenannt zu bleiben.

Verbreitet wird dieser Argumentation entgegengehalten, dass verschiedene Gerichte übereinstimmend anders entschieden hätten. Dies trifft tatsächlich zu. Allerdings handelte es sich dabei um Urteile, die in anderen Bundesländern oder auf Bundesebene getroffen wurden.[9] Ihnen lagen Datenschutzregelungen zu Grunde, die sich von denen des Brandenburgischen Datenschutzgesetzes in einem Punkt wesentlich unterscheiden: Sie verlangen nicht nur die Abwägung zwischen den entgegenstehenden Interessen des Beschuldigten und des Informanten, sondern auch eine Berücksichtigung des öffentlichen Interesses. Beispielsweise regelt § 19 Absatz 4 Bundesdatenschutzgesetz, dass die Auskunft unterbleibt, soweit ansonsten die ordnungsgemäße Aufgabenerfüllung der Behörde oder die öffentliche Sicherheit oder Ordnung gefährdet würden bzw. sonst dem Wohle des Bundes oder eines Landes Nachteile entstünden. Das Brandenburgische Datenschutzgesetz

[9] beispielsweise Urteil des Bundesverwaltungsgerichts vom 3. September 1991 (1 C 48/88) oder Urteil des Bundesverwaltungsgerichts vom 27. Februar 2003 (2 C 10.02)

enthält eine solche Regelung nicht. Die gerichtlichen Entscheidungen sind daher auf die brandenburgische Rechtslage nicht übertragbar. Ob die Behörde zur Erfüllung ihrer Aufgabe auf vertrauliche Hinweise angewiesen ist oder ob ihr diese nützlich sein können, ist für eine Abwägung auf der Grundlage des Brandenburgischen Datenschutzgesetzes nicht relevant.

1.3.2 Ordnungswidrigkeitenverfahren

In einem Verfahren zur Verfolgung von Ordnungswidrigkeiten hat der Beschuldigte ebenfalls Informationsrechte. Auf der Grundlage des § 49 Absatz 1 Ordnungswidrigkeitengesetz kann dem Beschuldigten Einsicht gewährt werden, soweit nicht überwiegende schutzwürdige Interessen Dritter entgegenstehen. Sind solche nicht zu erkennen, steht der Behörde also – anders als im Anwendungsbereich des Brandenburgischen Datenschutzgesetzes – ein Ermessen zu. Bei der Abwägung hat die Behörde auch öffentliche Interessen wie zum Beispiel eine mögliche Gefährdung der Untersuchung zu berücksichtigen. Dem Rechtsanwalt des Angezeigten hingegen steht nach § 46 Absatz 1 Ordnungswidrigkeitengesetz in Verbindung mit § 147 Strafprozessordnung in der Regel ein Anspruch auf Einsicht zu.

1.3.3 Abgabenrecht

Die für die Besteuerung anzuwendende Abgabenordnung enthält keine Regelung zum datenschutzrechtlichen Informationsanspruch des Steuerpflichtigen. In der Vergangenheit haben die Steuerbehörden stets argumentiert, die Abgabenordnung sei wegen des bewussten Verzichts des Gesetzgebers, eine solche Regelung aufzunehmen, als abschließend anzusehen. Neben der Abgabenordnung sei das Brandenburgische Datenschutzgesetz somit nicht anwendbar. Die Finanzverwaltung gewährte dem Steuerpflichtigen folglich nur nach pflichtgemäßem Ermessen Zugang zu den „eigenen“ Daten. Einer Offenlegung entgegenstehende Geheimhaltungsinteressen – wie zum Beispiel die Angewiesenheit auf vertrauliche Hinweise zum Zweck der Verfolgung von Steuerbetrug – mussten in dieser Ermessensentscheidung konsequenterweise berücksichtigt werden.

Spätestens seit das Bundesverfassungsgericht mit seinem Beschluss vom 10. März 2008[10] festgestellt hat, dass der Anspruch auf Informationen aus der eigenen Steuerakte verfassungsrechtlich geboten ist, sind aber auch hier die datenschutzrechtlichen Regelungen zu beachten, die der jeweilige Gesetzgeber vorgesehen hat. In Brandenburg gilt somit auch im Abgabenrecht der oben beschriebene Anspruch des Betroffenen nach § 18 Brandenburgisches

[10] Urteil des Bundesverfassungsgerichts vom 10. März 2008 (1 BvR 2388/03)

Datenschutzgesetz auf Zugang zu Daten, die zu seiner Person gespeichert sind.

1.3.4 Sozialrecht und Jugendhilfe

Auch im Sozialrecht besteht für den Betroffenen einer Datenverarbeitung grundsätzlich das Recht, Auskunft über die zu seiner Person gespeicherten Daten – also auch über die Identität eines Anzeigeerstatters – zu erhalten. Im Rahmen einer Abwägungsentscheidung nach § 83 Abs. 4 Zehntes Buch Sozialgesetzbuch hat die Sozialbehörde allerdings nicht nur zu prüfen, ob gegebenenfalls überwiegende berechtigte Interessen des Informanten einer Offenlegung entgegenstehen. Die Auskunftserteilung unterbleibt nach dieser Vorschrift vielmehr auch, soweit ansonsten die ordnungsgemäße Aufgabenerfüllung oder die öffentliche Sicherheit gefährdet oder dem Wohle des Bundes oder eines Landes sonstige Nachteile bereitet würden. Das öffentliche Geheimhaltungsinteresse ist im Sozialrecht somit – anders als im Anwendungsbereich des brandenburgischen Datenschutzgesetzes – Bestandteil der Ermessensausübung. Dies betrifft beispielsweise eine Sozialbehörde, die ohne einen Vertrauensschutz für außenstehende Hinweisgeber ihre Aufgaben zur Aufdeckung von Korruption oder Sozialleistungsbetrug nicht effektiv erledigen kann. Wird dem Jugendamt ein Fall von Kindeswohlgefährdung angezeigt, überwiegt aus vergleichbaren Gründen regelmäßig das öffentliche Interesse an der Geheimhaltung der Identität des Hinweisgebers. Ohne Informationen aus dem sozialen Umfeld des Kindes könnte die Behörde ihrem Schutzauftrag bei Kindeswohlgefährdungen im Sinne des § 8a Achtes Buch Sozialgesetzbuch nicht nachkommen.

1.3.5 Schweigepflicht im Gesundheitswesen

Eine Ausnahme des Regelfalls der Offenlegung von Informantendaten stellt die nach § 203 Strafgesetzbuch strafbewährte ärztliche Schweigepflicht dar. Neben den eigentlichen Ärzten richtet sie sich beispielsweise auch an Psychologen oder Sozialarbeiter in staatlich anerkannten Beratungseinrichtungen. Auch § 16 Abs. 2 Brandenburgisches Gesundheitsdienstgesetz verpflichtet alle im öffentlichen Gesundheitsdienst tätigen Personen zu besonderer Verschwiegenheit. Die Verschwiegenheitspflicht des § 55 Abs. 4 Brandenburgisches Psychisch-Kranken-Gesetz richtet sich an sämtliche Beschäftigte von Einrichtungen zur Versorgung psychisch kranker und seelisch behinderter Personen. Diese Vorschriften schützen ein fremdes Geheimnis, das einem Schweigepflichtigen in dienstlichem Zusammenhang anvertraut wurde. Auch die Identität eines Hinweisgebers kann im Einzelfall ein solches Geheimnis darstellen. Bei der ärztlichen Schweigepflicht handelt es sich um eine spezielle und damit vorrangige Rechtsvorschrift im Sinne des § 18 Abs. 3 Brandenburgisches Datenschutzgesetz.

1.3.6 Ergebnis

Die Verwaltung auf Missstände hinzuweisen, ist unzweifelhaft sinnvoll, wenn diese daraufhin beseitigt werden können. Mit Denunziation hat ein solcher Hinweis nichts zu tun – in vielen Fällen handelt es sich um einen Akt von Zivilcourage. Es ist aber nicht Aufgabe der öffentlichen Hand, durch den Vertrauensschutz von Informanten Spekulationen, falschen Verdächtigungen und neuen Streitigkeiten Vorschub zu leisten.

Die Ausführungen beziehen sich vor allem auf Anzeigen, die von Nachbarn, Bekannten oder anderen Außenstehenden an die Verwaltung gegeben werden. Soweit der Hinweisgeber keine natürliche Person, sondern eine andere Behörde ist, müssen zudem die Ausnahmen des § 18 Abs. 5 Brandenburgisches Datenschutzgesetz beachtet werden. Soweit ein Hinweis vom Verfassungsschutz, einem Nachrichtendienst, der Staatsanwaltschaft, der Polizei, von Landesfinanzbehörden oder von militärischen Behörden stammt, müssen diese Behörden einer Offenlegung in der Regel zustimmen. Diese Situation unterscheidet sich wesentlich von innerbetrieblichen oder innerbehördlichen Hinweisen, mit denen Arbeitnehmer auf rechtswidrige Zustände in ihrem eigenen beruflichen Umfeld aufmerksam machen („Whistleblower“). Hier sind Verfahren zu schaffen, die den Hinweisgeber vor ungerechtfertigten Nachteilen am Arbeitsplatz schützen.[11]

Die Frage, wie mit Informantendaten umzugehen ist, stellt sich naturgemäß nur, wenn die Behörde die Identität des Hinweisgebers kennt. Von der Problematik der Vertraulichkeit zu unterscheiden sind anonyme Hinweise. Sie sind datenschutzrechtlich nicht relevant.

Wer von einem anderen angezeigt wird, hat grundsätzlich das Recht, die Identität dieser Person zu erfahren. Informanten haben nur in Ausnahmefällen einen Anspruch auf Vertraulichkeit.

[11] Siehe auch Anlage 4.2.1: Entschließung der Konferenz der Informationsfreiheitsbeauftragten in Deutschland „Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern“ vom 24. Juni 2009

2 Technisch-organisatorische Entwicklungen

2.1 Virtualisierung – ein anhaltender Trend

Seit einigen Jahren gewinnt das Thema „Virtualisierung von Rechenressourcen“ auch in der öffentlichen Verwaltung zunehmend an Bedeutung. Die Technik verspricht eine bessere Auslastung von Hardware und einen flexibleren, kostengünstigeren IT-Einsatz. Allerdings stellen sich beim Einsatz der Virtualisierung auch neue Fragen zur Gewährleistung des Datenschutzes und der IT-Sicherheit.

Technische Grundlage der Virtualisierung ist im Allgemeinen eine spezielle Virtualisierungsschicht, welche Hardware und Betriebssystem (bzw. Applikationen) entkoppelt – meist in Form von zusätzlicher Software. Sie gestattet es, auf einem physischen Rechner (Wirtssystem) mehrere so genannte virtuelle Maschinen (Gastsysteme) einzurichten, die von außen als eigenständige Computer genutzt werden können. Grundsätzlich ist es möglich, dass die einzelnen virtuellen Maschinen mit den gleichen oder verschiedenen Betriebssystemen und/oder Applikationen ausgestattet werden. Die Virtualisierungsschicht sorgt dafür, dass die virtuellen Maschinen auf derselben Hardware zwar gleichzeitig nebeneinander, jedoch voneinander isoliert arbeiten. Sie vermittelt und koordiniert auch den Zugriff aus den einzelnen virtuellen Maschinen auf die physisch vorhandenen Hardwarekomponenten (Festplatten, Netzschnittstellen, Peripheriegeräte), falls dieser zugelassen und konfiguriert ist.

Typische Einsatzgebiete der Virtualisierung sind einerseits die Bereitstellung von Test- und Entwicklungsumgebungen für unterschiedliche Rechner- und Betriebssystemplattformen. Auch eingeschränkte Laufzeitumgebungen lassen sich hiermit gut realisieren. Andererseits ermöglicht die Virtualisierung, vorhandene Hardwareressourcen effizienter und flexibler zu nutzen. Insbesondere ist hier die Serverkonsolidierung zu nennen: Dabei werden Serverdienste, die bislang auf getrennter, jedoch meist wenig ausgelasteter Hardware angeboten wurden, in virtuelle Maschinen auf einer gemeinsamen, leistungsfähigen und nun besser ausgelasteten Hardware verlagert. Dies hilft nicht nur, die Anzahl der physischen Server zu reduzieren – auch Energie, Platz und Anschaffungskosten lassen sich einsparen. Weiterhin können virtuelle Maschinen flexibel und z. T. auch dynamisch auf vorhandene Hardwareressourcen verteilt werden. Dadurch werden kürzere Ausfall- und schnellere Wiederherstellungszeiten im Fehlerfall ermöglicht.

Die Nutzung der Virtualisierung in produktiven Umgebungen (z. B. zur Serverkonsolidierung) erfordert gesonderte Überlegungen bezüglich des Datenschutzes und der IT-Sicherheit. So ist z. B. zu gewährleisten, dass keine

unberechtigten Zugriffe zwischen den virtuellen Maschinen untereinander bzw. zwischen den einzelnen Gastsystemen und dem Wirtssystem stattfinden. IT-Sicherheitsmaßnahmen sind sowohl für das Wirtssystem als auch für jede virtuelle Maschine zu realisieren. Dabei ist zu beachten, dass sich das Gesamtschutzniveau einer physischen Komponente nach dem Maximumprinzip aus dem höchsten Schutzbedarf der auf dieser Komponente laufenden Verfahren ergibt. Es kann somit empfohlen werden, auf einer physischen Hardware nur virtuelle Maschinen bzw. DV-Verfahren mit gleichem Schutzbedarf einzurichten.

Weiterhin muss berücksichtigt werden, dass bei der Serverkonsolidierung ein neuer „Single Point of Failure“ entsteht: Fällt die physische Hardware aus, auf der eine Reihe virtueller Maschinen laufen, dann fallen auch alle diese virtuellen Maschinen aus. Dies bedeutet einen Verlust an Verfügbarkeit bzgl. der benötigten DV-Verfahren. Darüber hinaus können eine nicht ausreichend dimensionierte Hardware oder Konfigurationsfehler zu Problemen mit dem Antwortzeitverhalten und dem Datendurchsatz bei den jeweiligen virtuellen Maschinen führen. Durch geeignete Maßnahmen sind hier entsprechende Vorkehrungen zu treffen.

Zusätzliche Hinweise zum sicheren Einsatz der Virtualisierung können den Grundschutzkatalogen des Bundesamtes für Sicherheit in der Informationstechnik (Maßnahme M 2.392) entnommen werden.

Die Virtualisierung stellt Mittel für einen effizienteren und flexibleren IT-Einsatz bereit. Im Rahmen der Serverkonsolidierung müssen jedoch auch die Anforderungen des Datenschutzes und der IT-Sicherheit berücksichtigt werden. Insbesondere sind Maßnahmen zu ergreifen, die die Isolation der virtuellen Maschinen bzw. der darauf laufenden DV-Verfahren sowie deren Verfügbarkeit sicherstellen.

2.2 Cloud Computing – Rechnen in der Wolke auf eigene Gefahr?

In Zeiten leerer Kassen haben neue und kosteneffiziente technische Entwicklungen besonders gute Marktchancen. So verheißt die Idee des Cloud Computing auf den ersten Blick eine willkommene Entlastung für die Datenverarbeitung auch öffentlicher Stellen.

Mit der Einführung des Cloud Computing soll eine Form der automatisierten Datenverarbeitung etabliert werden, die es ermöglicht, komplette Geschäftsprozesse in die „Internetwolke“ zu transferieren. Die Idee besteht darin, hoch skalierbare und verwaltete IT-Infrastrukturen sowie Applikationen im Internet bereitzuhalten und deren Nutzung nach Verbrauch abzurechnen. Vom Cloud-

Dienstleister werden nicht nur die Lizenzen zur Verfügung gestellt, sondern z. B. auch Speicherplatz und Datenbanken. Damit verlagert man die Verarbeitung personenbezogener Daten in das nebulöse Internet. Die dafür erforderlichen Schlüsseltechnologien wie Virtualisierung[12] und Grid Computing sowie die Anbindung an breitbandige Internetzugänge sind verfügbar und werden bereits von verschiedensten am Markt befindlichen Cloud-Dienstleistern (z. B. Amazon, Google oder Microsoft) genutzt.

Auf den ersten Blick erweckt Cloud Computing den Eindruck eines Paradigmenwechsels in der Art und Weise, wie IT-Dienste demnächst bereitgestellt werden könnten. Informationstechnik (Hard- und Software) wird zum Gebrauchsgut wie Wasser und Strom. Diese Vorstellung manifestiert sich in den vielfach beschriebenen Vorzügen der neuen Technologie. So soll es z. B. möglich werden, IT wesentlich kostengünstiger nutzen zu können. Die Einführung von Verfahren soll dadurch beschleunigt werden, dass Hardware nicht mehr beschafft werden muss, sondern als Dienst in Form von Server-Kapazität von einem Dienstleister bezogen wird. Daraus könnten Personaleinsparungen im Bereich der Systemadministration abgeleitet werden. Hohe Flexibilität aufgrund der theoretisch unbegrenzten Skalierbarkeit der Dienste, eine rasche Anpassung an veränderte Anforderungen sowie die verbrauchsabhängige Abrechnung inkl. kurzer Vertragslaufzeiten sind oft genannte Argumente.

Dem gegenüber stehen jedoch erhebliche Bedenken hinsichtlich der Umsetzung technischer und organisatorischer Sicherheitsmaßnahmen sowie deren Nachvollziehbarkeit für die an die Cloud übergebenen personenbezogenen Daten. Cloud Computing impliziert eine hohe Komplexität durch verteilte Strukturen. Die Daten werden üblicherweise nicht ortsbezogen vom Vertragspartner verarbeitet, sondern weltweit von mehreren unterschiedlichen Servern oder Server-Farmen, die einem oder auch unterschiedlichen Anbietern gehören. Der Vertragspartner (Cloud-Dienstleister) greift in der Regel über Virtualisierungstechniken auf die weltweit verteilten physischen Server zu und verwaltet sie wie eigene Maschinen. Es entstehen komplexe Vertragsverhältnisse, deren rechtliche Anforderungen – insbesondere die datenschutzrechtlichen Rahmenbedingungen – zu klären sind.

Eine öffentliche Stelle des Landes Brandenburg, die personenbezogene Daten mittels Cloud-Diensten verarbeitet, bleibt gem. § 11 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) als auftraggebende Stelle für die Einhaltung der Bestimmungen des BbgDSG und anderer Vorschriften über den Datenschutz verantwortlich. Finden die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung (z. B. bei nicht-öffentlichen Stellen),

[12] vgl. auch A 2.1

hat der Auftraggeber vertraglich sicherzustellen, dass der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und jederzeit von ihm veranlasste Kontrollen ermöglicht. Der Auftraggeber ist auch für die Sicherstellung der Vertraulichkeit und Integrität der personenbezogenen Daten verantwortlich. Dieser Verantwortung kann er auf Basis der etablierten Cloud-Strukturen im Allgemeinen jedoch nicht gerecht werden, zumal Dienste angeboten werden (z. B. Google Apps) bei denen der Dienstleister selbst keine Auskunft über den Ort der Datenverarbeitung geben kann. Vor dem Hintergrund der hohen Internationalisierung und Globalisierung der Clouds, inkl. der unterschiedlichen Qualitätsstandards bezüglich Datensicherheit und Datenschutz, ist zurzeit an eine datenschutzgerechte Datenverarbeitung in der Wolke nicht zu denken. Erst wenn wirksame und durchgängige Sicherheitsarchitekturen entwickelt worden sind und ein einheitliches Schutzniveau für die Verarbeitung der personenbezogenen Daten existiert, sind globale Cloud-Dienste für öffentliche Stellen vorstellbar.

Auf internationaler Ebene hat sich die Cloud Security Alliance (CSA)[13] gegründet. Diese Organisation hat sich u. a. zum Ziel gesetzt, Richtlinien für sicheres Cloud Computing zu erarbeiten. Die CSA hat bereits ein erstes Papier[14] dazu herausgegeben.

Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder befasst sich in Zusammenarbeit mit den Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, dem Düsseldorfer Kreis, mit den damit verbundenen datenschutzrechtlichen Problemen und wird Lösungsansätze erarbeiten.

Da die Einhaltung der Vorschriften des Brandenburgischen Datenschutzgesetzes mit den aktuell am Markt befindlichen Cloud-Systemen nicht gewährleistet werden kann, ist von der Verarbeitung personenbezogener Daten in der Internetwolke dringend abzuraten.

2.3 Tracking Tools – Ich kenn' dich besser als du denkst!

Tracking Tools („Verfolgungswerkzeuge") versetzen den Betreiber einer Website in die Lage, detaillierte Informationen über das Navigationsverhalten sowie Angaben zur technischen Ausstattung der Besucher zu erlangen. So wertvoll die Daten für einen Betreiber sind, so eindeutig sind die gesetzlichen Anforderungen an derartige Tools.

13 siehe http://www.cloudsecurityalliance.org

14 siehe http://www.cloudsecurityalliance.org/csaguide.pdf (Security Guidance for Critical Areas of Focus in Cloud Computing)

Die aus der Protokollierung des Besuchs der Website gewonnenen Informationen dienen vor allem dem Zweck der bedarfsgerechten Gestaltung des Webangebots aber auch der Marktforschung und Werbung. Am Markt haben sich sowohl unentgeltliche (z. B. Google – Google Analytics)[15] als auch kostenpflichtige (z. B. etracker – Web Analytics)[16] Werkzeuge etabliert, die in der Lage sind, umfängliche Daten über die Besucher zu liefern.

Betreiber von Websites – das können auch öffentliche Stellen sein – die sich für das kostenfreie Google Analytics Tool entscheiden, erheben die gewünschten Daten mit einem im Browser des Besuchers ausgeführten JavaScript-Programms, dem Google Analytics Code (GAC). Der GAC selbst ist nicht Bestandteil der zu analysierenden Website. Er wird durch die Einbindung eines Tracking Codes (ebenfalls JavaScript-Programm) auf derselben vielmehr erst auf den Rechner des Besuchers geladen. Umfang und Inhalt der erhobenen Daten sind für ihn nicht nachvollziehbar. Ferner hinterlegt der GAC einen Cookie auf dem Zielrechner, der den Website-Besucher mittels einer eindeutigen Identifikationsnummer kenntlich macht. Die gesammelten Informationen werden an einen Google-Server in die USA übertragen, dort verarbeitet sowie ggf. an Dritte weitergeleitet. Dem Website-Betreiber werden die gesammelten Daten aufbereitet und mittels Berichten über das Surf-Verhalten der Besucher zur Verfügung gestellt.

Eine Zusammenführung mit Nutzungsdaten anderer Google-Dienste ist nicht ausgeschlossen. Das Unternehmen gewinnt dadurch von vielen Surfern im Internet detaillierte Nutzungs- und Interessenprofile, die für Werbezwecke verwendet werden können. Der Surfer selbst merkt nicht, dass er „getrackt“ wird. Das liegt im Wesentlichen an dem fehlenden Hinweis zum Einsatz des Tools. Gemäß den Allgemeinen Geschäftsbedingungen von Google Analytics ist der Website-Betreiber zwar verpflichtet, an prominenter Stelle darauf hinzuweisen, dass ein Cookie gesetzt wird, die erzeugten Informationen (einschließlich der IP-Adresse) an einen Google-Server in den USA übertragen und dort verarbeitet sowie die Daten ggf. an Dritte weitergeleitet werden. Allerdings halten sich nur wenige an diese Verpflichtung.

Generell dürfen personenbezogene Daten (dazu zählt auch die IP-Adresse) eines Nutzers nach dem Telemediengesetz (TMG) nur erhoben und verarbeitet werden, soweit dies erforderlich ist, um die Inanspruchnahme des Dienstes zu ermöglichen und abzurechnen. Da es sich aber bei der Analyse um die Verarbeitung der Daten zum Zweck der Werbung, Marktforschung und bedarfsgerechten Gestaltung der Website handelt, ist gem. § 15 Abs. 3 TMG die Verarbeitung der Nutzungsdaten zu Nutzungsprofilen höchstens unter der

[15] siehe http://www.google.de/analytics/

[16] siehe http://www.etracker.com/de/

Verwendung von Pseudonymen zulässig, sofern der Nutzer dem nicht widerspricht. Vorher ist er auf sein Widerspruchsrecht im Rahmen der Unterrichtung über die Datenverarbeitung gem. § 13 Abs. 1 TMG hinzuweisen (z. B. im Rahmen der Datenschutzerklärung). Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. Wird die vollständige IP-Adresse zur Analyse des Nutzungsverhaltens verwendet, muss eine bewusste und eindeutige Einwilligung vorhanden sein.

Die rechtliche Pflicht, den Nutzer zu informieren (Einwilligung, Widerspruch, Aufklärung), liegt bei dem Betreiber der Website. Ferner handelt es sich beim Web Tracking in der Regel um eine Datenverarbeitung im Auftrag, mit allen Pflichten, die sich aus § 11 Brandenburgisches Datenschutzgesetz ergeben.

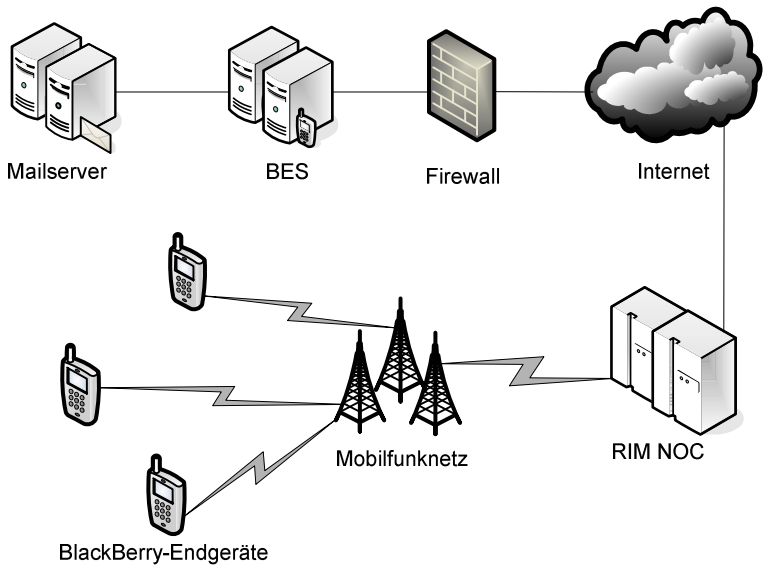
Die personenbezogene Sammlung und Auswertung von Web-Nutzungsstatistiken ist ohne Einwilligung unzulässig. Sofern der Internetnutzer nicht widerspricht, können Nutzungsdaten pseudonymisiert zum Zweck der Werbung, Marktforschung und bedarfsgerechten Gestaltung der Website verarbeitet werden. Verwendet der Betreiber einer Website Tracking Tools, muss er an prominenter Stelle seinen Informationspflichten nachkommen.

2.4 BlackBerry – Smartphones in der öffentlichen Verwaltung

In unserem letzten Tätigkeitsbericht[17] hatten wir über die erforderlichen technisch-organisatorischen Maßnahmen für die Einführung eines E-Mail-Push-Dienstes mit BlackBerry berichtet. Inzwischen werden in der Landesverwaltung BlackBerry-Dienste angeboten. Inwieweit sind die erforderlichen Sicherheitsmaßnahmen umgesetzt und der Datenschutz gewährleistet?

Das BlackBerry des Unternehmens Research in Motion (RIM) ist ein mobiles Endgerät (PDA, Smartphone), mit dem man neben Telefonie und Internet auch E-Mail-Funktionen nutzen kann. Dazu wird dem BlackBerry Enterprise Server (BES) vom Mailserver der Eingang einer Nachricht signalisiert. Der BES sendet die Information verschlüsselt via Internet an das RIM Network Operating Center (RIM NOC), das seinerseits die Nachricht über Mobilfunknetze an die BlackBerry-Endgeräte weiterleitet. Auf dem Endgerät wird die Nachricht entschlüsselt und der Benutzer kann entscheiden, was mit der E-Mail geschehen soll (z. B. lesen, löschen etc.). Eine auf dem BlackBerry-Endgerät erstellte E-Mail wird verschlüsselt über Mobilfunk an das NOC geschickt und von dort an den entsprechenden BES weitergeleitet, wo die Nachricht entschlüsselt und dem Mailserver übergeben wird.

[17] vgl. Tätigkeitsbericht 2006/2007, A 2.8



Generalisierte Darstellung einer BlackBerry-Infrastruktur

Die beim Transport genutzten kryptografischen Verfahren (3DES, AES) entsprechen dem derzeitigen Stand der Technik und sind grundsätzlich geeignet, personenbezogene Daten normalen Schutzbedarfs über Weitverkehrsnetze (z. B. Internet, GSM, UMTS) sicher zu übertragen. Für die Übertragung sensitiver personenbezogener Daten werden allerdings zusätzliche Sicherheitsmaßnahmen wie der Einsatz des von BlackBerry angebotenen S/MIME-Pakets für eine durchgängige Verschlüsselung vom Sender zum Empfänger benötigt. Der BES dient auch als zentrale Verwaltungsstelle für BlackBerry-Endgeräte. Hier können die Sicherheitspolicies an alle BlackBerrys verteilt werden, wie z. B. Regeln für den Einsatz von Benutzerpasswörtern oder für die lokale Geräteverschlüsselung. Im Notfall, z. B. bei Verlust, kann ein BlackBerry-Endgerät über den BES deaktiviert bzw. der Gerätespeicher komplett gelöscht werden.

Das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) hat im Jahre 2008 BlackBerry unter definierten Bedingungen eingehend analysiert und dafür ein Sicherheitszertifikat[18] verliehen. Zertifiziert wurden die Wahrung der Vertraulichkeit und Integrität der übertragenen Daten sowie die Unangreifbarkeit der Endgerätesoftware. Die Sicherheit der Kommunikation zwischen den getesteten BlackBerry Smartphones und BlackBerry Enterprise Servern wurde bestätigt. Das Zertifikat gilt ausschließlich für die im Zertifikatsbericht getesteten Bestandteile unter den dort genannten Bedingungen und nur in Verbindung mit dem E-Mail-Server Microsoft Exchange. Es muss jedoch betont werden, dass weder eine generelle Sicherheit für den Einsatz von BlackBerrys noch eine vollständige Risikofreiheit der getesteten Konfiguration attestiert wurde.

[18] siehe http://testlab.sit.fraunhofer.de/content/output/certificates.php?s=1

In der Landesverwaltung wird seit September 2008 ein BlackBerry-Dienst angeboten. Das heißt, es können E-Mails von den Mailservern der Verwaltung über eine BlackBerry-Infrastruktur an BlackBerry-Endgeräte bzw. umgekehrt gesandt werden. Hierzu hatten wir bereits 2006 gegenüber dem damaligen Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben als Dienstleister die erforderlichen technischen und organisatorischen Maßnahmen benannt, die Voraussetzung für den Datenschutz beim Einsatz von BlackBerry sind. Trotz mehrfacher Nachfrage liegt uns allerdings kein Sicherheitskonzept vor, in dem die notwendigen Maßnahmen systematisch festgehalten und die Umsetzung der Maßnahmen belegt ist. Nach unserem letzten Kenntnisstand entspricht z. B. die Passwortsicherheit nicht dem heutigen Sicherheitsstandard. Auch kann von den Nutzern auf den Endgeräten Fremdsoftware installiert werden. Diese Praxis birgt erhebliche Sicherheitsgefahren durch Schadsoftware. Inwieweit die übrigen von uns geforderten bzw. empfohlenen Maßnahmen zur Erhöhung der BlackBerry-Sicherheit beim Brandenburgischen IT-Dienstleister bzw. den Nutzern der Landesverwaltung berücksichtigt wurden, können wir derzeit nicht schlüssig beurteilen.

Es ist dringend erforderlich, dass eine Risikoanalyse und ein umfassendes Sicherheitskonzept für die BlackBerry-Infrastruktur in der Landesverwaltung erstellt werden, um Gefahren zu erkennen, Sicherheitsmaßnahmen festzulegen und mit Hilfe eines Realisierungsplanes zügig umzusetzen.

2.5 Telearbeit am häuslichen Arbeitsplatz

Zur Verwirklichung der Ziele einer besseren Vereinbarkeit von Beruf und Familie sowie einer effizienteren Verwaltung bedarf es auch in öffentlichen Stellen neuer Konzepte des Personaleinsatzes. Eines davon ist die Telearbeit am häuslichen Arbeitsplatz.

Der Schutz der Unversehrtheit und Vertraulichkeit von personenbezogenen Daten sowie die Sicherung der Verfügbarkeit der eingesetzten informationstechnischen Systeme ist ein wesentliches Anliegen des Datenschutzes. Bei der Telearbeit entstehen zusätzliche Risiken, denen durch Umsetzung von technischen und organisatorischen Maßnahmen begegnet werden muss. Nach dem Brandenburgischen Datenschutzgesetz (BbgDSG) ist Folgendes zu berücksichtigen:

- Der Beschäftigte bleibt weiterhin Bediensteter seiner Behörde, die betroffene Dienststelle Daten verarbeitende Stelle im Sinne von § 3 Abs. 4 Nr. 1 BbgDSG. Es findet keine Datenverarbeitung im Auftrag gem. § 11 BbgDSG statt.

- Aufgrund der erhöhten Sicherheitsrisiken dürfen grundsätzlich keine sensitiven personenbezogenen Daten auf dem Heimarbeitsplatzcomputer (Heim-APC) verarbeitet werden.

- Werden personenbezogene Daten zwischen dem Heim-APC und der jeweiligen Dienststelle übertragen, sind diese mit sicheren kryptografischen Verfahren zu verschlüsseln und digital zu signieren.

- In einer Dienstanweisung sind die erforderlichen technisch-organisatorischen Maßnahmen festzuschreiben. Der Beschäftigte muss sich schriftlich zur Einhaltung dieser geforderten Maßnahmen verpflichten.

- Die Erstellung eines IT-Sicherheitskonzeptes gem. § 7 Abs. 3 BbgDSG, in dem die zu realisierenden technischen und organisatorischen Maßnahmen konkret festgeschrieben werden, ist unabdingbar.

- Erforderlich ist der Einsatz von Virenscannern und Firewallsystemen auf dem Heim-APC.

- Es dürfen grundsätzlich nur dienstliche Arbeitsplatzcomputer (APC) eingesetzt werden. Bei der Verwendung von privaten APC sind diese von der IT-Abteilung der Dienststelle des Heimarbeiters entsprechend der im IT-Sicherheitskonzept festgeschriebenen Vorgaben zu konfigurieren.

- Der Heim-APC darf nur für dienstliche Aufgaben genutzt werden. Eine private Nutzung des Heim-APC ist aufgrund der erheblichen Risiken durch technische und organisatorische Maßnahmen auszuschließen.

- Der Heim-APC ist vor dem Zugriff Unberechtigter zu schützen, indem beispielsweise entsprechende Sicherheitssoftware bzw. -hardware installiert wird.

- Es sind nur die unbedingt erforderlichen personenbezogenen Daten auf dem Heim-APC zu verarbeiten. Personenbezogene Daten sollten nach Möglichkeit vor der Verarbeitung anonymisiert bzw. pseudonymisiert werden. Eine verschlüsselte Speicherung von personenbezogenen Daten ist zwingend erforderlich.

- Eine sichere Aufbewahrung von dienstlichen Unterlagen und Datenträgern im häuslichen Bereich muss gewährleistet sein. Familienangehörige sowie Besucher dürfen keinen Zugang zu diesen Unterlagen erhalten. Der Arbeitgeber muss deshalb bei Bedarf entsprechende Sicherungsschränke zur Verfügung stellen.

Aufgrund der in der Verfassung festgeschriebenen Unverletzlichkeit der Wohnung existieren keine rechtlichen Grundlagen zur Durchführung von Kontrollen gem. § 26 Abs. 1 Nr. 2 BbgDSG im häuslichen Bereich. Der Beschäftigte muss in entsprechende Kontrollen einwilligen. Ohne seine schriftliche Einwilligung ist die Telearbeit nicht zulässig. Gem. § 65 Nr. 4 Personalvertretungsgesetz ist das Mitbestimmungsrecht des Personalrats bei der Einrichtung von Telearbeitsplätzen zu berücksichtigen.

Bei der Nutzung von Telearbeitsplätzen entstehen Risiken, denen nur durch Realisierung von zusätzlichen technischen und organisatorischen Maßnahmen begegnet werden kann. Die Verarbeitung von sensitiven personenbezogenen Daten durch Telearbeit ist grundsätzlich nicht zulässig.

2.6 Wartung und Fernwartung

Aufgrund festgestellter Unsicherheiten und unzureichender Wartungsverträge mit externen Dienstleistern in öffentlichen Stellen greifen wir noch einmal das Thema Wartung und Fernwartung auf.

Der Trend, externe Dienstleister mit der Wartung von IT-Systemen zu beauftragen, ist nach wie vor ungebrochen. Wie unsere Umfrage unter den brandenburgischen Kommunen[19] ergeben hat, lassen ca. 70% der Kommunen IT-Technik (Soft- und/oder Hardware) durch Dritte warten. Zu Wartungsarbeiten gehören beispielsweise das Kontrollieren der Systemeinstellungen, das Installieren von Updates und Patches und die Behebung von Störungen und Fehlern. Findet die Wartung nicht vor Ort, sondern durch Fernzugriff (Remote Access) über ein Netzwerk statt, liegt eine Fernwartung vor.

Grundsätzlich gilt, dass eine Wartung gemäß § 11a Abs. 2 Brandenburgisches Datenschutzgesetz durch andere als die Daten verarbeitende Stelle nur aufgrund schriftlicher Vereinbarungen erfolgen darf. Von den Kommunen, die eine Wartung durch externe Dienstleister durchführen lassen, haben allerdings nur ca. 58% schriftliche Vereinbarungen abgeschlossen. Die rechtswidrige Praxis, Wartungsverträge nur mündlich zu verabreden, ist zügig abzustellen; entsprechende Vereinbarungen müssen schriftlich nachgeholt werden. Problematisch daran ist, dass sich Firmen im Nachhinein weigern können, notwendige Regelungen zu unterschreiben und öffentliche Stellen damit in eine Zwangslage bringen. Aus dieser können sie sich aufgrund der am Markt häufigen Verquickung von proprietären Systemen und Wartungsmonopolen u. U. nur durch einen kompletten Systemwechsel mit entsprechenden erheblichen Investitionen an Zeit, Geld und Arbeitskraft wieder befreien. Um solche Situationen von vornherein zu vermeiden, sollte bereits

[19] vgl. A 1.1

im Zuge der Einführung neuer Systeme das Thema Wartung von Anfang an berücksichtigt und mitverhandelt werden.

Kann der Zugriff auf personenbezogene Daten bei der Wartung nicht ausgeschlossen werden, sind in der Wartungsvereinbarung auch technische und organisatorische Maßnahmen festzulegen, durch die ein entsprechender Zugriff auf das unbedingt erforderliche Maß beschränkt wird. Die mit den Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten. Die Daten sind ausschließlich für Zwecke der Wartung zu verwenden und nach Abschluss der Wartungsarbeiten oder der Fehlersuche unverzüglich von den Wartungssystemen zu löschen. Jeder Wartungsvorgang darf nur mit vorheriger Zustimmung und unter Aufsicht qualifizierter Mitarbeiter der Daten verarbeitenden Stelle stattfinden.

In der schriftlichen Wartungsvereinbarung sollten darüber hinaus u. a. noch Regelungen zu folgenden Punkten getroffen werden:

- Aussagen zu Art und Umfang der Wartung,
- Bestimmungen zu Rechten und Pflichten von Auftraggeber und Auftragnehmer,
- Protokollierungspflichten bei Auftraggeber und Auftragnehmer,
- Verpflichtung des Auftragnehmers, sich an Weisungen des Auftraggebers zum Umgang mit den Daten zu halten,
- technische und organisatorische Maßnahmen zur Sicherstellung transparenter und kontrollierbarer Wartungsvorgänge und zur Wahrung des Datenschutzes vor, während und nach der Wartung,
- Recht des Auftraggebers, die Einhaltung des Datenschutzes beim Auftragnehmer zu überprüfen.

Die Regelungen in Wartungsvereinbarungen sind grundsätzlich immer an den Schutzbedarf der gewarteten Systeme und Daten anzupassen. Je höher dieser ist, desto größer sind auch die Anforderungen an Sicherheit und Kontrollierbarkeit der Wartungsvorgänge durch den Auftraggeber. Letzteres muss sich daher in den vertraglichen Vereinbarungen zwischen Auftraggeber und Auftragnehmer zur Wartung der IT-Systeme widerspiegeln.

Wartung und Fernwartung von IT-Systemen durch externe Dienstleister dürfen nur auf Basis schriftlicher Vereinbarungen erfolgen, die Regelungen zu Rechten und Pflichten von Auftraggeber und Auftragnehmer und die zu treffenden technischen und organisatorischen Maßnahmen enthalten.

2.7 Serviceportal der Landesverwaltung

Im Zuge von Verwaltungsmodernisierung und E-Government werden Verwaltungsdienstleistungen zunehmend über das Internet angeboten. Das Serviceportal der Landesverwaltung[20] vermittelt einen Zugang zu online verfügbaren Verfahren. Die technischen und rechtlichen Anforderungen werden allerdings noch nicht in vollem Umfang erfüllt.

Der Masterplan der Landesregierung sieht das E-Government als ein zentrales Zukunftsprojekt zum Auf- und Ausbau leistungsfähiger Strukturen in der staatlichen und kommunalen Verwaltung. Der prinzipiell begrüßenswerte Ansatz, Bürgern einen schnellen und unkomplizierten Online-Zugang zu diversen Verwaltungsdienstleistungen zu gewähren, birgt allerdings sowohl in technischer als auch in rechtlicher Hinsicht einige Stolpersteine:

- Vervielfachung der Gefahren für die IT- und Datensicherheit

Durch das Angebot im Internet werden Web-Schnittstellen zu Verwaltungsverfahren einem unbekannten Personenkreis über ein strukturell unsicheres Netz zugänglich. Die Gefahren für die IT- und Datensicherheit vervielfachen sich dadurch potenziell, sodass mehr technisches Wissen und Erfahrung und auch zusätzliche finanzielle Mittel erforderlich sind, um die Bedrohungen über angemessene Gegenmaßnahmen stetig abzuwehren.

- Problem der Authentisierung von Nutzern

Die in der „Offline-Welt“ relativ unproblematische Authentisierung durch Vorlage eines Personalausweises oder Passes muss im Internet mit anderen Mitteln durchgeführt werden. Nicht für alle der derzeitigen Portalanwendungen der Landesverwaltung ist die Frage der Authentisierung bei sensitiven Daten bislang hinreichend gelöst.

- Problem der Verschlüsselung

Eine lückenlose Verschlüsselung der Übertragung von personenbezogenen Daten vom Anwender zur Serviceplattform muss für alle Portalanwendungen

[20] siehe http://service.brandenburg.de

umgesetzt werden. Allerdings sind teilweise noch Defizite in der Umsetzung notwendiger Verschlüsselung feststellbar.

- Problem der datenschutzrechtlichen Verantwortlichkeiten

Es müssen alle rechtlichen Zuständigkeiten und Verantwortlichkeiten aus dem Telemediengesetz und aus dem Brandenburgischen Datenschutzgesetz klar geregelt sein. Insbesondere müssen die Daten verarbeitenden Stellen benannt sein und Verpflichtungen zur Erstellung von Sicherheitskonzepten, Verfahrensverzeichnissen und zur Freigabe von Verfahren erfüllt werden. Hier besteht dringender Handlungsbedarf.

- Fehlende Einwilligungserklärungen

Des Weiteren darf die Erhebung, Speicherung oder Übermittlung personenbezogener Daten durch die neuen Anwendungen und Plattformen im Internet nach dem Telemediengesetz in der Regel nur mit ausdrücklicher und informierter Einwilligung der Betroffenen erfolgen. Für entsprechende Einwilligungserklärungen wird auf den Portalseiten allerdings oftmals nicht in ausreichendem Maße gesorgt.

- Fehlendes Sicherheitskonzept für Basiskomponenten des Serviceportals

Obwohl E-Government-Anwendungen den Bürgern über das Serviceportal schrittweise zugänglich gemacht werden, ist uns für den Basisbetrieb des Serviceportals noch kein umfassendes Sicherheitskonzept vorgelegt worden.

In den folgenden Beiträgen stellen wir Teile des Serviceportals Brandenburg vor und beleuchten anhand dieser Beispiele einige der genannten datenschutzrechtlichen Probleme näher.

E-Government-Anwendungen dürfen den Bürgern über das Serviceportal der Landesverwaltung nur dann zugänglich gemacht werden, wenn die technischen und rechtlichen Anforderungen erfüllt sind.

2.7.1 E-Payment

Zur Bezahlung von Waren und Dienstleistungen im Internet werden sichere Bezahlsysteme benötigt, über die verschiedene Zahlungsarten wie Überweisung, Lastschrift, Kreditkartenzahlung etc. abgewickelt werden können. Für kostenpflichtige Online-Dienstleistungen wurde eine zentrale Zahlungsverkehrsplattform für Land und Kommunen entwickelt.

Verwaltungsdienstleistungen sind für Bürger oftmals gebührenpflichtig. Bei der Inanspruchnahme einer Dienstleistung vor Ort können die Gebühren bar oder mit EC-Karte bezahlt und der Zahlungsnachweis durch Quittung bzw. am EC-Kartenlesegerät umgehend erbracht werden. Werden dagegen Dienstleistungen online angeboten, müssen Zahlung und Zahlungsnachweis auf anderen Wegen erfolgen. Dafür wurde vom Brandenburgischen IT-Dienstleister die elektronische Bezahlplattform ePayBL als Service für die Landesverwaltung und die Kommunen installiert. Diese Plattform kann als Schnittstelle zwischen den Anbietern von Serviceleistungen bzw. den angeschlossenen Online-Verfahren (sog. E-Shops) und dem Haushaltsverfahren verstanden werden, in dem die entsprechenden Buchungen stattfinden. Für jeden zahlungspflichtigen Kunden wird ein Nutzerkonto mit personenbezogenen Daten wie Name, Kundennummer, Anschrift und Bankdaten in ePayBL angelegt. Informationen zu Zahlungseingängen, Rücklastschriften etc. werden vom Haushaltsverfahren an ePayBL gemeldet, wo sie dem Bewirtschafter des E-Shops zur Verfügung stehen.

Darüber hinaus beinhaltet die Bezahlplattform die Möglichkeit für automatisierte Bonitätsbewertungen und manuell geführte Blacklists. Eine Bonitätsprüfung erfolgt ausschließlich auf Basis der bereits über ePayBL durchgeführten Zahlungen des entsprechenden Kunden. Fremdanbieter wie Schufa o. ä. werden nicht in Anspruch genommen. Einen Eintrag in die Blacklist kann ein Kunde beispielsweise durch Veranlassen einer Rücklastschrift erhalten. Eine gute Bonität kann sich für einen Kunden in höheren Zahlungsgrenzen oder in der Zulassung zu anderen Zahlungsverfahren (z. B. Lastschriftverfahren) auswirken. Mögliche Folge eines Blacklisteintrags ist die Sperrung des Zugangs zu bestimmten Online-Zahlverfahren (z. B. Lastschriftverfahren).

Sämtliche Vorgänge, die über ePayBL abgewickelt und bei denen personenbezogene Daten verarbeitet werden, dürfen ausschließlich auf Basis einer informierten Einwilligung des Nutzers erfolgen. Dies gilt insbesondere für Bonitätsprüfungen und das Führen der Blacklist.

Wollen Stellen des Landes oder der Kommunen die Bezahlung für Dienste und Produkte über die Bezahlplattform abwickeln lassen, müssen folgende Voraussetzungen erfüllt sein:

- Den Kunden sind umfassende und transparente Einwilligungserklärungen zur Verfügung zu stellen, die den Anforderungen des Telemediengesetzes gerecht werden.

- Auf technischer Ebene muss dafür gesorgt werden, dass eine lückenlose Verschlüsselung der Datenübertragung vom Kunden über den E-Shop zur Bezahlplattform vorhanden ist. Der E-Shop selbst muss dem Stand der Technik entsprechen und darf nur von geeigneten und berechtigten Personen administriert und bewirtschaftet werden.

In beiden Bereichen bestehen allerdings teilweise noch erhebliche Defizite. Für eine datenschutzgerechte Lösung müssen die beteiligten Stellen umgehend nachbessern, damit der Einsatz von E-Payment in Brandenburg den technischen und rechtlichen Anforderungen voll genügt.

Sollen personenbezogene Daten über Online-Bezahlsysteme verarbeitet werden, müssen die Nutzer vor Abgabe ihrer Daten umfassend über die Datenverarbeitung informiert werden und Einwilligungserklärungen nach dem Telemediengesetz abgeben. Die Übertragung der Daten über Strecken, zu denen unberechtigte Dritte Zugang haben können, darf nur verschlüsselt erfolgen.

2.7.2 Identitätsmanagement

Als elementare Komponente im Portal service.brandenburg.de ist ein Identitätsmanagementsystem vorgesehen, das der zentralisierten Verwaltung und Bereitstellung von Benutzerdaten dienen soll. Das vorliegende Konzept wirft allerdings einige datenschutzrechtliche Fragen auf.

Damit sich Nutzer nicht für jede Anwendung bzw. Dienstleistung des Serviceportals gesondert registrieren müssen, ist die Implementierung eines Identitätsmanagementsystems (IDM) für die Identifikation, Authentifizierung von Nutzern und Personalisierung von Inhalten vorgesehen. Ein Anwender muss sich dann im IDM registrieren und pro Sitzung nur einmal authentisieren, um verschiedene Anwendungen und Dienstleistungen nutzen zu können (Single-Sign-On-Prinzip). Die Drittapplikationen greifen direkt auf die im IDM hinterlegten Daten zu. Das Konzept sieht vor, dass die Benutzer detailliert in ihrem Benutzerkonto einstellen können, welche ihrer Daten sie welchen Anwendungen zur Verfügung stellen wollen. Diese Steuerungsfähigkeit durch den Nutzer ist datenschutzrechtlich positiv. Problematisch sind dagegen folgende Punkte:

- Datentrennungsgebot

Die Spezifikation zum IDM sieht vor, dass Drittapplikationen beliebige Daten in den IDM-Benutzerkonten ablegen können. So lange es sich dabei um rein technische, nicht personenbezogene Daten handelt, ist dagegen nichts einzuwenden. Wenn allerdings personenbezogene Daten im IDM von anderen Anwendungen abgelegt werden, wird dadurch das Datentrennungsgebot verletzt. Danach sollten zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden. Eine datenschutzgerechte Lösung muss vorsehen, verfahrensspezifische personenbezogene Daten in der entsprechenden Anwendung selbst und nicht im Identitätsmanagementsystem zu speichern.

- Stärke der Authentisierung

Die Standard-Authentisierungsmethode im IDM besteht aus Benutzername und Passwort. Diese Authentisierungsform ist aber in der Regel nur für die Verarbeitung normal schutzbedürftiger Daten geeignet. Die Stärke der verwendeten Authentisierungsverfahren muss sich am Schutzbedarf der verarbeiteten personenbezogenen Daten in den Drittapplikationen richten. Entsprechend müssen im Identitätsmanagement Funktionen vorgesehen werden, die es ermöglichen, verschiedene Authentisierungsverfahren zu verwenden und Authentisierungsverfahren mit einer Drittapplikation so zu koppeln, dass Benutzer nur dann Zugang zu der Anwendung erhalten, wenn sie sich mit der geforderten Methode authentisieren.

Sollten innerhalb einer Drittanwendung unterschiedlich hohe Schutzniveaus vorhanden sein, muss Benutzern, die sich nicht entsprechend authentisiert haben, der Zugang zu Funktionen höheren Schutzbedarfs verwehrt werden.

Bei der Verwendung eines Identitätsmanagementsystems zur Verwaltung von Benutzerdaten muss gewährleistet sein, dass das Prinzip der Datentrennung eingehalten wird und die Authentifizierungsmechanismen auf den Schutzbedarf der verarbeiteten Daten abgestimmt werden.

2.7.3 Virtuelles Bauamt

Das Virtuelle Bauamt – Bauen Online ist ein wichtiges E-Government-Leitprojekt der Landesregierung. Es fungiert als Plattform für die elektronische Vorbereitung und Einreichung von Bauanträgen über das Internet und ist als solches in das Portal service.brandenburg.de integriert. Alle beteiligten Personen können darüber sämtliche Formalitäten im Rahmen eines Bauvorhabens online abwickeln.

Der erste Schritt zur Nutzung des Virtuellen Bauamtes ist die Benutzerregistrierung, die zurzeit noch direkt an der Plattform und zukünftig über ein Identitätsmanagementsystem[21] erfolgt. Danach können sich die Nutzer am Virtuellen Bauamt anmelden. Hier können sie Projekträume anlegen, in denen ein neuer Bauantrag vorbereitet wird, bzw. ihre aktuellen oder bereits abgeschlossenen Projekte ansehen. Ein Projektraum wird zunächst als virtueller Vorbereitungsraum eingerichtet, in dem Anträge ausgewählt, mit Hilfe von Formular-Assistenten ausgefüllt und erforderliche Dokumente für den Bauantrag (Bauvorlagen etc.) auf die Plattform geladen werden können. Darüber hinaus kann der Antragsteller weitere beteiligte Dritte (z. B. Architekten oder Statiker) per E-Mail in den Projektraum einladen, um mit ihnen gemeinsam den Bauantrag vorzubereiten.

Liegen alle Unterlagen vor, muss der Bauantrag qualifiziert elektronisch signiert werden und an die zuständige Baubehörde über die Bauplattform abgeschickt werden. Mit der formalen Antragstellung wird der bisherige Vorbereitungsraum in den sogenannten Genehmigungsraum überführt. Der Antrag wird an die entsprechende untere Baubehörde weitergeleitet, bei der die Antragsbearbeitung im Baufachverfahren beginnt. Werden von der Baubehörde noch Unterlagen benötigt, können diese wiederum über den Projektraum des Virtuellen Bauamtes eingereicht werden.

Die Baugenehmigung wird dem Antragsteller ebenso über das Virtuelle Bauamt zur Kenntnis gegeben wie die Gebührenbescheide. Die angefallenen Gebühren können anschließend über das E-Payment-Verfahren[22] bezahlt werden.

Als technisch und rechtlich sehr komplexes Projekt weist das Virtuelle Bauamt eine Vielzahl von Aspekten auf, die Einfluss auf die datenschutzrechtliche Bewertung haben.

---

21 vgl. A 2.7.2

22 vgl. A 2.7.1

Positiv hervorzuheben sind folgende Punkte:

- Die Spezifikation der Plattform-Software sieht vor, dass die Zugriffsrechte für die Bauunterlagen und die erlaubten Aktionen auf die entsprechende Nutzerrolle abgestimmt sind. So soll gewährleistet werden, dass die Beteiligten im Bauantragsverfahren nur auf die für sie erforderlichen Daten zugreifen können.

- Die Datenübertragung über das Internet erfolgt SSL-verschlüsselt.

- Zwischen der Bauplattform und den unteren Baubehörden erfolgt die Datenübertragung OSCI-verschlüsselt.[23]

- Für den Bauantrag und die Baugenehmigung ist die qualifizierte elektronische Signatur verpflichtend vorgeschrieben.

Datenschutzrechtlich unzureichend geklärt sind bislang allerdings folgende Bereiche:

- Unklar ist, welche der beteiligten Stellen für welche Komponenten des Virtuellen Bauamtes Daten verarbeitende Stelle im Sinne des Brandenburgischen Datenschutzgesetzes bzw. Telemedienanbieter im Sinne des Telemediengesetzes ist.

- Rechtlich besonders problematisch ist die Komponente des Vorbereitungsraums in der Plattform, da es sich hierbei nicht um eine Pflichtaufgabe des Landes handelt und daher nicht eindeutig ableitbar ist, welche Stelle dafür die datenschutzrechtliche Verantwortung zu tragen hat.

- Für den Vorbereitungsraum sind geeignete und wirksame technische und organisatorische Maßnahmen vorzusehen, die einen Missbrauch der Plattform für illegale Zwecke verhindern.

- Nach § 13 Telemediengesetz hat der Diensteanbieter den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten in allgemein verständlicher Form zu unterrichten. Eine Verarbeitung personenbezogener Daten im Virtuellen Bauamt darf außerdem nur mit der bewussten und eindeutigen Einwilligung der Benutzer erfolgen. Bislang genügen allerdings die Hinweise über die Datenverarbeitung auf der Registrierungs- und Anmeldeseite des Virtuellen Bauamtes in keiner Weise den Anforderungen. Einwilligungserklärungen nach dem Telemediengesetz sind nicht vorhanden. Dies

[23] siehe http://www.osci.de

stellt einen Verstoß gegen gesetzliche Bestimmungen dar, der umgehend abzustellen ist.

Das Beispiel Virtuelles Bauamt macht deutlich, dass die Entwicklung und Einführung von komplexen E-Government-Anwendungen von Beginn an mit klar verteilten Verantwortlichkeiten sowohl rechtlich als auch technisch begleitet werden muss, damit nicht nur Teilaspekte des Datenschutzes umgesetzt werden.

3 Medien und Telekommunikation

3.1 Datenschutzgerechte Nachweise zur Befreiung von Rundfunkgebühren

Über das Verfahren zur Rundfunkgebührenbefreiung hatten wir bereits mehrfach berichtet. Seit dem 1. September 2008 besteht für die Betroffenen die Möglichkeit, den Nachweis des Bezugs von Sozialleistungen mittels der so genannten Drittbescheinigung zu erbringen.

Die bis zu diesem Zeitpunkt rechtlich unverbindliche Vereinbarung mit dem Rundfunk Berlin-Brandenburg und der Gebühreneinzugszentrale (GEZ), statt des kompletten Sozialleistungsbescheides lediglich eine Bestätigung des Leistungsträgers (Drittbescheinigung) über die Möglichkeit der Befreiung von den Rundfunkgebühren vorzulegen, wurde nunmehr im Gesetz[24] verankert. Die Vorlage des Sozialleistungsbescheids kann auch weiterhin im Original oder als beglaubigte Kopie erfolgen. Zu beachten ist, dass alle drei Alternativen gleichrangig nebeneinander stehen. Der Betroffene kann somit selbst entscheiden, in welcher Form er den Nachweis erbringt. Der Nachweis ist zusammen mit dem Antrag auf Gebührenbefreiung an die GEZ zu übersenden.

Im Vergleich zur Offenlegung beispielsweise des vollständigen ALG-II-Leistungsbescheids ist die Drittbescheinigung die datensparsamere Variante. Sie beinhaltet lediglich folgende Angaben:

[24] Rundfunkgebührenstaatsvertrag (RGebStV – Art. 4 des Staatsvertrages über den Rundfunk im vereinten Deutschland) vom 31. August 1991 (GVBl. I S. 580, 602), zuletzt geändert durch Artikel 6 des Zwölften Rundfunkänderungsstaatsvertrags vom 18. Dezember 2008 (Gesetz vom 15. April 2009, GVBl. I S. 70, 93)

- Name und Anschrift des Betroffenen,
- Leistungsanspruch nach dem Zweiten Buch Sozialgesetzbuch,
- Leistungszeitraum,
- Anspruch auf einen Zuschlag nach § 24 Zweites Buch Sozialgesetzbuch und
- ggf. den Empfänger des Zuschlags.

Darüber hinausgehende Angaben beispielsweise zur Höhe der bezogenen Sozialleistung, wie sie mehrfach von der GEZ verlangt wurden, sind unzulässig.

Um den Leistungsempfängern das Verfahren zur Befreiung von der Rundfunkgebührenpflicht zu erleichtern und Bürokratieaufwand in den Dienststellen zu reduzieren, hat die Bundesagentur für Arbeit ihre bisherige Verfahrensweise zur Bestätigung des Leistungsbezugs geändert. Nunmehr wird mit jedem zentral erstellten Bewilligungsbescheid die Drittbescheinigung zur Vorlage bei der GEZ an den Leistungsempfänger versandt.

Die Bürger sind nicht verpflichtet, ihre Leistungsbescheide im Original oder in Kopie an die GEZ zu übersenden. Die Bestätigung des Leistungsbezugs mittels der so genannten Drittbescheinigung genügt und ist nun auch rechtlich verankert.

3.2 Vorratsdatenspeicherung in der elektronischen Kommunikation – ein Status quo

Die Vorratsdatenspeicherung,[25] mit der die Bundesregierung die europäische Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten umgesetzt hat, ist seit dem 1. Januar 2008 in Kraft und noch immer umstritten.

Nach der Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung veröffentlichte das Bundesministerium der Justiz eine selbst beauftragte Studie des Max-Planck-Instituts für ausländisches und internationales Strafrecht, in der die Nutzung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung evaluiert wurde. Die

[25] Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 (BGBl. I S. 3198)

Studie bestätigt unsere bereits früher geäußerte Kritik[26] zum Gesetz. So wird konstatiert, dass Verkehrsdaten ein hohes Überwachungspotenzial in sich tragen und besser als andere Daten dazu geeignet sind, soziale Netzwerke nachzuweisen, Beziehungen zu identifizieren und Informationen über Individuen zu generieren. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber in einer Entschließung[27] aufgefordert, die Regelungen unter Berücksichtigung unter Anderem folgender Aspekte zügig nachzubessern:

- Die Straftatenschwelle für die Verkehrsdatenabfrage ist auf schwere Straftaten anzuheben.

- Für die Verkehrsdatenabfrage sollten qualifizierte Begründungspflichten in der Strafprozessordnung vorgesehen werden.

- 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.

Ferner wird auch an die Strafverfolgungsbehörden und Gerichte appelliert, die Konsequenzen aus der Studie zu ziehen. Ein besonderes Augenmerk ist auf die Prüfung der Angemessenheit der Maßnahmen zu richten. Die gesetzlich festgeschriebene, dem Grundrechtsschutz dienende Benachrichtigungs-, Löschungs- und Dokumentationspflicht ist in der Praxis stets zu berücksichtigen.

Das Bundesverfassungsgericht befasste sich zum Zeitpunkt des Redaktionsschlusses unseres Berichts mit einer Sammelbeschwerde von über 34.000 Menschen gegen die Vorratsdatenspeicherung. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach die Möglichkeit genutzt, eine gemeinsame Stellungnahme in den Verfassungsbeschwerdeverfahren[28] zur Vorratsdatenspeicherung und zu anderen Ermittlungsmaßnahmen abzugeben.

Die Herausgabe anlasslos gespeicherter Verkehrsdaten wurde seit März 2008 nach Anordnung des Bundesverfassungsgerichts auf die Verfolgung schwerer Straftaten begrenzt. Im Oktober 2009 wurde die Anordnung um

---

26 vgl. Tätigkeitsbericht 2006/2007, A 1.3.1

27 siehe Anlage 3.5.5: Entschließung „Abfrage von Telekommunikationsverkehrsdaten einschränken: Gesetzgeber und Praxis müssen aus wissenschaftlichen Erkenntnissen Konsequenzen ziehen“ vom 6./7. November 2008

28 1 BvR 256/08, 1 BvR 263/08 und 1 BvR 586/08

sechs Monate verlängert. Zugleich wurde die Bundesregierung beauftragt, erneut über die praktischen Auswirkungen der vorgesehenen Datenspeicherung und der einstweiligen Anordnung unter Zuarbeit der Länder und des Generalbundesanwalts zu berichten.

Das Bundesverfassungsgericht prüft, ob das Gesetz zur Neuregelung der Telekommunikationsüberwachung und Einführung der Vorratsdatenspeicherung einen Verstoß gegen das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung darstellt.

3.3 Internetsperren – ein geeignetes Mittel im Kampf gegen Kinderpornografie?

Am 18. Juni 2009 beschloss der Bundestag ein Gesetz zur Bekämpfung der Kinderpornografie in Kommunikationsnetzen (Zugangserschwerungsgesetz). Ziel des Gesetzes ist die Sperrung von kinderpornografischen Internetseiten, sodass diese in Deutschland nicht mehr abrufbar sind. Das Gesetzgebungsverfahren wurde von einer sehr kontroversen Debatte in der Öffentlichkeit und unter Fachleuten begleitet.

Nach dem Willen des Gesetzgebers soll das Bundeskriminalamt eine Liste mit zu sperrenden Angeboten im Internet erstellen. Diese „Sperrliste“ soll an alle größeren Anbieter von Internetzugangsdiensten weitergeleitet werden, damit diese dann den Zugang zu den Webseiten für ihre Kunden sperren und sie auf eine Seite mit einem abgebildeten Stoppschild umleiten. Die „Sperrliste“ ist geheim und soll durch ein Gremium beim Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kontrolliert werden.

Weshalb stößt dieses Gesetz auf Widerstand? Im Rahmen des Gesetzgebungsverfahrens wurde kritisiert, die vorgesehenen Sperren auf der Ebene vollqualifizierter Domainnamen, Internetprotokoll-Adressen oder Zieladressen von Telemedienangeboten seien sehr leicht zu umgehen. Da kinderpornografisches Material vor allem über E-Mail, Tauschbörsen, Mobiltelefone oder externe Datenträger verteilt wird, sei das Gesetz nicht dazu geeignet, die Verbreitung geschweige denn den Missbrauch selbst zu verhindern.

Die Sperranordnungen stellten schwerwiegende Eingriffe in die Grundrechte aller Beteiligten dar. Insofern müsse die Entscheidung darüber, ob ein Internetangebot in die Sperrliste aufgenommen wird, ein Richter treffen. Weiterhin sei nur vorgesehen, die Zugangsanbieter, nicht jedoch die Inhalteanbieter über die Aufnahme in die Sperrliste zu informieren. Letztere könnten sich deshalb – entgegen rechtsstaatlichen Regeln – nicht wehren.

Zu dem Gesetzentwurf gab es zahlreiche Beratungen und Anhörungen. Einige der vorgebrachten Bedenken wurden aufgegriffen und sind in das verabschiedete Gesetz eingeflossen. So wurden die Regelungen zur Sperrung von Internetseiten mit kinderpornografischem Inhalt nicht im Telemediengesetz sondern in einer spezialgesetzlichen Regelung, dem Zugangserschwerungsgesetz verankert. Damit soll klargestellt werden, dass die Zugangserschwerung nicht ohne weiteres auf andere Inhalte ausgedehnt werden kann. Des Weiteren wurde der Grundsatz „Löschen vor Sperren“ eingefügt. Danach kommt eine Sperrung nur dann in Betracht, wenn Maßnahmen gegen den Verantwortlichen nicht oder nicht in angemessener Zeit möglich sind. Eine Verwendung von personenbezogenen Daten, die bei der Umleitung auf ein Stoppschild anfallen, darf für Zwecke der Strafverfolgung nicht erfolgen. Somit brauchen Nutzer, die gegebenenfalls unbeabsichtigt auf Seiten, die auf der Sperrliste stehen, zugegriffen haben, nicht die Einleitung eines Ermittlungsverfahrens befürchten.

Ob und wann das Gesetz in Kraft tritt, ist unklar.

Trotz der erreichten Verbesserungen ist das verabschiedete Zugangserschwerungsgesetz kein geeignetes Mittel zur wirksamen Bekämpfung von Kinderpornografie.

3.4 Wie sich der Bund vor Viren und Würmern schützen will

Fast jeder Nutzer eines Computers hat schon einmal schlechte Erfahrungen mit Viren, Würmern und Hackern gemacht. Aber auch die IT-Systeme öffentlicher Stellen sind durch derartige Angriffe bedroht. Mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) soll nun gegengesteuert werden.

Das BSI-Gesetz[29] erweitert die Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik, um Angriffe auf die IT-Infrastruktur des Bundes abwehren zu können. Die Behörde ist als zentrale Meldestelle für IT-Sicherheit verpflichtet, Informationen über Sicherheitslücken und neue Angriffsmuster auf die Sicherheit der Informationstechnik zu sammeln und auszuwerten.

Der ursprüngliche Gesetzentwurf sah u. a. vor, dass das Bundesamt für Sicherheit in der Informationstechnik zum Aufspüren von Hackern und Schadsoftware die gesamte Sprach- und Datenkommunikation zwischen

[29] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) vom 14. August 2009 (BGBl. I S. 2821)

Bürgern und Bundesbehörden routinemäßig und ohne Anlass überwachen darf. Dies hätte beispielsweise bedeutet, dass jede an eine Bundesbehörde geschickte E-Mail vom Bundesamt automatisiert ausgewertet und gespeichert werden dürfte. Es wäre nicht nur kontrolliert worden, wann eine E-Mail von welchem Absender an welche Adresse gesendet wurde, sondern auch die Inhalte der E-Mail. Diese Befugnis, so sah es der Gesetzentwurf vor, hätte gleichfalls den privaten Anbietern von Telemedien durch eine Änderung des Telemediengesetzes eingeräumt werden sollen. Das Bundesamt hätte darüber hinaus auch bei nicht erheblichen Straftaten, wenn sie mittels Telekommunikation begangen wurden, Daten an die Strafverfolgungsbehörden übermitteln sollen.

Von Seiten der Datenschutzbeauftragten des Bundes und der Länder wurde der Gesetzentwurf als unausgewogen kritisiert. Zwar muss der Staat seine IT-Systeme vor Angriffen schützen, dies darf jedoch nicht zu Lasten der Privatsphäre der Nutzerinnen und Nutzer gehen. Mit einer Entschließung[30] forderten die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf zu prüfen, ob datenschutzfreundliche Ansätze das erforderliche Sicherheitsniveau nicht ebenso gewährleisten würden. Die Festlegung von strengeren und einheitlichen Sicherheitsstandards, die Pseudonymisierung von Protokolldateien und E-Mail-Daten sowie die Information der Unternehmen, Bürgerinnen und Bürger über bekannt gewordene Sicherheitslücken und Schadprogramme oder die Warnung vor Angriffen wären aus Sicht der Datenschutzbeauftragten geeignete Maßnahmen.

Der Gesetzgeber hat aufgrund der massiven Kritik am Gesetzentwurf die allgemeine Befugnis zur Übermittlung der Daten an Sicherheitsbehörden auf die Straftatbestände des Ausspähens und Abfangens von Daten, sowie die Datenveränderung und Computersabotage eingeschränkt. Auch für die Weitergabe von Zufallsfunden gelten durch die Einführung eines Richtervorbehalts höhere Schranken. Darüber hinaus wurden Pflichten zur nachträglichen Benachrichtigung der Betroffenen eingefügt. Verbesserungen aus datenschutzrechtlicher Sicht wurden ebenfalls durch die gesetzlich verankerte Pflicht zur unverzüglichen Löschung von Daten, die dem Kernbereich der privaten Lebensgestaltung zuzuordnen sind, erreicht. Für die Kommunikation von zeugnisverweigerungsberechtigten Berufsgruppen mit der Bundesverwaltung wurde ein Beweisverwertungsverbot eingefügt, welches jedoch einer Verhältnismäßigkeitsprüfung unterliegt. Die besonders umstrittene Erlaubnis für die Anbieter von Telemedien zur Speicherung von Nutzerdaten zur Störungsbekämpfung wurde gestrichen.

[30] siehe Anlage 3.4: Entschließung „Stärkung der IT-Sicherheit – aber nicht zu Lasten des Datenschutzes“ vom 18. Februar 2009

Bemerkenswert ist, dass der Bundesrat mit seiner Zustimmung zum Gesetz eine Entschließung verabschiedet hat, in welcher er die Erwartung der Länder äußert, an der Erarbeitung der Regelungen, die sich auf die Informationstechnik in der Verantwortung der Länder und Kommunen auswirken können, umfassend beteiligt zu werden.

Grundsätzlich sind bei allen Maßnahmen zur Stärkung der IT-Sicherheit auch die Privatsphäre und der Datenschutz der Betroffenen zu berücksichtigen.

4 Inneres

4.1 Polizei- und Ordnungsbehörden

4.1.1 Der Datenaustausch zwischen Polizei und Staatsanwaltschaft funktioniert nicht!

Bei der Bearbeitung einer Eingabe stellten wir fest, dass das Polizeiliche Auskunftssystem POLAS, die Datenbank zur Erfassung von Straftaten, eine große Anzahl von Datensätzen enthält, bei denen das Ergebnis der staatsanwaltlichen Ermittlungen bzw. der Ausgang des Gerichtsverfahrens, der sog. Verfahrensausgang fehlte. Dies ist kein neuer Mangel: Bereits seit 1993[31] hatten wir immer wieder über den fehlenden Verfahrensausgang und seine negativen Auswirkungen auf die Persönlichkeitsrechte der Betroffenen sowie auf die polizeiliche Arbeit als solche zu berichten.

Nach der Einführung der Mehrländer-Staatsanwaltschafts-Automation MESTA bei den hiesigen Staatsanwaltschaften wurde der Datenaustausch zwischen Polizei und Staatsanwaltschaft bereits im Jahr 2000 durch die Einrichtung einer Schnittstelle zwischen den jeweiligen Datenverarbeitungssystemen automatisiert. Leider funktioniert diese immer noch nicht in vollem Umfang.

Bei einem Besuch der Staatsanwaltschaft Potsdam haben wir uns über die Bedienung der Schnittstelle informiert. Die Datenverarbeitung in MESTA einschließlich Schnittstelle wird über eine Zentrale Erfassungsstelle pro Staatsanwaltschaft abgewickelt. Dabei ist technisch sichergestellt, dass der Schnittstelle jede Änderung des Verfahrensstands und somit auch der Verfahrensausgang zugeleitet wird. Dass die Daten danach in POLAS nicht ankommen, ist neben den unterschiedlichen Arbeitsabläufen der beiden Behörden auf eine beträchtliche Anzahl von Mängeln und Fehlern zurückzu-

[31] vgl. 2. Tätigkeitsbericht 1993, 3.6.2.2

führen, auf die teilweise bereits bei dem Vorführungstermin hingewiesen wurde oder die sich erst im weiteren Verlauf der Ursachenerforschung herausstellten.

Alle Beteiligten waren sich einig, dass der Zustand nicht hingenommen werden konnte. Bei einer gemeinsamen näheren Untersuchung wurden zunächst die Anzahl der mangelhaften Datensätze festgestellt, die Ursachen der Mängel ermittelt und einige in ersten Bereinigungsschritten beseitigt. Im Ergebnis blieben ca. 3000 Datensätze übrig, bei denen der Verfahrensausgang fehlte. Bis Ende Januar 2010 soll auch hier die Nacherfassung abgeschlossen und die noch vorhandenen Mängel durch die Einrichtung einer neuen Schnittstelle bzw. mit der Einführung der Version 7.2 des Polizeilichen Vorgangsbearbeitungssystems ComVor beseitigt werden. Schon jetzt wurde durch Änderungen bei den Dateninhalten sowie dem Organisationsablauf die Datenqualität in der Schnittstelle verbessert.

Zwar könnte der Datenaustausch zwischen Polizei und Staatsanwaltschaft auf technischer Ebene ab 2010 endlich funktionieren. Damit ist jedoch nicht zu rechnen, denn die fehlerhafte Bedienung der Schnittstelle und die unzulängliche Einpflege der Verfahrensausgänge in den Kriminalaktenhaltungen sind damit nicht behoben. Auch fehlt an dieser Stelle ein regelmäßiger Austausch zwischen Polizei und Staatsanwaltschaft über die Ursachen der Mängel.

Beide Behörden sind gleichermaßen für die Aufklärung von Straftaten zuständig und daher auf gegenseitige Informationen angewiesen. Gerade wegen der unterschiedlichen Arbeitsabläufe und der darauf zurückzuführenden unterschiedlichen Anforderungen, welche die Polizei auf der einen und die Staatsanwaltschaft auf der anderen Seite beispielsweise an Art, Umfang, Verfügungszeit und Inhalt der Daten stellen, scheint uns die Einrichtung eines gemeinsamen Gremiums unerlässlich. Es sollte die Probleme nicht nur besprechen, sondern auch verbindliche Vorschläge zu ihrer Behebung erarbeiten. Neben Technikern sollten ihm insbesondere auch Anwender der Arbeitsebene beider Behörden angehören. Bedauerlicherweise scheint beim Generalstaatsanwalt – anders als bei der Polizei – derzeit keine Bereitschaft zur Einrichtung einer solchen Arbeitsgruppe zu bestehen.

Weitere Mängelursachen sind Bedienungsfehler und die nie ganz abzustellenden Fehler bei der Dateneingabe. Häufig können die über die Schnittstelle in ComVor eingehenden Verfahrensmitteilungen keinem Datensatz in POLAS zugeordnet werden, weil der zuständige Bearbeiter die Schnittstelle falsch bedient hat. Ein nicht unbeträchtlicher Teil dieser Fehler ist auch auf die Unkenntnis der Anwender über die Systemanforderungen zurückzuführen. Diesem Problem könnte mit einer gründlichen Schulung aller Vollzugsbeam-

ten, die mit ComVor/PoLAS und der Schnittstelle umgehen, begegnet werden. Der Infobrief, in dem der Zentraldienst der Polizei häufige Bedienungsfehler und ihre Korrektur zusammengestellt hat, reicht hierfür nicht aus.

Nicht gelöst ist auch der problematische Transfer des Verfahrensausgangs von ComVor nach POLAS. Die Automatisierung erstreckt sich nur bis ComVor. In POLAS müssen die Verfahrensausgänge durch die Kriminalaktenhaltung noch immer einzeln eingepflegt werden. Dagegen ist eigentlich auch nichts einzuwenden, weil die Mitteilung des Verfahrensausgangs der klassische Einzelfall für die Erforderlichkeitsprüfung gem. § 47 Abs. 2 Nr. 3 Brandenburgisches Polizeigesetz (BbgPolG) ist. Viel zu häufig wird die Einpflege aber unterlassen und in der Folge auch die Erforderlichkeitsprüfung, zu der im Übrigen auch immer die Kriminalakte hinzugezogen werden müsste. Beides erfordert aber einen Zeit- und Personalaufwand, der in den Arbeitsabläufen häufig nicht zur Verfügung steht.

Ungeachtet der vorgeschriebenen Erforderlichkeitsprüfung im Einzelfall, die wohl überhaupt nicht mehr vorgenommen würde, wenn die händische POLAS-Einpflege wegfiele, hätte die Automatisierung viele Vorteile. Damit wäre sichergestellt, dass in POLAS ein Datenbestand zur Verfügung steht, der alle Informationen einschließlich des Verfahrensstands enthält und so verlässliche Rückschlüsse ermöglicht. Der Verwaltungsaufwand würde dadurch erheblich reduziert. Er entsteht derzeit beispielsweise bei der Bearbeitung von Auskunftsanträgen Betroffener, Anfragen und Auskunftsersuchen anderer Stellen oder Zuverlässigkeitsprüfungen. Vor deren Beantwortung muss zunächst zu jedem erfassten Tatvorwurf der Verfahrensausgang bei der zuständigen Staatsanwaltschaft schriftlich oder telefonisch abgefragt werden, wenn die Auskunft vollständig und richtig sein soll.

Um den verlässlichen Datenaustausch zwischen Polizei und Staatsanwaltschaft in Zukunft sicherzustellen, bedarf es neben technischen Vorkehrungen der Einrichtung eines gemeinsamen Gremiums beider Behörden. Es sollte Lösungsvorschläge für fachliche sowie technische Probleme erarbeiten. Zudem sollten die Beschäftigten, die mit der Schnittstelle umgehen müssen, gründlich geschult und die Datenpflege in den Kriminalakten verbessert werden. Ausreichende zeitliche sowie personelle Kapazitäten sind hierfür zur Verfügung zu stellen.

4.1.2 Überprüfung von Stellenbewerbern

Schon immer hat die Polizei ihre Stellenbewerber anhand der kriminalpolizeilichen Sammlungen überprüft. Die Bewerbungsunterlagen enthalten dazu ein Formular, in dem der Bewerber aufgefordert wird, alle gegen ihn geführten Ermittlungsverfahren wahrheitsgemäß anzugeben und die

Einwilligung zur Überprüfung seiner Angaben zu erteilen. Die Polizei am Wohnort des Bewerbers gleicht die Daten ab und teilt der Einstellungsbehörde jedes Ermittlungsverfahren unabhängig von Delikt und Verfahrensausgang mit. Eine Gerichtsentscheidung stellt diese Praxis nun aber in Frage.

Aufgrund der erteilten Einwilligungen der Stellenbewerber hielten wir diese „Zuverlässigkeitsprüfungen“ bisher für zulässig. Der Beschluss des Verwaltungsgerichts Stuttgart[32] legt nun eine andere Sicht auf die ständig zunehmende Einstellungspraxis nahe, der wir uns anschließen.

Der Abgleich der personenbezogenen Daten eines Stellenbewerbers mit den kriminalpolizeilichen Sammlungen ist eine im Polizeigesetz nicht vorgesehene Zweckänderung. Die Polizei ist als Einstellungsbehörde nicht Polizeibehörde, sondern öffentlicher Dienstherr. Sie kann als solcher nicht mehr am privilegierten Datenverkehr der Polizei („Datenweitergabe“ nach § 41 Abs. 5 Brandenburgisches Polizeigesetz – BbgPolG) teilnehmen. Die kriminalpolizeilichen Sammlungen des eigenen Bundeslandes, des Bundes und der anderen Bundesländer stehen ihr nur dann zur Verfügung, wenn die Daten zur Erfüllung ihrer Aufgaben als Polizeibehörde erforderlich sind.

Unter diesen Umständen kommt nur eine Datenübermittlung nach § 43 Abs. 3 Nr. 3, 1. Alternative BbgPolG in Betracht – die voraussetzt, dass sie zur Abwehr erheblicher Nachteile für das Gemeinwohl erforderlich ist. Nach § 41 Abs. 3 BbgPolG trägt die übermittelnde Polizeibehörde die Verantwortung für die Übermittlung und muss die Zulässigkeit prüfen. Die ersuchende Behörde, hier die polizeiliche Einstellungsbehörde, muss ihrerseits das Ersuchen mit Angaben über die Gemeinwohlgefährdung und die Erforderlichkeit der Übermittlung untermauern. Die angefragte Polizeibehörde hat gem. § 47 Abs. 2 Nr. 3, 2. Alternative BbgPolG zunächst zu prüfen, ob die Daten zur – polizeilichen! – Aufgabenerfüllung erforderlich sind. Wird dies verneint, muss die Übermittlung unterbleiben. Die Behörde hat die Daten zu löschen.

Soweit einer Einstellungsbehörde gem. § 43 BbgPolG auf Ersuchen im Einzelfall Daten über einen Stellenbewerber übermittelt werden sollen, ist Folgendes zu beachten:

- Die Polizeibehörde muss anhand der Angaben der Einstellungsbehörde die Zulässigkeit der Übermittlung prüfen. Bei unzulänglichen Angaben darf nicht übermittelt werden.

[32] 3 K 1886/08 vom 1. August 2008

- Vor jeder Übermittlung ist die Erforderlichkeit der zu übermittelnden Daten zur polizeilichen Aufgabenerfüllung zu prüfen. Die Übermittlung unterbleibt, wenn die Daten dazu nicht mehr erforderlich sind.

- Informationen zu Ermittlungsverfahren, die nach § 170 Abs. 2 Strafprozessordnung (StPO) eingestellt wurden, dürfen nur übermittelt werden, wenn der trotz Verfahrenseinstellung fortbestehende polizeiliche Tatverdacht in der Kriminalakte dokumentiert ist.

- Informationen zu Verfahren, die nach anderen Vorschriften der Strafprozessordnung eingestellt wurden, dürfen nicht übermittelt werden, wenn es sich um Bagatelldelikte handelt.

Die Einwilligung des Betroffenen in die Einsichtnahme in über ihn ggf. bei der Polizei vorhandene Datenspeicherungen erlaubt lediglich der für seinen Wohnort zuständigen Polizeidienststelle den dazu erforderlichen Datenzugriff. Sie kann jedoch weder die fehlende polizeirechtliche Vorschrift zur Nutzung der Daten zu Zwecken der Einstellung noch die gesetzlichen Regelungen zur Datenübermittlung ersetzen.

Mit der Einwilligung des Betroffenen werden bei diesen gesetzlich nicht normierten „Zuverlässigkeitsprüfungen“ darüber hinaus die Schutzvorschriften des Bundeszentralregistergesetzes (BZRG) umgangen. Diese Vorschriften sollen mit dem Ziel der Resozialisierung sicherstellen, dass einem Betroffenen nicht jedwede strafrechtliche Verfehlung sein ganzes Leben vorgehalten, sondern nach Fristablauf eben nicht mehr mitgeteilt werden darf, um ihm den Weg in ein straffreies Leben nicht über Gebühr zu erschweren.

Abgesehen von einer vorgesehenen Beschäftigung in einem sicherheitsrelevanten Bereich, bei der die gesetzlich geregelte Sicherheitsüberprüfung weitergehende Datenzugriffe ermöglicht, gelten die Verwertungs- und Vorhalteverbote des Bundeszentralregistergesetzes in Einstellungsverfahren grundsätzlich uneingeschränkt. Die Einstellungsbehörde darf daher bei ihrer Prüfung nicht alle einschlägigen Tatsachen ermitteln und verwerten. Im Fall der Verwertung von Informationen über Straftaten darf vom Verwertungsverbot des § 51 Abs. 1 BZRG grundsätzlich nur unter der Voraussetzung der Ausnahmeregelung des § 52 Abs. 1 Nr. 4 BZRG abgewichen werden, wenn demnach die Einstellung zu einer erheblichen Gefährdung des Allgemeinwohls führen könnte. Darauf muss der Bewerber in den Bewerbungsunterlagen hingewiesen werden, wenn er nach gegen ihn anhängigen strafrechtlichen Ermittlungsverfahren gefragt wird.

Es gibt somit nicht nur keine Rechtsgrundlage für die bislang geübte Einstellungspraxis in den Polizeidienst sowie in zahlreiche andere Arbeitsverhältnis-

se, lediglich auf der Grundlage der Einwilligung die Zuverlässigkeit der Stellenbewerber anhand der kriminalpolizeilichen Sammlungen zu prüfen, sondern diese Praxis verstößt auch gegen das Bundeszentralregistergesetz. Der rechtlich gebotene Verzicht auf diese Form der Eignungsprüfung bedeutet nicht, dass der Einstellungsbehörde jeglicher Informationszugang zur Straffälligkeit eines Bewerbers versperrt ist. Sie kann von ihm verlangen, ein Führungszeugnis zur Vorlage bei einer Behörde gem. § 30 Abs. 5 BZRG beizubringen.

Dass die Einstellungsbehörde keine Kenntnis von laufenden Ermittlungsverfahren erhält, dürfte im Hinblick auf die Ausbildungs- und Probezeiten hinnehmbar sein, da diese ihr genügend Zeit und Gelegenheit geben, die Eignung des Kandidaten festzustellen.

Die Einwilligung des Stellenbewerbers ersetzt weder die fehlende Rechtsgrundlage zur Nutzung der kriminalpolizeilichen Sammlungen für Zwecke des Einstellungsverfahrens noch die Vorschriften zur Datenübermittlung an öffentliche Stellen. Soweit letztere nicht erfüllt sind, beschränkt sich der Zugang zu Informationen über Vorstrafen des Bewerbers auf die Vorlage eines Führungszeugnisses.

Nicht-öffentlichen Arbeitgebern kann nur dann Auskunft aus den kriminalpolizeilichen Sammlungen über einen Stellenbewerber erteilt werden, wenn ein Gesetz eine solche Zuverlässigkeitsprüfung vorsieht.

4.1.3 Bußgeldverfahren bei Verkehrsverstößen mit im Ausland zugelassenen Fahrzeugen

Mit ca. 180.000 im Ausland zugelassenen Fahrzeugen werden jährlich Verkehrsverstöße – meist Geschwindigkeitsübertretungen – auf brandenburgischen Straßen begangen, Tendenz steigend. Die von den Geräten zur automatisierten Verkehrsüberwachung erfassten Daten wurden bisher gelöscht, weil eine Verfolgung keinen Erfolg versprach. Mit einem neuen Verfolgungsansatz sollen die verantwortlichen Fahrer jetzt zur Kasse gebeten werden.

Seit Sommer 2009 werden die mittels automatisierter Verkehrsüberwachung registrierten Verkehrsverstöße von Fahrzeugen mit ausländischem Kennzeichen in einem gesonderten Bestand der für die Verfolgung von Ordnungswidrigkeiten von der Polizei betriebenen Datenbank SC-OWI als offener Vorgang mit Vorgangsdaten, Kennzeichen und Foto des Fahrers bis zum Ablauf der Verfolgungsfrist von drei Monaten für Verkehrsordnungswidrigkeiten gespeichert. Kommt ein im Ausland zugelassenes Fahrzeug in eine allgemeine Verkehrskontrolle, wird das Kennzeichen mit diesem Bestand, auf den alle

Streifenpolizisten zugreifen können, abgeglichen. Im Trefferfall erhält der kontrollierende Beamte eine Kopie des im Vorgang erfassten Fotos des Fahrers. Bei Personengleichheit wird ein Bußgeldverfahren eingeleitet.

Datenschutzrechtlich ist gegen diese Praxis nichts einzuwenden. Rechtsgrundlage ist § 46 i. V. m. § 49c Ordnungswidrigkeitengesetz (OWiG). Danach hat die Verfolgungsbehörde, hier also die Polizei, dieselben Rechte und Pflichten wie die Staatsanwaltschaft im Strafverfahren. Sie muss die Verkehrsordnungswidrigkeit aufklären und darf dazu Ermittlungen anstellen. Gem. § 49c OWiG darf sie personenbezogene Daten nicht nur für die Zwecke des Bußgeldverfahrens speichern und nutzen. Zulässig ist auch – wie im vorliegenden Fall – die Speicherung zum Zweck der zukünftigen Verfolgung von Ordnungswidrigkeiten, allerdings nur solange die Daten zu dem o. g. Zweck erforderlich sind. Daher muss durch Löschverfahren sichergestellt werden, dass Daten spurlos aus SC-OWI verschwinden, wenn die Verfolgungsfrist von drei Monaten abgelaufen ist. Auch wenn ein Bußgeldverfahren eingeleitet wird, sind die dazu gehörigen Daten im gesonderten Bestand zu löschen.

Daten von Fahrzeugen mit ausländischen Kennzeichen und ihrer Fahrer, die anlässlich einer Verkehrskontrolle anfallen, dürfen mit dem Bestand von innerhalb der dreimonatigen Verfolgungsfrist gespeicherten personenbezogenen Daten aus zurückliegenden Verkehrsverstößen desselben Personenkreises abgeglichen werden, um das Bußgeldverfahren gegen den Fahrer durchzuführen.

4.1.4 Überflüssige Mitteilungen der Bußgeldstellen über Fahrverbote und Fahrerlaubnisentziehungen an die Wohnortpolizei

Von Datenschutzbeauftragten anderer Bundesländer sind wir darüber informiert worden, dass die dortigen für den Wohnort Betroffener zuständigen Polizeidienststellen regelmäßig Mitteilungen über die Erteilung eines von brandenburgischen Bußgeldstellen veranlassten Fahrverbots bzw. einer Fahrerlaubnisentziehung gem. § 25 Straßenverkehrsgesetz (StVG) erhalten. Durch eine Umfrage bei den Bußgeldstellen der Landkreise und kreisfreien Städte haben wir festgestellt, dass fast die Hälfte der angefragten Stellen im Falle von Fahrerlaubnisentziehungen regelmäßig Mitteilungen über die von ihnen in amtliche Verwahrung genommenen Führerscheine der Polizei übermittelt hat.

Für die Mitteilung aller Fahrverbote bzw. Fahrerlaubnisentziehungen gem. § 25 Straßenverkehrsgesetz (StVG) der Bußgeldstellen an die Polizei gibt es keine Rechtsgrundlage, sie ist daher unzulässig.

Zwar enthalten sowohl das Ordnungswidrigkeitengesetz mit § 49a als auch das Straßenverkehrsgesetz mit § 3 Vorschriften zur Mitteilung eines Fahrverbots bzw. einer Fahrerlaubnisentziehung an andere Stellen. Dennoch können beide Vorschriften für die in Rede stehenden regelmäßigen Mitteilungen aller Fahrverbote bzw. aller Fahrerlaubnisentziehungen nicht herangezogen werden.

§ 49a Ordnungswidrigkeitengesetz (OWiG) begründet keine Übermittlungspflicht, sondern nur eine, durchgängig an die Voraussetzung der Erforderlichkeit geknüpfte Befugnis. Bereits nach der Generalklausel in Absatz 1 ist die übermittelnde Stelle verpflichtet, vor der Übermittlung von Amts wegen die Erforderlichkeit der zu übermittelnden Information für die Aufgabenerfüllung der empfangenden Stelle zu prüfen. Durch die Verpflichtung zur Erforderlichkeitsprüfung sind regelmäßige Mitteilungen ausgeschlossen. Zudem gilt § 3 StVG nur für Fahrerlaubnisbehörden, sodass auch nur sie – und nicht Bußgeldstellen – gemäß Abs. 5 befugt sind, der Polizei im Einzelfall – also nicht regelmäßig – die in Rede stehenden Informationen zu übermitteln.

Der Polizei selbst fehlt ebenfalls eine Rechtsgrundlage für die Aufbewahrung eingehender Mitteilungen. Gem. § 5 Brandenburgisches Polizeigesetz dürfen polizeiliche Maßnahmen, auch Datenverarbeitungsmaßnahmen, nur gegen den für die Gefahr verantwortlichen Störer gerichtet werden. Führerscheinentzug oder ein Fahrverbot machen einen Betroffenen nicht automatisch zu einem Störer der öffentlichen Sicherheit. Erst wenn die Polizei bei einer Verkehrskontrolle feststellt, dass ein Fahrer keinen Führerschein vorweisen kann, darf sie Daten über ihn erheben und verarbeiten.

Die Mitteilung des Fahrverbots bzw. der Fahrerlaubnisentziehung an die Wohnortpolizei des Betroffenen ist zudem nicht erforderlich, auch nicht zum Zweck der allgemeinen Verkehrsüberwachung oder anlassbezogener Verkehrskontrollen. Gem. § 28 Abs. 3 StVG sind Fahrverbote und Fahrerlaubnisentziehungen im Verkehrszentralregister (VZR) einzutragen, auf das die Polizei uneingeschränkten Zugriff hat. Wird nun ein Fahrzeugführer bei einer polizeilichen Maßnahme ohne Führerschein angetroffen, kann die Polizei zur Klärung des Sachverhalts seine Angaben mittels VZR-Abfrage überprüfen. Die o. g. Mitteilungen werden dazu nicht benötigt.

Die Erforderlichkeit der Mitteilungen wurde uns gegenüber mit postalisch oder datenverarbeitungstechnisch bedingten Zeitverzögerungen zwischen dem Beginn des Fahrverbots und der Eintragung im Verkehrszentralregister begründet. Dies überzeugt nicht. Zum einen erhöht es den Verwaltungsaufwand, wenn Mängel des automatisierten Mitteilungsverfahrens dadurch behoben werden, dass ein zweiter Meldeweg in Papierform eröffnet wird. Zielführender wäre es, an der Verbesserung des automatisierten Verfahrens

anzusetzen, beispielsweise durch die elektronische Übersendung der Mitteilungen an die Führerschein- bzw. Bußgeldstellen vor dem Postversand. Zum anderen dürfte die Zeitverzögerung des Postwegs auch bei der Übersendung der Mitteilungen an die Wohnortpolizei auftreten, mit der Folge, dass dieser die Information auch nicht mit Beginn des Fahrverbots vorliegt.

Für die regelmäßige Mitteilung aller Fahrverbote und Fahrerlaubnisentziehungen an die Polizei gibt es keine Rechtsgrundlage. Bußgeld- und Führerscheinstellen müssen diese auf den Einzelfall beschränken.

4.1.5 „Runter vom Gas“ verärgert Briefempfänger

Die Zentrale Bußgeldstelle der Brandenburgischen Polizei ist für die Abwicklung aller von der Polizei eingeleiteten Ordnungswidrigkeitsverfahren zuständig. Sie beteiligt sich seit Ende 2008 an einer Kampagne des Bundesverkehrsministeriums zur Erhöhung der Verkehrssicherheit und bedruckt ihre gesamte Ausgangspost mit der Aufschrift „Runter vom Gas!“ sowie der Information, dass jährlich ungefähr fünftausend Personen bei Verkehrsunfällen sterben. Dies hat seither erstaunlich viele Briefempfänger und eine Empfängerin dazu veranlasst, sich bei uns über die vermeintliche Prangerwirkung zu beschweren.



Aus datenschutzrechtlichen Gründen ist gegen den Aufdruck jedoch nichts einzuwenden, da Dritte (z. B. Briefträger, Familienangehörige, Nachbarn) dadurch oder durch die Absenderangabe keine inhaltlichen Einzelheiten der in diesen Umschlägen befindlichen Schreiben erfahren. Welche Vermutungen, wenn überhaupt, sie darüber anstellen mögen, ist der datenschutzrechtlichen Beurteilung entzogen. Mit ihren Briefumschlägen hält sich die Bußgeldstelle auch an das Gebot in § 10 Brandenburgisches Datenschutzgesetz, durch geeignete technisch-organisatorische Maßnahmen die Vertraulichkeit personenbezogener Daten sicherzustellen, da die Versendung in einem verschlossenen Briefumschlag als ausreichender technischer Standard gilt.

Entgegen landläufiger Auffassung besteht im Briefverkehr kein datenschutzrechtlicher Anspruch auf eine Versandart, die mit einem sog. neutralen Umschlag den Absender nicht erkennen lässt. Vielmehr ist es hiesiger Poststandard, dass dem Briefumschlag nicht nur der Empfänger, sondern auch der Absender der Sendung zu entnehmen ist. Nur so ist im Fall fehlerhafter Zustellungen die Rücksendung möglich, ohne dass zur Feststellung des Absenders der Umschlag geöffnet und dabei zwangsläufig der dem Briefgeheimnis unterliegende Inhalt zur Kenntnis genommen werden müsste. Bei Behördenschreiben ist es zudem im Interesse des Empfängers, wenn er durch die Absenderangabe schon „von außen“ erkennen kann, dass es sich ggf. um eine Fristsache handeln könnte, auf deren Inhalt er möglichst kurzfristig reagieren sollte, um Rechte zu wahren und Kosten zu vermeiden. Dies gilt vor allem in Bußgeldsachen.

Die Geheimhaltung des Absenders ist datenschutzrechtlich ebenso wenig geboten wie ein Verzicht auf Werbeaufdrucke. Diese sind vielmehr hinzunehmen, soweit sie keinen Straftatbestand erfüllen oder gegen die guten Sitten verstoßen. Beides ist hier nicht der Fall.

Die Aufschrift „Runter vom Gas“ auf den Briefumschlägen der Zentralen Bußgeldstelle ist datenschutzrechtlich nicht zu beanstanden. Sie stellt keine unzulässige Prangerwirkung dar.

4.2 Verfassungsschutz

IT-Sicherheitskonzept beim Verfassungsschutz

Der Verfassungsschutz des Landes Brandenburg verarbeitet personenbezogene Daten mittels automatisierter Verfahren. Seiner gesetzlichen Pflicht zur Erstellung eines Sicherheitskonzepts ist er bislang nur zögerlich nachgekommen. Es befand sich zum Ende des Berichtszeitraums immer noch in Arbeit.

Bereits in unserem letzten Tätigkeitsbericht[33] haben wir darauf hingewiesen, dass der Verfassungsschutz des Landes Brandenburg seit Jahren Verfahren ohne Sicherheitskonzept betreibt. Dieser Verstoß gegen das Brandenburgische Datenschutzgesetz wurde von der Behörde auch nach unserer Berichterstattung nicht behoben. Daraufhin hat die Landesbeauftragte das Fehlen eines aus einer Risikoanalyse entwickelten IT-Sicherheitskonzepts im April 2008 gem. § 25 Abs. 1 Brandenburgisches Datenschutzgesetz (BbgDSG) als Verstoß gegen § 7 Abs. 3 i. V. m. § 10 BbgDSG beanstandet.

[33] vgl. Tätigkeitsbericht 2006/2007, A 5.2

Die aufgrund dieser Beanstandung ergriffenen Maßnahmen beschränkten sich zunächst auf die Übersendung eines Datenträgers mit einer Erhebung auf der Grundlage der IT-Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik. Diese genügte den datenschutzrechtlichen Anforderungen nicht. Im September 2008 wurde die Beanstandung in einer Sitzung des Ausschusses für Inneres des Landtags Brandenburg besprochen. Dieser unterrichtete die Parlamentarische Kontrollkommission und die G 10-Kommission des Landtags über das Fehlen des IT-Sicherheitskonzepts der Verfassungsschutzbehörde. Im Ergebnis brachte der Verfassungsschutz zum Jahreswechsel 2008/2009 trotz Personalmangels einen Sicherheitsprozess und die systematische Erarbeitung des Sicherheitskonzepts auf den Weg. Der nun vorliegende Zwischenstand (Dezember 2009) ist eine geeignete Grundlage für die Entwicklung eines datenschutzgerechten Sicherheitskonzepts.

Der Verfassungsschutz des Landes Brandenburg hat im Ergebnis unserer Beanstandung einen Entwurf für ein Sicherheitskonzept vorgelegt.

4.3 Ausländer

Datenübermittlung der Ausländerbehörde an die Sozialbehörde

Ein Rechtsanwalt hat uns auf ein Formular zur Datenübermittlung einer Ausländerbehörde an eine Sozialbehörde hingewiesen, das nicht den gesetzlichen Anforderungen entsprach. Auch die auf unser Drängen hin überarbeitete Fassung wies noch Mängel auf. Die Ausländerbehörde hat zwischenzeitlich zugesagt, unsere Hinweise bei einer weiteren Überarbeitung zu berücksichtigen.

Zuständig für die Sozialleistungen an Ausländer ist gem. § 10 Asylbewerberleistungsgesetz (AsylbLG) die örtliche Sozial-, nicht die Ausländerbehörde. Da das verfügbare Einkommen und Vermögen der Leistungsempfänger bei der Leistungsfestsetzung zu berücksichtigen ist (§ 7 Abs. 1 AsylbLG), muss die Ausländerbehörde der Amts angehörigen Sozialbehörde grundsätzlich Daten über einen Ausländer übermitteln, wenn sie Kenntnis von Sachverhalten hat, die für dessen Sozialleistungsbezug relevant sein können. Rechtsgrundlagen für Übermittlungen der Ausländer- an Sozialbehörden sind § 90 Aufenthaltsgesetz (AufenthG) aber auch § 1a AsylbLG und § 8 Abs. 2a Asylverfahrensgesetz (AsylVfG).

Gem. § 90 AufenthG muss die Ausländerbehörde der Sozialbehörde zu folgenden Sachverhalten personenbezogene Daten über einen Ausländer übermitteln:

- Erwerbstätigkeit ohne den dazu erforderlichen Aufenthaltstitel,
- Verstoß gegen Mitwirkungs- und Meldepflichten soweit sie für den Sozialleistungsbezug relevant sein können oder
- Verstoß gegen das Schwarzarbeitsbekämpfungsgesetz,
- aufenthaltsrechtliche Entscheidungen und Maßnahmen, die sich auf die Leistungsgewährung nach dem Asylbewerberleistungsgesetz auswirken,
- Maßnahmen im Zusammenhang mit Arbeitserlaubnissen nach dem Asylbewerberleistungsgesetz sowie
- Zuständigkeitswechsel.

Gem. § 1a AsylbLG müssen wirtschaftliche Fluchtgründe immer dann mitgeteilt werden, wenn bei der Ausländerbehörde belegbare Hinweise vorliegen, dass der Betroffene sich nach Deutschland begeben hat, um Sozialleistungen zu erhalten. Nach § 8 Abs. 2a AsylVfG ist die Sozialbehörde darüber hinaus über Umstände und Maßnahmen nach dem Asylverfahrensgesetz sowie über Maßnahmen in Zusammenhang mit Arbeitserlaubnissen zu unterrichten, die für die Gewährung von Sozialleistungen relevant sind.

Als Übermittlungsvoraussetzung ist in § 90 Abs. 1 AufenthG auf „konkrete Anhaltspunkte“ für die dort genannten übermittlungspflichtigen Sachverhalte und in den Fällen der Abs. 3 und 4 auf „belegbare Tatsachen“ wie z. B. ausländerrechtliche Entscheidungen oder den Stand des ausländerrechtlichen Verfahrens abgestellt. Strafanzeigen erfüllen die Voraussetzung nicht, da eine Strafanzeige nach allgemeiner Definition lediglich die Mitteilung des Verdachts einer Straftat ist. Sie hat demnach noch nicht die Qualität eines konkreten Anhaltspunktes bzw. einer belegbaren Tatsache. Diese Voraussetzungsschwelle ist erst mit einem straf- oder ordnungswidrigkeitsrechtlichen Verfahrensabschluss erreicht, der den Verdacht der Strafanzeige bestätigt. Dies gilt insbesondere bei der Übermittlung von Delikten wie Zigaretten- oder Drogenhandel.

Bei rechtskonformem Verwaltungshandeln aller beteiligten Stellen müssten bei der Ausländerbehörde gesicherte Erkenntnisse über von einem Ausländer tatsächlich begangene Straftaten vorliegen. Gem. § 87 Abs. 4 AufenthG sowie § 42 Anordnung über Mitteilungen in Strafsachen (MiStra) sind die

Strafverfolgungs- und Ordnungsbehörden und die Gerichte verpflichtet, der Ausländerbehörde unverzüglich die Einleitung und den Verfahrensabschluss eines Strafverfahrens oder Ordnungswidrigkeitenverfahrens von erheblicher Bedeutung bei der Staatsanwaltschaft, dem Gericht bzw. der Verwaltungsbehörde einschließlich der einschlägigen Rechtsvorschriften mitzuteilen. Allerdings ist in § 42 Abs. 1 MiStra auch festgelegt, dass die anderen Stellen ihrer Mitteilungspflicht nicht nachkommen müssen, wenn der Akte zu entnehmen ist, dass die Ausländerbehörde bereits von der Polizei unterrichtet wurde. Da bei der Polizei der Verfahrensabschluss zahlreicher Ermittlungsverfahren jedoch nicht bekannt ist,[34] erhält die Ausländerbehörde über die Polizei nur Kenntnis von der Strafanzeige, nicht aber vom Verfahrensausgang.

Dennoch sind wir, anders als das Innenministerium, der Ansicht, dass sehr wohl hohe Anforderungen an die Qualität der „konkreten Anhaltspunkte“ als Übermittlungsvoraussetzung gestellt werden müssen. Schließlich soll die Sozialbehörde darauf einen Verwaltungsakt wie beispielsweise die Kürzung des Leistungsbezugs stützen. Ohne Kenntnis des Verfahrensausgangs muss daher die Übermittlung von Delikten unterbleiben. Wenn sie solche Daten dennoch übermitteln will, muss die Ausländerbehörde den Verfahrensausgang vorher bei der Staatsanwaltschaft abfragen.

Vor der Übermittlung ist die Ausländerbehörde gehalten, in jedem Einzelfall zu prüfen, ob sie nach Sachlage für die Leistungsfestsetzung der Sozialbehörde erforderlich ist.

Es ist geboten, die Ausländerbehörden in einem Erlass über die rechtlichen Schranken und Voraussetzungen sowie ihre Prüfungspflichten bei der Übermittlung an die Sozialbehörden zu informieren. Das Ministerium des Innern hat dazu bisher lediglich mitgeteilt, dass es dies zu gegebener Zeit beabsichtige.

In den von den Ausländerbehörden zur Datenübermittlung an die Sozialbehörden genutzten Formularen sollten nur die tatsächlich relevanten Übermittlungsvorschriften genannt werden. Das Ministerium des Innern sollte in einem Erlass die rechtlichen Schranken und Voraussetzungen der Übermittlungen erläutern und die Prüfpflichten der Ausländerbehörden vor einer Übermittlung verdeutlichen.

[34] vgl. A 4.1.1

4.4 Melderecht

4.4.1 Änderungen im Melderecht

In seiner letzten Sitzung der 4. Legislaturperiode verabschiedete der Landtag das Dritte Gesetz zur Änderung des Brandenburgischen Meldegesetzes.[35] Mit dem Gesetz wurde ein bereits im Jahre 2004 angelaufenes Projekt zur Schaffung eines landesweiten elektronischen Meldedatenauskunftsregisters umgesetzt. Brandenburg hat sich damit der großen Mehrheit der Bundesländer angeschlossen, die über ein „Landesmelderegister" verfügen.

Aufgrund verschiedener rechtlicher und politischer Vorgaben der EU, des Bundes und des Landes Brandenburg zur verbesserten Online-Bereitstellung von Informationen, sollte das Meldegesetz funktionsfähiger und bedarfsgerechter gestaltet werden. Erklärtes Ziel des Regierungsentwurfs war es, die Verfügbarkeit von Meldedaten für die behördliche Aufgabenerfüllung zu erhöhen und die kommunalen Meldebehörden bei regelmäßigen Datenübermittlungen an andere Behörden und sonstige öffentliche Stellen (§ 29 Brandenburgisches Meldegesetz – BbgMeldeG) sowie bei einfachen Melderegisterauskünften zu entlasten, soweit diese in Online-Verfahren nachgefragt werden. Insbesondere wurde ein zentrales Auskunftsregister als wichtiger Baustein der E-Government Strategie des Landes gesehen, um eine beschleunigte, von Bürodienstzeiten unabhängige und effiziente elektronische Auskunftserteilung an Sicherheits- und Justizbehörden zu ermöglichen.

Seit Inkrafttreten des Gesetzes am 15. Juli 2009 regelt § 37 BbgMeldeG die Aufgaben der zentralen Registerbehörde in Brandenburg, die ein Landesmelderegister ausschließlich für regelmäßige Datenübermittlungen insbesondere im Wege des automatisierten Abrufs nach § 29 BbgMeldeG führen darf. Die kommunalen Meldebehörden übermitteln der Registerbehörde alle bei ihnen gespeicherten Einwohner-Grunddaten, d. h. im Wesentlichen die der Identitätsfeststellung und dem Wohnungsnachweis dienenden Angaben, Auskunftssperren sowie die Tatsache, ob und wann eine waffenrechtliche Erlaubnis erteilt worden ist. Die Meldebehörden sind für die Richtigkeit und Aktualität der übermittelten Daten verantwortlich und teilen der Registerbehörde unverzüglich Änderungen und Löschungen mit.

Damit stellt das Landesmelderegister ein „Spiegelregister" von Meldedaten dar, die die Registerbehörde nur für die Zwecke der regelmäßigen auch automatisierten Datenübermittlungen an Behörden oder sonstige öffentliche

[35] Gesetz über das Meldewesen im Land Brandenburg (Brandenburgisches Meldegesetz – BbgMeldeG) in der Fassung der Bekanntmachung vom 17. Januar 2006 (GVBl. I S. 6), zuletzt geändert durch Artikel 1 des Gesetzes vom 7. Juli 2009 (GVBl. I S. 255)

Stellen verwenden darf. Private Dritte können auf den Datenbestand nicht zurückgreifen. Die bisherige Zuständigkeit der Meldebehörden etwa zur Erteilung von Melderegisterauskünften an Private wird durch die Aufgaben des zentralen Registers nicht berührt.

Die technischen Voraussetzungen für eine landesweite Online-Melderegisterauskunft wurden beim Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben aufgebaut, der seit dem 1. Januar 2009 in dem Brandenburgischen IT-Dienstleister aufgegangen ist. Als Registerbehörde ist er verpflichtet, Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit zu treffen. Der Minister des Innern ist ermächtigt, einen verbindlichen IT-Standard für die Datenübermittlung von Meldebehörden zum Landesmelderegister festzulegen.

Wir waren von Beginn an in die Planungen einbezogen und hatten Gelegenheit, sowohl zu den rechtlichen Vorschriften als auch zum IT-Sicherheitskonzept des Verfahrens Stellung zu nehmen. Der Einrichtung eines Landesmelderegisters standen und stehen wir grundsätzlich positiv gegenüber. Die technischen und organisatorischen Maßnahmen für eine sichere und bedarfsgerechte Datenübermittlung können durch den zentralen Dienstleister aufgrund der technischen und personellen Ausstattung und des vorhandenen Fachwissens über IT-Sicherheit insbesondere im Hinblick auf den automatisierten Abruf über das Internet besser umgesetzt werden als in vielen Kommunen. Allerdings müssen potenzielle Risiken, die dadurch entstehen könnten, dass die Meldedatenbestände aller Kommunen des Landes an einer zentralen Stelle gespeichert werden, durch geeignete Sicherheitsvorkehrungen minimiert werden. Zu nennen sind hier z. B. die getrennte Speicherung der Meldedatenbestände sowie ein umfangreiches Rechte- und Rollenkonzept.

Der Brandenburgische IT-Dienstleister wird das zentrale Melderegister des Landes betreiben. Risiken für den Datenschutz und die IT-Sicherheit sind durch geeignete Vorkehrungen zu beherrschen.

4.4.2 Prüfung des Verfahrens zur Beantragung von Reisepässen

Im Berichtszeitraum prüften wir in drei Passbehörden des Landes das Verfahren zur Beantragung und Ausstellung von Reisepässen mit biometrischen Merkmalen (ePass-Verfahren). Die Prüfungen ergaben Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen.

In unserem letzten Tätigkeitsbericht[36] informierten wir über die Einführung von elektronischen Reisepässen. Wir kündigten an, die Beantragung und Ausstellung der elektronischen Reisepässe Anfang 2008 datenschutzrechtlich zu kontrollieren und zu überprüfen, ob die notwendigen technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes getroffen worden sind. Im Folgenden berichten wir über wesentliche Ergebnisse der bei drei Passbehörden durchgeführten Prüfungen.

Erstellung von IT-Sicherheitskonzepten

Gemäß § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) ist von der Daten verarbeitenden Stelle zu untersuchen, ob von einem Verfahren zur Verarbeitung personenbezogener Daten spezifische Risiken ausgehen können. Die Freigabe darf nur erteilt werden, wenn ein aus einer Risikoanalyse entwickeltes IT-Sicherheitskonzept ergeben hat, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch technische und organisatorische Maßnahmen nach § 10 Abs. 1 und 2 BbgDSG beherrscht werden können. In keiner der geprüften Passbehörden konnte jedoch ein vollständiges IT-Sicherheitskonzept vorgelegt werden. Aufgrund der Verarbeitung von sensitiven personenbezogenen Daten haben wir die Erstellung eines ganzheitlichen IT-Sicherheitskonzeptes nach den Standards 100-2 und 100-3 des Bundesamtes für Sicherheit in der Informationstechnik von den Passbehörden gefordert.

Unzulässige Speicherung der Fingerabdrücke

In allen drei Passbehörden erfolgt eine tägliche Datensicherung. Aufgrund der Aufbewahrungsfristen der Sicherungsdatenträger werden unter Umständen auch Fingerabdrücke der Betroffenen länger als zulässig gespeichert. Nach § 16 Abs. 2 Passgesetz (PaßG) sind die bei der Passbehörde gespeicherten Fingerabdrücke spätestens nach Aushändigung des Passes an den Antragsteller zu löschen. Diese Forderung kann derzeit in der Praxis nicht bzw. nur mit unverhältnismäßig hohem Aufwand umgesetzt werden. Hier sind die Hersteller der Meldebehördensoftware gefordert, entsprechende Mechanismen zu implementieren, die sicherstellen, dass die Fingerabdruckdaten nicht in die regelmäßige Datensicherung einbezogen werden. Der sehr unwahrscheinliche Fall, dass Fingerabdrücke durch Systemabstürze verloren gehen, bevor sie zur Bundesdruckerei übertragen werden, sollte hierbei in Kauf genommen werden. Tritt dieser Fall ein, so müssten die Betroffenen ihren Fingerabdruck erneut abgeben. Denkbar wäre auch, dass die Fingerabdruckdaten kurzzeitig auf einem separaten Datenträger (z. B. USB-Stick, externe Festplatte) gesichert werden. Auch in diesem Fall müsste der Her-

[36] vgl. Tätigkeitsbericht 2006/2007, A 1.2.6

steller eine Anpassung der Software vornehmen. Aus unserer Sicht lässt sich das Problem der unzulässigen Datensicherung über einen längeren Zeitraum nur gemeinsam mit dem Hersteller der Software lösen. In einer der geprüften Passbehörden wurden die Datenbanken zwischenzeitlich getrennt und damit die Möglichkeit geschaffen, die Fingerabdrücke der Antragsteller aus der täglichen Datensicherung auszuschließen.

Überprüfung des Fingerabdruckes durch Antragsteller bei Abholung des Passes

Bei den ePass-Lesegeräten der zweiten Generation werden die Fingerabdrücke lediglich auf einem Display angezeigt. Die Vorgaben des Artikels 4 der Verordnung (EG) Nr. 2252/204 des Rates vom 13. Dezember 2004 werden damit jedoch nicht erfüllt. In der Verordnung heißt es u. a.:

„Unbeschadet datenschutzrechtlicher Bestimmungen haben Personen, denen ein Pass oder ein Reisedokument ausgestellt worden ist, das Recht, die personenbezogenen Daten in dem Pass oder dem Reisedokument zu überprüfen und gegebenenfalls eine Berichtigung oder Löschung zu beantragen."

Diese Forderung ist den Passbehörden bekannt, kann aber durch sie allein nicht umgesetzt werden. Aus diesem Grund haben die Datenschutzbeauftragten des Bundes und der Länder das zuständige Bundesministerium des Innern aufgefordert, dafür zu sorgen, dass bei nachfolgenden Generationen der ePass-Lesegeräte die Antragsteller bei Abholung ihres Reisepasses den Fingerabdruck rechtskonform überprüfen können. Überprüfen bedeutet hierbei, die erneute Eingabe des Fingerabdruckes und der softwaretechnische Vergleich mit dem auf dem ePass gespeicherten Fingerabdruck. Das Ministerium hat eine Prüfung zugesichert.

Verschlüsselung sensitiver Daten

Derzeit werden die in den lokalen Netzen übertragenen sowie die in den Datenbanken der Passbehörden gespeicherten personenbezogenen Daten hohen Schutzbedarfs (u. a. Fingerabdrücke) nicht verschlüsselt. Aufgrund ihrer Sensitivität ist eine Verschlüsselung jedoch unabdingbar. Im Zuge der Erstellung des IT-Sicherheitskonzeptes ist daher ein Kryptokonzept zu erarbeiten, in dem die diesbezüglich zu realisierenden Maßnahmen beschrieben werden. Die Verschlüsselung der in der Datenbank gespeicherten Daten kann auch in diesem Fall nur gemeinsam mit dem Hersteller des Verfahrens realisiert werden.

Der Arbeitskreis „Technische und organisatorische Fragen des Datenschutzes" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

hat zu den Problematiken des ePass-Verfahrens Gespräche mit dem Bundesministerium des Innern, den Verfahrensherstellern, dem Bundesamt für Sicherheit in der Informationstechnik und der Bundesdruckerei geführt, in denen Lösungsansätze diskutiert wurden. Das Ministerium hat zudem das Bundesamt beauftragt, eine Handreichung zur Informationssicherheit bei deutschen Passbehörden zu erstellen. Diese Handreichung[37] liegt momentan in der Version 1.5 vor.

Die Prüfung des ePass-Verfahrens in Passbehörden des Landes ergab Mängel bei der Umsetzung von technischen und organisatorischen Maßnahmen. Einige Mängel sind jedoch nur gemeinsam mit den Herstellern der Verfahren und dem für das Verfahren zuständigen Bundesministerium abzustellen.

4.4.3 Unberechtigte Zugriffe auf die Online-Melderegisterauskunft

Im Berichtszeitraum führten wir aufgrund von Informationen eines Fernsehmagazins Kontrollen des Fachverfahrens Online-Melderegisterauskunft in mehreren Kommunalverwaltungen durch. Hierbei bestätigte sich, dass ein unberechtigter Zugriff auf Meldedaten einiger Kommunen möglich war. Weiterhin wurden erhebliche Mängel bei der Umsetzung technisch-organisatorischer Maßnahmen festgestellt.

Bereits vor Ausstrahlung des Fernsehbeitrages wandten sich die Redakteure an uns. Wir erhielten die Information, dass eine Firma, die Meldebehörden mit Software ausstattet, sowohl Benutzername als auch Initialpasswort eines autorisierten Nutzerzugangs im Internet publiziert. Da mehrere Kommunen dieses Initialpasswort nicht änderten, waren mit der Zugangsberechtigung Bürgerdaten öffentlich zugänglich. Eine Überprüfung des Sachverhaltes ergab, dass die betreffende Internetseite durch die Softwarefirma bereits abgeschaltet wurde. Die Inhaltsdaten waren jedoch noch über den Google-Cache einsehbar. Aufgrund der bundesweiten Verbreitung der eingesetzten Software waren nicht nur Brandenburger Kommunen von dem Sicherheitsvorfall betroffen. Insofern informierten wir unverzüglich die Kollegen der anderen Bundesländer über die eventuell bestehende Sicherheitslücke.

Auch die Fachaufsicht für die Meldebehörden im Ministerium des Innern wurde eingeschaltet. Sie erteilte die Anweisung, alle Verfahren zur Online-Melderegisterauskunft mit sofortiger Wirkung abzuschalten.

[37] siehe http://www.lda.brandenburg.de → Informationsmaterial → Orientierungshilfen und Handlungsempfehlungen→ Handreichung „Informationssicherheit für deutsche Passbehörden“

Unsere vor Ort im Beisein der Fachaufsicht durchgeführten Kontrollen ergaben, dass bei zwei Meldebehörden unberechtigte Zugriffe nachvollzogen werden konnten, die vermutlich den Recherchen der Journalisten zuzurechnen sind. Anhaltspunkte, die diese Vermutung stützen, sind der Zeitpunkt der Recherchen sowie die im Fernsehbeitrag gezeigten Abrufe. Es kann jedoch nicht mit Sicherheit ausgeschlossen werden, dass weitere unberechtigte Zugriffe erfolgt sind. Dies resultiert aus der Tatsache, dass es in der Software Unregelmäßigkeiten in der Protokollierung gab bzw. über den genannten Zugang Protokolle hätten manipuliert werden können.

In allen geprüften Meldebehörden waren die Unterlagen zur Verfahrensdokumentation unvollständig oder nicht vorhanden. Dies betraf insbesondere die Sicherheitskonzepte nach § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) sowie die Verfahrensverzeichnisse nach § 8 BbgDSG. Eine gründliche Betrachtung der technisch-organisatorischen Maßnahmen gemäß § 10 BbgDSG ist von Seiten der Kommunalverwaltungen ebenfalls nicht erfolgt. Bei Beachtung der gesetzlichen Anforderungen wäre ein unberechtigter Zugriff auf die Meldedaten leicht zu verhindern gewesen: Spätestens bei der Prüfung der Umsetzung des Sicherheitskonzeptes hätte auffallen müssen, dass das Initialpasswort für den Zugang zum Online-Melderegister nicht geändert wurde.

Für die Wiederaufnahme des Verfahrens in den betreffenden Kommunen war es notwendig, die verfahrensspezifischen IT-Systeme neu aufzusetzen und neue Zugangsrechte und Passwörter zu vergeben, da nicht ausgeschlossen werden konnte, dass sich eine Person während eines unberechtigten Zugriffs einen eigenen Nutzerzugang eingerichtet hatte. In Vorbereitung der Wiederaufnahme des Verfahrens waren die Kommunen angehalten, ihrer Pflicht zur

- Sicherstellung des Datenschutzes, insbesondere der Verpflichtung zur Durchführung einer Risikoanalyse und zur Erstellung eines Sicherheitskonzeptes gemäß § 7 Abs. 3 BbgDSG,
- Erstellung eines Verfahrensverzeichnisses gemäß § 8 BbgDSG,
- Meldung automatisierter Verfahren gemäß § 9 BbgDSG sowie
- Festlegung und Umsetzung von technischen und organisatorischen Maßnahmen gemäß § 10 BbgDSG

nachzukommen. Bislang hat nur eine Kommune diese Anforderungen erfüllt und das Verfahren wieder aufgenommen.

Die Änderung von Initialpasswörtern gehört zu den grundlegenden technischen Sicherheitsmaßnahmen, die vor Inbetriebnahme eines Verfahrens umzusetzen sind. In den betreffenden Kommunen wurden die Sorgfaltspflichten grob verletzt.

4.5 Datenverarbeitung, Statistik, Wahlen

4.5.1 Vorbereitungen zur Volkszählung 2011

In der Bundesrepublik Deutschland wird am 9. Mai 2011 eine Volkszählung (Zensus) durchgeführt. Diese erfolgt, wie bereits im letzten Tätigkeitsbericht[38] dargestellt, registergestützt. Zur Vorbereitung der Zählung sind umfangreiche Vorarbeiten notwendig, die durch entsprechende Gesetze und Regelungen klar definiert werden müssen. Zu den jeweiligen Gesetzgebungsverfahren gaben wir unsere Stellungnahmen ab, die nicht immer vollständig berücksichtigt wurden.

Der von der Europäischen Union verbindlich vorgeschriebene Zensus wird durchgeführt, um verlässliche Bevölkerungszahlen als Grundlage für politische und wirtschaftliche Entscheidungen zu erhalten. Bereits im Dezember 2007 wurde das Zensusvorbereitungsgesetz[39] verabschiedet. Damit wurden die rechtlichen Voraussetzungen für die Vorbereitung des Zensus 2011 gelegt. Insbesondere regelt das Gesetz den Aufbau eines Anschriften- und Gebäuderegisters sowie eines Verzeichnisses zum Geburtsort und Geburtsstaat. Es legt weiterhin fest, welche Daten die Behörden aus ihren Registern dem Statistischen Bundesamt und den Statistischen Landesämtern zu übermitteln haben.

In unserer Stellungnahme zum anschließenden Entwurf des Zensusgesetzes 2011 bemängelten wir u. a., dass bei den Stichprobenerhebungen zusätzlich zu dem von der EU vorgegebenen Datenkatalog[40] das Merkmal „Zugehörigkeit zu einer Religionsgemeinschaft“ aufgenommen wurde. Unser Vorschlag, dieses Merkmal zu streichen, fand jedoch keine Berücksichtigung und wurde in der im Juli 2009 in Kraft getretenen Fassung des Zensusgesetzes[41] sogar noch erweitert. Bei den Stichprobenerhebungen wird nun auch nach dem

38 vgl. Tätigkeitsbericht 2006/2007, A 5.3.4

39 Gesetz zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2011 vom 8. Dezember 2007 (BGBl. I S. 2808)

40 Verordnung (EG) Nr. 763/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über Volks- und Wohnungszählungen (Abl. EU Nr. L 218 S. 14)

41 Gesetz über den registergestützten Zensus im Jahre 2011 (Zensusgesetz 2011 – ZensG 2011) vom 8. Juli 2009 (BGBl. I S. 1781)

Bekenntnis zu einer Religion, Glaubensrichtung oder Weltanschauung gefragt.

Zurzeit wird die Umsetzung der Volkszählung in den Bundesländern vorbereitet. Dazu müssen die Länder Ausführungsgesetze erlassen. Unsere Behörde ist dabei von Beginn an vom zuständigen Ministerium des Innern und dem für die Durchführung des Zensus zuständigen Amt für Statistik Berlin-Brandenburg beteiligt worden. Wichtig wird es unter anderem sein, bei den Datenerhebungen darauf zu achten, dass dem verfassungsrechtlichen Gebot der Abschottung der amtlichen Statistik vom Verwaltungsvollzug[42] Genüge getan wird.

Die Daten der Volkszählung sind nur für die damit verbundenen Zwecke zu nutzen. Personenbezogene Daten Einzelner dürfen nicht in die Verwaltungen fließen.

4.5.2 IT-Sicherheitskonzepte der Ministerien – eine Bestandsaufnahme

Im Ergebnis der Behandlung unseres letzten Tätigkeitsberichts fasste der Brandenburgische Landtag im November 2008 einen Beschluss,[43] der die Landesregierung u. a. aufforderte, unserer Behörde „zeitnah die Sicherheitskonzepte der Landesministerien vorzulegen". Hierdurch ergab sich für uns die Möglichkeit einer umfassenden Bestandsaufnahme.

Jede Daten verarbeitende Stelle hat gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) jedes Verfahren, in dem personenbezogene Daten automatisiert verarbeitet werden und für das ein Verfahrensverzeichnis gem. § 8 BbgDSG zu erarbeiten ist, freizugeben. Die Freigabe darf nur dann erteilt werden, wenn nachgewiesen ist, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch geeignete technische und organisatorische Sicherheitsmaßnahmen beherrscht werden können. Hierzu ist ein Sicherheitskonzept zu erstellen und umzusetzen.

Auch die IT-Sicherheitsleitlinie für die Landesverwaltung Brandenburg[44] verlangt die Erarbeitung und Umsetzung von IT-Sicherheitskonzepten. Sie

---

42 BVerfGE 65, 1 vom 15. Dezember 1983

43 vgl. Landtag Brandenburg, Drucksache 4/6891-B

44 Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg vom 2. Oktober 2007, zuletzt geändert durch Runderlass der Landesregierung vom 22. September 2009

bezieht sich dabei nicht nur auf Verfahren zur Verarbeitung personenbezogener Daten, sondern schließt auch alle anderen IT-Verfahren ein.

Die Landesregierung beauftragte das Ministerium des Innern mit der Koordinierung der Umsetzung des genannten Landtagsbeschlusses. Mit den Verantwortlichen erörterten wir die konkrete Vorgehensweise. Dabei wurde festgelegt, dass uns zunächst alle Ministerien eine Übersicht über die Verfahren, in denen personenbezogene Daten verarbeitet werden, zusammen mit dem jeweils aktuellen Stand hinsichtlich der entsprechenden IT-Sicherheitskonzepte zukommen lassen. Über weitere Aktivitäten unsererseits sollte nach Vorliegen und Auswertung dieser Übersichten entschieden werden.

Insgesamt dauerte es sieben Monate, bis alle Antworten aus den einzelnen Ministerien vollständig vorlagen. Es ergab sich ein sehr heterogenes und z. T. unbefriedigendes Bild:

- Ein Ressort führte überhaupt keine konkreten Verfahren an und berichtete pauschal, dass Sicherheitskonzepte „zurzeit überarbeitet oder neu erstellt werden“.

- Bei mehreren Ressorts fehlten in der Übersicht einzelne Verfahren, deren Vorhandensein uns aus dem regelmäßigen Arbeitskontakt jedoch bekannt war (z. B. Verfahren zur Personaldatenverwaltung oder zum Haushalts-, Kassen- und Rechnungswesen).

- In einem Fall wurde ein Sicherheitskonzept als „fertig“ gemeldet, obwohl unsere Beratungstätigkeit hierzu anschließend noch mehrere Monate in Anspruch nahm.

- Ein Ressort berichtete, dass nur Verfahren mit normalem Schutzbedarf im Einsatz seien. Die Übersicht enthielt jedoch z. B. auch ein System zur Personaldatenverwaltung.

- Auffällig war, dass mehrere Ressorts die Fortschreibung ihrer Konzepte just für 2009/10 vorgesehen hatten.

Wir behalten uns vor, stichprobenartig einzelne Ressorts bzw. Verfahren in der Zukunft genauer zu prüfen.

Die Erarbeitung, Umsetzung und regelmäßige Fortschreibung von IT-Sicherheitskonzepten ist nicht nur aufgrund rechtlicher Bestimmungen erforderlich. Sicherheitskonzepte bilden auch eine unverzichtbare Arbeitsgrundlage für die verantwortlichen Systemadministratoren und ein wesentliches Element eines kontinuierlichen und systematischen IT-Sicherheitsmanagements. Wir fordern die Landesministerien auf, noch bestehende Lücken in diesem Bereich unverzüglich zu schließen.

4.5.3 IT-Sicherheitsmanagement in der Landesverwaltung

Im Herbst des Jahres 2007 erließ die Landesregierung die IT-Sicherheitsleitlinie[45] für die Landesverwaltung Brandenburg. Diese beschreibt den Aufbau und den Betrieb eines zentral koordinierten, ressortübergreifenden Managementsystems zur Informationssicherheit. Was hat sich seitdem Konkretes getan?

Wesentliche Festlegungen, die in der IT-Sicherheitsleitlinie für die Landesverwaltung getroffen werden, beziehen sich auf den Aufbau einer Organisationsstruktur für das Informationssicherheitsmanagement, die Durchsetzung von Mindeststandards für IT-Sicherheit und die Etablierung eines landesweiten IT-Sicherheitsprozesses. In allen drei Gebieten sind für den Berichtszeitraum erste Ergebnisse zu verzeichnen:

- Das landesweite IT-Sicherheitsmanagement-Team hat sich im Januar 2008 konstituiert. Vertreten sind die IT-Sicherheitsbeauftragten aller Ressorts. Unsere Behörde wirkt beratend mit. Die Leitung des Teams obliegt dem IT-Sicherheitsmanager des Landes. Nach einer zwischenzeitlichen, mehrmonatigen Vakanz ist dessen Stelle seit Mitte 2009 wieder besetzt.

- Einzelne Ressorts haben ressortspezifische IT-Sicherheitsrichtlinien als Spezialisierungen und Untersetzungen der zentralen landesweiten IT-Sicherheitsleitlinie verabschiedet. Zum Teil wurden wegen der Größe des nachgeordneten Bereichs auch innerhalb der Geschäftsbereiche von Ministerien hierarchische Strukturen für die Sicherheitsorganisation gebildet.

- Beim Brandenburgischen IT-Dienstleister befindet sich das CERT BB (Computer Emergency Response Team Brandenburg) als Anlaufstelle für präventive und reaktive Maßnahmen der IT-Sicherheit im Aufbau. Darüber hinaus wird vom Dienstleister zurzeit ein landesweites Sicherheitsinforma-

[45] Leitlinie zur Gewährleistung der IT-Sicherheit in der Landesverwaltung Brandenburg vom 2. Oktober 2007, zuletzt geändert durch Runderlass der Landesregierung vom 22. September 2009

tionssystem zur effektiven Unterstützung des IT-Sicherheitsmanagementprozesses eingerichtet und getestet.

- Der Stand bei der Durchsetzung von Mindeststandards im Bereich der IT-Sicherheit ist in einzelnen Ressorts sehr unterschiedlich.[46] Wir erwarten, dass in den betreffenden Bereichen noch fehlende ressortspezifische IT-Sicherheitsrichtlinien erarbeitet und die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik zur Gewährleistung des IT-Grundschutzes umfassend und zügig umgesetzt werden (Sicherheitskonzepte, Realisierung von Sicherheitsmaßnahmen).

- Im Rahmen der Beratungen des IT-Sicherheitsmanagement-Teams stellten verschiedene landesweite IT-Projekte die jeweiligen IT-Sicherheitskonzepte vor. Weiterhin wurden Maßnahmepläne zur Reaktion auf Stör- oder Notfälle in IT-Systemen der Landesverwaltung diskutiert und abgestimmt.

Der Aufbau und Betrieb des landesweit koordinierten, ressortübergreifenden Informationssicherheitsmanagementsystems muss in den kommenden Jahren zielgerichtet und auf der Basis der IT-Sicherheitsleitlinie des Landes fortgeführt werden. Dabei sind auch Aktivitäten zur Prüfung der Wirksamkeit und der Qualität der Umsetzung von IT-Sicherheitskonzepten bzw. Sicherheitsmaßnahmen durchzuführen (Sicherheitsaudits, Penetrationstests). Darüber hinaus müssen aus den in der Leitlinie vorgesehenen jährlichen Berichten zum Stand der IT-Sicherheit in der Landesverwaltung Arbeitsschwerpunkte und strategische Entwicklungslinien abgeleitet werden.

Die Etablierung, Aufrechterhaltung und Verbesserung eines Informationssicherheitsmanagementprozesses ist eine dauerhafte Aufgabe für jede Verwaltung. Die hierfür erforderlichen personellen, materiellen und zeitlichen Ressourcen sind von der jeweiligen Leitung zur Verfügung zu stellen.

4.5.4 Neuer Brandenburgischer IT-Dienstleister

Zu Beginn des Jahres 2009 wurde der Brandenburgische IT-Dienstleister (ZIT-BB) als zentraler IT-Dienstleister für die Landesverwaltung Brandenburg gegründet. Eine seiner wesentlichen Aufgaben ist die Konsolidierung der IT-Infrastruktur der brandenburgischen Landesverwaltung.

Im Juli 2008 hat die Landesregierung die Errichtung eines zentralen IT-Dienstleisters[47] für das Land Brandenburg (Brandenburgischer IT-Dienst-

[46] vgl. A 4.5.2

[47] siehe http://www.zit-bb.brandenburg.de

leister) zum 1. Januar 2009 beschlossen.[48] Der ehemalige Landesbetrieb für Datenverarbeitung und IT-Serviceaufgaben (LDS) wurde in den neuen Brandenburgischen IT-Dienstleister überführt. Weiterhin ist vorgesehen, in einer ersten Phase den überwiegenden Teil der dezentralen IT-Infrastukturen sowie des dazugehörigen Personals aus den Ressorts und deren nachgeordneten Bereichen in den ZIT-BB überzuleiten. Diese Phase soll im Jahr 2010 abgeschlossen werden. Daran anschließend erfolgt die Konsolidierung der Infrastruktur durch Migration der vom ZIT-BB übernommenen dezentralen IT-Infrastukturen auf einheitliche Plattformen. Die Landesregierung erhofft sich dadurch Synergieeffekte.

Die Aufgaben des Brandenburgischen IT-Dienstleisters werden in § 2 der Anlage zum Errichtungserlass[49] wie folgt aufgeführt:

1. Operative Planung, Bereitstellung und Betrieb der technischen Infrastruktur (z. B. Landesverwaltungsnetz, Daten- und Telekommunikations-Verbund des Landtages, der Ministerien, der Staatskanzlei und des Landesrechnungshofes, Server, Arbeitsplatzcomputer, Endgeräte) und der ressortübergreifenden Fach- und Querschnittsverfahren (z. B. Bürokommunikation, E-Mail, Internet- und Intranetdienste, Telekommunikationsdienste), insbesondere zur Modernisierung der Verwaltung (z. B. E-Government), in der Regel einschließlich des technischen Betriebes der ressortspezifischen Fachverfahren, sowie Beratung hierzu unter Beachtung der Sicherheitsanforderungen,

2. IT-Sicherheitsmanagement für IT-Infrastruktur der Landesverwaltung; Betrieb eines Computer-Emergency-Response-Teams (CERT) zur Bündelung operativer Sicherheitsaufgaben,

3. Beobachtung und Erprobung von fachlichen, technischen und organisatorischen Entwicklungen im Rahmen der allgemeinen Aufgabenstellung,

4. IT-Projektmanagement,

5. Operative Steuerung des IT-Sicherheitsmanagements sowie Beratung und Serviceleistungen im Zusammenhang mit Datenschutz und IT-Sicherheit,

6. Beratung und Unterstützung des Ausschusses der Ressort Information Officers (RIO-Ausschuss) bei Fragen des IT-Einsatzes,

---

48 Beschluss Nr. 796/08 der Landesregierung vom 15. Juli 2008

49 Erlass des Ministeriums des Innern zur Errichtung des Landesbetriebes „Brandenburgischer IT-Dienstleister" und zur Auflösung des Landesbetriebes für Datenverarbeitung und IT-Serviceaufgaben (LDS) vom 15. Dezember 2008

7. Verfahrensentwicklung, -pflege und -betreuung für Querschnittsverfahren und ressortübergreifende Fachverfahren, soweit diese nicht gemäß länderübergreifenden Vereinbarungen in Verbünden entwickelt, gepflegt oder betreut werden,

8. Ausbildungsbetrieb für IT-Berufe,

9. IT-Fortbildung entsprechend IT-Fortbildungsprogramm.

Das Ministerium des Innern hat unsere Behörde im Juni 2008 über die Errichtung eines zentralen IT-Dienstleisters informiert. Durch die frühzeitige Einbeziehung erhielten wir die Möglichkeit, unsere Forderungen bezüglich der Umsetzung von technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes in den Prozess einzubringen. Nachfolgend werden einige wesentliche Forderungen, die bei der Errichtung des zentralen IT-Dienstleisters zu berücksichtigen sind, zusammengefasst:

- Bei der Übertragung der Aufgaben von den Ressorts und ihrem jeweils nachgeordneten Bereich auf den ZIT-BB handelt es sich um eine Datenverarbeitung im Auftrag gem. § 11 Brandenburgisches Datenschutzgesetz (BbgDSG), bei der die Ressorts als Daten verarbeitende Stellen den Auftragnehmer ZIT-BB mit der Verarbeitung ihrer Daten beauftragen und insoweit weisungsbefugt sind. Dazu bedarf es gem. § 11 BbgDSG eines Vertrages. Der Vertrag muss u. a. das Weisungsrecht der Ressorts klar ausgestalten und eine Kündigungsmöglichkeit der Vertragspartner für den Fall vorsehen, dass die vertraglichen Pflichten nicht eingehalten werden. Weiterhin ist im Vertrag festzulegen, dass die jeweilige Daten verarbeitende Stelle eine Risikoanalyse gem. § 7 BbgDSG hinsichtlich der Verarbeitung personenbezogener Daten vornimmt, da nur sie beurteilen kann, ob davon spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen. Der ZIT-BB sollte das Sicherheitskonzept anhand der örtlichen und personellen Gegebenheiten sowie des Ergebnisses der Risikoanalyse entwickeln. Damit der Auftraggeber seiner Verantwortung als Daten verarbeitende Stelle auch im Zusammenhang mit den technisch-organisatorischen Maßnahmen beim Auftragnehmer gerecht werden kann, muss er das Sicherheitskonzept genehmigen. Es sollte daher ebenso wie die Risikoanalyse Bestandteil des Vertrages werden.

- Die Daten verarbeitenden Stellen als Auftraggeber müssen entsprechend qualifizierte Bedienstete benennen oder IT-Kopfstellen bilden, die die weiter bestehende datenschutzrechtliche Verantwortung der Daten verarbeitenden Stelle gegenüber dem ZIT-BB wahrnehmen und gegebenenfalls entsprechende Weisungen an dessen Bedienstete erteilen können. Die

Auftraggeber müssen personell und organisatorisch in der Lage sein, die Verarbeitung der Daten in ihrem Auftrag beim ZIT-BB zu kontrollieren.

- Die Zentralisierung von IT-Strukturen, insbesondere die von Servern, zieht zwangsläufig eine Veränderung der Datenflüsse nach sich. Die Realisierung von technischen und organisatorischen Maßnahmen hängt im starken Maße davon ab, ob die Server im dezentralen Bereich der Daten verarbeitenden Stelle oder bei einem IT-Dienstleister in einem Rechenzentrum untergebracht sind. Befindet sich beispielsweise der E-Mail-Server im lokalen Netz (LAN) einer Behörde und versendet ein Mitarbeiter personenbezogene Daten an einen Mitarbeiter derselben Behörde, so werden die Daten vom Arbeitsplatzcomputer (APC) zum E-Mail-Server und dann zum APC des empfangenden Mitarbeiters übertragen. Die Daten verlassen das lokale Netz der Behörde nicht. Ist der E-Mail-Server bei einem zentralen IT-Dienstleister untergebracht, ergibt sich eine völlig andere Konstellation. Die Daten werden über das LAN der Behörde und dann über das Landesverwaltungsnetz (LVN) zum E-Mail-Server und wieder zurück zum Empfänger der E-Mail übertragen. Bei der dezentralen Lösung haben nur die lokalen Administratoren eine Zugriffsmöglichkeit auf die auf dem E-Mail-Server gespeicherten Dateien. Anders verhält es sich bei zentraler Speicherung: Hier kann der Zugriff der Administratoren des IT-Dienstleisters auf die Daten des E-Mail-Servers sowie der Zugriff von Dritten auf die im LVN übertragenen E-Mails nicht ausgeschlossen werden. Wenn personenbezogene Daten im LVN übertragen werden, so sind diese mit sicheren kryptographischen Verfahren zu verschlüsseln. Kryptographische Verfahren (z. B. symmetrische und asymmetrische Verschlüsselung, digitale Signatur) sind besonders geeignet, um Verletzungen des Datenschutzes beim Transport schutzwürdiger, elektronisch gespeicherter Daten zu verhindern. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler nachweisen und die unberechtigte Kenntnisnahme verhindern. Derartige Verfahren sind heute Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden.

- Bei der Zentralisierung von IT-Strukturen ist § 7 Abs. 1 BbgDSG zu beachten. Danach soll die Datenverarbeitung so organisiert sein, dass bei der Verarbeitung von personenbezogenen Daten die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist. Das gilt insbesondere für Datenbankanwendungen. Werden beispielsweise sensitive personenbezogene Daten (z. B. Personaldaten, Gesundheitsdaten) bei einem IT-Dienstleister verarbeitet, so müssen die Daten in verschiedenen Datenbanken abgelegt werden. Eine Verschlüsselung der in der Datenbank gespeicherten sensitiven personenbezogenen Daten ist ebenfalls unabdingbar.

Bei der Errichtung des Brandenburgischen IT-Dienstleisters müssen die Belange des Datenschutzes berücksichtigt werden. Die Zentralisierung von IT-Strukturen erfordert die zusätzliche Realisierung von technisch-organisatorischen Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten. Jede Daten verarbeitende Stelle muss ihrer Kontrollpflicht gegenüber dem Dienstleister nachkommen.

4.5.5 Die elektronische Akte in der Landesverwaltung – EL.DOK BB nimmt Fahrt auf

Entsprechend der IT-Strategie des Landes Brandenburg wurde im Frühjahr 2008 die Entscheidung zur Einführung eines einheitlichen Dokumentenmanagement- und Vorgangsbearbeitungssystems (DMS/VBS) in der Landesverwaltung getroffen.

Über die wesentlichen Ziele, die mit der Einführung eines einheitlichen DMS/VBS in der gesamten Landesverwaltung verfolgt werden, hatten wir bereits in unserem letzten Tätigkeitsbericht[50] informiert. Dort berichteten wir auch darüber, dass in der Ausschreibung wesentliche Anforderungen an das zukünftige System aus der Sicht des Datenschutzes und der IT-Sicherheit festgeschrieben worden waren. Die Umsetzung dieser Anforderungen konnten wir im Rahmen des aktuellen Projekts EL.DOK BB zur Einführung des DMS/VBS begleiten.

Im Fokus stand zunächst die Ableitung einer geeigneten Systemarchitektur. Vereinbart wurde, dass das einheitliche DMS/VBS für die Landesverwaltung zentral beim Brandenburgischen IT-Dienstleister betrieben wird. Zur Umsetzung des Grundsatzes der Trennung der Datenverarbeitung nach den jeweils verfolgten Zwecken und den Gruppen von Betroffenen werden für jedes Ressort eigene Applikationsserver (hier als virtuelle Maschinen) sowie eine eigene Datenhaltung in einer Datenbank realisiert. Diese Systemtrennung sichert auch das Prinzip der Ressorthoheit und erlaubt eine Anpassung und Weiterentwicklung des jeweiligen ressortspezifischen DMS/VBS an die konkreten lokalen Anforderungen und Verwaltungsprozesse. Die einheitliche funktionelle Basis wird im Rahmen eines Landesreferenzmodells festgelegt. Dieses deckt die grundlegenden Abläufe in der Landesverwaltung ab, wie sie in der gemeinsamen Geschäftsordnung festgelegt sind.

Spezielle DMS/VBS-Systeme werden für den Landtag (ELVIS – Elektronisches Landtagsvorgangsbearbeitungs- und -informationssystem) und das Brandenburgische Landeshauptarchiv vorgesehen. Der ressortübergreifenden Kooperation dienen die Systeme EL.KIS (Elektronisches Kabinettinfor-

[50] vgl. Tätigkeitsbericht 2006/2007, A 5.3.2

mationssystem) und EL.ZA (Werkzeug für projekt- oder gremienbezogene Zusammenarbeit).

Zur Sicherung der Vertraulichkeit der Geschäftsabläufe bzw. der Dokumente und im Vorgriff auf die zu erwartenden Anforderungen, das DMS/VBS auch für Daten mit hohem Schutzbedarf verwenden zu können, wurden bereits in einer frühen Projektphase folgende Festlegungen getroffen:

- Alle Daten werden nach Ressorts getrennt und verschlüsselt in einer Datenbank gespeichert.

- Spezifische Mechanismen des Datenbankservers garantieren, dass Systemadministrations- und Wartungspersonal keinen Zugriff auf die gespeicherten Daten erhält.

- Jegliche Kommunikation zwischen den zentralen Systemkomponenten beim Brandenburgischen IT-Dienstleister und den dezentralen Clients in den Ressorts erfolgt verschlüsselt. Gleiches gilt auch für die Kommunikation zwischen Applikations- und Datenbankserver innerhalb des Rechenzentrums.

Entscheidet sich ein Ressort, Daten mit hohem Schutzbedarf im DMS/VBS zu verarbeiten, sind ggf. weitere IT-Sicherheitsmaßnahmen aus den jeweils im Einzelfall zu betrachtenden Risiken abzuleiten. Diese könnten z. B. die Integrität und Authentizität von Dokumenten durch den Einsatz qualifizierter elektronischer Signaturen sicherstellen, eine starke Mehrfaktorauthentisierung der Nutzer verlangen oder die Verwendung von Chipkarten zur Verwaltung privater Schlüssel vorsehen.

Ein weiterer Schwerpunkt unserer Beratungstätigkeit im Projekt EL.DOK BB war die Erfüllung der formalen Anforderungen des Brandenburgischen Datenschutzgesetzes (BbgDSG) im Zuge der Einführung des DMS/VBS in einem Ressort. Hier ist zu beachten, dass aufgrund der konsequenten Systemtrennung grundsätzlich jedes Ressort selbst Daten verarbeitende Stelle ist und damit den gesetzlichen Verpflichtungen nachkommen muss. Dies betrifft z. B. die Freigabe des Verfahrens gem. § 7 Abs. 3 BbgDSG, die Erstellung einer Risikoanalyse und eines Sicherheitskonzepts gem. § 7 Abs. 3 BbgDSG, die Erarbeitung eines Verfahrensverzeichnisses gem. § 8 BbgDSG, ggf. die Vorabkontrolle durch den behördlichen Datenschutzbeauftragten gem. § 10a BbgDSG oder die Vertragsgestaltung bei der Datenverarbeitung im Auftrag durch den IT-Dienstleister gem. § 11 BbgDSG.

Wie in dem Projekt PERIS[51] bestehen auch in EL.DOK BB bei den einzelnen ressortspezifischen DMS/VBS weitgehend einheitliche Anforderungen bzgl. Datenschutz und IT-Sicherheit (bei Beschränkung auf das Landesreferenzmodell und Nutzung der vereinbarten technischen Infrastruktur). Dadurch war es ähnlich der Vorgehensweise in PERIS möglich, aus Projektmitteln die Erarbeitung eines gemeinsamen Sicherheitskonzepts für die zentral beim Brandenburgischen IT-Dienstleister betriebenen Systemkomponenten zu finanzieren. Das Konzept liegt mittlerweile vor. Die dort abgeleiteten Sicherheitsmaßnahmen sind durch den Dienstleister für jede DMS/VBS-Installation in gleicher Weise umzusetzen. Der Abschluss der Arbeiten ist für Mitte des Jahres 2010 avisiert.

Das existierende DMS/VBS-Sicherheitskonzept enthält auch Sicherheitsrichtlinien bzw. Mustersicherheitskonzepte für die Clientseite der DMS/VBS. Sie sind vor Einführung eines ressortspezifischen DMS/VBS entsprechend den dortigen Besonderheiten (wie z. B. der konkreten Infrastruktur oder dem Schutzbedarf der im DMS/VBS zu verarbeitenden Dokumente) zu spezialisieren. Gleiches gilt für die lokale Ausprägung und evtl. erforderliche Anpassung des Rechte- und Rollenkonzepts. Im Rahmen des Freigabeverfahrens sowie ggf. der Vorabkontrolle durch den jeweiligen behördlichen Datenschutzbeauftragten ist auch die Umsetzung der Sicherheitskonzepte zu prüfen.

EL.DOK BB hat sich als äußerst komplexes und anspruchsvolles Projekt in der Landesverwaltung erwiesen. Durch unsere frühe Einbindung konnten die hohen Anforderungen an Datenschutz und IT-Sicherheit bei der Einführung des landesweit einheitlichen DMS/VBS rechtzeitig berücksichtigt werden. Spezielle Anforderungen im DMS/VBS eines Ressorts oder wesentliche Abweichungen von den im Landesreferenzmodell festgelegten Funktionen müssen zu einer Fortschreibung des zentral bereitgestellten Sicherheitskonzepts führen. Hierfür ist allein das jeweilige Ressort als Daten verarbeitende Stelle verantwortlich.

4.5.6 IP-Telefonie im LVN 3.0

Zwar wird in zunehmendem Maße über das Datennetz der Landesverwaltung telefoniert, technischen und organisatorischen Maßnahmen für einen sicheren Betrieb der paketvermittelten Kommunikation sind jedoch noch nicht vollständig umgesetzt.

Die Richtlinien und Empfehlungen für das Telefonieren über das Datennetz – Voice over IP, IP-Telefonie –, insbesondere die Anforderungen[52] an einen

51 vgl. A 4.6.3

52 vgl. Tätigkeitsbericht 2006/2007, A 2.5

datenschutzgerechten und sicheren Betrieb liegen bereits seit Anfang des Jahres 2007 vor. Sie wurden in der ressortübergreifenden Arbeitsgruppe „IP-Telefonie im LVN“ abgestimmt.

Trotz der stetig steigenden Teilnehmerzahlen, die sich in der Anzahl der vom Brandenburgischen IT-Dienstleister betreuten IP-Telefonie-Endgeräte widerspiegelt (Ende 2008 ca. 1200 IP-Telefone), sind die informationssicherheitsbezogenen Vorgaben der genannten Arbeitsgruppe nicht vollständig realisiert. So fehlt es noch immer an der kryptografischen Absicherung der Sprachdaten (Ende-zu-Ende-Verschlüsselung) und der Signalisierungsströme zur Wahrung des grundrechtsrelevanten Fernmeldegeheimnisses.

Das für die Freigabe des automatisierten Verfahrens gem. § 7 Abs. 3 Brandenburgisches Datenschutzgesetz erforderliche Sicherheitskonzept liegt bislang nur in einer unvollständigen und nicht dem Schutzbedarf angemessenen Vorabversion vor, dessen Überarbeitung dringend notwendig ist.

Der Brandenburgische IT-Dienstleister hat zugesagt, die vereinbarten Sicherheitsfunktionen nach Umstellung des Call Manager Clusters auf die Softwareversion 7 umgehend zu aktivieren.

Trotz mehrjähriger Nutzung ist bei der IP-Telefonie im Landesverwaltungsnetz das Fernmeldegeheimnis noch immer gefährdet. Ein vollständiges Sicherheitskonzept steht aus.

4.6 Personaldaten

4.6.1 Novellierung des Landesbeamtengesetzes

Mit der Föderalismusreform und dem Beamtenstatusgesetz[53] eröffnete sich für das Land Brandenburg ein Handlungsspielraum, das öffentliche Dienstrecht neu zu regeln. Das Ministerium des Innern beteiligte uns frühzeitig mit der Übersendung eines Entwurfs des novellierten Landesbeamtengesetzes.

Der Entwurf sah unter anderem vor, dass eine Kenntnisnahme von Personalaktendaten im Rahmen der Datensicherung oder Sicherung des ordnungsgemäßen Betriebs eines Systems zur Datenverarbeitung zugelassen sein sollte, wenn diese nach dem Stand der Technik nicht oder nur mit unverhältnismäßigem Aufwand zu vermeiden wäre.

53 Gesetz zur Regelung des Statusrechts der Beamtinnen und Beamten in den Ländern vom 17. Juni 2008 (BGBl. I S. 1010)

Eine solche Aufweichung der bislang geltenden engen Zugriffsbeschränkungen war aus unserer Sicht nicht erforderlich. Im Rahmen der Datensicherung (Backups) kann durch den Einsatz geeigneter kryptographischer Verfahren nach dem heutigen Stand der Technik zuverlässig die Kenntnisnahme von Personalaktendaten ausgeschlossen werden. Gleiches gilt für die Sicherung des ordnungsgemäßen Betriebs hinsichtlich der Aussperrung von Systemadministratoren. Fachadministratoren können dagegen im Ausnahmefall z. B. zur Fehlersuche und -behebung oder bei Wartungsarbeiten Personalaktendaten einsehen, falls dies erforderlich ist. Hierbei sind die Grundsätze von § 11a Brandenburgisches Datenschutzgesetz (BbgDSG) zu beachten. Alle derartigen Kenntnisnahmen sind zu protokollieren.

Mit dem Ministerium wurde ein Konsens gefunden und die beabsichtigte Regelung aus dem Entwurf gestrichen. Die allgemeinen Grundsätze der §§ 10 und 11a BbgDSG gelten unmittelbar.

Im Hinblick auf die im Entwurf enthaltene automatisierte Personalaktenführung konnte jedoch keine Einigung erzielt werden. Die damit verbundenen Folgeprobleme wurden weder im Gesetzentwurf noch in dessen Begründung beachtet. Wir haben deshalb angeregt, im Gesetz eine Verordnungsermächtigung vorzusehen, um die Einzelheiten zur Einführung der automatisierten Personalakte zu regeln. Das novellierte Landesbeamtengesetz[54] trat ohne eine solche Ermächtigung in Kraft, da das Ministerium sie nicht für erforderlich hielt.

Eine Verordnung halten wir nach wie vor für notwendig. Vor dem Hintergrund der fehlenden gesetzlichen Ermächtigung sollte das Ministerium folgende Punkte in einer Verwaltungsvorschrift übergangsweise regeln:

- Umgang mit Hybridakten (d. h. solchen, die teilweise elektronisch und teilweise auf Papier geführt werden), Vermeidung von Doppelerfassung in Papier- und elektronischer Akte, Festlegung der führenden Akte,

- Einsatz digitaler Signaturen für Teile der elektronischen Akte, Abbildung des Schriftformerfordernisses,

- verschlüsselte Speicherung sensitiver Personalaktendaten,

- Protokollierung von Zugriffen auf die Akte,

- Möglichkeiten zur elektronischen Akteneinsicht,

---

[54] Beamtengesetz für das Land Brandenburg (Landesbeamtengesetz – LBG) vom 3. April 2009 (GVBl. I S. 26), zuletzt geändert durch Artikel 3 des Gesetzes vom 7. Juli 2009 (GVBl. I S. 198, 199)

- Regelungen im Falle der Anhörung des Beamten,

- Nachvollziehbarkeit und Zurechenbarkeit bei der Entfernung von Unterlagen aus der elektronischen Akte,

- Festlegungen zur Sicherung der Integrität der Personalakte während der Aufbewahrungsfristen.

Wegen der zu erwartenden Schwierigkeiten bei der Einführung der automatisierten Personalakte, der Komplexität des gesamten Themas und der Neuheit der technischen Umsetzung halten wir zumindest eine Verwaltungsvorschrift hierzu für unverzichtbar.

4.6.2 Der Personalrat darf nicht alles wissen!

Hat ein Personalrat das Recht, Gleitzeitbögen der Beschäftigten einzusehen? Muss die Dienststelle ihm mitteilen, welche Mitarbeiterinnen schwanger sind? Besteht ein Anspruch regelmäßig zu wissen, wer von den Beschäftigten schwerbehindert ist? Diese oder ähnliche Fragen erreichen uns immer wieder.

Um beispielsweise die Einhaltung einer Dienstvereinbarung zu kontrollieren, steht dem Personalrat kein generelles Recht auf Vorlage der Zeiterfassungsbögen zu. Aus den Vorschriften des § 60 Personalvertretungsgesetz für das Land Brandenburg (PersVG) i. V. m. §§ 29, 14 Brandenburgisches Datenschutzgesetz (BbgDSG) lässt sich kein solcher Anspruch ableiten.

Sinn und Zweck der Unterrichtungspflicht der Dienststelle (§ 60 PersVG) und des damit korrespondierenden Rechts des Personalrats auf umfassende Information bestehen darin, diesem die zur Erfüllung seiner Aufgaben notwendigen Fakten und Daten zur Verfügung zu stellen, damit er seinem Vertretungsauftrag gerecht werden und eine sachgerechte Entscheidung treffen kann. Daraus folgt, dass der Umfang der Informationspflicht der Dienststelle nur so weit reicht wie die gesetzlichen Zuständigkeiten der Personalvertretung. Die Kontrolle der Einhaltung einer Dienstvereinbarung fällt nicht unter diese Zuständigkeiten. Eine darüber hinausgehende Auskunftspflicht der Dienststelle gegenüber dem Personalrat besteht nicht.

Auch § 29 Abs. 1 i. V m. § 14 Abs. 5 BbgDSG erlaubt die Übermittlung der Beschäftigtendaten an den Personalrat in der Regel nur, wenn sie zur Durchführung beispielsweise personeller oder organisatorischer Maßnahmen erforderlich und im Rahmen der personalvertretungsrechtlichen Vorschriften zulässig ist.

Erteilen die Beschäftigten ihre Einwilligung, steht dem Wunsch des Personalrats jedoch nichts entgegen. Ebenso können dem Personalrat Übersichten zur Verfügung gestellt werden, aus denen ein Personenbezug nicht erkennbar ist.

Gleiches gilt für die Mitteilungen von Schwangerschaften an den Personalrat. Dieser hat zwar über die Einhaltung mutterschutzrechtlicher Bestimmungen zu wachen, dennoch gebietet es der Schutz der Persönlichkeitsrechte der werdenden Mutter, dass der Personalrat von der Dienststelle nicht verlangen kann, über eine Schwangerschaft informiert zu werden, wenn die Betroffene ihre Einwilligung nicht erteilt hat.

Auch die regelmäßige Übersendung von Listen mit personenbezogenen Daten Schwerbeschädigter an den Personalrat folgt diesen Regeln und ist ohne eine gesetzlich geforderte Zweckbestimmung rechtswidrig. Hinzu kommt, dass es sich bei den Angaben in dieser Liste um Personalaktendaten handelt. Der Personalrat darf nur mit Zustimmung des Beschäftigten die Personalakte einsehen.

Personenbezogene Daten von Beschäftigten dürfen nur im Umfang der gesetzlich geregelten Beteiligungsrechte an den Personalrat übermittelt werden.

4.6.3 Personalinformationssystem PERIS

In unserem letzten Tätigkeitsbericht[55] informierten wir über ein Pilotprojekt zur Einführung eines neuen DV-Verfahrens für die Integrierte Personal- und Stellenverwaltung (iPSv) in ausgewählten Bereichen der Landesverwaltung, das auch wegen Mängeln im Bereich des Datenschutzes und der IT-Sicherheit eingestellt wurde. Im Frühjahr 2008 lud uns das Ministerium des Innern dann ein, in einer Projektgruppe zur Weiterentwicklung des existierenden Personalinformationssystems PERIS mitzuwirken.

Wesentliches Ziel des aktuellen Projekts ist die Weiterentwicklung der zurzeit eingesetzten Version von PERIS zu einer Landesbasislösung, die als einheitlicher Standard in der gesamten Landesverwaltung genutzt wird. In diesem Zuge sollen auch Eigenentwicklungen in einzelnen PERIS-Installationen, die spezifische Anforderungen von Personalbereichen der Landesverwaltung abdecken und eine zentrale Pflege zunehmend erschweren, integriert werden. Darüber hinaus wird im Projekt angestrebt, über eine geeignete elektronische Schnittstelle für das Bezügeverfahren des Landes vergütungsrelevan-

55 vgl. Tätigkeitsbericht 2006/2007, A 5.4.5

te Daten bereitzustellen und so den Aufwand für den Austausch papierner Mitteilungen zwischen den Personalstellen und der Zentralen Bezügestelle zu vermindern.

Bereits vor mehr als 10 Jahren waren wir an den Arbeiten zur erstmaligen Einführung des Personalinformationssystems PERIS in der Landesverwaltung beteiligt. Damals gelang es, zentrale Forderungen des Datenschutzes und der IT-Sicherheit im System zu verankern. Insbesondere sind hier das strenge Rollen- und Rechtekonzept, die Trennung der Personaldatenverarbeitung nach Ressorts bzw. nachgeordneten Einrichtungen, die verschlüsselte Speicherung der Personaldaten in der Datenbank sowie die Ende-zu-Ende-Verschlüsselung bei der Datenübertragung im Landesverwaltungsnetz zu nennen. Diese Eigenschaften des Verfahrens bleiben selbstverständlich auch in der weiterentwickelten Version bestehen.

Im Rahmen unserer Beteiligung in der aktuellen Projektgruppe konnten wir an verschiedenen Stellen Einfluss auf die datenschutzgerechte Gestaltung der künftigen Landesbasislösung nehmen. Die Schwerpunkte der Diskussionen waren im Einzelnen:

- Einhaltung des Grundsatzes der Datensparsamkeit, Verzicht auf nicht erforderliche Daten, explizite Begründung bei der Verwendung von Freitextfeldern in Bildschirmmasken, ggf. Ersetzung von Freitextfeldern durch Kataloge auswählbarer Werte,

- Beachtung von rechtlichen Regelungen zu Aufbewahrungsfristen für Personaldaten, Überwachung von Löschfristen, automatisiertes und rückstandsfreies Löschen von Daten im System bei Ablauf der Fristen,

- Fortschreibung des IT-Sicherheitskonzepts, Berücksichtigung des zentralen Betriebs beim Brandenburgischen IT-Dienstleister, Anpassung an die aktuelle Hard- und Softwareinfrastruktur, Erweiterung um Systemkomponenten zum Datenaustausch mit dem Bezügeverfahren.

Besonderer Beratungsbedarf bestand im Projekt bezüglich des zuletzt genannten Punktes. Da PERIS als einheitliche Softwarelösung in der gesamten Landesverwaltung eingesetzt werden soll und der Betrieb zentral beim Brandenburgischen IT-Dienstleister erfolgt, bestehen bei allen Personalbereichen als Daten verarbeitenden Stellen gleiche Anforderungen bzgl. der IT-Sicherheit (solange nicht wesentlich von der Landesbasislösung bzw. der vereinbarten technischen Infrastruktur abgewichen wird). Die entsprechenden Sicherheitsmaßnahmen lassen sich in einem gemeinsamen IT-Sicherheitskonzept zusammenfassen, das die zentral betriebenen Verfahrenskomponenten abdeckt und für jede Installation (d. h. für jede Daten verarbeitende Stelle)

durch den Dienstleister umzusetzen ist. Ergänzt werden die zentralen Festlegungen durch Sicherheitsrichtlinien bzw. Mustersicherheitskonzepte für die PERIS-Clients in den Personalbereichen. Diese Richtlinien bzw. Muster sind ggf. auf die jeweiligen lokalen Gegebenheiten anzupassen und vor Ort umzusetzen. Auch die Freigabe muss jeweils für die einzelnen Daten verarbeitenden Stellen getrennt erfolgen. Die behördlichen Datenschutzbeauftragten haben zuvor das Verfahren im Rahmen der Vorabkontrolle gem. § 10a Brandenburgisches Datenschutzgesetz zu prüfen.

Das IT-Sicherheitskonzept für die zentralen Komponenten des PERIS-Verfahrens wurde im Auftrag der Projektleitung von einem externen Dienstleister fortgeschrieben. Es enthielt zunächst keine Angaben zu Prioritätensetzungen, Zeitplänen und Verantwortlichkeiten für die Umsetzung noch fehlender IT-Sicherheitsmaßnahmen. Vor dem Hintergrund des hohen Schutzbedarfs der in dem Verfahren verarbeiteten Personaldaten haben wir darauf gedrungen, diesbezüglich konkrete Festlegungen zu treffen. Außerdem war festzustellen, dass aus den Lücken in der Umsetzung des Sicherheitskonzepts z. T. erhebliche Risiken für die Personaldaten der Beschäftigten hätten entstehen können. Insofern lehnten wir eine Produktivsetzung zentraler Komponenten des Verfahrens vor der Beseitigung der wesentlichen Schwachstellen ab.

Entsprechend den Empfehlungen im IT-Sicherheitskonzept wurden in einer gemeinsamen Beratung mit den Projektverantwortlichen aus dem Ministerium des Innern und dem Brandenburgischen IT-Dienstleister Prioritäten für die Umsetzung der fehlenden Sicherheitsmaßnahmen festgelegt, verantwortliche Personen bzw. Organisationseinheiten benannt und Termine fixiert. Die Abarbeitung dieses Realisierungsplans dauerte zum Zeitpunkt der Erstellung dieses Berichts an. Gleiches gilt für die Formulierung von Sicherheitsrichtlinien bzw. Mustersicherheitskonzepten für die PERIS-Clients.

Bei der Entwicklung und Umsetzung einer einheitlichen Landesbasislösung für ein Personalinformationssystem muss dem hohen Schutzbedarf der verarbeiteten Personaldaten der Beschäftigten besondere Rechnung getragen werden. Eine Produktivsetzung des Verfahrens kann erst dann erfolgen, wenn alle erforderlichen IT-Sicherheitsmaßnahmen sowohl für zentral als auch für dezentral betriebene Verfahrenskomponenten realisiert sind. Eine entsprechende Prüfung ist im Rahmen der Vorabkontrolle durch die behördlichen Datenschutzbeauftragten der Daten verarbeitenden Stellen durchzuführen.

4.6.4 Gesundheitsdaten Angehöriger für Sozialauswahl?

Ein Personalrat fragte nach der Zulässigkeit der Erhebung personenbezogener Daten Dritter im Rahmen der Sozialauswahl für den Personalausgleich bei den Finanzämtern. Insbesondere war die Frage zu klären, ob der Arbeitgeber detaillierte Nachweise fordern kann, die belegen, welche Krankheit oder Behinderung die Pflege von Verwandten erforderlich macht.

Der Hauptpersonalrat hat mit dem Ministerium der Finanzen zur Durchführung des Personalausgleichs in den Finanzämtern eine Dienstvereinbarung geschlossen, die eine Datenverarbeitung im Sinne von § 29 Abs. 1 Brandenburgisches Datenschutzgesetz erlaubt. Die Vertragsparteien hatten sich darauf verständigt, dass – über die Pflichtangabe hinausgehend – auch „sonstige Gründe“, die ein Verbleiben am bisherigen Dienstort erfordern, angegeben werden können. Davon sind möglicherweise auch Daten über pflegebedürftige Angehörige betroffen.

Das Ministerium der Finanzen hatte die Mitarbeiterinnen und Mitarbeiter einerseits auf die Freiwilligkeit der zusätzlichen Angaben hingewiesen, andererseits aber erklärt, dass entsprechende Nachweise nur auf Verlangen des Arbeitgebers oder Dienstherrn erhoben würden. Die Betroffenen wurden im Unklaren gelassen, welche personenbezogenen Daten für eine Nachweiserbringung erforderlich und zu welchem Zeitpunkt sie zu erbringen sind.

Das Verfahren barg im Ergebnis die Gefahr in sich, dass derjenige Mitarbeiter begünstigt wird, der die weitesten Einblicke in seine Privatsphäre gestattet, indem er bereits von sich aus eine Vielzahl von Beweisunterlagen (die nicht zwangsläufig für die Entscheidung erforderlich sind) beifügt. Dem Recht auf informationelle Selbstbestimmung nicht nur des Betroffenen sondern auch des Dritten wurde nicht ausreichend Rechnung getragen.

Für ein datenschutzgerechtes Verfahren haben wir folgende Lösungsvorschläge unterbreitet:

- Grundsätzlich ist bei allen Abfragen das Prinzip der Datensparsamkeit zu beachten.

- Als häufiger Grund wird die Pflege von Angehörigen in Betracht kommen. Hierfür sollte von vornherein festgelegt werden, welche Unterlagen beizubringen sind, um die Pflegebedürftigkeit nachzuweisen. Die Erstabfrage sollte grundsätzlich ohne Belege erfolgen. Allerdings halten wir es an dieser Stelle schon für zulässig, die Pflegestufe des Angehörigen zu erfragen.

- Nur in Einzelfällen wird es darüber hinaus erforderlich sein, Gesundheitsdaten Dritter zu erheben. Weil hier in deren Rechte eingegriffen wird, halten wir die Erhebung nur dann für zulässig, wenn die Dritten hierfür ihre Einwilligung erteilt haben.

- Die Betroffenen müssen erkennen können, welche Gewichtung bestimmte Lebenssituationen bei der Sozialauswahl haben. Typische Fälle (wie z. B. Pflege bezogen auf die verschiedenen Pflegestufen) sollten in das bestehende Punkteschema zur Auswertung der Angaben aufgenommen werden. Das Verfahren wird damit für den Betroffenen transparenter.

Ohne klare Regelungen über die „sonstigen Gründe“ besteht die Gefahr, dass die Betroffenen übermäßig viele Informationen zur Verfügung stellen, die nicht erforderlich sind. In einem solchen Fall sind die Unterlagen sofort an den Betroffenen zurück zu senden. Eine Verarbeitung dieser Daten darf nicht erfolgen. Gibt ein Betroffener hingegen nur knapp an, dass er einen Angehörigen pflegt, müssen seitens des Arbeitgebers oder Dienstherrn die näheren Umstände (z. B. Pflegestufe) nachgefragt werden, sodass ein Gleichmaß an Bewertung vorgenommen werden kann.

Bei einer Sozialauswahl hat der Arbeitgeber das Verfahren so zu gestalten, dass nicht in Rechte Dritter eingegriffen wird.

4.6.5 Kontrolle von E-Mail und Internet am Arbeitsplatz

Hat der Arbeitgeber nur die dienstliche Nutzung von E-Mail und Internetdiensten am Arbeitsplatz erlaubt, hat er gleichzeitig ein Interesse daran zu kontrollieren, ob das Verbot der privaten Nutzung befolgt wird. Einigen Verwaltungen mussten wir diesbezüglich Grenzen aufzeigen.

Das Ausmaß und die Art der Nutzung von E-Mail und Internet am Arbeitsplatz durch die Beschäftigten unterliegen dem Weisungsrecht des Arbeitgebers oder Dienstherrn. Auch bei einem Verbot der privaten E-Mail-Nutzung dürfen erkennbar private Nachrichten vom Arbeitgeber nicht gelesen werden. Selbst dienstlicher E-Mail-Verkehr darf nicht systematisch überwacht werden.

Um dem allgemeinen Persönlichkeitsrecht des Beschäftigten Rechnung zu tragen, hat immer eine Abwägung zwischen diesem und dem Direktionsrecht des Arbeitgebers zu erfolgen. Für Kontrollen sind immer Maßnahmen mit geringster Eingriffsintensität zu wählen. Bei einem konkreten Missbrauchsverdacht ist eine Protokollierung und Einsichtnahme von E-Mails durch den Arbeitgeber erlaubt. Den Beschäftigten muss das Verfahren der Kontrolle jedoch vorher bekannt und mit dem Personalrat sollte eine Dienstvereinbarung abgeschlossen sein. Soweit die Nutzung von E-Mail und Internetdiens-

ten zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung des ordnungsgemäßen Betriebes der Verfahren protokolliert wird, dürfen diese Daten nur für diese Zwecke genutzt werden. Eine Auswertung der Protokolle zur Verhaltens- und Leistungskontrolle ist unzulässig!

Ist eine private Internetnutzung nicht erlaubt, muss auch hier hinsichtlich der Überwachung des Nutzerverhaltens der Beschäftigten zwischen dem allgemeinen Persönlichkeitsrecht und dem Direktionsrecht abgewogen werden. Erlaubt sind lediglich stichprobenartige Kontrollen, ob das Surfen tatsächlich dienstlicher Natur ist. Hingegen ist eine automatisierte Vollkontrolle wegen der Schwere des Eingriffs in das Persönlichkeitsrecht der Beschäftigten nur bei konkretem Missbrauchsverdacht im Einzelfall zulässig. In einer Dienstvereinbarung sollten technische und organisatorische Fragen der Protokollierung eindeutig geregelt sein.

Dürfen E-Mail und Internetdienste ausschließlich zu dienstlichen Zwecken genutzt werden, sind Kontrollen nur stichprobenweise und bei konkretem Missbrauchsverdacht zulässig. Zu Fragen der Protokollierung und Auswertung empfehlen wir den Abschluss einer Dienstvereinbarung.

4.6.6 Veröffentlichung von Mitarbeiterdaten im Internet

Müssen Mitarbeiter der öffentlichen Verwaltung die Bekanntgabe ihres Namens, der Funktion sowie der dienstlichen Erreichbarkeit im Internet hinnehmen? Hierzu hat das Oberverwaltungsgericht Rheinland-Pfalz eine Entscheidung[56] getroffen, die wir auch in unserer Arbeit berücksichtigen.

Im Interesse einer transparenten, bürgernahen öffentlichen Verwaltung ist der Dienstherr von Rechts wegen nicht gehindert, Namen, Funktion und dienstliche Erreichbarkeit jedenfalls solcher Mitarbeiter, die mit Außenkontakten betraut sind, auch ohne deren Einverständnis im Internet bekannt zu geben. Etwas anderes gilt lediglich dann, wenn der Bekanntgabe Sicherheitsbedenken oder Fürsorgepflichten entgegenstehen.

Das Landesbeamtengesetz ermächtigt den Dienstherrn zur Erhebung personenbezogener Daten, soweit dies zur Durchführung organisatorischer Maßnahmen erforderlich ist. Die Veröffentlichung des Namens und der dienstlichen Kontaktdaten können zur Durchführung einer organisatorischen Maßnahme – nämlich der Außendarstellung einer Behörde – erforderlich sein. Insoweit bezieht sich das Kriterium der Erforderlichkeit nicht auf die organisatorische Maßnahme, sondern nur auf die Übermittlung personenbezogener

56 Urteil des Oberverwaltungsgerichts Rheinland-Pfalz vom 10. September 2007 (2 A 10413/07)

Daten zu deren Durchführung. Die Entscheidung des Dienstherrn für einen „personalisierten“ Behördenauftritt obliegt seinem Organisationsermessen und begegnet keinen rechtlichen Bedenken.

Bei Veröffentlichung der Daten nur solcher Mitarbeiter, die mit der Nennung einverstanden sind, lässt sich das Ziel einer „persönlichen“ Verwaltung nicht verwirklichen. Dieses ist Ausdruck eines modernen staatlichen Selbstverständnisses und öffentlichen Dienstes, denen sich ein Mitarbeiter aufgrund seiner Stellung als Teil seiner Beschäftigungsbehörde nicht verschließen kann, es sei denn, beachtliche Sicherheitsbedenken stehen dagegen.

Auch das Brandenburgische Datenschutzgesetz enthält eine Regelung, wonach die Übermittlung personenbezogener Daten von Beschäftigten an andere als öffentliche Stellen zulässig ist, soweit dies aus dienstlichen Gründen geboten ist. Hier gelten die gleichen Kriterien für eine Veröffentlichung personalisierter Organisationspläne.

Die Bekanntgabe personenbezogener Organisationspläne unterliegt dem Organisationsrecht des Dienstherrn und ist datenschutzrechtlich nicht zu beanstanden.

4.7 Kommunales

4.7.1 Wie oft duschen Sie? – Datenerhebung eines Abwasserbetriebes

Wir wurden darauf aufmerksam, dass der Abwasserbetrieb einer Gemeinde eine Kundenbefragung zum Trink- und Abwasserverbrauch bei den Abgabepflichtigen durchgeführt hat. Unter Hinweis auf ihre Auskunftspflicht sollten die Betroffenen Fragen zur Personenanzahl und Wohnfläche beantworten, darüber hinaus aber auch Details ihres Verbrauchsverhaltens, wie z. B. die Häufigkeit des Badens und Duschens oder die Nutzung der Spül- oder Waschmaschine darlegen.

Hintergrund der Erhebung war, dass dem Eigenbetrieb im Hinblick auf die in den Haushalten (Verbrauchsstellen) gemeldeten Personen die gemessenen Verbrauchswerte nicht plausibel erschienen. Diese waren im vergangenen Abrechnungszeitraum ungewöhnlich niedrig gewesen, was sich aufgrund der Berechnungsmaßstäbe auch auf die Abwassermengengebühr auswirkte. Die Gemeinde wollte dem auf den Grund gehen. Sie berief sich dabei auf die in der gemeindlichen Abwasserbeseitigungssatzung aufgenommene und durchaus übliche Bestimmung, dass die Abgabepflichtigen jede Auskunft zu erteilen haben, die für die Festsetzung und Erhebung der Abgaben erforderlich ist. Besonderes Gewicht wurde der Kundenbefragung noch dadurch

verliehen, dass die Gemeinde bei Nichtbeantwortung angekündigt hatte, ein Verwaltungsverfahren gegen die Betroffenen einzuleiten.

Auf unsere Aufforderung informierte uns die Gemeinde, dass die Befragung auch aufgrund von Bürgerprotesten aufgegeben worden sei. Unsere datenschutzrechtliche Beurteilung ergab, dass nicht alle abgefragten Daten unzulässig erhoben worden waren. § 12 Brandenburgisches Datenschutzgesetz legt den Grundsatz fest, dass personenbezogene Daten erhoben werden dürfen, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der durch Gesetz der erhebenden Stelle zugewiesenen Aufgabe und für den jeweils damit verbundenen Zweck erforderlich ist. So bestehen keine Bedenken, die Anzahl der unter der Verbrauchsstelle wohnhaften Personen festzustellen oder abzufragen, ob Trinkwasser für den Garten genutzt wird und gesonderte Gartenwasserzähler vorhanden sind. Bei diesen Angaben ist ein direkter Bezug zu der dem Abwasserbetrieb übertragenen Aufgabe, den Verbrauch zu verifizieren und Abwassergebühren festzusetzen, erkennbar.

Die Abfrage darüber hinausgehender Details zum persönlichen Verbrauchsverhalten der Abgabepflichtigen verstößt jedoch gegen den Erforderlichkeitsgrundsatz. Der Gemeinde standen im konkreten Fall andere Maßnahmen zur Verfügung, um den Wasserverbrauch zu ermitteln. Bei konkreten Zweifeln an der Richtigkeit von Messergebnissen durch Wasserzähler durfte die Gemeinde oder Beauftragte diese bei den betreffenden Haushalten an Ort und Stelle prüfen und ggf. eine Schätzung vornehmen. Für den Fall, dass weder Wasserzähler noch Abwassermesseinrichtungen vorhanden sind, war die Gemeinde laut Satzung berechtigt, einen Pauschalverbrauch pro Einwohner in Ansatz zu bringen. Die Berufung der Gemeinde auf die in der Abwasserbeseitigungssatzung festgelegte Auskunftspflicht war hinsichtlich der persönlichen Informationen zum Wasserverbrauch unzulässig.

Wir haben die Gemeinde auf ihr datenschutzwidriges Verhalten hingewiesen und die Löschung aller unzulässig erhobenen Daten verlangt. Da die Gemeinde die Erhebung sofort abgebrochen und uns zugesichert hat, die eingegangenen Daten nicht verwendet zu haben, konnte auf weitere Maßnahmen unsererseits verzichtet werden. Eine weitere Kundenbefragung wurde nach Auskunft der Gemeinde nicht durchgeführt.

Abgabepflichtige müssen auch dann keine Details ihres persönlichen Wasserverbrauchs gegenüber einem kommunalen Abwasserbetrieb offenlegen, wenn Zweifel an der Richtigkeit von Angaben zum Wasserverbrauch bestehen.

4.7.2 Mobiler Bürgerservice

Drei brandenburgische Kommunen planten, sich gemeinsam an dem Modellversuch „Mobiler Bürgerservice“ zu beteiligen, der vom Ministerium des Inneren, dem Institut für E-Government und dem Städte und Gemeindebund ausgeschrieben und gefördert wurde. Der Mobile Bürgerservice dient dazu, Leistungen der Kommunalverwaltung außerhalb der Verwaltungsgebäude und herkömmlicher Bürozeiten anzubieten, um z. B. Berufstätigen Dienste servicefreundlich auch am Samstagvormittag bereitzustellen. Zu diesem Zweck wollten die Gemeinden einen Stand in der Ladenpassage eines zentral gelegenen Einkaufszentrums einrichten.

Das Leistungsspektrum, das die Verwaltungen mobil anbieten wollten, umfasste An- und Abmeldungen, Anträge auf Personaldokumente, Erlaubnisse nach der Hundehalterverordnung, Wohnberechtigungsscheine, Kita-Plätze in der jeweiligen Gemeinde, Befreiung von der GEZ-Gebühr, Wahlscheine sowie die Anmeldung von Feuerwerken, die Anzeige von Verlustgegenständen als auch Aushänge und allgemeine Informationen. Die Bearbeitung sollte mit einem Laptop als Terminal erfolgen, über den sich die Mitarbeiter in das System der jeweiligen Gemeinde und die Fachverfahren einwählen können. Eine lokale Speicherung von Daten und Dokumenten war nicht gestattet. Außerdem war vorgesehen, Mobiltelefon, Drucker, Kopierer, Fingerabdruckscanner und EC-Karten-Lesegerät vor Ort zu haben. Die Vertraulichkeit und Integrität der Daten sollte nach den gleichen Vorgaben gewährleistet werden wie bei der Nutzung in einem Amt. Am Einsatzort sollte der Mobile Bürgerservice ständig von zwei Mitarbeitern betreut und durch Trenn- bzw. Sichtschutzwände abgeschirmt werden.

Wegen erheblicher Sicherheitsbedenken, die angesichts des vorgesehenen Standorts mit Laufpublikum bestanden, haben wir empfohlen, andere Varianten in Betracht zu ziehen (wie etwa geschlossene Räumlichkeiten oder einen Bus). Auch von technischer Seite gab es Verbesserungsbedarf hinsichtlich der Verfahrensarchitektur, technischer Sicherheitsmaßnahmen (z. B. Verschlüsselung) und der erforderlichen Dokumentation. Während unsere Vorgaben für die technischen Anforderungen an die Datensicherheit umsetzbar waren, wollten die Gemeinden an dem Standort unbedingt festhalten. Wir hatten die Möglichkeit, uns den geplanten Standort anzuschauen und auf seine Eignung für einen datenschutzgerechten Bürgerservice zu überprüfen. Bei der Ortsbesichtigung nahmen wir verschiedene Standorte im Laufkorridor der Ladenpassage und Räumlichkeiten in den Ladenlokalen des Einkaufszentrums in Augenschein und diskutierten mit den Beteiligten, wie diese abzusichern wären. Dabei bestätigte sich unser Eindruck, dass die Vertraulichkeit und Datensicherheit gefährdet sind, weil sich in der Ladenpassage gerade an Samstagen ständig Menschenströme bewegen sowie Sonderakti-

onen und Verzehrgelegenheiten den Publikumsverkehr sowie die Verweildauer in unmittelbarer Nähe des Mobilen Bürgerservice erhöhen.

Wir kamen zu dem Ergebnis, dass das Projekt an dem geplanten Standort nur unter erheblichen Bedenken in der Form eines nach drei Seiten geschlossenen Arbeitsplatzes mit Sichtschutz und Abstandsfläche umsetzbar wäre. Damit könnte verhindert werden, dass Unbeteiligte unberechtigt das gesprochene Wort mithören, Einsicht nehmen oder auf Dokumente zugreifen. Die Gemeinden machten deutlich, dass sie für unsere Bedenken nur begrenzt Verständnis haben. Gleichwohl erwägen sie, ersatzweise den Mobilen Bürgerservice mit Hilfe eines speziellen Busses oder in gemeindeeigenen Räumen einzuführen.

Um die sichere Verarbeitung von teilweise sensitiven personenbezogenen Daten auch durch Mobile Bürgerämter zu gewährleisten, müssen umfangreiche Sicherheitsvorkehrungen getroffen werden. Auch sollte das erhöhte Risiko eines unberechtigten Datenzugriffs durch Dritte berücksichtigt und Gefahren für die Vertraulichkeit der angebotenen Dienste mit dem Standortvorteil abgewogen werden. Für datenschutzrechtliche Belange erweist sich der Standort im Laufkorridor einer Ladenpassage als grundsätzlich ungeeignet.

5 Justiz

5.1 Brandenburgisches Dolmetschergesetz

Das Bundesverwaltungsgericht hatte im Jahr 2007 eine gesetzliche Grundlage mit hinreichend klaren Bestimmungen über die zu erfüllenden Voraussetzungen und das einzuhaltende Verfahren für die allgemeine Beeidigung von Dolmetschern bzw. die Ermächtigung von Übersetzern gefordert. Der Entwurf eines Brandenburgischen Dolmetschergesetzes wurde uns Ende 2008 vom Justizministerium frühzeitig vorgelegt.

Zwei Punkte waren uns bei diesem Gesetz besonders wichtig. Zum einen sollte bei den Zugangsregelungen zu dem Dolmetscher- und Übersetzerverzeichnis das Grundrecht auf Datenschutz im angemessenen Umfang berücksichtigt werden. Zum anderen waren Datenerhebungsbefugnisse der Landgerichtspräsidenten bzw. Vorlagepflichten der Betroffenen zu den Nachweisen der praktischen Tätigkeit und der persönlichen Zuverlässigkeit zu regeln.

Das Justizministerium prüfte auf unsere Anregung hin, ob und für wen an der Gewährung eines Zugriffs auf das Dolmetscher- und Übersetzerverzeichnis des Oberlandesgerichts ein überwiegendes Allgemeininteresse besteht. Im Ergebnis der Prüfung wird das Verzeichnis vorrangig für die Arbeit der Gerichte und Justizbehörden verwendet und diesen Stellen auf gesetzlicher Grundlage zur Verfügung gestellt. Eine Veröffentlichung im Internet wird von einer Einwilligung der Betroffenen abhängig gemacht. Außerdem hat das Justizministerium eine Verordnung zur Ausführung des Brandenburgischen Dolmetschergesetzes erlassen, mit der die Rechtsklarheit beim Umgang mit Nachweisen für praktische Tätigkeiten und die persönliche Zuverlässigkeit erhöht wird.

Beide Regelungen sind inzwischen in Kraft getreten.[57]

Das Dolmetscher- und Übersetzerverzeichnis wird nur im Internet veröffentlicht, soweit die Betroffenen einwilligen.

5.2 Untersuchungshaftvollzugsgesetz

Gemeinsam mit Justizministerien weiterer Bundesländer erarbeitete das Ministerium der Justiz des Landes Brandenburg einen Musterentwurf für ein Untersuchungshaftvollzugsgesetz. Es legte uns den entsprechenden Entwurf für ein Landesgesetz vor.

Der Entwurf sah zunächst im § 7 Abs. 2 vor, dass beim Zugangsgespräch andere Gefangene „in der Regel“ nicht anwesend sein dürfen. Der Begründung war zu entnehmen, dass beispielsweise bei unüberwindbaren sprachlichen Verständigungsschwierigkeiten ausnahmsweise ein zuverlässiger Gefangener hinzugezogen werden könnte. Solche Ausnahmefälle hätten gemäß Art. 11 Abs. 2 Landesverfassung Brandenburg als Einschränkungen des Grundrechts auf Datenschutz bereits im Gesetzestext festgelegt werden müssen. Außerdem wäre ein überwiegendes Allgemeininteresse an dem Grundrechtseingriff darzulegen gewesen. Bevor an das Einbeziehen eines Mitgefangenen gedacht werden kann, muss vor allem die Möglichkeit, einen beeidigten Dolmetscher oder ermächtigten Übersetzer einzubeziehen, ausgeschöpft sein. Ungeklärt war auch, wie einem Mitgefangenen eine Schweigepflicht auferlegt werden sollte, die einen wirksamen Schutz für die personenbezogenen Daten des Betroffenen gewährleisten kann. Im Gesetz[58] ist

[57] Gesetz über die allgemeine Beeidigung von Dolmetschern und Ermächtigung von Übersetzern des Landes Brandenburg (Brandenburgisches Dolmetschergesetz – BbgDolmG) vom 7. Juli 2009 (GVBl. I S. 252) und Verordnung zur Ausführung des Brandenburgischen Dolmetschergesetzes vom 23. September 2009 (GVBl. II S. 709)

[58] Gesetz über den Vollzug der Untersuchungshaft im Land Brandenburg (Brandenburgisches Untersuchungshaftvollzugsgesetz – BbgUVollzG) vom 8. Juli 2009 (GVBl. I S. 271)

auf unsere Empfehlung hin nun erfreulicherweise klar geregelt, dass andere Gefangene beim Zugangsgespräch nicht anwesend sein dürfen.

In folgenden Fällen konnten wir allerdings keine datenschutzrechtliche Verbesserung erreichen:

- Die Erlaubnis des Anstaltsleiters für einen Untersuchungsgefangenen, auf eigene Kosten externen ärztlichen Rat einzuholen, kann versagt werden, wenn der Untersuchungsgefangene den Arzt seines Vertrauens und den ärztlichen Dienst der Anstalt nicht wechselseitig von der Schweigepflicht entbindet. Nach der Gesetzesbegründung soll so eine Beeinträchtigung der Behandlung vermieden werden. Es liegt jedoch regelmäßig in der freien Entscheidung eines Patienten, wem er welche Gesundheitsdaten offenbart und ob er verschiedene Ärzte untereinander von der Schweigepflicht entbindet. Die Verantwortung für die Beeinträchtigung seiner Behandlung durch fehlende Information trägt er selbst. Wir hatten gefordert, ein überwiegendes Interesse der Allgemeinheit an der Einschränkung des Grundrechts auf Datenschutz darzulegen. Die Gesetzesbegründung blieb jedoch unverändert.

- Die Kommunikation eines Untersuchungsgefangenen mit seinem Verteidiger sowie der Schriftwechsel mit Abgeordneten oder unserem Hause ist besonders geschützt. Ein geringerer Schutz besteht für die Kommunikation mit Rechtsanwälten und Notaren. Der Kontakt mit anderen Berufsgeheimnisträgern wie Geistlichen, Schwangerschafts- oder Drogenberatungsstellen ist gar nicht besonders geregelt. Wir wiesen unter anderem darauf hin, dass so der Schutz sensitiver Informationen nicht hinreichend berücksichtigt wird.

- Die Empfehlung, dem Betroffenen auf seinen Wunsch hin – wie bei sonstigen Regelungen – generell Akteneinsicht in Unterlagen zu seiner Person zu gewähren und nur im Ausnahmefall auf eine bloße Auskunft zurückzugreifen, fand ebenfalls kein Gehör. Ein Untersuchungsgefangener erhält nun im Regelfall lediglich eine Auskunft zu seinen personenbezogenen Daten. Nur soweit eine Auskunft für die Wahrnehmung seiner rechtlichen Interessen nicht ausreicht und er deshalb auf eine Akteneinsicht in die Gefangenenakte angewiesen ist, wird diese ausnahmsweise gewährt.

Den Datenschutzrechten von Untersuchungsgefangenen wird durch das Untersuchungshaftvollzugsgesetz nur unzureichend Rechnung getragen.

5.3 Datenverarbeitung im Justizvollzug

Mit der Migration auf das neue Datenverarbeitungssystem der brandenburgischen Justizvollzugsanstalten BASIS-Web wurde das bisherige Verfahren BASIS abgelöst. An der Umstellung wurden wir kontinuierlich beteiligt.

Das Verfahren BASIS-Web ist eine Neuentwicklung der strafvollzugsspezifischen Software BASIS (Buchhaltungs- und Abrechnungssystem im Strafvollzug), die auf unterschiedlichen Hardwareplattformen bereits seit den 90er Jahren in den Justizvollzugsanstalten des Landes Brandenburg eingesetzt wird. Das Verfahren unterstützt die Verwaltung der Gefangenenstammdaten einschließlich der Strafzeitberechnung und der zugehörigen Terminverwaltung. Weiterhin ist es ein wichtiges Instrument zur Verwaltung von Urlauben und Ausgängen, erzeugt die notwendigen Papiere und stellt sicher, dass die vorgeschriebenen Benachrichtigungen, z. B. der Polizei, erfolgen. Weitere Funktionen des Verfahrens beinhalten u. a. die Abwicklung von Gefangenentransporten, die Geldverwaltung sowie die Lohnabrechnung der Gefangenen.

BASIS-Web ist ein länderübergreifendes Projekt einer integrativen EDV-Organisationslösung zur Abwicklung der Aufgaben der Verwaltung und des Vollzugs in Justizvollzugseinrichtungen. An der Verbundlösung sind die Länder Berlin, Brandenburg, Bremen, Hamburg, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt, Schleswig Holstein sowie das Großherzogtum Luxemburg beteiligt.

Die Einführung des Verfahrens in Brandenburg wurde in einer Justizvollzugsanstalt pilotiert. Nach Funktionstests des Migrationssystems wurde der Pilotbetrieb für diese Einrichtung im August 2008 unter Echtbedingungen gestartet. Mit dessen Abschluss gab das Ministerium der Justiz das Fachverfahren BASIS-Web frei und schuf somit die Grundlage für seine Einführung in den weiteren Justizvollzugsanstalten des Landes Brandenburg.

Durch die ADV-Leitstelle für den Justizvollzug des Landes Brandenburg wurde ein umfangreiches Sicherheitskonzept für den Einsatz des Verfahrens BASIS-Web erarbeitet, welches aber an die jeweiligen Gegebenheiten der Justizvollzugsanstalten angepasst werden muss.

Wegen des hohen Schutzbedarfs der Daten von Gefangenen, der in BASIS-Web bestehenden Kommunikationsverbindungen zwischen einzelnen Programmteilen sowie der Möglichkeiten zentralen und dezentralen Zugriffs sind besondere technische Maßnahmen zur Gewährleistung von Datenschutz und IT-Sicherheit zu treffen. Während die verschlüsselte Übertragung von Daten zwischen Standorten und ein strenges Rollen-Rechte-Konzept bereits reali-

siert sind, wurden eine Verschlüsslung der Datenübertragung innerhalb lokaler Netze sowie die verschlüsselte Speicherung der Daten noch nicht umgesetzt. Neben der applikationsbasierten Verschlüsselung der Daten wurden im Rahmen der Zusammenarbeit mit der ADV-Leitstelle auch weitere Möglichkeiten zur Absicherung des Verfahrens diskutiert.

Wir werden die Einführung und Nutzung von BASIS-Web auch zukünftig beratend begleiten. Anforderungen an Datenschutz und IT-Sicherheit sollten bei länderübergreifend entwickelten Verfahren möglichst frühzeitig eingebracht werden, da sie im Nachhinein nur schwer umgesetzt werden können.

5.4 Justizzentrum Potsdam

Im Jahre 2008 wurde das Justizzentrum Potsdam als neuer Dienstsitz für das Verfassungsgericht des Landes Brandenburg, das Landgericht Potsdam, die Staatsanwaltschaft Potsdam und Teile des Amtsgerichts Potsdam eröffnet. Im Rahmen der Zusammenführung der Dienststellen unter einem Dach und der gemeinsamen Nutzung von DV-Systemen der beteiligten Stellen sind die Anforderungen an eine datenschutzgerechte Verarbeitung der personenbezogenen Mitarbeiterdaten und an die Gestaltung der Datenverarbeitung im Auftrag erst im Nachhinein beachtet worden.

Mit Bezug des Justizzentrums Potsdam sind verschiedene IT-Verfahren (z. B. Zutrittskontrollsystem, Zeiterfassung, Videoüberwachungsanlage, Telekommunikationsanlage) in den Produktivbetrieb übergegangen, die durch alle beteiligten Stellen gleichermaßen genutzt, jedoch nur von einer Stelle betrieben werden. Da in den jeweiligen Verfahren Daten der Mitarbeiter der einzelnen Gerichte und der Staatsanwaltschaft verarbeitet werden, besteht nach § 11 Brandenburgisches Datenschutzgesetz (BbgDSG) zwischen den einzelnen Institutionen innerhalb des Justizzentrums ein Verhältnis der Auftragsdatenverarbeitung zum jeweiligen Betreiber des Verfahrens. Entsprechende schriftliche Verträge existierten jedoch nicht. Auch anderen Anforderungen des Brandenburgischen Datenschutzgesetzes für die Einführung der IT-Verfahren sind die beteiligten Stellen nicht nachgekommen. So fehlte es z. B. für das IT-Verfahren der Zutrittskontrolle an der Risikoanalyse und dem Sicherheitskonzept (§ 7 Abs. 3 BbgDSG), dem Verfahrensverzeichnis (§ 8 BbgDSG) und einer Freigabeerklärung. Weiterhin gab es keine Dienstvereinbarungen mit dem Staatsanwaltsrat und dem örtlichen Personalrat mit Regelungen u. a. zur Protokollierung von Zutritten.

Während der Gespräche mit den beteiligten Stellen stellte sich heraus, dass diesen nicht bewusst war, wer innerhalb des Justizzentrums Daten verarbeitende Stelle, Auftragnehmer und Auftraggeber für eine Datenverarbeitung im

Auftrag ist. Organisatorische Regelungen des Ministeriums der Justiz vor dem Erstbezug des Justizzentrums fehlten.

Bei genauerer Betrachtung der DV-Systeme im Verfahrensbetrieb stellte sich zudem heraus, dass das Verfahren der Zutrittskontrolle eine hohe Anzahl von personenbezogenen Daten speicherte und die Zutritte der Mitarbeiter zu den Räumen des Justizzentrums protokollierte. Seitens des Personalrats und des Staatsanwaltsrats wurde hier interveniert und der Fortbetrieb des Verfahrens abgelehnt. Auch die Landesbeauftragte sah in der Möglichkeit der Erstellung von Bewegungsprofilen einen nicht vertretbaren Eingriff in das Selbstbestimmungsrecht der Mitarbeiter. In Folge dessen ist das Zutrittskontrollsystem überarbeitet und teilweise ausgetauscht worden.

Im Rahmen unserer Beratungsgespräche mit den beteiligten Stellen wurde klar, dass das Landgericht Potsdam als Hausherr des Justizzentrums auch Betreiber der gemeinsamen DV-Verfahren ist. Diesem fehlt aber das technische Personal, um den ordnungsgemäßen Betrieb zu gewährleisten. Im Rahmen einer mündlichen Vereinbarung wird die Administration derzeit durch einen abgeordneten Mitarbeiter der Generalstaatsanwaltschaft des Landes Brandenburg übernommen. Dieser ist gleichzeitig einziger IT-Mitarbeiter innerhalb des Justizzentrums.

Die Probleme des Einsatzes eines einzigen IT-Mitarbeiters für die Administration der o. g. Verfahren, der Bestimmung der Zuständigkeiten für die DV-Verfahren und des Fehlens von Vereinbarungen zur Datenverarbeitung im Auftrag wurden durch die Landesbeauftragte mit Vertretern der ansässigen Gerichte, der Staatsanwaltschaft und des Ministeriums der Justiz ausführlich erörtert.

Grundlage für den rechtskonformen Betrieb der DV-Anlagen im Justizzentrum Potsdam müssen Verträge über die Datenverarbeitung im Auftrag sein. Zukünftig ist bei der räumlichen Zusammenlegung von Behörden der Landesverwaltung auf entsprechende organisatorische Regelungen und Rahmenbedingungen zu achten.

5.5 Optimierung der Führungsaufsicht über entlassene Strafgefangene

Im Berichtszeitraum hat das Justizministerium beschlossen, die Ausgestaltung der Führungsaufsicht insgesamt zu überprüfen und zu optimieren. Grund war das 2007 in Kraft getretene Gesetz zur Reform der Führungsaufsicht sowie offensichtliche Mängel im Zusammenwirken der an der Führungsaufsicht beteiligten Stellen.

Die Führungsaufsicht soll den Übergang besonders rückfallgefährdeter Strafgefangener aus dem Vollzug in die Freiheit im Interesse des Verurteilten durch soziale Hilfen erleichtern und zugleich die Allgemeinheit vor weiteren Straftaten schützen. Dieses Ziel kann nur erreicht werden, wenn die beteiligten Stellen – Justizvollzugsanstalt, Staatsanwaltschaft, Gericht, Führungsaufsichtsstelle, Bewährungshelfer, forensische Ambulanz, ggf. auch Polizei und Jugendamt – aufeinander abgestimmt zusammenwirken.

Wenn das Instrument der Führungsaufsicht so funktionieren soll, dass der aus der Haft Entlassene tatsächlich durch ein enges Geflecht von Hilfe und Überwachung an der Begehung neuer Straftaten gehindert wird, müssen die beteiligten Stellen zusammenarbeiten und sich unter Beachtung ihrer gesetzlichen Vorgaben gegenseitig über ihre Maßnahmen und Erkenntnisse informieren.

Rechtsgrundlagen für die „Führungsaufsicht“ finden sich sowohl in der Strafprozessordnung als auch im Strafgesetzbuch. Weiterhin sind die einschlägigen Vorschriften der beteiligten Stellen sowie der mit den Justizbehörden im Rahmen der Führungsaufsicht kooperierenden Behörden zu beachten. Gerade die Sozialgesetzbücher setzen dem Informationsaustausch mit Sozialbehörden einschließlich Jugendämtern auch im Rahmen der Führungsaufsicht sehr enge Grenzen.

Eine Arbeitsgruppe, an deren Sitzungen wir regelmäßig teilnahmen, untersuchte im Rahmen einer Stellungnahme die rechtlichen Grundlagen für das Zusammenwirken der an der Führungsaufsicht beteiligten Stellen und die sich daraus ergebenden Rechte und Pflichten zur Verarbeitung personenbezogener Daten, insbesondere ihrer Übermittlung. Ausgehend von der jeweils Daten übermittelnden Stelle werden zu jeder Daten empfangenden Stelle in einem Kapitel die Rechtsgrundlagen für die Informationsweitergabe dargestellt. Damit ist die Stellungnahme so aufgebaut, dass sie später als Nachschlagwerk genutzt werden kann.

Die Stellungnahme „Optimierung der Führungsaufsicht – Informationsrechte und -pflichten der Beteiligten“ fasst die Rechtsgrundlagen für den Informationsaustausch über Haftentlassene zusammen. Sie soll den Beteiligten als Nachschlagewerk dienen, indem sie die rechtlichen Möglichkeiten aber auch die Schranken der gegenseitigen Informationsweitergabe darstellt.

6 Bildung, Jugend und Sport

6.1 Novellierung der Datenschutzverordnung Schulwesen zur Umsetzung des Brandenburgischen Schulgesetzes

Bereits im letzten Tätigkeitsbericht[59] hatten wir ausführlich über die Neuerungen im Brandenburgischen Schulgesetz berichtet, insbesondere über die Veränderungen in der Schulstatistik sowie über die Einführung einer automatisierten Schülerdatei und von Schülerlaufbahnstatistiken. Schon zum damaligen Zeitpunkt wiesen wir darauf hin, dass vor der Anwendung der neuen Regelungen Einzelheiten hierzu in einer Rechtsverordnung festzulegen sind.

Mit dem zuständigen Ministerium für Bildung, Jugend und Sport einigten wir uns darauf, dass zunächst nur die wichtigsten Änderungen in der stark veralteten und anpassungsbedürftigen Datenschutzverordnung Schulwesen vorgenommen werden sollten, um eine zügige Anwendung der Neuregelungen des Brandenburgischen Schulgesetzes zu ermöglichen. Neben der Anpassung der Datenschutzverordnung an die Änderungen des Schulgesetzes selbst waren auch die zwischenzeitlich erfolgten Änderungen des Brandenburgischen Datenschutzgesetzes sowie der aktuelle Stand der Technik zu berücksichtigen. Eine umfassende Novellierung der Datenschutzverordnung Schulwesen sollte bis zum Ende des Berichtszeitraums erfolgen.

Einen ersten Entwurf zur Änderung der Datenschutzverordnung Schulwesen sandte uns das Ministerium im Juli 2008 zu. Dieser war jedoch in verschiedener Hinsicht anpassungsbedürftig. In mehreren zeitintensiven Abstimmungsgesprächen diskutierten wir mit den Verantwortlichen die notwendigen Änderungen.

Neben der Verbesserung von redaktionellen Fehlern waren z. B. Festlegungen zu IT-Sicherheitskonzepten für schulische DV-Verfahren, zu einzelnen technischen und organisatorischen Maßnahmen, zur Bestellung behördlicher Datenschutzbeauftragter sowie zum Führen von Verfahrensverzeichnissen zu ergänzen, um die Rechtskonformität des Entwurfs mit dem geltendem Schul- bzw. Datenschutzgesetz herzustellen.

Mit den neu in die Datenschutzverordnung Schulwesen aufzunehmenden §§ 13 bis 15 beabsichtigte das Ministerium, Einzelheiten zur Schulstatistik, zur automatisierten Schülerdatei sowie zur Schülerlaufbahnstatistik festzulegen. Hierbei bemängelten wir z. T. unklare Regelungen zu einzelnen Schritten der Datenverarbeitung, den verantwortlichen bzw. die Verarbeitung

59 vgl. Tätigkeitsbericht 2006/2007, A 6.4

durchführenden Stellen, den Datenflüssen zwischen diesen Stellen sowie zu Einschränkungen des Zugriffs auf die Daten. Auch in diesen Punkten wurde der Entwurf mit unserer Unterstützung nachgebessert.

Bezüglich der Schulstatistik bzw. der Schülerlaufbahnstatistiken ist zu beachten, dass hierfür personenbezogene Daten der Schüler mit z. T. hohem Schutzbedarf aufbereitet werden, die von den Schulen für festgelegte Zeiträume zu bestimmten Stichtagen an eine zentrale Stelle zu übermitteln sind. Der Umfang dieser Daten ist in einer Anlage der Datenschutzverordnung Schulwesen bzw. im Schulgesetz abschließend geregelt.

Zur Verhinderung des Missbrauchs der übermittelten personenbezogenen Einzeldaten forderten wir, dass der Zugriff darauf streng reglementiert sein muss. Weder das Ministerium für Bildung, Jugend und Sport noch die staatlichen Schulämter oder die Schulträger benötigen ihn für ihre Aufgaben. Der Zugriff darf nur einer den Grundsätzen des Brandenburgischen Statistikgesetzes verpflichteten Stelle möglich sein. Falls das Ministerium die Daten innerhalb des eigenen Geschäftsbereichs selbst statistisch aufbereiten möchte, hat es deshalb eine eigene Statistikstelle einzurichten. Dabei ist sicherzustellen, dass diese Stelle räumlich, organisatorisch und personell von der übrigen Verwaltungsstruktur abgegrenzt ist. Durch geeignete technische und organisatorische Maßnahmen ist die Trennung der personenbezogenen Daten von anderen Verwaltungsdaten sowie ihre Verwendung ausschließlich für Zwecke der Erstellung von Statistiken zu gewährleisten. Die mit der Datenaufbereitung befassten Beschäftigten dürfen die aus ihrer Tätigkeit gewonnenen personenbezogenen Erkenntnisse nicht in anderen Verfahren oder für andere Zwecke verwenden oder offenbaren.

Das Ministerium für Bildung, Jugend und Sport folgte unseren Forderungen und fügte entsprechende Regelungen in den Entwurf der Datenschutzverordnung Schulwesen ein. Dessen letzter Stand datiert vom 3. Juni 2009. Zu einer Veröffentlichung als Voraussetzung des In-Kraft-Tretens der Verordnung kam es allerdings bis zum Redaktionsschluss dieses Berichts nicht.

Im Rahmen der Novellierung der Datenschutzverordnung Schulwesen haben wir das Ministerium für Bildung, Jugend und Sport mehrfach intensiv beraten. Trotz der uns gegenüber stets angemahnten Eile gelang es dem Ministerium jedoch im Berichtszeitraum nicht, die Arbeiten zur Festlegung der erforderlichen Einzelheiten zu den mittlerweile über zwei Jahre bestehenden Neuregelungen des Brandenburgischen Schulgesetzes abzuschließen. Auch eine umfassende Überarbeitung der Datenschutzverordnung Schulwesen ist weiter nicht in Sicht.

6.2 Sprachstandsfeststellung vor der Einschulung

Im Frühjahr 2009 bat uns das Ministerium für Bildung, Jugend und Sport um Hinweise zu dem uns zur Kenntnis gegebenen Entwurf der Verordnung zur Durchführung der Sprachstandsfeststellung und kompensatorischen Sprachförderung.[60] Zu regeln waren darin insbesondere datenschutzgerechte Meldungen über die Teilnahme der Vorschulkinder an Sprachförderkursen.

In der Vergangenheit wurde bei den Schuleingangsuntersuchungen regelmäßig ein sehr großer Anteil von Kindern mit Sprachauffälligkeiten und Sprachstörungen festgestellt. Deshalb hat der Gesetzgeber in § 37 Abs. 1 Brandenburgisches Schulgesetz für alle Kinder im Jahr vor der Einschulung die Pflicht zur Teilnahme an einer Sprachstandsfeststellung vorgesehen. Wird im Rahmen dieses Verfahrens ein Sprachförderbedarf festgestellt, besteht wiederum eine Pflicht zur Teilnahme an einem entsprechenden Sprachförderkurs in einer Kita.

Sofern die Eltern ihrer Verpflichtung zur Sicherstellung der Teilnahme ihres Kindes an einem Sprachförderkurs nicht nachkommen, sah der Entwurf der Verordnung zunächst vor, dass die Kindertagesstätten die (vermeintlich) zuständige Grundschule darüber zu unterrichten haben. Hiergegen hatten wir datenschutzrechtliche Bedenken. Da insbesondere noch kein öffentlich-rechtliches Schulverhältnis begründet wurde, erlauben es schulrechtliche Vorschriften der Schule ohnehin nicht, auf Schulpflichtverletzungen einzuwirken.

Liegt der Sprachförderkurs zeitlich vor der Anmeldung des schulpflichtigen Kindes an der örtlich zuständigen Schule, kann die Kindertagesstätte gar nicht wissen, welche Schule die zuständige ist. Kommen mehrere Schulen für die Anmeldung infrage, wählen beispielsweise die Eltern die Schule aus. Es war somit nicht sichergestellt, dass auch die Schule, mit der das Schulverhältnis letztendlich begründet wird, die erforderlichen personenbezogenen Daten erhält. Dem gegenüber hätten Schulen, mit denen gerade kein Schulverhältnis begründet wird, Daten erhalten, die für ihre Aufgabenerfüllung nicht erforderlich gewesen wären.

Das Ministerium berücksichtigte unsere Bedenken und änderte den Entwurf. Nunmehr unterrichten die Kitas nicht mehr die Grundschulen, sondern das zuständige staatliche Schulamt.

---

60 Verordnung zur Durchführung der Sprachstandsfeststellung und kompensatorischen Sprachförderung (SprachfestFörderverordnung – SfFV) vom 3. August 2009 (GVBl. II S. 505)

Über die mangelnde Teilnahme eines Vorschulkindes an einem verpflichtenden Sprachförderkurs darf die Kindertagesstätte ausschließlich das regional zuständige staatliche Schulamt unterrichten.

6.3 Gegensprechanlage mit Überwachungsmöglichkeit

In einer Förderschule für geistig behinderte Kinder wurde eine Gegensprechanlage installiert, die das unbemerkte Abhören der Unterrichtsräume ermöglichte.

Im Zuge des Umbaus eines Gebäudes zu einer Förderschule hat der zuständige Schulträger, eine Wechselsprechanlage installiert, damit Lehrkräfte im Notfall schnell das Sekretariat alarmieren können. Es gab Grund zur Annahme, dass diese Anlage missbräuchlich genutzt werden könnte.

Im Ergebnis einer unangekündigten Kontrolle bestätigte sich der Verdacht, dass jede Person vom Sekretariat aus eine Verbindung zu den Nebenstellen in den Fach-, Klassen-, Aufenthalts- und Büroräumen hätte aufbauen können. Da die Nebenstellen den Aufbau einer Verbindung weder optisch noch akustisch anzeigten, bestand die Möglichkeit des unbemerkten Abhörens von Lehrern und Schülern.

Wir haben die Schulleitung, den Schulträger sowie den Vermieter des Schulgebäudes darauf hingewiesen, dass entsprechend der momentanen Konfiguration der Wechselsprechanlage ein datenschutzgerechter Betrieb nicht möglich ist. Da ein Umbau technisch ausgeschlossen war, musste eine Lösung gefunden werden, bei der die Anlage nur in einer Richtung zu betreiben ist, um das Absetzen eines Notrufes von der Nebenstelle zum Sekretariat zu ermöglichen.

Nach intensiver Beratung durch unsere Behörde ist das zentrale Bedienteil in einem elektromechanisch verriegelten Kompaktschaltschrank mit manipulationssicherem Ereignisspeicher eingebettet worden. Dieser ermöglicht den Zugriff erst nach einer Authentifizierung mittels eines personalisierten Schlüssels. Der Lautsprecher wurde so angeordnet, dass der Notruf von der Nebenstelle zum Sekretariat jederzeit dort akustisch wahrgenommen werden kann. Somit können alle anwesenden Personen, auch wenn sie nicht über einen Schlüssel verfügen, entsprechende Hilfsmaßnahmen ergreifen.

Da der Betrieb der Gegensprechanlage geeignet ist, das Verhalten oder die Leistung der Beschäftigten zu überwachen, handelt es sich gem. § 65 Nr. 2 Personalvertretungsgesetz um eine mitbestimmungspflichtige Angelegenheit, bei der der Lehrerrat im Rahmen einer Dienstvereinbarung zu beteiligen ist. Diese Dienstvereinbarung muss im Wesentlichen Festlegungen zur Umset-

zung der getroffenen Maßnahmen, zu Zugangsberechtigungen sowie zur Art und Weise der Auswertung der Protokolldateien enthalten.

Aus unserer Sicht sind die nunmehr getroffenen technischen und organisatorischen Maßnahmen geeignet, die missbräuchliche Nutzung des unbemerkten Abhörens von Schülern und Lehrern weitestgehend zu verhindern.

Die Freigabe einer Wechselsprechanlage darf nur erfolgen, wenn durch technische und organisatorische Maßnahmen einschließlich einer Dienstvereinbarung sichergestellt ist, dass die Risiken für die Betroffenen beherrscht werden.

6.4 Tagespflegestatistik – keine Auskunftspflicht für Tagespflegepersonen

Durch eine Eingabe wurden wir darauf aufmerksam, dass ein Landkreis Tagesmütter dazu aufforderte, Angaben über die von ihnen betreuten Kinder für eine Bundesstatistik personenbezogen (mit Namen und Geburtstag) zu melden. Da nur die Tagespflegepersonen die aktuellen und vollständigen Daten kennen, verfielen noch etliche andere Jugendämter auf die Idee, die Tagesmütter in das Verfahren einzubeziehen. Die einen ließen sich die Angaben zuschicken, um ihren eigenen Datenbestand abzugleichen, andere veranlassten die Tagespflegepersonen zu einer Übermittlung der Daten an das Amt für Statistik Berlin-Brandenburg.

Während der fragliche Landkreis zunächst hartnäckig seine Vorgehensweise verteidigte, weil er es für seine Pflicht hielt, das Formular für die Bundesstatistik möglichst vollständig und mit aktuellen Angaben auszufüllen, teilte das Ministerium für Bildung, Jugend und Sport unsere Auffassung: § 102 Abs. 2 Achtes Buch Sozialgesetzbuch sieht eine Auskunftspflicht für Tagespflegepersonen nicht vor. Angesichts der abschließenden Aufzählung der Auskunftspflichtigen besteht auch kein Raum für eine Auslegung der Vorschrift. Der Landkreis darf somit die ihm für die Statistik fehlenden Angaben nicht von den Tagesmüttern erfragen und muss in diesem Fall in Kauf nehmen, keine vollständigen Daten zur Bundesstatistik beitragen zu können.

Eine Nutzung der für die Statistik erhobenen Angaben für andere Zwecke wie etwa einen Abgleich mit vorhandenen Verwaltungsdaten hielten das Ministerium und wir ebenfalls für unzulässig.

Vorgaben in statistischen Erhebungsbögen verleiten leicht dazu, die erfragten Angaben kritiklos zu erheben. Stattdessen ist stets zu prüfen, ob eine gesetzliche Grundlage hierfür besteht.

7 Arbeit, Soziales, Frauen und Familie

7.1 Zum Umgang mit persönlichen Daten der Empfänger von Arbeitslosengeld II

Seit nunmehr fünf Jahren gibt es die Möglichkeit, Leistungen zur Grundsicherung für Arbeitsuchende zu beantragen. Seit dieser Zeit erreichen uns Fragen von Bürgern, ob und wenn ja, welche Dokumente sie den Hartz-IV-Behörden vorlegen müssen. Was darf in den Akten gespeichert, was an Dritte übermittelt werden?

7.1.1 Vorlage von Kontoauszügen

Die von uns und anderen Datenschutzbeauftragten seit Jahren vertretene Rechtsauffassung wurde nun durch ein Urteil des Bundessozialgerichts bestätigt.[61] Grundsätzlich ist die Anforderung von Kontoauszügen der letzten ein bis drei Monate bei der erstmaligen oder Folgebeantragung von Leistungen sowie von einmaligen Beihilfen zulässig. Kontoauszüge eines längeren Zeitraums dürfen zum Zweck der Klärung einer konkreten Frage zu den Einkommens- und Vermögensverhältnissen des Antragstellers verlangt werden, wenn die Vorlage anderer Unterlagen dazu nicht ausreicht bzw. wenn konkrete Zweifel an der Vollständigkeit oder Richtigkeit der Angaben bestehen. Die Schwärzung einzelner Buchungstexte ist insbesondere bei Sollbuchungen über geringe Beträge zulässig. Dies gilt in jedem Fall, wenn der Buchungstext Rückschlüsse auf politische, weltanschauliche oder religiöse Ansichten zulässt. Das Amt ist verpflichtet, bereits bei der Anforderung der Kontoauszüge auf die Möglichkeit des Schwärzens hinzuweisen. Kopien der vorgelegten Kontoauszüge dürfen nur zu den Akten genommen werden, wenn diese ausschließlich leistungsrelevante Angaben enthalten.[62]

7.1.2 Mehrbedarf für kostenaufwändige Ernährung

Für die Beantragung eines ernährungsbedingten Mehrbedarfs wurde dem Betroffenen vom Grundsicherungsamt für Arbeitsuchende ein Formular zur Vorlage bei seinem Arzt ausgehändigt. Neben der Angabe, welche Erkrankung den Mehrbedarf bedingt, sollte der behandelnde Arzt Körpergröße und -gewicht des Betroffenen eintragen. Diese Angaben sind für die Feststellung, ob eine Erkrankung einen Mehrbedarf auslöst, jedoch nicht erforderlich. Es genügt, dass der behandelnde Arzt lediglich die Krankheit im Ankreuzverfahren angibt, für die Mehrkosten bei der Ernährung entstehen. Außerdem fehlte

---

61 Urteil des Bundessozialgerichts vom 19. September 2008 (B 14 AS 45/07 R)

62 siehe auch http://www.lda.brandenburg.de → Infos zum Datenschutz → Arbeit, Soziales, Gesundheit und Familie/Frauen → Hinweise zur datenschutzgerechten Ausgestaltung der Anforderungen von Kontoauszügen bei der Beantragung von Sozialleistungen

auf dem Formular eine Erklärung zur Entbindung des Arztes von der Schweigepflicht. Auf unsere Empfehlung änderte das Grundsicherungsamt das Formular.

7.1.3 Speicherung von Gesundheitsdaten

Im Rahmen einer von der Hartz-IV-Behörde beauftragten Untersuchung erstellt der Arzt ein Gutachten zur Erwerbsfähigkeit des Antragstellers. Dabei ist auf eine strikte Datentrennung zu achten: Die medizinische Dokumentation verbleibt beim Arzt; die sozialmedizinische Stellungnahme wird an den Arbeitsvermittler übermittelt. Letzterer enthält also lediglich das für die Vermittlung relevante Ergebnis (z. B. „kein schweres Heben“ oder „keine Schichtarbeit“). Angaben zur Diagnose oder zu Therapien darf der Arzt nicht an die Hartz-IV-Behörde übermitteln. Die Bundesagentur für Arbeit verwendet inzwischen Formulare, die eine entsprechende Unterteilung vorsehen.

7.1.4 Datenerhebung beim potenziellen Arbeitgeber

Empfänger von Arbeitslosengeld II müssen in der Regel ihre Bemühungen um einen Arbeitsplatz gegenüber dem Grundsicherungsamt belegen. In der mit dem Leistungsempfänger abzuschließenden Eingliederungsvereinbarung wird festgelegt, wie viele Bewerbungen monatlich nachzuweisen sind und in welcher Form der Nachweis zu erfolgen hat. Geeignete Mittel sind das Bewerbungsanschreiben oder die Bestätigung der Bewerbung durch den Arbeitgeber.

Grundsätzlich sind diese Sozialdaten gemäß § 67a Abs. 2 Satz 1 Zehntes Buch Sozialgesetzbuch beim Leistungsempfänger zu erheben. Nicht selten kommt es jedoch vor, dass das Grundsicherungsamt direkt mit dem potenziellen Arbeitgeber Kontakt aufnimmt und nachfragt, ob und mit welchem Erfolg sich der Leistungsempfänger beworben habe. Ohne Anhaltspunkte für missbräuchliches Verhalten des Leistungsempfängers halten wir diese routinemäßige Abfrage unter Umgehung des Ersterhebungsgrundsatzes für unzulässig. Sollte es im Einzelfall Anlass zu einer Nachfrage beim Arbeitgeber geben, so wird die Dokumentation der Gründe dafür empfohlen.

7.1.5 Datenerhebung beim Vermieter

Eine Hartz-IV-Behörde hat sich ohne Wissen der Betroffenen an die Wohnungsgenossenschaft gewandt, um Einzelheiten zum Mietverhältnis zu erfahren. Sie hielt dieses Vorgehen zur Vermeidung einer zeitlichen Verzögerung bei der Antragsbearbeitung für notwendig, da die Betroffenen in ihrer Korrespondenz mit der Behörde ihre Telefonnummer zuvor nicht angegeben hatten.

Durch dieses Vorgehen erfuhr die Genossenschaft davon, dass die betreffenden Mieter auf Sozialleistungen angewiesen sind.

Für ein Abweichen vom Ersterhebungsgrundsatz reicht die Tatsache, dass die Rufnummer oder die E-Mail-Adresse nicht angegeben worden war, nicht aus. Die Angabe von Telefonnummern ist freiwillig. Empfänger von Arbeitslosengeld II sind lediglich zur Sicherstellung der postalischen Erreichbarkeit verpflichtet. Das Amt hätte die Betroffenen vielmehr schriftlich auffordern müssen, die noch ausstehenden Unterlagen beizubringen. Insofern war die direkte Kontaktaufnahme mit der Wohnungsgenossenschaft unzulässig.

Das Amt teilte uns mit, dass es sich unserer Rechtsauffassung anschließe und künftig den Grundsatz der Ersterhebung beim Betroffenen beachten werde.

7.1.6 Daten auf dem Flur

Selbstverständlich sollte es sein, dass Daten, die dem Sozialgeheimnis unterliegen, nicht für jedermann einsehbar aufbewahrt werden. Dennoch mussten wir bei einem Kontrollbesuch in einem Grundsicherungsamt feststellen, dass im Flur des Empfangsbereiches offene Posteingänge, Leistungsbescheide, schriftliche Geldanweisungen an Hartz-IV-Empfänger sowie komplette Leistungsakten ungesichert gelagert wurden. Jedem Besucher war es damit möglich, ungestört ihre Inhalte zur Kenntnis zu nehmen. Dies ist ein grober Verstoß gegen sozialdatenschutzrechtliche Vorschriften. Aufgrund der sofortigen Beendigung des rechtswidrigen Zustandes haben wir jedoch von einer Beanstandung abgesehen.

7.1.7 Datenerhebung bei Selbstständigen

Empfänger von Arbeitslosengeld II, die zugleich eine selbstständige Tätigkeit ausüben, müssen ihre Einkünfte offenlegen. Zur Berechnung des Einkommens sind die tatsächlich geleisteten notwendigen Ausgaben von den Betriebseinnahmen abzuziehen, was eine äußerst umfangreiche Datenerhebung zur Folge hat. Mehrfach wurde dabei von Hartz-IV-Behörden die Bekanntgabe von Kundendaten des Selbstständigen oder die Vorlage von Arbeitsverträgen seiner Angestellten verlangt. Dies ist grundsätzlich für die Einkommensberechnung nicht erforderlich. Gegebenenfalls sind nicht notwendige Daten zu schwärzen.

7.1.8 Datenzugriff im Verfahren A2LL

Die Arbeitsgemeinschaften nutzen bei der Datenverarbeitung die Leistungs- und Berechnungssoftware A2LL. Wie wir bereits zu einem früheren Zeit-

punkt[63] bemängelt hatten, besteht für die Sachbearbeiter ein uneingeschränkter bundesweiter Zugriff auf alle Daten der Leistungsempfänger. Dieser datenschutzrechtliche Mangel wurde zwar nicht behoben; eine Protokollierung der Zugriffe ermöglicht jetzt zumindest eine nachträgliche Aufklärung im Fall von unberechtigter Kenntnisnahme.

So war es uns möglich, den wiederholten Zugriff eines unzuständigen Mitarbeiters auf sensitive Daten eines Leistungsempfängers (z. B. auf Einkommensdaten, den beruflichen Werdegang, anstehende Weiterbildungsmaßnahmen, Erkrankungen) aufzuklären. Für diese Recherchen gab es keinen fachlichen Anlass. Sie stellen somit eine bewusste, systematische Verletzung des Sozialdatenschutzes dar.

Zuständigkeitshalber haben wir den Vorfall an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit weitergeleitet. Dieser prüft nun, ob gegenüber der Arbeitsgemeinschaft eine Beanstandung ausgesprochen werden muss.

Die Arbeitsgemeinschaften sind als Daten verarbeitende Stellen für den Schutz des Sozialgeheimnisses ihrer Leistungsempfänger zumindest mitverantwortlich. Sie sollten dazu verpflichtet werden, stichprobenartig einmal im Quartal oder halbjährlich die im Programm A2LL erzeugten Protokolle auf unberechtigte Zugriffe zu überprüfen und bei Auffälligkeiten entsprechende Maßnahmen einzuleiten.

Die Hartz-IV-Behörden dürfen nur solche Daten erheben, die für die Feststellung des Leistungsanspruchs unerlässlich sind. Der Ersterhebungsgrundsatz ist dabei stets zu beachten.

Solange die Software A2LL keine Einschränkung von Zugriffen auf das erforderliche Maß ermöglicht, sind die Zugriffsprotokolle zumindest stichprobenartig auf unberechtigte Abfragen zu überprüfen.

Eine regelmäßige Schulung der Mitarbeiter zum Sozialdatenschutz ist notwendig.

63 vgl. Tätigkeitsbericht 2004/2005, A 1.5.1

7.2 Sozialdatenschutz im Verfahren zur Feststellung einer Behinderung

Das Landesamt für Soziales und Versorgung benötigt zur Prüfung eines Antrags auf Feststellung des Vorliegens einer Behinderung und deren Grades medizinische Unterlagen über den Antragsteller. Bislang forderte es die Befunde von den Ärzten, Leistungsträgern und anderen Einrichtungen nur unter Vorlage der Erklärung des Betroffenen zur Einwilligung in die Datenverarbeitung sowie zur Entbindung von der ärztlichen Schweigepflicht an. Im Frühjahr des Jahres 2008 änderte das Landesamt diese Vorgehensweise und sah fortan davon ab, diese Erklärungen vorzulegen.

Hintergrund für die geänderte Praxis war die Absicht, das Verfahren zur Feststellung einer Behinderung sowie zur Ausstellung eines Schwerbehindertenausweises nach § 69 Neuntes Buch Sozialgesetzbuch zu vereinfachen. Das Landesamt ging davon aus, dass die Übersendung der Erklärungen des Antragstellers zur Einwilligung in die Datenverarbeitung sowie zur Entbindung von der ärztlichen Schweigepflicht der geplanten Einführung des neuen, speziell für diese Angelegenheit beschafften IT-Verfahrens schweb.NET im Wege stünde. Die Behörde war der Auffassung, es genüge, wenn die Sachbearbeiter den Ärzten lediglich mitteilen, dass solche Erklärungen in der Akte vorliegen. Dieser Rechtsauffassung folgten wir nicht.

Leistungsträger im Sinne des § 35 Erstes Buch Sozialgesetzbuch (SGB I) müssen das dort verankerte Sozialgeheimnis beachten. Danach ist eine Übermittlung von Sozialdaten an Dritte – also auch an das Landesamt für Soziales und Versorgung – grundsätzlich nur zulässig, wenn entweder eine gesetzliche Übermittlungsbefugnis vorliegt oder der Betroffene eingewilligt hat. Um dies zu beurteilen, muss sie prüfen können, ob die Einwilligungserklärung nach § 67b Abs. 2 Zehntes Buch Sozialgesetzbuch (SGB X) wirksam erteilt wurde. Dies kann sie nur, wenn ihr die Erklärung auch zur Verfügung steht. Die Verantwortung für die Zulässigkeit einer Übermittlung trägt die übermittelnde Stelle (§ 67d Abs. 2 Satz 1 SGB X).

Für alle anderen, nicht in § 35 SGB I genannten medizinischen Einrichtungen sowie für Ärzte gelten die Vorschriften des Bundesdatenschutzgesetzes sowie des Brandenburgischen Datenschutzgesetzes. Beide Rechtsgrundlagen enthalten ebenfalls keine Pflicht der ersuchten Stellen, die Daten des Betroffenen ohne Prüfung seiner Erklärung über die Einwilligung in die Datenverarbeitung an das Landesamt für Soziales und Versorgung zu übermitteln. Die ärztliche Schweigepflicht kann auch in diesen Fällen nur unter Vorlage einer wirksamen Entbindungserklärung aufgehoben werden.

Im Ergebnis einer Abstimmung mit dem Ministerium für Arbeit, Soziales, Gesundheit und Familie folgte das Landesamt für Soziales und Versorgung unserer Rechtsauffassung. Künftig werden die Erklärung des Antragstellers über die Einwilligung in die Datenverarbeitung sowie die Entbindung von der ärztlichen Schweigepflicht gescannt, in dem neuen Verfahren schweb.NET digital hinterlegt und jedem Auskunftsersuchen der Behörde an Ärzte, medizinische Einrichtungen oder Leistungsträger beigefügt. Bis zur vollständigen technischen Umsetzung des neuen Verfahrens werden die Erklärungen fotokopiert und den entsprechenden Schreiben beigefügt.

Ärzte, medizinische Einrichtungen oder Leistungsträger können Gesundheitsdaten nur an das Landesamt für Soziales und Versorgung übermitteln, wenn der betroffene Antragsteller wirksam in die Datenverarbeitung einwilligt und die Ärzte von der Schweigepflicht entbindet. Um zu prüfen, ob dies der Fall ist, muss ihnen die Erklärung des Betroffenen zur Verfügung stehen.

7.3 Kontendatenabruf durch Sozialleistungsträger

Im letzten Tätigkeitsbericht[64] wiesen wir auf die Aufnahme einer Regelung in die Abgabenordnung (AO) hin, die es unter anderem den für die Grundsicherung für Arbeitsuchende zuständigen Behörden ermöglicht, beim Bundeszentralamt für Steuern Kontostammdaten abzufragen. Die Kontenabfrage ist streng geregelt und darf nur im begründeten Einzelfall erfolgen. Wir haben stichprobenartig ein JobCenter auf die Einhaltung der datenschutzrechtlichen Anforderungen bei der Durchführung der Kontendatenabfrage kontrolliert.

Das Kontendatenabrufverfahren nach § 93 Abs. 8 AO ist zur Überprüfung des Vorliegens der Anspruchsvoraussetzungen für den Leistungsbezug zulässig, sofern die Abfrage erforderlich ist und ein vorheriges Auskunftsersuchen bei dem Betroffenen nicht zum Ziel geführt hat oder keinen Erfolg verspricht.

In einer Geschäftsanweisung[65] legt die Bundesagentur für Arbeit die Voraussetzungen und das Verfahren für den Abruf von Kontenstammdaten durch die Arbeitsgemeinschaften bzw. JobCenter fest. Die Geschäftsanweisung beinhaltet eine ausführliche Dokumentationspflicht hinsichtlich der Ermessenserwägungen, wodurch dem Erforderlichkeitsprinzip des § 93 Abs. 8 AO im Einzelfall Rechnung getragen werden soll. Es werden die einzelnen für die Ermessenserwägungen relevanten Kriterien (Verhältnismäßigkeit der Mittel, zur Erforderlichkeit, Zumutbarkeit, Treu und Glauben und zum Willkür- und Übermaßverbot) aufgeführt. Die Mitarbeiter sind angewiesen, die fallbezoge-

64 vgl. Tätigkeitsbericht 2006/2007, A 9.1.2

65 HEGA 08/07 – 22 – GA Nr. 27 vom 20. August 2007

nen Erwägungen zu diesen Kriterien in der Akte zu dokumentieren. Insbesondere sollen die Gründe, weshalb die Durchführung des Abrufes erforderlich ist, sowie die erfolgte Information des Betroffenen vor und nach der Abfrage beim Bundeszentralamt für Steuern vermerkt werden. Bestandteil der Geschäftsanweisung ist weiterhin ein Vordruck für das Abrufersuchen, der zwischen dem Bundeszentralamt für Steuern, dem Bundesministerium für Finanzen und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit abgestimmt wurde. Der vollständig ausgefüllte Vordruck soll durch den Teamleiter unterzeichnet werden.

In den von uns geprüften Einzelfällen wurden die Betroffen mit Übersendung des Fortzahlungsantrages über die Möglichkeit des Kontendatenabrufs informiert. Gleichfalls erfolgte diese Information über das Merkblatt zur Grundsicherung für Arbeitsuchende der Bundesagentur für Arbeit.

Im Ergebnis der Prüfung mussten wir feststellen, dass zwar der zur Abfrage bereitgestellte Vordruck genutzt, jedoch nicht konsequent am Einzelfall orientiert ausgefüllt wurde. Insofern konnte die Entscheidung des JobCenters, den Kontendatenabruf vorzunehmen, nicht komplett nachvollzogen werden. Darüber hinaus war der ausgefüllte Vordruck durch den Teamleiter abgezeichnet worden, doch befand sich in den Akten keine Kopie des Abfrageersuchens, sondern lediglich ein nicht unterzeichneter Computerausdruck.

Die unvollständige Aktenführung wurde von uns ebenso kritisiert, wie die dadurch bedingte fehlende Nachvollziehbarkeit der Verwaltungsentscheidung. Unsere Hinweise wurden von der Geschäftsleitung des JobCenters aufgenommen und die Änderung der Verfahrensweise zugesichert.

Zur Nachprüfbarkeit der rechtlichen Voraussetzungen von Kontendatenabrufen muss künftig auf eine aussagekräftige und vollständige Dokumentation des Verfahrensablaufs und der Entscheidungen geachtet werden.

7.4 Prüfung des Verfahrens Open/Prosoz

Mit dem Verfahren Open/Prosoz werden sensitive personenbezogene Daten der Antragsteller von Leistungen im Sozialbereich verarbeitet. Im Berichtszeitraum führten wir eine Kontrolle der Anwendung dieses Verfahrens in einem Amt für Jugend, Soziales und Wohnen durch.

Aufgrund der Sensitivität der verarbeiteten Daten sind die erforderlichen technischen und organisatorischen Maßnahmen besonders restriktiv umzusetzen. Im Folgenden berichten wir über wesentliche Ergebnisse der Prüfung.

7.4.1 Erstellung eines IT-Sicherheitskonzepts

Vor dem erstmaligen Einsatz von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden, ist gemäß § 7 Abs. 3 Brandenburgisches Datenschutzgesetz (BbgDSG) von der Daten verarbeitenden Stelle zu untersuchen, ob von diesen Verfahren spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können. Die Freigabe eines automatisierten Verfahrens darf nur erteilt werden, wenn ein aus einer Risikoanalyse entwickeltes IT-Sicherheitskonzept ergeben hat, dass die Gefahren durch technisch-organisatorische Maßnahmen nach § 10 Abs. 1 und 2 BbgDSG beherrscht werden können. Entsprechend der technischen Entwicklung ist die Ermittlung der zu treffenden technischen und organisatorischen Maßnahmen in angemessenen Abständen zu wiederholen. Durch die Erstellung eines IT-Sicherheitskonzeptes lassen sich die Gefahren identifizieren und bewerten sowie angemessene Sicherheitsmaßnahmen ableiten.

Während der Prüfung stellten wir fest, dass ein gemäß § 7 Abs. 3 BbgDSG zu erstellendes IT-Sicherheitskonzept nicht vorhanden war. Nach Angaben des geprüften Amtes für Jugend, Soziales und Wohnen ist ein solches erst in Arbeit. Wir haben das Amt aufgefordert, es schnellstmöglich fertigzustellen und die im Realisierungsplan aufgeführten Maßnahmen konsequent umzusetzen.

7.4.2 Verschlüsselung sensitiver Daten

Derzeit werden die in der Open/Prosoz-Datenbank gespeicherten sensitiven Daten (u. a. Grad und Art der Behinderung, Pflegestufe, ernährungsbedingte Mehrbedarfe) nicht verschlüsselt. Aufgrund des hohen Schutzbedarfs der personenbezogenen Daten ist eine Verschlüsselung jedoch zwingend erforderlich. Im Zuge der Erstellung des IT-Sicherheitskonzepts ist daher ein Kryptokonzept zu erarbeiten, in dem die zu realisierenden Maßnahmen zur Verschlüsselung der Daten beschrieben werden. Die Verschlüsselung der in der Datenbank gespeicherten Daten kann nur gemeinsam mit dem Hersteller des Verfahrens realisiert werden.

7.4.3 Sicherung der Arbeitsplatzcomputer

Auf den Arbeitsplatzcomputern (APC) ist das Betriebssystem Windows XP installiert. Zum Zeitpunkt der Kontrolle waren die USB-Schnittstellen nicht gesperrt, sodass nicht ausgeschlossen werden kann, dass sensitive personenbezogene Daten unberechtigt aus dem System auf externe Datenträger (z. B. USB-Stick) kopiert werden. Auch das Einspielen von schadhaften Programmen (u. a. Viren und Trojanern) stellt ein nicht zu vernachlässigendes Risiko dar. Zur Erhöhung der Datensicherheit haben wir die Sperrung der

USB-Schnittstelle gefordert. Ist dies nicht möglich – z. B. durch Nutzung von externen Gräten, die einen USB-Anschluss benötigen (Tastatur, Maus, Drucker usw.) – muss die Benutzung der USB-Schnittstelle durch zusätzliche Sicherheitssoftware eingeschränkt werden. Auf dem Markt sind Produkte verfügbar, die eine zentrale Administration der USB-Schnittstelle ermöglichen.

7.4.4 Passwortgestaltung

Die minimale Passwortlänge ist derzeit bei der Anmeldung am System auf fünf und bei der Anmeldung am Fachverfahren Open/Prosoz auf sechs Zeichen festgelegt. Die Gültigkeitsdauer der Passwörter beträgt bei Open/Prosoz 90 Tage. Die Systempasswörter sind in der Gültigkeit derzeit nicht eingeschränkt. Zur Erhöhung der Datensicherheit haben wir eine restriktive Konfiguration von Passwörtern gefordert. Die minimale Passwortlänge muss nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik einheitlich auf acht Zeichen und die Gültigkeitsdauer der Passwörter einheitlich auf 90 Tage festgelegt werden.

7.4.5 Protokollierung von Nutzerzugriffen

Die Zugriffe der Nutzer werden zum Teil protokolliert. Aufgrund einer Versionsumstellung von Open/Prosoz konnte zum Zeitpunkt der Prüfung nicht abschließend geklärt werden, welche Datenfelder konkret protokolliert werden. Wir haben daher gefordert, in einer Dienstanweisung zur Protokollierung genau festzulegen, welche Zugriffe gespeichert werden, wer die Protokolldateien auswertet und wann die Protokolldateien gelöscht werden. Diese organisatorische Maßnahme ist aus Gründen der Nachvollziehbarkeit derzeit besonders wichtig, weil die sensitiven Daten auf dem Server noch unverschlüsselt gespeichert werden. Auch haben wir eine regelmäßige Überprüfung der Protokolldateien gefordert.

Die Prüfung des Verfahrens Open/Prosoz ergab Mängel. Das kontrollierte Amt für Jugend, Soziales und Wohnen muss die Erstellung des IT-Sicherheitskonzeptes unter Berücksichtigung der Standards des Bundesamtes für Sicherheit in der Informationstechnik zügig abschließen und den daraus resultierenden Maßnahmekatalog konsequent umsetzen.

7.5 ELENA-Verfahren

Zum 1. Januar 2010 wurde der Elektronische Entgeltnachweis (ELENA) eingeführt.[66] Seit diesem Zeitpunkt sind die Arbeitgeber verpflichtet, monatlich die Entgeltdaten ihrer Beschäftigten an eine Zentrale Speicherstelle zu melden; die Nutzung der Daten soll frühestens zwei Jahre später erfolgen. Die datenschutzrechtlichen Bedenken gegen die Schaffung einer bundesweiten zentralen Datenbank konnten bislang nicht vollständig ausgeräumt werden.

Mit dem ELENA-Verfahren will der Gesetzgeber unter anderem eine Entlastung der Wirtschaft von Bürokratiekosten erreichen. Die bisher vom Arbeitgeber in Papierform erstellten Gehaltsbescheinigungen soll der Sozialleistungsbehörde elektronisch zur Verfügung stehen, nachdem der Antragsteller sie mit seiner individuellen elektronischen Signaturkarte für diesen Zweck freigegeben hat. Dennoch werden die Daten nicht wie bisher erst in einem solchen Bedarfsfall erhoben, sondern bereits vorab der zentralen Datenbank pauschal übermittelt. Betroffen davon sind die Einkommensdaten aller abhängig Beschäftigten, Beamten, Richter und Soldaten, obwohl ein Großteil von ihnen vermutlich nie Sozialleistungen in Anspruch nehmen wird. Der überwiegende Teil der Daten dürfte also niemals benötigt werden. Die Speicherung der Daten wäre somit nutzlos, weckt jedoch wie jede derart umfangreiche Datenbank Begehrlichkeiten. Auf die Risiken und verfassungsrechtlichen Bedenken wiesen die Datenschutzbeauftragten des Bundes und der Länder bereits in einer Entschließung hin.[67]

In der Zentralen Speicherstelle werden die Daten erfasst, die bislang in Antragsverfahren von Sozialbehörden (Arbeitsagentur, Wohngeldstelle, Elterngeldstelle) auf amtlichen Vordrucken erhoben wurden. Die Angaben dienen der Prüfung, ob ein Anspruch auf die Sozialleistung besteht. Im Einzelnen sollen die gespeicherten Daten für folgende Bescheinigungen genutzt werden:

- Arbeitsbescheinigung nach § 312 Drittes Buch Sozialgesetzbuch (SGB III),
- Nebeneinkommensbescheinigung nach § 313 SGB III,
- Auskunft über die Beschäftigung nach § 315 Abs. 3 SGB III,

---

66 Gesetz über das Verfahren des elektronischen Entgeltnachweises (ELENA-Verfahrensgesetz) vom 28. März 2009 (BGBl. I S. 634)

67 siehe Anlage 3.5.6: Entschließung „Weiterhin verfassungsrechtliche Zweifel am ELENA-Verfahren“ vom 7. November 2008

- Auskünfte über den Arbeitsverdienst zum Wohngeldantrag nach § 23 Abs. 2 Wohngeldgesetz,

- Einkommensnachweise nach § 2 Abs. 7 Satz 4 und § 9 Bundeselterngeld- und Elternzeitgesetz.

Wie im November 2009 der Verfahrensbeschreibung zu ELENA zu entnehmen war, sollte der Arbeitgeber nicht nur die Lohn- und Gehaltsdaten der Beschäftigten, sondern gleichfalls sämtliche Details, die im Zusammenhang mit einer Kündigung stehen können, sowie die Teilnahme an Streiks an die Zentrale Speicherstelle melden. Zwar wurden diese Daten auch bisher schon in den amtlichen Vordrucken der Bundesagentur für Arbeit zur Arbeitsbescheinigung nach § 312 SGB III erhoben. Die Datenerhebung erfolgte jedoch nur im Falle des streikbedingten Arbeitsplatzverlustes. Durch die pauschale Übernahme aller Angaben aus den Vordrucken in den elektronischen Datensatz und der Pflicht der Arbeitgeber, alle Felder auszufüllen, würde der datenschutzrechtliche Erforderlichkeitsgrundsatz unterlaufen.

Wir unterstützen die Kritik des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an der elektronischen Erfassung derart sensitiver Daten. Seinem Bemühen um die Begrenzung der Datensätze wurde bereits insoweit Rechnung getragen, als die Streikdaten nicht mehr zu übermitteln sind. Den Verfahrensverantwortlichen wurde aufgegeben, sämtliche Felder in der ELENA-Datenbank auf ihre Rechtmäßigkeit zu prüfen.

Die Erforderlichkeit des umfangreichen Datensatzes im ELENA-Verfahren ist zu überprüfen. Nicht jede Angabe ist für die Feststellung des Sozialleistungsanspruchs notwendig. Eine anlasslose Vorratshaltung personenbezogener Daten ist unzulässig.

8 Wirtschaft

Umsetzung der europäischen Dienstleistungsrichtlinie

Die europäische Dienstleistungsrichtlinie[68] soll den grenzüberschreitenden Handel mit Dienstleistungen im gemeinsamen Binnenmarkt fördern und bestehende Hindernisse abbauen. Sie war bis zum 28. Dezember 2009 auch im Land Brandenburg umzusetzen.

[68] Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (Abl. EU Nr. L 376 S. 36)

Die Umsetzung der Dienstleistungsrichtlinie im Land Brandenburg wird durch das Ministerium für Wirtschaft und Europaangelegenheiten koordiniert. Dank unserer frühzeitigen Einbindung konnten wir sowohl die Einführung des Binnenmarktinformationssystems als auch des Einheitlichen Ansprechpartners datenschutzrechtlich begleiten.

Das Binnenmarktinformationssystem der EU (Internal Market Information System – IMI) dient dem grenzüberschreitenden Datenaustausch mit zuständigen Behörden in anderen Mitgliedstaaten sowie den drei am Europäischen Wirtschaftsraum (EWR) beteiligten Staaten Norwegen, Island und Liechtenstein. Es unterstützt dadurch die von der Richtlinie vorgesehene, verstärkte europäische Verwaltungszusammenarbeit auf dem Gebiet der Dienstleistungen. Dies soll unter anderem dazu dienen, den Verwaltungsaufwand für die Unternehmen zu verringern und frühzeitig gegen unzuverlässige Unternehmen vorzugehen zu können. Das Modell wird in Brandenburg dezentral umgesetzt, d. h. alle zuständigen Stellen erhalten die Möglichkeit, das Binnenmarktinformationssystem eigenständig zu nutzen. Zur Anwendung des Binnenmarktinformationssystems ermächtigt das einschlägige Gesetz[69] die Landesregierung zum den Erlass einer Rechtsverordnung. Einen ersten Entwurf dieser Verordnung haben wir erhalten. Ihm fehlte aus unserer Sicht ein eindeutiger Hinweis auf die Zweckbindung der personenbezogenen Daten. Außerdem wiesen wir darauf hin, dass der besondere Schutzbedarf der sensitiven personenbezogenen Daten deutlich herausgestellt werden muss. Für ihre Verarbeitung bedarf es der Umsetzung angemessener technischer und organisatorischer Maßnahmen.

Der Einheitliche Ansprechpartner (EAP) soll Dienstleistungserbringern in ganz Europa als zentrale Kontaktstelle zur Verfügung stehen, um alle Verfahren koordinieren zu können. Als Unternehmensservice bietet er ihnen Informationen und vereinfacht Behördengänge. Im Land Brandenburg wurde der Einheitliche Ansprechpartner im Geschäftsbereich des Ministeriums für Wirtschaft und Europaangelegenheiten eingerichtet.[70] Es ist vorgesehen, das bereits bestehende Dienstleistungsportal der Landesverwaltung[71] durch eine Online-Plattform zu ergänzen, um die Kommunikation zwischen den Unternehmen, dem Einheitlichen Ansprechpartner und den zuständigen Behörden zu unterstützen. Das zu diesem Zweck erstellte Fachkonzept zur IT-Umsetzung des Portals für den Einheitlichen Ansprechpartner für das Land Brandenburg enthält keine ausreichenden Festlegungen zur Registrierung

---

69 § 9 des Gesetzes über den Einheitlichen Ansprechpartner für das Land Brandenburg (BbgEAPG) vom 7. Juli 2009 (GVBl. I S. 262)

70 Erlass des Ministers für Wirtschaft zur Errichtung der Einrichtung „Einheitlicher Ansprechpartner für das Land Brandenburg" (EAPBbg) vom 6. Oktober 2009 (ABl. 41/09 S. 2053)

71 siehe http://service.brandenburg.de

und Authentifizierung, um die zugriffsberechtigten Dienstleistungserbringer eindeutig identifizieren und damit die Daten jederzeit ihrem Ursprung zuordnen zu können. Unklarheit bestand auch hinsichtlich der Art und Struktur der Daten, die der Einheitliche Ansprechpartner verarbeitet sowie über die Prozesse und Verfahrensschritte, die über das Portal abgewickelt werden sollen. Für die Bestimmung des Schutzbedarfs und die daraus abzuleitenden Maßnahmen ist die Kenntnis dieser Punkte jedoch unabdingbar. So verwundert es nicht, dass auch der zugesagte Entwurf eines Sicherheitskonzepts noch immer aussteht.

Zu datenschutzrechtlichen Fragen im Zusammenhang mit der Umsetzung der Dienstleistungsrichtlinie steht eine Stellungnahme[72] des Europäischen Datenschutzbeauftragten zur Verfügung.

Die Umsetzung der Europäischen Dienstleistungsrichtlinie lässt in Brandenburg noch immer Defizite hinsichtlich des Einsatzes angemessener organisatorischer und technischer Maßnahmen zum Schutz der verarbeiteten personenbezogenen Daten erkennen.

9 Umwelt, Gesundheit und Verbraucherschutz

9.1 Novellierung des Krankenhausgesetzes

Im letzten Tätigkeitsbericht[73] haben wir über die Absicht der Landesregierung informiert, die Datenschutzvorschriften für die Krankenhäuser nunmehr unmittelbar im Gesetz selbst anstatt wie bisher in einer separaten Verordnung festzuschreiben. Was ist aus diesem Vorhaben geworden?

Nachdem uns die Landesregierung zwar von Anfang an bei der Erarbeitung des Gesetzentwurfs eingebunden hatte, ergaben sich im Laufe des parlamentarischen Gesetzgebungsverfahrens sowohl Streichungen sinnvoller Regelungen als auch neue Kritikpunkte. Das Brandenburgische Krankenhausentwicklungsgesetz ist in der Zwischenzeit in Kraft getreten.[74] Es ersetzt

72 Stellungnahme des Europäischen Datenschutzbeauftragten zur Entscheidung der Kommission vom 12. Dezember 2007 über den Schutz personenbezogener Daten bei der Umsetzung des Binnenmarktinformationssystems (IMI) (2008/49/EG) vom 22. Februar 2008 (Abl. EU Nr. C 270 S. 101)

73 vgl. Tätigkeitsbericht 2006/2007, A 8.7.2

74 Gesetz zur Entwicklung der Krankenhäuser im Land Brandenburg (Brandenburgisches Krankenhausentwicklungsgesetz – BbgKHEG) vom 08. Juli 2009 (GVBl. I S. 310)

das bisherige Krankenhausgesetz und hat unter anderem zum Ziel, die Zusammenarbeit der Krankenhäuser untereinander, mit den niedergelassenen Ärzten sowie den Einrichtungen des Gesundheits- und Sozialwesens zu fördern.

Eine wichtige Neuregelung ist eine Vorschrift für alle behandelnden Krankenhausärzte, das Jugendamt zu informieren, wenn sie Anzeichen für eine Misshandlung, Vernachlässigung oder einen sexuellen Missbrauch von Kindern bzw. Jugendlichen feststellen. Die Regelung lehnt sich an bereits bestehende Vorschriften für niedergelassene Ärzte an, lässt jedoch die gänzlich unterschiedlichen Strukturen eines Krankenhauses außer Acht. Sie verlangt, dass jeder einzelne Arzt eine solche Meldung zu übermitteln hat. Im Sinne der Datensparsamkeit hätte es genügt, eine einzige Meldung durch das jeweilige Krankenhaus vorzusehen.

Das Achte Buch Sozialgesetzbuch fordert als Voraussetzung für das Tätigwerden des Jugendamtes „gewichtige Anhaltspunkte“ für die Gefährdung des Kindeswohls. Mit der Neuregelung des Krankenhausentwicklungsgesetzes sind die Ärzte der Klinik aber bereits zur Meldung verpflichtet, wenn lediglich „Anhaltspunkte“ vorliegen. Auch dieses Missverhältnis kann zu überflüssigen Datenübermittlungen führen.

Der Datenschutz in den Krankenhäusern wird nicht mehr durch eine separate Verordnung, sondern durch das Krankenhausentwicklungsgesetz geregelt. Erst seine Anwendung in der Praxis wird zeigen, ob die Übermittlung von Daten an die Jugendämter unter Beachtung der Datensparsamkeit erfolgen wird.

9.2 Kinder- und Jugendgesundheitsdienstverordnung

Nach der Novellierung des Brandenburgischen Gesundheitsdienstgesetzes[75] wurde auch die darauf beruhende Verordnung zum Kinder- und Jugendgesundheitsdienst neu gefasst. Außerdem wurde ein ca. 200 Seiten starkes Handbuch für den Kinder- und Jugendgesundheitsdienst im Land Brandenburg den aktuellen Verhältnissen angepasst. Von einer erweiterten Datenerhebung durch die bereits vor In-Kraft-Treten der Verordnung überarbeiteten Formulare (Fragebögen) erhielten wir nur durch eine Beschwerde von Eltern Kenntnis.

75 vgl. Tätigkeitsbericht 2006/2007, A 8.7.3

9.2.1 Verordnung

Bei der Verordnung stellte sich vorrangig die Frage, ob diese insgesamt von der Ermächtigungsgrundlage gedeckt wird. Datenerhebungen in Förderschulen und bei Sechstklässlern sowie die Durchbrechung der ärztlichen Schweigepflicht bei der Teilnahme einer sozialpädagogischen Fachkraft an einer Reihenuntersuchung im Kindergarten, aber auch Regelungen zur Gesundheitsberichterstattung und zum Betreuungscontrolling hielten wir insoweit für problematisch. Das Gesundheitsministerium teilte diese Bedenken jedoch nicht und verwies auch auf die Prüfung durch das Ministerium der Justiz.

9.2.2 Fragebögen

Bei den Erhebungsbögen stand die Frage der Erforderlichkeit der abgefragten Daten im Vordergrund. Wir setzten uns dafür ein, die Frage nach der Anzahl der im Haushalt lebenden Kinder und Erwachsenen sowie die nach der Schulbildung bzw. Berufstätigkeit der Eltern zu streichen. Bei einer Ablehnung der Streichung regten wir an, diese Fragen wenigstens in den Elternfragebögen zu stellen, sodass die Betroffenen selbst entscheiden können, ob und inwieweit sie antworten wollen. Auch sollten Minderjährige nicht in die Lage geraten, bei einer Untersuchung Fragen über ihre Eltern beantworten zu müssen.

Die Fragen nach einer konkreten fremden Muttersprache und nach der Zweisprachigkeit waren bisher nicht erfolgt und sollen in Zukunft auch nur zu Kindern im Kita-Alter gestellt werden, sodass wir die Erforderlichkeit dieser Punkte problematisierten. Dasselbe gilt für die Fragen nach der Dauer der Kinderbetreuung und nach der Teilnahme(-dauer) an einem Netzwerk „Gesunde Kinder“. Unsere Einwände wurden jedoch nicht berücksichtigt.

Wir stellten auch klar, dass nach dem Brandenburgischen Schulgesetz die Eltern und Kinder die erforderlichen Angaben für die Einschulungsuntersuchung zu erteilen haben und baten, den Hinweis auf die Freiwilligkeit der Angaben aus dem Fragebogen für die Schuleingangsuntersuchung zu entfernen. Im Unterschied zu den sonstigen Untersuchungen, können Familien hierbei nämlich nicht frei entscheiden, ob ihr Kind an der Untersuchung teilnehmen soll und ob sie Angaben dafür machen möchten. Dennoch wird der entsprechende Erhebungsbogen nach wie vor einen Hinweis auf die Freiwilligkeit enthalten. Auch unser Vortrag, dass dies schon in der Vergangenheit viele Betroffene irritiert hatte, sofern sie zugleich im Anschreiben des zuständigen Gesundheitsamtes über die Vorgaben des Brandenburgischen Schulgesetzes aufgeklärt wurden, nützte nichts.

Das Brandenburgische Schulgesetz gibt zur Einschulungsuntersuchung ausdrücklich vor, dass über die Erforderlichkeit hinausgehende Fragen nicht gestellt werden dürfen. Diese Anforderung könnte durch die aktuelle Fassung der Formulare weiterhin unterlaufen werden. Auch stellten wir verwundert fest, dass bei der Schuleingangsuntersuchung z. B. nach dem Schwangerschaftsverlauf gefragt wurde, diese Erhebung bei den um Jahre jüngeren Kindergartenkindern jedoch verzichtbar erschien.

9.2.3 Handbuch

Weitere Datenverarbeitungen waren nicht einmal in der Verordnung, sondern lediglich im sog. Handbuch für den Kinder- und Jugendgesundheitsdienst geregelt. Dadurch sollen fortlaufende Änderung ermöglicht werden. Die Empfehlungen im Handbuch entsprachen in einigen Fällen aber nicht den gesetzlichen Datenverarbeitungsbefugnissen.

9.2.3.1 Untersuchungen von Dreijährigen

Nach einer neuen Bestimmung des Brandenburgischen Gesundheitsdienstgesetzes soll allen etwa dreijährigen Kindern eine Untersuchung durch die Gesundheitsämter angeboten werden. Dazu erhalten diese Behörden von den Meldeämtern personenbezogene Angaben der betroffenen Familien. Im Handbuch wurde empfohlen, Namenslisten von Kindertagesstätten und Tagespflegestellen zu erheben und die genannte Altersgruppe herauszufiltern. Die Listen der Kinder in Tagespflege sollten dabei quartalsweise über das Jugendamt erhoben werden. Zuletzt war ein Abgleich der Meldedaten mit den Daten aus den Tagesbetreuungslisten vorgesehen, um sog. Hauskinder herauszufiltern. Diese sollten als einzige Einladungsschreiben per Post von den Gesundheitsämtern erhalten, während man die anderen Kinder über ihre Tagesbetreuungseinrichtungen oder -personen erreichen wollte.

Das Ministerium für Bildung, Jugend und Sport schloss sich unserer Ansicht an, dass eine Übermittlungsbefugnis für die Jugendämter an die Gesundheitsämter insoweit nicht besteht. Das Gesundheitsministerium erklärte sich bereit, die Vorgabe aus dem Handbuch zu streichen.

Wir sahen auch im Kindertagesstättengesetz keine Übermittlungsbefugnis für Kindertagesstätten bzw. Tagespflegestellen an die Gesundheitsämter. Dort gibt es lediglich eine allgemeine Unterstützungspflicht, die dazu führt, dass Räume für Untersuchungen bereitgestellt werden, Informationen allgemeiner Art an die Eltern verteilt werden u. Ä. Selbst das allgemeine Datenschutzrecht lässt nur erforderliche Datenverarbeitungen zu. Damit sind Datenanforderungen zu anderen Kindern als solchen vom 30. bis 42. Lebensmonat, für die das Gesetz die Untersuchung vorsieht, von vornherein ausgeschlossen.

Außerdem ist nach unserer Auffassung durch die Kindertagesstätte oder Tagespflegeperson zunächst die betroffene Familie zu befragen, ob sie an der Untersuchung teilnehmen will. Nur bei vorhandenem Teilnahmewillen kann eine Übermittlung ihrer Daten überhaupt erforderlich sein.

Unsere Empfehlung lautete daher, alle betroffenen Familien mit Hilfe der Meldedaten anzuschreiben. Im Anschreiben hätte darauf hingewiesen werden können, dass Kinder, die in Brandenburg nach dem Kindertagesstättengesetz betreut werden, in der Einrichtung untersucht werden, sofern dort das Einverständnis mit der Untersuchung erklärt wird. Anderen Sorgeberechtigten sollte für den Fall, dass sie eine Untersuchung wünschen, nach unserer Vorstellung in dem Schreiben eine Kontaktmöglichkeit mit dem Gesundheitsamt aufgezeigt werden.

Das Entwicklungsscreening im Kita-Alter soll in Anwesenheit einer Vertrauensperson oder einer sozialpädagogischen Fachkraft erfolgen. Die Sorgeberechtigten müssen unseres Erachtens damit einverstanden sein, wenn andere Personen als Mitarbeiter des Gesundheitsamtes an der Untersuchung teilnehmen sollen. Andernfalls könnte es zu einer unbefugten Durchbrechung der ärztlichen Schweigepflicht kommen. Eine datenschutzgerechte Vorgehensweise setzt für die Teilnahme von Erziehern an Untersuchungen der Kindergartenkinder als erstes eine Information der Eltern über dieses Detail, aber auch über ihre Entscheidungsbefugnis – und schließlich ihr Einverständnis damit, voraus.

Erzieherinnen konnten nach dem Handbuch außerdem zu einzelnen Sprach- und Sprachverständnisleistungen des Kindes Angaben machen. Von der Einrichtung ist aber nach unserer Auffassung und der des Ministeriums für Bildung, Jugend und Sport vorab zu klären, ob solche Mitteilungen von den Sorgeberechtigten gewünscht werden.

9.2.3.2 Betreuungscontrolling

Sieht das Gesundheitsamt nach einer Untersuchung Handlungsbedarf, so informiert es die Sorgeberechtigten und bietet eine Begleitung der Behandlung an (sog. Betreuungscontrolling). Reagieren Eltern auf dieses Angebot nicht, empfahl das Handbuch als letzte Möglichkeiten einen Hausbesuch und nach dessen Scheitern einen Informationsaustausch mit dem Jugend- bzw. Sozialamt. Während bei den Nachfragen an Ärzte, Beratungsstellen u. Ä. eine Einverständniserklärung der Eltern bedacht wurde, ließ das Handbuch offen, inwieweit bei Hausbesuchen oder einem Informationsaustausch mit den Sozialbehörden der Willen der Sorgeberechtigten Berücksichtigung finden bzw. welche gesetzliche Grundlage dafür gesehen würde. Wenn Familien keine weiteren Gesundheitsdaten preisgeben wollen bzw. lieber mit

dem Arzt ihres Vertrauens als mit dem Gesundheitsamt zusammenarbeiten, ist dies zu akzeptieren. Es ist das Recht der Betroffenen, ein Angebot abzulehnen oder eine Alternative zu suchen, die sie selbst mehr überzeugt. Eine Grenze dieser elterlichen Rechte wird erst dann erreicht, wenn gewichtige Anhaltspunkte für eine Gefährdung des Kindeswohls vorliegen.

Das Ministerium für Arbeit, Soziales, Gesundheit und Familie betonte, dass eine vertrauensvolle Zusammenarbeit mit den Sorgeberechtigten wesentlich und gegen deren Willen nicht möglich sei. Es konnte nicht klären, wieso das Sozialamt ggf. beim Betreuungscontrolling einzuschalten wäre, und sagte zu, diesen Punkt im Handbuch zu streichen. Das Jugendamt soll auch nach Auffassung des Gesundheitsministeriums nur dann informiert werden, wenn gewichtige Anzeichen für eine Kindeswohlgefährdung vorliegen.

9.2.3.3 Vorgehen nach der Meldung einer Nichtteilnahme an Früherkennungsuntersuchungen

Nach dem Brandenburgischen Gesundheitsdienstgesetz (BbgGDG) sollen die Gesundheitsämter, denen von der Zentralen Stelle für das Einladungs- und Rückmeldewesen[76] eine (vermutliche) Nichtteilnahme an einer Untersuchung gemeldet wird, geeignete und angemessene Maßnahmen ergreifen.

Das Handbuch empfahl den Gesundheitsämtern insoweit zunächst eine schriftliche Kontaktaufnahme zu den Sorgeberechtigten mit der Bitte um Nachweis der Untersuchung durch ein beigefügtes Rückmeldeformular. Zugleich sollte eine Kontaktaufnahme angeboten und ein Hausbesuch für den Fall, dass keine Rückmeldung erfolgen sollte, angekündigt werden. Selbst einzelne Gesundheitsämter standen aber bereits einem aufsuchenden Kontakt nach erfolglosem Anschreiben kritisch gegenüber, da sie sich zum einen der Freiwilligkeit der Früherkennungsuntersuchungen und des Grundrechts auf Unverletzlichkeit der Wohnung bewusst waren, zum anderen aber wohl auch den Aufwand eines – ggf. auch noch erfolglosen – Hausbesuches für die eigene Behörde bedachten. Als letzte Maßnahme riet das Handbuch zu einer Zusammenarbeit mit dem Jugendamt.

Bereits im letzten Tätigkeitsbericht[77] haben wir darauf hingewiesen, dass angesichts der fehlenden Teilnahmepflicht an den Untersuchungen allenfalls eine Beratung oder das Angebot einer Untersuchung durch das Gesundheitsamt geeignete und angemessene Maßnahmen wären.

Bei einer ablehnenden Haltung der Erziehungsberechtigten bzw. einer fehlenden Rückmeldung durch diese kann zunächst einmal nur davon ausge-

[76] vgl. A 9.3

[77] vgl. Tätigkeitsbericht 2006/2007, A 8.8

gangen werden, dass sie die insgesamt freiwilligen Angebote nicht wahrnehmen wollen. Das Gesundheitsamt nimmt daher seine Aufgaben im Regelfall durch schriftliche oder telefonische Versuche einer Kontaktaufnahme mit den Eltern hinreichend wahr. Es gehört nicht zu den Aufgaben des Gesundheitsamtes, ergänzend dem Jugendamt Angebote zu ermöglichen. In § 7 BbgGDG ist eine generelle Übermittlungsmöglichkeit einer (vermutlichen) Nichtteilnahme an einer Früherkennungsuntersuchung an das Jugendamt nicht geschaffen worden. Möglich bleibt selbstverständlich eine Übermittlung im Einzelfall zur Abwehr einer gegenwärtigen nicht unerheblichen Gefahr gemäß § 16 BbgGDG. Dafür müssen jedoch mehr Anhaltspunkte vorliegen als das Ablehnen einer freiwilligen Leistung. Das Gesundheitsministerium hat betont, dass nur in sehr seltenen Fällen ein Einbeziehen des Jugendamtes durch das Gesundheitsamt wegen der Früherkennungsuntersuchungen erfolge.

Durch unsere Stellungnahmen konnten wir überflüssige Datenverarbeitungen verhindern und eine weitere Sensibilisierung des öffentlichen Gesundheitsdienstes für den Datenschutz erreichen.

9.3 Kontrolle der Zentralen Stelle Einladungs- und Rückmeldewesen

Durch das novellierte Brandenburgische Gesundheitsdienstgesetz[78] wurde ein Einladungs- und Rückmeldewesen für die Teilnahme von Kindern und Jugendlichen an Früherkennungsuntersuchungen eingeführt. Das Landesamt für Soziales und Versorgung ist in seiner Funktion als Landesgesundheitsamt für die Koordination des Verfahrens zuständig. Wir haben es im Berichtszeitraum kontrolliert.

Die Tätigkeit des Landesgesundheitsamts als gesetzlich vorgesehene Zentrale Stelle umfasst beispielsweise die Einladung der Kinder und Jugendlichen und den Abgleich ihrer Daten aus dem Melderegister mit denen aus den Rückmeldungen der untersuchenden Ärzte. Darüber hinaus meldet das Landesamt Kinder und Jugendliche, von denen nicht bekannt ist, ob sie an der Untersuchung teilgenommen haben, an das örtliche Gesundheitsamt der kreisfreien Stadt oder des Landkreises.

Die Rückmeldungen der Ärzte erfolgen derzeit per Telefax. Dem Landesgesundheitsamt ist bewusst, dass dies keine datenschutzgerechte Lösung ist. Eine verschlüsselte Versendung der Patientendaten scheitert aber an der Ausstattung der Arztpraxen. Wir haben daher vereinbart, nach der flächende-

[78] Gesetz über den Öffentlichen Gesundheitsdienst im Land Brandenburg (Brandenburgisches Gesundheitsdienstgesetz – BbgGDG) vom 23. April 2008 (GVBl. I S. 95)

ckenden Einführung der elektronischen Gesundheitskarte zu prüfen, ob die in den Arztpraxen dann vorhandene Infrastruktur für eine datenschutzfreundlichere Übertragung genutzt werden kann.

Die Rückmeldungen der Ärzte werden vom Brandenburgischen IT-Dienstleister über einen Faxserver entgegengenommen. Wir prüften daher, ob das Brandenburgische Gesundheitsdienstgesetz in Verbindung mit dem Brandenburgischen Datenschutzgesetz eine solche Datenverarbeitung im Auftrag von Gesundheitsdaten zulässt. Im Ergebnis forderten wir, dass entweder eine Kenntnisnahme der Daten durch den Auftragnehmer mittels technisch-organisatorischer Maßnahmen ausgeschlossen oder der Auftragnehmer ein Schweigepflichtiger nach § 203 Strafgesetzbuch sein muss.

Das Gesetz legt die Zeitpunkte, zu denen Einladungen an die Betroffenen, diesbezügliche Erinnerungsschreiben und Meldungen an die Gesundheitsämter wegen fehlender Rückmeldung über eine Untersuchungsteilnahme erfolgen sollen, nicht fest. Die Terminierung blieb daher dem Landesgesundheitsamt überlassen. Dieses plante zunächst, den Gesundheitsämtern schon mit Ablauf des Untersuchungszeitraumes eine „Nichtteilnahme“ zu melden. Unser Bestreben war es, diese Meldung so spät wie möglich anzusetzen, da die Krankenkassen auch eine spätere Untersuchung tolerieren. Es sollte aber möglichst vermieden werden, dass Familien, die eine Untersuchung erst spät vornehmen lassen, dem zuständigen Gesundheitsamt bereits als „Nichtteilnehmer“ gemeldet werden. Das Ziel im Auge, dass die zuständigen Gesundheitsämter noch auf eine Teilnahme an einer Untersuchung im Toleranzzeitraum hinwirken können, ging das Landesgesundheitsamt noch vor der ersten Meldung einer „Nichtteilnahme“ auch auf unser Anliegen ein: Die Information an die Gesundheitsämter erfolgte von Anfang an immerhin erst einen Monat nach Ende der Untersuchungsfrist.

Findet die Untersuchung in einem anderen Bundesland statt, ist der Arzt nicht zur Rückmeldung an die Zentrale Stelle verpflichtet. Aber auch brandenburgische Ärzte nehmen die Rückmeldungen noch nicht durchgängig vor. In beiden Fällen müssen die Betroffenen damit rechnen, trotz ihrer tatsächlich stattgefundenen Teilnahme an der Untersuchung von der Zentralen Stelle als „Nichtteilnehmer“ an das örtliche Gesundheitsamt gemeldet zu werden. Die Betroffenen sind also letztlich dazu gezwungen, selbst die Initiative zu ergreifen, um trotz korrekten Verhaltens einer Meldung als „Problemfall“ zu entgehen. Daran zeigt sich, dass die von uns im letzten Tätigkeitsbericht[79] kritisierten Verfahren weiterhin Mängel aufweisen.

[79] vgl. Tätigkeitsbericht 2006/2007, A 8.8

Die Betriebsdokumentation für die Software zur Unterstützung des Einladungs- und Rückmeldewesens, die uns aufgrund unserer ersten Anfrage von der Zentralen Stelle überlassenen wurde, ging an verschiedenen Stellen von Rückmeldungen der Gesundheitsämter an das Landesgesundheitsamt aus. Eine rechtliche Grundlage für diese Datenverarbeitung gab es im Brandenburgischen Gesundheitsdienstgesetz jedoch nicht. Das Landesgesundheitsamt stellte klar, dass dies allein Überlegungen der Firma, die das Programm erstellte, gewesen seien, die aber von der Zentralen Stelle abgelehnt wurden. Wir baten insoweit um eine Bereinigung der Texte.

Schließlich haben wir beim Landesgesundheitsamt darauf hingewirkt, dass für die Zentrale Stelle ein Sicherheitskonzept erarbeitet wird. Eine Meinungsverschiedenheit über die dabei zugrunde zu legende Schutzstufe konnte mit Hilfe des Ministeriums für Arbeit, Soziales, Gesundheit und Familie entschieden werden: Da die verarbeiteten Daten der ärztlichen Schweigepflicht unterliegen, besteht ein hoher Schutzbedarf.

Wir sind zuversichtlich, dass unsere Empfehlungen für ein datenschutzgerechtes Einladungs- und Rückmeldewesen von der Zentralen Stelle berücksichtigt werden.

9.4 Babybegrüßungsdienste

Angesichts verschiedener Fälle von Vernachlässigungen, Misshandlungen oder Tötungen von Babys und Kleinkindern suchen auch die kreisfreien Städte und Landkreise in Brandenburg nach Wegen, um so früh wie möglich mit Eltern in Kontakt zu treten und auf das Wohlergehen der Kinder hinzuwirken. Ein Ergebnis sind Babybegrüßungsdienste. Die jungen Familien erhalten angemeldeten Besuch einer Behörde, Informationsmaterial und eventuell sogar ein Geschenk. Auf diese Weise erhält der Babybegrüßungsdienst einen gewissen Eindruck von der Familiensituation.

Der Babybegrüßungsdienst kann von unterschiedlichen Ämtern wahrgenommen werden. In einem konkreten Fall haben wir empfohlen, ihn beim Kinder- und Jugendgesundheitsdienst des Gesundheitsamtes anzubinden, da dieser auf der Grundlage der Meldedatenübermittlungsverordnung von den Meldebehörden regelmäßig über Geburtsfälle informiert wird.

Andere Stellen ordneten den Babybegrüßungsdienst dem Jugendamt zu, dem auf der Grundlage einer internen Dienstanweisung die erforderlichen Daten überlassen wurden. Interne Dienstanweisungen können jedoch fehlende gesetzliche Grundlagen für die Weitergabe von Daten nicht ersetzen. Wir wiesen deshalb darauf hin, dass die Meldebehörden oder Gesundheitsämter

den Jugendämtern nur mit Einwilligung der Betroffenen eine Mitteilung über einen Geburtsfall machen dürfen. Um die Entscheidung der Eltern, ob sie einen Besuch wünschen, in Erfahrung zu bringen, empfahlen wir ein Adressmittlungsverfahren. Dabei wendet sich zunächst die Meldebehörde an die Familie, um ihr das Angebot des Jugendamtes zu unterbreiten.

In den Anschreiben sind die Familien darüber zu informieren, dass sie frei entscheiden können, ob sie einen Besuch durch den Babybegrüßungsdienst wollen oder nicht. Außerdem sind ihnen für diese Entscheidung alle mit dem Besuch verbundenen Zwecke vorab mitzuteilen.

Ein Babybegrüßungsdienst sah vor, in einem Fragebogen Namen und Anschrift der Familienmitglieder sowie Angaben zur Hebamme und zum Kinderarzt zu erfassen, um die Zufriedenheit mit der Infrastruktur für Kinder vor Ort und eventuellen Verbesserungsbedarf zu ermitteln. Datenschutzrechtlich problematisch war die personenbezogene Ausgestaltung des Fragebogens. Auf unseren Hinweis hin werden nur noch Angaben ohne Personenbezug dazu erbeten, ob den Betroffenen das Vorhandensein eines Kinderarztes wichtig ist und wie sie das Kinderarztangebot in ihrem Stadtteil verwirklicht sehen.

Ein anderer Babybegrüßungsdienst sah umfangreiche Protokollierungen des Hausbesuches vor. Unter anderem sollten Grundversorgung und Schutz des Kindes sowie die familiäre Situation bewertet werden. Die Familien wurden im Ergebnis in solche ohne ersichtlichen Hilfebedarf, solche mit Hilfebedarf im Alltag und solche mit erheblichem Unterstützungsbedarf kategorisiert. Da der Dienst die Angaben für den Hausbesuch ohne Einwilligung der Betroffenen erhielt, bei der Ankündigung seines Besuches stillschweigend das Einverständnis der Eltern voraussetzte und die mit dem Besuch verfolgten Zwecke nicht preisgab, war eine Erfassung und Bewertung nahezu aller Familien mit Neugeborenen beim Jugendamt möglich. Dies war nicht zulässig.

Ein Landkreis beabsichtigte, zusätzlich zu diesem Babybegrüßungsdienst ein umfangreiches Netzwerk einzurichten. Kooperierende Personen oder Stellen sollten anhand vager oder gar unzulässiger Kriterien „Problemfälle“ an das Jugendamt melden. Vielfach war auch eine Rückmeldung des Jugendamtes an die kooperierende Stelle vorgesehen. Beide Vorgehensweisen sind datenschutzrechtlich nicht vertretbar. Dies hat uns veranlasst, alle Landkreise und kreisfreien Städte mit einem Rundschreiben über datenschutzrechtliche Schranken und datenschutzgerechte Lösungswege bei Babybegrüßungsdiensten und kommunalen Netzwerken zu informieren.

Dauerhafte Verbesserungen von unbefriedigenden familiären Situationen sind unterhalb der Schwelle von Zwangsmaßnahmen nur zu erzielen, wenn zwischen Behördenmitarbeitern und Familien ein Vertrauensverhältnis besteht. Die Beachtung datenschutzrechtlicher Schranken durch den Babybegrüßungsdienst stellt die erste vertrauensbildende Maßnahme gegenüber den Betroffenen dar.

9.5 Weitergabe von Daten Krankenversicherter an Lieferanten

Versicherte, die Inkontinenzartikel benötigen, wurden von ihrer Krankenkasse schriftlich darauf hingewiesen, dass ab dem Jahre 2009 eine Versorgung mit entsprechenden Hilfsmitteln nur noch über einen bestimmten Anbieter möglich sei. Zugleich wurde angekündigt, dass die Krankenkasse diesem Lieferanten Namen und Anschrift sowie Telefonnummer des Betroffenen mitteilen würde, sofern dieser nicht bis zu einem bestimmten Zeitpunkt mittels eines beigefügten Formulars dieser Verfahrensweise widerspräche.

Das Gesetz fordert in § 127 Abs. 5 Fünftes Buch Sozialgesetzbuch lediglich, dass die Krankenkassen ihre Versicherten über die zur Versorgung berechtigten Vertragspartner informieren. Eine Übermittlung von Versichertendaten von der gesetzlichen Krankenversicherung an den Hilfsmittellieferanten ist im Gesetz nicht vorgesehen. Sie ist angesichts der Information an die Versicherten auch nicht erforderlich. Es ist deshalb schon fraglich, ob eine Einwilligung der Betroffenen in diesen Fällen möglich gewesen wäre. Eine Widerspruchslösung war aber ganz sicher nicht der richtige Weg. Die Krankenkasse sah dies prompt ein. Sie forderte die bis dahin an die potenziellen Lieferanten übergebenen Datenträger mit Versichertenangaben zurück und führte sie einer datenschutzgerechten Vernichtung zu. Wir baten darum, nach Beendigung dieser Aktion auch die Widerspruchsschreiben zu löschen.

Inzwischen lässt die Krankenkasse neue Leistungsfälle direkt durch den verordnenden Arzt oder das Krankenhaus an die ausschließlich lieferberechtigten Leistungserbringer verweisen.

Widerspruchslösungen bedürfen einer gesetzlichen Grundlage, denn sie wahren die Rechte der Betroffenen deutlich schlechter als ein Einwilligungserfordernis.

10 Finanzen

10.1 Neues Finanzmanagement in der Landesverwaltung

10.1.1 Datenschutzrechtliche Anforderungen bei der Einführung des gemeinsamen Verfahrens

In unserem letzten Tätigkeitsbericht[80] hatten wir über den Beschluss der Landesregierung berichtet, das Neue Finanzmanagement (NFM) in der gesamten Landesverwaltung einzuführen. Teil des Projekts war die Modernisierung des Haushalts-, Kassen- und Rechnungswesens (HKR) und dessen Umstellung auf ein SAP R/3-System. Im Berichtszeitraum wurden die Projektarbeiten planmäßig weitergeführt.

Die Einführung des Neuen Finanzmanagements in der Landesverwaltung gliedert sich in ein zentrales Projekt unter Federführung des Ministeriums der Finanzen und dezentrale Vorhaben in den einzelnen Ressorts bzw. ihren nachgeordneten Bereichen. Damit der Datenschutz im Gesamtsystem ressortübergreifend gewährleistet wird, müssen alle beteiligten Stellen ihre jeweilige datenschutzrechtliche Verantwortung erkennen und ausfüllen.

Das NFM-Projekt und seine technische Realisierung unterscheiden sich dabei grundlegend von anderen komplexen, ressortübergreifenden IT-Projekten, die aktuell in der Landesverwaltung bearbeitet und durch unsere Behörde begleitet werden. Im Gegensatz zu den Projekten EL.DOK BB[81] und PERIS,[82] bei denen die einzelnen Daten verarbeitenden Stellen und ihre Verantwortung klar abgegrenzt werden können, haben wir es bei NFM mit einem gemeinsamen DV-Verfahren zu tun. Dieses zeichnet sich dadurch aus, dass mehrere Daten verarbeitende Stellen über einem gemeinsamen Datenbestand operieren (müssen) – hier u. a. zur Bewirtschaftung des Finanzhaushalts.

Leider gibt es bislang keine klaren Regelungen im Brandenburgischen Datenschutzgesetz, die sich mit solchen gemeinsamen Verfahren befassen. Da diese Lücke uns zuletzt mehrfach beschäftigte (z. B. bei gemeinsamen Bund-Länder-Verfahren, gemeinsamen Verfahren mehrerer Stellen der Landesverwaltung oder mehrerer Kommunen), haben wir gegenüber dem Ministerium des Innern angeregt, bei der nächsten Novellierung des Gesetzes eine entsprechende Ergänzung in den parlamentarischen Prozess einzubringen. Dabei ist insbesondere zu regeln, dass vor Einführung und Betrieb eines

---

80 vgl. Tätigkeitsbericht 2006/2007, A 9.3

81 vgl. A 4.5.5

82 vgl. A 4.6.3

konkreten gemeinsamen Verfahrens die Zuständigkeiten und Verantwortlichkeiten für die Erfüllung einzelner datenschutzrechtlicher Anforderungen (Freigabe, Sicherheitskonzept, Verfahrensverzeichnis usw.) zu bestimmen und klar abzugrenzen sind. Ein „Verdunsten“ der Verantwortung oder Lücken bei der Umsetzung der Anforderungen darf es nicht geben.

Im Vorgriff auf eine solche gesetzliche Regelung haben wir für das NFM-Projekt mit allen Verantwortlichen Folgendes vereinbart:

- Federführend bei der Planung, Einrichtung, Durchführung und Weiterentwicklung des Verfahrens ist das Ministerium der Finanzen. Dies ergibt sich auch aus der Geschäftsverteilung in der Landesregierung. In diesem Kontext kann das Ministerium auch Verträge über eine Datenverarbeitung im Auftrag mit externen Dienstleistern für die gesamte Landesverwaltung abschließen.

- Das Ministerium der Finanzen übernimmt die Verantwortung für die Erstellung eines Sicherheitskonzepts für das NFM-Verfahren. Dieses besteht aus einem „zentralen Teil“ für die gemeinsam von allen Daten verarbeitenden Stellen genutzten Verfahrenskomponenten und einem „dezentralen Teil“. Letzterer wird in Form eines Mustersicherheitskonzepts bzw. von Sicherheitsrichtlinien für die Clientseite ausgeführt.

- Bezüglich der gemeinsam genutzten Komponenten des NFM-Verfahrens erstellt das Ministerium der Finanzen das Verfahrensverzeichnis und erteilt die Freigabe. Dabei ist auch die Umsetzung der Sicherheitsmaßnahmen für die gemeinsam genutzten Verfahrenskomponenten zu prüfen.

- Die das NFM-Verfahren einführenden Stellen sind für die Umsetzung der datenschutzrechtlichen Anforderungen jeweils in ihrem eigenen Zuständigkeitsbereich verantwortlich. Insbesondere sind die Sicherheitsrichtlinien für die Clientseite entsprechend der lokalen Besonderheiten anzupassen, zu spezialisieren und umzusetzen. Dies betrifft auch die lokale Ausprägung des zentral erarbeiteten Rechte- und Rollenkonzepts zur Regelung des Zugriffs auf die Verfahrensdaten.

- Weiterhin erteilen die das NFM-Verfahren einführenden Stellen die Freigabe und erstellen das Verfahrensverzeichnis jeweils eingeschränkt für ihren Verantwortungsbereich. Bezüglich der gemeinsamen Verfahrenskomponenten können sie auf die vom Ministerium der Finanzen erarbeiteten Dokumente (Sicherheitskonzept, Freigabe, Verfahrensverzeichnis) verweisen.

Wir haben im Berichtszeitraum auf der Basis dieser Absprachen ein Ressort bzgl. der Umsetzung der Anforderungen an die „dezentralen Stellen“ geprüft.

Zunächst war zwar noch Überzeugungsarbeit zu leisten, damit das Ressort die datenschutzrechtliche Zuständigkeit für den eigenen, lokalen Verantwortungsbereich anerkennt. Letztlich konnte aber Einvernehmen über die Notwendigkeit erzielt werden, die verfahrensspezifischen Dokumente inklusive der Freigabeerklärung eingeschränkt auf den Verantwortungsbereich vor Ort vorzuhalten und zu pflegen. Nach Prüfung der Konzepte und weiteren klärenden Gesprächen konnte im Ergebnis festgestellt werden, dass die datenschutzrechtlichen Anforderungen in der geprüften dezentralen Stelle eingehalten werden.

Auch bei der Einführung gemeinsamer Verfahren sind alle datenschutzrechtlichen Anforderungen zu erfüllen. Durch eine Ergänzung des Brandenburgischen Datenschutzgesetzes sollte Rechtssicherheit dahin gehend geschaffen werden, dass bei solchen Verfahren rechtzeitig und umfassend Vereinbarungen zur Aufteilung der Verantwortlichkeiten zwischen allen beteiligten Daten verarbeitenden Stellen getroffen werden können.

10.1.2 Erarbeitung und Umsetzung des Sicherheitskonzepts

Bereits in unserem letzten Tätigkeitsbericht[83] hatten wir darauf hingewiesen, dass bei der Modernisierung des Verfahrens zum Haushalts-, Kassen- und Rechnungswesens (HKR) im Rahmen der Einführung des Neuen Finanzmanagements (NFM) in der Landesverwaltung das entsprechende IT-Sicherheitskonzept fortzuschreiben ist. Dabei muss insbesondere der hohe Schutzbedarf der verarbeiteten Daten berücksichtigt werden.

Das Brandenburgische Datenschutzgesetz verlangt, dass die wesentliche Änderung von automatisierten Verfahren, mit denen personenbezogene Daten verarbeitet werden und für die ein Verfahrensverzeichnis zu erstellen ist, der Freigabe bedarf. Zuvor ist im Rahmen eines aus einer Risikoanalyse entwickelten Sicherheitskonzepts nachzuweisen, dass die von dem Verfahren ausgehenden Gefahren für die Rechte und Freiheiten der Betroffenen durch technische und organisatorische Maßnahmen beherrscht werden können.

Die Modernisierung des HKR-Verfahrens für die Landesverwaltung ist eine solche wesentliche Änderung, da u. a. die verwendete Basissoftware Pro-Fiskal durch SAP R/3 ersetzt werden sollte und somit die IT-Sicherheitsmaßnahmen neu abzuleiten und umzusetzen waren. Bei der Erarbeitung und Realisierung des Sicherheitskonzepts ging es jedoch zunächst nur schleppend voran. Zwar wurde ein hoher Schutzbedarf bei der Integrität und z. T. auch bei der Vertraulichkeit der Daten festgestellt und eine

83 vgl. Tätigkeitsbericht 2006/2007, A 9.3

Reihe von Sicherheitsmaßnahmen wie eine Ende-zu-Ende-Verschlüsselung, der Einsatz von Chipkarten und die Anwendung digitaler Signaturen empfohlen. Aussagen über den Umsetzungsgrad dieser Maßnahmen wurden jedoch nicht getroffen. Auch zu den ansonsten notwendigen Basissicherheitsmaßnahmen lagen kaum Angaben über die Umsetzung vor. Obwohl ein Sicherheitskonzept ohne Beschreibung des Umsetzungsstatus unvollständig ist, erteilte das Ministerium der Finanzen die Freigabe des HKR-Verfahrens.

Auf unsere Nachfrage hin erklärten die Projektverantwortlichen, dass die Ende-zu-Ende-Verschlüsselung mittels SNC (Secure Network Communication) bereits beschlossen sei und demnächst umgesetzt werde. Die Vorlage eines vollständigen Sicherheitskonzepts wurde bis zum Ende des NFM-Projekts in Aussicht gestellt. Dies war für uns allerdings nicht hinnehmbar, da der Produktivbetrieb mit dem SAP-System für einzelne Verwaltungen bereits zum 1. August 2008 gestartet war. Nach Intervention unserer Behörde hat der Landtag das federführende Ministerium der Finanzen per Beschluss[84] zur Vorlage des NFM-Sicherheitskonzepts innerhalb von sechs Monaten aufgefordert.

Im Ergebnis dieses Beschlusses wurde die Erstellung des Sicherheitskonzeptes mit größerem Nachdruck betrieben. Schrittweise verbesserte sich dessen Qualität. Der Umsetzungsstatus von Sicherheitsmaßnahmen wurde schließlich ebenfalls dokumentiert. Dabei wurde deutlich, dass einige Maßnahmen – insbesondere beim externen Dienstleister – nicht oder nur unzureichend realisiert waren.

Positiv zu bemerken ist, dass die Ende-zu-Ende-Verschlüsselung mittels SNC nach Vorliegen der entsprechenden Entscheidung zügig eingeführt wurde. Das Ministerium der Finanzen hatte diese Aufgabe zusätzlich zur Umstellung auf das SAP-System zu organisieren und trotz des damit verbundenen erheblichen Aufwands erfreulich schnell sowohl für die bereits an SAP angebundenen als auch für die noch anzuschließenden Stellen umgesetzt. Auch die engagierte Mitarbeit der Administratoren in den Ressorts und nachgeordneten Stellen ist hier positiv zu erwähnen. Dennoch bleibt die Kritik, dass die notwendige Ende-zu-Ende-Verschlüsselung nicht von Anfang an in die Planung zur Einführung des HKR-Verfahrens eingeflossen ist und erst nach seiner Produktivsetzung aufgrund unserer beharrlichen Forderungen beschlossen wurde.

Ein weiterer Kritikpunkt bezieht sich auf die unverschlüsselte Speicherung der Daten in der Datenbank. Problematisch ist dabei insbesondere, dass das Verfahren grundsätzlich gar keine Möglichkeit zur verschlüsselten Speiche-

[84] vgl. Landtag Brandenburg, Drucksache 4/6891-B

rung anbietet, sodass hier nur über Weiterentwicklungen oder den Umstieg auf eine andere Software Abhilfe geschaffen werden könnte. Von Seiten des Ministeriums der Finanzen sieht man allerdings keinen Handlungsbedarf. Wenn man bedenkt, dass alle verfahrensspezifischen Daten des Landes somit unverschlüsselt bei einem externen IT-Dienstleister liegen, ist diese Haltung bestenfalls sorglos zu nennen.

Weiterhin offen sind außerdem folgende Sicherheitsmaßnahmen:

- revisionssichere Protokollierung von Nutzeraktivitäten,
- Konzepte zur Löschung von Daten im Verfahren und deren Umsetzung,
- Nutzung digitaler Signaturen zur Sicherung der Integrität und Authentizität von Datensätzen,
- Verwendung von Chipkarten zur sicheren Verwaltung und Nutzung privater Schlüssel bei Authentifizierungs- und Signaturprozessen.

Mittlerweile nutzen alle Behörden der Landesverwaltung das modernisierte HKR-Verfahren auf der Basis von SAP R/3. Wir werden auch zukünftig das Neue Finanzmanagement beratend begleiten und dabei auf die Bearbeitung der noch offenen Punkte drängen.

Bei der Modernisierung des HKR-Verfahrens für die Landesverwaltung konnte nur schrittweise eine Verbesserung der IT-Sicherheit und des Datenschutzes erreicht werden. Noch immer bestehen Lücken bei der vollständigen Umsetzung des IT-Sicherheitskonzepts.

10.1.3 Kontrolle der SAP-Leitstelle im Ministerium der Finanzen

Im Rahmen der datenschutzrechtlichen Begleitung der Einführung des Neuen Finanzmanagements (NFM) haben wir eine Kontrolle in der SAP-Leitstelle durchgeführt. Schwerpunktmäßig wurden dabei die Passworteinstellungen für SAP-Nutzer, die Systemeinstellungen der mit umfassenden Rechten ausgestatteten SAP-Standardprofile und SAP-Standardnutzerkonten sowie die Benutzer- und Berechtigungsverwaltung in der Leitstelle überprüft.

Nach unseren Feststellungen ist die Benutzer- und Berechtigungsverwaltung des SAP-Systems im Ministerium der Finanzen gut organisiert. Zur Einrichtung, Änderung und Sperrung von Benutzern wird ein dreistufiges Verfahren verwendet, um eine kritische Häufung von Rechten auf administrativer Ebene zu verhindern. Das sog. Customer Competence Center (CCC) im Ministerium

der Finanzen wurde für die abgestufte Berechtigungsverwaltung von SAP zertifiziert.

Die allgemein bekannten Initialpasswörter der SAP-Standardnutzer wurden bei der Systeminstallation geändert, die aktuell gültigen Passwörter sind sicher verwahrt. Profile mit umfassenden SAP-Rechten sind restriktiv vergeben und gelten nicht für Mandanten mit Fachdaten. SAP-Standardprofile werden von den Administratoren nur nach dem Vier-Augen-Prinzip eingesetzt und Aktivitäten systemtechnisch protokolliert. Allerdings erfolgt die Protokollierung nicht automatisch – sie muss manuell eingeschaltet werden. Wir haben angeregt, an dieser Stelle das Logging zu automatisieren, um dem Problem, dass die Protokollierung vergessen wird, vorzubeugen. Eine Fernwartung des SAP-Systems durch Mitarbeiter des externen Dienstleisters erfolgt nur nach expliziter Zustimmung und unter kontinuierlicher Beobachtung der Administratoren der SAP-Leitstelle.

Bei der Überprüfung der Passworteinstellungen für SAP-Nutzer in den Ressorts wurde klar, dass die Anforderungen an sichere Passwörter nach Standard des Bundesamtes für Sicherheit in der Informationstechnik hinsichtlich Mindestlänge, Mindestkomplexität und maximaler Gültigkeit noch nicht erfüllt sind. Die SAP-Leitstelle sieht sich hier in dem Dilemma, dass erhöhte Passwortanforderungen voraussichtlich einen sprunghaften Anstieg der Supportanfragen aufgrund vergessener Passwörter und damit eine stark steigende Arbeitsbelastung der Mitarbeiter erzeugen würden. Tatsächlich müsste eine neue Passwortstrategie gut vorbereitet und die SAP-Nutzer im Umgang mit sicheren und trotzdem merkbaren Passwörtern geschult werden. Ansonsten könnten erhöhte Anforderungen am Ende gar zu einer Verschlechterung des Sicherheitsniveaus aufgrund notierter Passwörter führen. Wir haben uns mit der SAP-Leitstelle darauf verständigt, eine Änderung der zentralen Passwortrichtlinien mit der Einführung einer Single-Sign-On-Lösung zusammenzulegen, um die antizipierten Probleme im Benutzersupport zu minimieren.

Die SAP-Leitstelle führt ihre Aufgaben kompetent aus. Sicherheitssensible Administrationstätigkeiten unterliegen einer geteilten Verantwortung bzw. dem Vier-Augen-Prinzip. Die Passwortrichtlinien sind noch verbesserungswürdig.

11 Landtag

Auskünfte und Akteneinsicht für Mitglieder des Landtags

Wendet sich ein Mitglied des Landtags mit dem Wunsch, Auskünfte zu erhalten oder Akten einzusehen an die Landesverwaltung, stellt sich die Frage, wie weit sein Informationsrecht reicht.

Neben seiner Aufgabe als Gesetzgeber hat der Landtag Brandenburg vor dem Hintergrund der Gewaltenteilung ein Kontrollrecht gegenüber der Landesverwaltung. Um dieses auszuüben, gibt Art. 56 Abs. 3 Verfassung des Landes Brandenburg seinen Mitgliedern ein umfangreiches Informationsrecht: Den Abgeordneten ist der Zugang zu Behörden und Dienststellen des Landes zu gewähren; ihnen ist eine umfassende Auskunft aus Dateien oder sonstigen Unterlagen zu erteilen. Diese sind ihnen auf Verlangen vollständig und unverzüglich vorzulegen. Dabei spielt es keine Rolle, welcher Fraktion die Abgeordneten angehören. Das Informationsrecht steht jedem gewählten Mitglied des Landesparlaments zu.

Im parlamentarischen Alltag sind Auskunfts- oder Einsichtsbegehren von Abgeordneten der Opposition politisch zumeist die brisanteren. Sie werden häufig mit dem Ziel gestellt, Informationen zu gewinnen, mit deren Hilfe sich eine mangelnde Aufgabenerfüllung der Regierung darlegen lässt. Um dem Spannungsverhältnis zwischen Regierung und Opposition an dieser Stelle Rechnung zu tragen, sollen diese Informationsbegehren nicht ohne Kenntnis der Regierung gestellt werden können. Mitglieder des Landtags dürfen daher nicht von sich aus an die Behörden und Dienststellen des Landes bzw. deren Beschäftigte herantreten und die Vorlage von Akten einfordern. Vielmehr müssen sie sich an die Landesregierung wenden, die in diesem Verfahren eine Vermittlerfunktion einnimmt. Sie ist grundsätzlich verpflichtet, den Abgeordneten alle Informationen umfassend vorzulegen.

Eine Ausnahme liegt nach Art. 56 Abs. 4 Verfassung des Landes Brandenburg nur vor, wenn „überwiegende öffentliche oder private Interessen an der Geheimhaltung dies zwingend erfordern“. Diese Einschränkung ist sehr eng auszulegen; auch vertrauliche Unterlagen sind vom Informationsanspruch der Mitglieder des Landtags umfasst. Um die Geheimhaltungsinteressen zu wahren, können die Abgeordneten zur besonderen Vertraulichkeit verpflichtet werden und dürfen bestimmte Sachverhalte nicht in öffentlicher Sitzung preisgeben.

Nur in wenigen Ausnahmefällen besteht der Informationsanspruch nicht, beispielsweise im Hinblick auf Angelegenheiten des Verfassungsschutzes.

Dieser wird ausschließlich durch einen kleinen, vom Landtag gewählten Kreis von Abgeordneten kontrolliert – der Parlamentarischen Kontrollkommission. Einem Abgeordneten, der nicht in diesem Gremium vertreten ist, kann eine entsprechende Information vorenthalten werden.

Neben dieser im öffentlichen Interesse liegenden Beschränkung kann die Verwaltung die Auskunft oder Akteneinsicht im Einzelfall auch dann verweigern, wenn besonders schützenswerte Interessen von Privatpersonen betroffen sind. Davon sind jedoch nicht sämtliche personenbezogene Daten umfasst, sondern lediglich höchst sensitive Informationen, beispielsweise aus der persönlichen Intimsphäre eines Betroffenen. Selbst personenbezogene Daten, die besonderen Verschwiegenheitspflichten wie dem Sozialgeheimnis unterliegen, sind Mitgliedern des Landtags offenzulegen, soweit sie die Tätigkeit der Landesverwaltung berühren. Die Verfassung trifft eine klare Entscheidung zugunsten einer funktionierenden parlamentarischen Kontrolle. Bürgerinnen und Bürger müssen es in der Regel hinnehmen, dass Angaben über sie an Abgeordnete weitergegeben werden.

Wendet sich ein Bürger mit der Bitte um Unterstützung gegenüber der Verwaltung an ein Mitglied des Landtags, kann es für den Abgeordneten erforderlich sein, Informationen zum Sachverhalt auf dem beschriebenen Wege zu beschaffen. Hierzu bedarf es zwar keiner formalen Vollmacht durch den Betroffenen. Allerdings ist es aus Gründen der Transparenz geboten, Daten zu seiner Person nicht ohne sein Wissen einzuholen.

Abgeordnete haben gegenüber der Landesregierung und ihren Dienststellen sehr weitgehende Auskunftsrechte. Ihnen können daher in der Regel weder bestehende Amtsgeheimnisse noch das Recht auf informationelle Selbstbestimmung entgegengehalten werden. Auskunftsbegehren müssen stets an die Landesregierung gerichtet werden. Es ist nicht zulässig, dass Abgeordnete sich in Wahrnehmung ihrer besonderen Rechte direkt an die Verwaltung wenden.

Teil B

Akteneinsicht und Informationszugang

1 Brennpunkt der Akteneinsicht: Veröffentlichung der Empfänger von Agrarsubventionen

1.1 Ausgangslage

Dass der Löwenanteil des Haushalts der Europäischen Union in Form von Subventionen an landwirtschaftliche Betriebe ausgezahlt wird, war nie ein Geheimnis. Unbekannt blieb jedoch, wer in welcher Höhe und für welche Zwecke davon profitiert. Auch wenn die – komplizierten – Kriterien für die Erlangung der Zuschüsse öffentlich zugänglich waren, wurden Ross und Reiter nicht genannt. Die Praxis der Herausgabe solcher Informationen war zwischen den einzelnen Mitgliedsstaaten allerdings sehr unterschiedlich. Informationszugangsanträge scheiterten in Deutschland letzten Endes auch am Datenschutz. Aber auch rechtlich nicht relevante Aspekte wie die Angst vor einer „Neiddebatte“ wurden immer wieder ins Feld geführt. Darin, dass Bedarf bestand, den Einsatz der Agrarsubventionen und seine Folgen zu erörtern, stimmten viele Akteure ungeachtet ihrer spezifischen politischen Interessenlage zwar überein: Steuerzahler, Umwelt- und Naturschützer, Verbraucherschützer, Experten für regionale und ländliche Entwicklung sowie Befürworter der bäuerlichen Landwirtschaft – nur fehlten ihnen belastbare Informationen für eine Diskussion.

1.2 Transparenzinitiative der Europäischen Kommission

Die von der Europäischen Kommission im Jahre 2005 initiierte Transparenzinitiative[85] hatte unter anderem zum Ziel, die Europäische Union offener und zugänglicher zu machen, besser über die Verwendung der EU-Haushaltsmittel zu informieren und der Öffentlichkeit mehr Rechenschaft über die Arbeit der europäischen Institutionen zu geben. Ergebnis dieser Initiative ist eine Verpflichtung, vollständig offen zu legen, wer Mittel aus dem Gemeinschaftshaushalt erhält.[86] Jeder Mitgliedsstaat muss auf einer eigenen Website die Subventionsempfänger – sowohl natürliche Personen, als auch Unter-

85 Grünbuch Europäische Transparenzinitiative vom 3. Mai 2006 KOM(2006) 194 endgültig

86 Verordnung (EG, Euratom) Nr. 1995/2006 des Rates vom 13. Dezember 2006 zur Änderung der Verordnung (EG, Euratom) Nr. 1605/2002 über die Haushaltsordnung für den Gesamthaushaltsplan der Europäischen Gemeinschaften

nehmen – unter anderem nach Name, Ort und Höhe der erhaltenen Mittel veröffentlichen. Diese Informationen sollen jährlich am 30. April für das vorangegangene Haushaltsjahr publiziert werden, erstmalig am 30. April 2009.[87]

1.3 Agrar- und Fischereifonds-Informationen-Gesetz

Ein Großteil der EU-Fördermittel wird durch die einzelnen Mitgliedsstaaten ausgereicht, die auf der Grundlage der europarechtlichen Verpflichtungen hierüber selbst informieren. Diesem Zweck dient die Umsetzung der europäischen Vorschriften in nationales Recht durch das Gesetz zur Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und Fischerei (Agrar- und Fischereifonds-Informationen-Gesetz) und die dazu erlassene Durchführungsverordnung.[88] Subventionsempfänger erklären sich durch ihre Unterschrift unter dem Fördermittelantrag mit der Veröffentlichung der entsprechenden Daten einverstanden.

Die Informationen werden auf einer vom Bund und den Ländern gemeinsam betriebenen Internetseite der Bundesanstalt für Landwirtschaft und Ernährung von den für die Zahlungen zuständigen Stellen des Bundes und der Länder veröffentlicht.[89] Die Europäische Kommission hat unter ihrer zentralen Internetadresse eine Website eingerichtet, die auf die entsprechenden Internetseiten aller Mitgliedstaaten hinweist.[90]

1.4 Gerichtsverfahren

Bei Subventionen, die jedem Betrieb unter bestimmten Voraussetzungen offen stehen und um deren Erlangung kein Wettbewerb geführt wird, handelt es sich nicht um Betriebs- oder Geschäftsgeheimnisse. Ein Schutzbedarf

---

87 Rechtsgrundlage für die Veröffentlichung der Angaben aus den Agrarfonds ist die Verordnung (EG) Nr. 1290/2005 des Rates vom 21. Juni 2005 über die Finanzierung der Gemeinsamen Agrarpolitik und Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 mit Durchführungsbestimmungen zur Verordnung (EG) Nr. 1290/2005 des Rates hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER); für den Europäischen Fischereifonds: Artikel 30 und 31 der Verordnung (EG) Nr. 498/2007 der Kommission vom 26. März 2007 mit Durchführungsbestimmungen zur Verordnung (EG) Nr. 1198/2006 des Rates über den Europäischen Fischereifonds (EFF).

88 Gesetz zur Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und Fischerei (Agrar- und Fischereifonds-Informationen-Gesetz – AFIG) vom 26. November 2008 (BGBl. I S. 2330) sowie Verordnung über die Veröffentlichung von Informationen über die Zahlung von Mitteln aus den Europäischen Fonds für Landwirtschaft und für Fischerei (Agrar- und Fischereifonds-Informationen-Verordnung – AFI-VO) vom 10. Dezember 2008 (eBAnz. 2008, AT147 V1)

89 siehe http://www.agrar-fischerei-zahlungen.de

90 siehe http://ec.europa.eu/agriculture/funding/index_de.htm

dieser Unternehmensdaten, deren Offenbarung keinen Wettbewerbsnachteil darstellt, ist somit nicht gegeben.[91] Bei kleineren landwirtschaftlichen Betrieben (z. B. Ein-Personen-Unternehmen) sind solche Unternehmensdaten jedoch gleichzeitig als personenbezogen zu betrachten. Ihre Herausgabe ist zulässig, wenn der Betroffene eingewilligt hat oder sie gesetzlich geregelt ist und der Grundsatz der Verhältnismäßigkeit beachtet wird.

Vor dem Stichtag der geplanten Veröffentlichung wandten sich einige Landwirte gegen die Bekanntgabe ihrer Daten und strengten Eilverfahren vor den Verwaltungsgerichten an. Ihr wichtigstes Argument: Die Offenlegung stelle eine Verletzung ihres Rechts auf informationelle Selbstbestimmung dar. Das Verwaltungsgericht Wiesbaden hat das Klageverfahren betroffener Landwirte daraufhin ausgesetzt und dem Europäischen Gerichtshof die Frage zur Vorabentscheidung vorgelegt, ob die EG-Verordnungen gültig sind. Es hielt die entsprechenden Vorschriften für unvereinbar mit dem Gemeinschaftsrecht und argumentierte, dass die Veröffentlichung aller Empfänger im Internet ein unverhältnismäßiger Eingriff in das Grundrecht auf Datenschutz sei. Ob die Veröffentlichung der Daten geeignet sei, die Kontrolle der Fördermittel zu verbessern, sei zweifelhaft und Transparenz kein Selbstzweck.[92]

Der überwiegende Anteil der Oberverwaltungsgerichte stellte hingegen fest, dass die Veröffentlichung der Empfänger von Agrarsubventionen keinen unverhältnismäßigen Eingriff in deren Persönlichkeitsrechte darstellt und somit zulässig ist. Im Rahmen einer Interessenabwägung spräche unter anderem die Stärkung der demokratischen Beteiligung der Bürger durch Transparenz für die Veröffentlichung.[93] Schließlich hob der Hessische Verwaltungsgerichtshof die oben genannte Entscheidung des Verwaltungsgerichts Wiesbaden auf und befand die Veröffentlichung für rechtmäßig.[94] Das Bundesverfassungsgericht hat eine Beschwerde gegen die Offenlegung der Subventionen gar nicht erst angenommen.

---

91 siehe auch Urteil des Bundesverwaltungsgerichts vom 28. Mai 2009 (7 C 18.08)

92 Beschlüsse des Verwaltungsgerichts Wiesbaden vom 27. Februar 2009 (z. B. 6 K 1352/08.WI und 6 K 1045/08.WI), des Verwaltungsgerichts Schleswig vom 23. April 2009 (1 B 6/09, 1 B 7/09, 1 B 8/09), des Oberverwaltungsgerichts Mecklenburg-Vorpommern vom 4. Mai 2009 (2 M 77/09) und des Verwaltungsgerichts Mainz vom 27. Mai 2009 (u. a. 1 L 471/09.MZ und 1 L 511/09.MZ)

93 Beschlüsse des Oberverwaltungsgerichts Nordrhein-Westfalen vom 24. April 2009 (16 B 485/09), des Verwaltungsgerichts Karlsruhe vom 19. Mai 2009 (10 K 932/09), des Oberverwaltungsgerichts Schleswig-Holstein vom 3. Juni 2009 (2 MB 7/09, 2 MB 8/09, 2 MB 9/09), des Verwaltungsgerichtshofs Baden-Württemberg vom 5. Juni 2009 (1 S 1166/09 und 1 S 1167/09), des Oberverwaltungsgerichts Rheinland-Pfalz vom 10. Juli 2009 (u.a. 10 B 10607/09.OVG) und des Oberverwaltungsgerichts Rheinland-Pfalz vom 14. Juli 2009 (10 B 10601/09.OVG)

94 Beschluss des Hessischen Verwaltungsgerichtshofs vom 9. Juni 2009 (10 B 1503/09)

1.5 Ergebnis

Aufgrund der zunächst unklaren Rechtslage verzögerten der Bund und die Länder die Veröffentlichung, sodass die Bundesrepublik der einzige Mitgliedsstaat der Europäischen Union war, der den Stichtag des 30. April 2009 nicht eingehalten hatte. Auch Brandenburg schob die Veröffentlichung auf, obwohl keine bindenden Gerichtsentscheidungen auf Landesebene vorlagen.

Vor dem Hintergrund eines drohenden Vertragsverletzungsverfahrens der Europäischen Kommission erfolgte schließlich am 16. Juni 2009 die Veröffentlichung der Daten, allerdings mit Ausnahme der Angaben aus dem Freistaat Bayern, der erst Wochen später seine Verweigerungshaltung aufgab. Seither können sämtliche Empfänger von Agrarbeihilfen auch in Deutschland über das Internet ermittelt werden. Ausgenommen sind teilweise jedoch die Daten jener Landwirte, deren Klagen noch anhängig sind.

Auch wenn die Auflistung der Empfänger öffentlicher Zuwendungen für die Landwirtschaft noch nicht vollständig ist, hat ihre Veröffentlichung der politischen Debatte um die Agrarpolitik neue Perspektiven eröffnet. Erstmals wurde konkret bekannt, wohin die Gelder geflossen sind: beispielsweise an Nahrungsmittelkonzerne, an einen großen Energiekonzern, an eine Fluggesellschaft, an einen Finanzdienstleister sowie an große Agrarbetriebe.[95]

Die Veröffentlichung der Empfängerdaten in Deutschland orientiert sich am Wortlaut der europarechtlichen Vorgaben und des Agrar- und Fischereifonds-Informationen-Gesetzes. Genannt werden somit Name des Empfängers, der Ort des Betriebs sowie die jeweilige Gesamthöhe der erhaltenen Mittel. Unklar bleibt weiterhin, für welche Zwecke die einzelnen Beihilfen gezahlt werden. Nur mit dieser Angabe ist jedoch eine inhaltliche Bewertung möglich, ob die Subventionen sinnvoll sind. Auch kann es nützlich sein, eine Rangliste der Empfänger nach Land sortiert (z. B. „Top-10-Empfänger in Brandenburg“) oder die Gesamtaufstellung einer Gemeinde zu erhalten. Da die Recherchemöglichkeiten in der Datenbank aber auf die Eingabe von Postleitzahlenbereichen beschränkt sind, ist eine solche Darstellung nicht möglich.

Wesentlich transparenter als die Veröffentlichungspraxis der Bundesrepublik Deutschland ist hingegen die „Transparenzdatenbank“ der Republik Österreich. Dort werden nicht nur die einzelnen Maßnahmen genannt, für die Beihilfen gezahlt wurden, sondern es wird auf derselben Seite in übersichtlicher Weise erläutert, aus welchen Programmen die Mittel stammen und

[95] siehe „Empfänger von Agrarsubventionen jetzt öffentlich“ in Frankfurter Allgemeine Zeitung vom 17. Juni 2009

welche Ziele und Voraussetzungen diese Programme haben. Eine Sortierung kann zudem nach Bundesland, Bezirk und Gemeinde erfolgen.[96]

Die Europäische Kommission veröffentlicht mittlerweile ebenso wie die Mitgliedsstaaten weitere Daten über Subventionsempfänger aus hier nicht dargestellten Fachbereichen.[97] Trotz des noch erheblichen Verbesserungsbedarfs der Datenbankrecherche kann festgestellt werden, dass die öffentliche Debatte um die Bekanntgabe der Empfänger von Agrarbeihilfen den Transparenzgedanken wesentlich befördert hat.

2 Entwicklung des Informationszugangsrechts in Brandenburg

2.1 Verbraucherinformationsgesetz

Der Informationszugang war bislang im Wesentlichen von zwei Gesetzen bestimmt – dem Akteneinsichts- und Informationszugangsgesetz und dem Umweltinformationsgesetz. Mit seinem In-Kraft-Treten am 1. Mai 2008 ist das Verbraucherinformationsgesetz[98] hinzugekommen. Hintergrund waren nicht zuletzt die zahlreichen Lebensmittelskandale der vergangenen Jahre. Ein informierter Verbraucher, so der Grundgedanke der Neuregelung, motiviert den am Wettbewerb teilnehmenden Hersteller, die Qualität seiner Produkte zu sichern.

Die Neuregelung basiert auf zwei Säulen: Durch die Anpassung des Lebensmittel- und Futtermittelgesetzbuches sowie des Weingesetzes soll die zuständige Behörde die Öffentlichkeit unter Nennung des Produkts und des verantwortlichen Unternehmens informieren, wenn der hinreichende Verdacht auf ein Gesundheitsrisiko besteht. Das eigentliche Verbraucherinformationsgesetz eröffnet einen individuellen Anspruch auf Zugang zu verbraucherrelevanten Behördeninformationen. Es bezieht sich auf Lebens- und Futtermittel, Wein, Kosmetika sowie auf bestimmte Bedarfsgegenstände. Durch Ausnahmetatbestände werden sowohl Datenschutzrechte natürlicher Personen als auch Betriebs- und Geschäftsgeheimnisse geschützt. Rechtsverstöße eines Unternehmens fallen nicht unter diese Ausnahmen.

---

96 siehe Website des Bundesministeriums für Land- und Forstwirtschaft, Umwelt und Wasserwirtschaft der Republik Österreich (www.transparenzdatenbank.at)

97 für Beispiele siehe http://www.lda.brandenburg.de → Infos zur Akteneinsicht → Informationsfreiheit national und international → Linkliste zu Informationen über Fördermittelempfänger

98 Das Gesetz zur Verbesserung der gesundheitsbezogenen Verbraucherinformationen (Verbraucherinformationsgesetz – VIG) wurde als Artikel 1 des Gesetzes zur Neuregelung des Rechts der Verbraucherinformationen vom 5. November 2007 (BGBl. I S. 2558) beschlossen.

Das bundesrechtliche Verbraucherinformationsgesetz gilt auch für das Land Brandenburg. Zuständig sind das Landesamt für Verbraucherschutz, Landwirtschaft und Flurneuordnung für Informationen des Landes und im Übrigen die Landkreise und kreisfreien Städte. Die Erhebung der – im Wesentlichen nach dem Zeitaufwand zu berechnenden – Kosten erfolgt auf der Grundlage der entsprechend geänderten Gebührenordnung des zuständigen Ministeriums.[99]

Ob das Verbraucherinformationsgesetz angesichts seines engen Anwendungsbereichs und seiner weit gefassten Ausnahmen dazu beiträgt, das Idealbild des „informierten Verbrauchers“ zu schaffen, bleibt abzuwarten.

2.2 Zunehmende Rechtszersplitterung

Weder für Antragsteller noch für Verwaltungsbeschäftigte wird es leichter, die richtige Rechtsgrundlage für ein Informationszugangsbegehren zu bestimmen:

Die spezielleren Regelungen des Umweltinformationsgesetzes und des Verbraucherinformationsgesetzes gehen denen des Akteneinsichts- und Informationszugangsgesetzes vor. Außerdem sind beispielsweise der datenschutzrechtliche Informationsanspruch für von der Datenverarbeitung Betroffene (§ 18 Brandenburgisches Datenschutzgesetz), der verfahrensrechtliche Zugangsanspruch für Verfahrensbeteiligte (§ 29 Verwaltungsverfahrensgesetz) oder die Möglichkeit zur Übermittlung personenbezogener Daten (§ 16 Brandenburgisches Datenschutzgesetz) vorrangig zu prüfen. Erst wenn keines dieser Gesetze zum Tragen kommt, ist das Akteneinsichts- und Informationszugangsgesetz anzuwenden. Die Schwierigkeiten, zur Einsicht beantragte Unterlagen einzustufen, sind offensichtlich.

Angesichts der höchst unterschiedlichen Ergebnisse kommt es entscheidend darauf an, die richtige Rechtsgrundlage zu wählen. Der Hauptgrund hierfür liegt in den – auch verglichen mit Informationsfreiheitsgesetzen anderer Bundesländer – sehr restriktiven Vorschriften des brandenburgischen Akteneinsichts- und Informationszugangsgesetzes. Dies soll an einem alltäglichen Beispiel verdeutlicht werden:

Die öffentliche Hand schließt zahlreiche Verträge mit privaten Unternehmen, sei es für Zwecke der Ver- und Entsorgung, für den Betrieb von Einrichtungen zur Kinderbetreuung oder zur Organisation und Durchführung von Stadtfesten. Solche Verträge enthalten oft wichtige Einzelheiten zu den im Rahmen

[99] Gebührenordnung des Ministeriums für Ländliche Entwicklung, Umwelt und Verbraucherschutz (GebOMLUV), geändert durch Artikel 1 der Verordnung vom 1. Dezember 2008 (GVBl. II S. 2).

des Auftrags vorgesehenen Maßnahmen, Vorgaben und Auflagen und haben selbstverständlich einen Unternehmensbezug. Nach dem Akteneinsichts- und Informationszugangsgesetz darf letzterer nur offen gelegt werden, wenn der Unternehmer zustimmt oder die Informationen ohnehin (z. B. auf dem Wege einer vorangegangenen öffentlichen Ausschreibung) allgemein bekannt sind. Auch ganz lapidare Angaben, deren Bekanntwerden dem Unternehmer gar keinen Schaden zufügen kann, sind ansonsten geheim zu halten. Ganz anders das Umweltinformationsgesetz: Es schützt lediglich Betriebs- und Geschäftsgeheimnisse, und dies auch nur, soweit das öffentliche Interesse an der Bekanntgabe nicht überwiegt. Das ist ein Unterschied wie Tag und Nacht: Soweit es sich um Umweltinformationen handelt, ist ein Vertrag im Regelfall offen zu legen. Das Akteneinsichts- und Informationszugangsgesetz hat hingegen die weitgehende Geheimhaltung zur Folge und entzieht Verträge mit Dritten so der öffentlichen Kontrolle.

Die Darstellung der Fälle im vorliegenden Tätigkeitsbericht konzentriert sich auf den Aspekt der Unternehmensdaten. Bei der Bearbeitung von Beschwerden über den verweigerten Informationszugang stehen gerade Verträge immer wieder im Mittelpunkt. Weder den Verwaltungsbeschäftigten, die entsprechende Informationszugangsbegehren zu bearbeiten haben, noch den Antragstellern erschließt sich das von der gewählten Rechtsgrundlage abhängige Ergebnis. Wesentliche Unterschiede bestehen im Übrigen auch im Hinblick auf den engen Anwendungsbereich, den Ausschluss der Einsichtnahme in laufenden Verfahren sowie in Aufsichtsakten, den weitgehenden Schutz von Unternehmensdaten und das fehlende Recht auf Herausgabe von Kopien. Abwägungen zwischen dem öffentlichen Einsichtsinteresse und dem jeweiligen Schutzinteresse sieht das Akteneinsichts- und Informationszugangsgesetz gar nicht erst vor. Durch die genannten Mängel erweist es sich zunehmend als Hindernis auf dem Weg zur Informationsfreiheit. Im Berichtszeitraum gab es Initiativen, dies zu ändern:

Nach der Novellierung der europäischen Umweltinformationsrichtlinie wurde es in der Bundesrepublik erforderlich, dass auch die Länder eigene Umweltinformationsgesetze verabschieden. Das entsprechende brandenburgische Gesetz war zunächst bis zum 31. Dezember 2008 befristet. Zweck dieser Befristung war, dass das Akteneinsichts- und Informationszugangsgesetz mit dem Brandenburgischen Umweltinformationsgesetz in der Zwischenzeit zusammengefasst werden sollte. Die von uns unterstützte Bearbeitung eines Prüfauftrags durch die zuständigen obersten Landesbehörden zeitigte allerdings kein konkretes Ergebnis. Schließlich entfristete der Gesetzgeber die Geltung des Umweltinformationsgesetzes des Landes Brandenburg.[100] Die

[100] Erstes Gesetz zur Änderung des Umweltinformationsgesetzes des Landes Brandenburg vom 19. Dezember 2008 (GVBl. I S. 372)

Chance, ein nutzerfreundliches Gesetz zu gestalten und gleichzeitig unübersichtliche Regelungen im Sinne des Abbaus von Normen zusammenzufassen, wurde damit zunächst vergeben.

2.3 Defizite im Akteneinsichts- und Informationszugangsgesetz

Ebenfalls folgenlos verlief eine Initiative des Landtags mit dem Ziel, das Akteneinsichts- und Informationszugangsgesetz um ein ausdrückliches Recht auf Herausgabe von Kopien zu ergänzen. Der Vorstoß des Parlaments ging zurück auf einen Fall, den wir in unserem letzten Tätigkeitsbericht dargestellt hatten: Eine Behörde weigerte sich unter Berufung auf den – uneindeutigen – Wortlaut des Gesetzes, Kopien herauszugeben.[101] Daraufhin empfahl der Landtag Brandenburg im November 2008, in das Gesetz die Verpflichtung aufzunehmen, neben der Einsicht in die Originaldokumente auf Verlangen des Antragstellers auch Vervielfältigungen zur Verfügung zu stellen.[102] Im Rahmen einer parlamentarischen Fragestunde teilte die Landesregierung im April 2009 mit, dass sie beabsichtige, diese Empfehlung bei passender, jedoch noch nicht zu datierender Gelegenheit umzusetzen.[103] Dazu ist es in der abgelaufenen Legislaturperiode nicht mehr gekommen.

Während eine Konvention des Europarats über den Zugang zu amtlichen Dokumenten[104] auf den Weg gebracht wurde, die Richtlinien der Europäischen Union, die den Zugang zu Informationen regeln, gegenwärtig einer Überprüfung unterzogen werden,[105] auf Bundesebene der Zugang zu Verbraucherinformationen geregelt und Informationsfreiheitsgesetze in anderen Bundesländern neu geschaffen,[106] ausgeweitet[107] oder zumindest debattiert werden,[108] blieb es im Berichtszeitraum in Brandenburg um die Informationsfreiheit ziemlich still.

---

101 vgl. Tätigkeitsbericht 2006/2007, B 1

102 Beschluss des Landtages Brandenburg vom 19. November 2008 (Landtags-Drucksache 4/6891-B)

103 siehe Landtag Brandenburg Plenarprotokoll 4/84 vom 2. April 2009, Frage 2309, S. 6272

104 Konvention des Europarates über den Zugang zu amtlichen Dokumenten (SEV-Nr.: 205)

105 siehe die Diskussion um die Überarbeitung der Transparenzverordnung EG Nr. 1049/2001 (KOM/2008/0229 endg.), die Überprüfung der Weiterverwendungsrichtlinie 2003/98/EG (KOM/2009/0212 endg.) sowie der Umsetzung der Umweltinformationsrichtlinie entsprechend Artikel 9 der Richtlinie 2003/4/EG

106 siehe Thüringer Informationsfreiheitsgesetz vom 20. Dezember 2007, Informationszugangsgesetz Sachsen-Anhalt vom 19. Juni 2008 sowie Landesinformationsfreiheitsgesetz Rheinland-Pfalz vom 26. November 2008

107 siehe novelliertes Hamburgisches Informationsfreiheitsgesetz vom 17. Februar 2009

108 siehe Gesetzentwürfe in Hessen und Niedersachsen

3 Einsicht in Verträge zwischen öffentlichen und privaten Stellen

Um große Volksfeste durchzuführen, beauftragen Städte und Gemeinden häufig private Veranstalter. Deren Aufgaben reichen je nach Vertrag von der Erstellung des Veranstaltungskonzepts über die Werbung bis hin zur Akquise von Schaustellern oder der Verantwortung für die Gastronomie. Auch um Finanzierung, Logistik, Sicherheit und Verkehr kümmern sich teilweise externe Auftragnehmer. Kann eine Stadt den Inhalt eines solchen Vertrages ohne Weiteres geheim halten?

Eine Bürgerinitiative, die sich dafür einsetzte, Belange der Anwohner im Veranstaltungskonzept des Festes stärker zu berücksichtigen, engagierte sich unter anderem für die Verringerung von Beeinträchtigungen z. B. durch Abfall, Lärm, Erschütterungen, Vandalismus sowie Schädigungen von Grünflächen in einer Stadt, die sich immerhin mit dem Prädikat „staatlich anerkannter Erholungsort“ schmückt. Um sich über die Einzelheiten der Organisation des im Frühjahr des Folgejahres stattfindenden Stadtfestes zu informieren und ihr Anliegen rechtzeitig in die öffentliche Diskussion einbringen zu können, beantragte sie im Juli des Jahres 2008 Akteneinsicht in den Vertrag mit dem Veranstalter. Diese wurde ihr im August mit der Begründung verwehrt, der Unternehmer habe der Offenlegung nicht zugestimmt. Er befürchte Nachteile im Wettbewerb. Eine Möglichkeit zur Aussonderung schützenswerter Unternehmensdaten habe nicht bestanden. In ihrem Ablehnungsbescheid bezog sich die Verwaltung auf das Akteneinsichts- und Informationszugangsgesetz.

Nachdem uns die Bürgerinitiative im September um Unterstützung bat, wiesen wir zwei Wochen später die Stadtverwaltung darauf hin, dass es sich bei den Informationen des Vertrags zumindest teilweise um Umweltinformationen handeln dürfte und somit das Umweltinformationsgesetz zum Tragen kommt. Dieses stellt die Offenlegung von Unternehmensdaten nicht, wie das Akteneinsichts- und Informationszugangsgesetz, in das weitgehende Belieben des Unternehmers. Vielmehr sind auf der Grundlage des Umweltinformationsgesetzes ausschließlich Betriebs- und Geschäftsgeheimnisse geheim zu halten – und das auch nur unter der Voraussetzung, dass deren Schutzbedarf das öffentliche Einsichtsinteresse überwiegt. Der Unternehmer ist zwar anzuhören, letztendlich hat aber die Akten führende Stelle zu entscheiden, ob tatsächlich ein Schutzbedarf vorliegt. In einem solchen Fall müsste sie die geheim zu haltenden Angaben aussondern und den übrigen Teil des Vertrags herausgeben.

Nachdem die Stadtverwaltung auf unser Schreiben nicht reagierte, erinnerten wir im Dezember und im darauffolgenden Januar an unser Anliegen. Gleich-

zeitig boten wir an, den Text des Vertrages zu begutachten und der Stadt im Ergebnis die informationszugangsrechtlichen Aspekte zu erläutern. Hiervon machte sie eine Woche später Gebrauch und übersandte das Dokument, nachdem sie zunächst mitteilte, unsere Schreiben nicht erhalten zu haben und nach erneuter Zusendung darauf hinwies, dem Widerspruch der Antragsteller fehle eine Begründung. Im selben Monat übermittelten wir der Stadtverwaltung ausführliche Hinweise auf die Rechtslage. Insbesondere erläuterten wir, dass es sich bei Tätigkeiten und Maßnahmen mit möglichen Umweltauswirkungen stets um Umweltinformationen handelt. Dies betrifft gerade auch vertragliche Pflichten zur Ausrichtung eines Festes, die nur in wenigen Ausnahmefällen als Betriebs- und Geschäftsgeheimnis einzustufen sind. Wir forderten die Stadt auf, den zwischenzeitlich begründeten Widerspruch unter Berücksichtigung unserer Hinweise zu prüfen.

Anfang April mussten wir die Stadt an die erbetene, aber noch immer nicht erfolgte Information zum Ergebnis der Prüfung erinnern. Daraufhin teilte sie mit, den Unternehmer bereits im März erneut angehört zu haben und das Ergebnis der Anhörung abwarten zu wollen. Erst im Juni – fast ein Jahr nach der Antragstellung durch die Bürgerinitiative – informierte uns die Verwaltung nach einer erneuten Erinnerung, dass der Unternehmer seine ablehnende Haltung nicht geändert und unsere rechtlichen Hinweise ihn nicht überzeugt hätten. Die Stadt hatte dem Wunsch des Unternehmers also erneut entsprochen, ohne die gesetzlich vorgeschriebene, eigene Entscheidung zu treffen. Das Stadtfest, um welches es der Bürgerinitiative ging, war zu diesem Zeitpunkt längst vergangen.

Die Angelegenheit zeigt anschaulich, wie wichtig es ist, dass die Verwaltung sich vor der eigentlichen Prüfung eines Antrags auf Informationszugang darüber klar wird, ob es sich um Umweltinformationen handelt. Ist dies der Fall, kommt das transparenzfreundliche Umweltinformationsrecht zum Tragen. Enthält die Akte hingegen allgemeine Informationen ohne Umweltbezug, gelten das Akteneinsichts- und Informationszugangsgesetz und dessen teilweise sehr restriktive Ausnahmetatbestände. Die Stadtverwaltung hat unsere Hinweise auf diese Rechtslage ignoriert. Da im Laufe unserer Bearbeitung der Beschwerde deutlich wurde, dass es sich vorwiegend um einen Informationszugangsantrag auf der Grundlage des Umweltinformationsgesetzes handelte, fehlte der Landesbeauftragten jedoch die Kompetenz, dies sowie die offensichtliche Verhinderungstaktik der Behörde zu beanstanden.

Verträge zwischen öffentlichen Stellen und privaten Unternehmen sind in der Regel zumindest soweit offen zu legen, als sie Maßnahmen oder Tätigkeiten regeln, die Umweltauswirkungen haben können. Betriebs- und Geschäftsgeheimnisse sind in solchen Vereinbarungen nur selten vorhanden.

4 Eigenbetriebe unterliegen dem Recht auf Akteneinsicht

Eine Stadtverwaltung verweigerte zunächst die Akteneinsicht in Unterlagen zum Brandschutz in einer Schule. Zuvor müsse der an der Aufgabe beteiligte städtische Immobilienbetrieb zustimmen. Die Stadt bot an, das Einverständnis einzuholen.

Antragsteller war ein Elternvertreter der Schule. Er wollte in Erfahrung zu bringen, welche Vorgaben die untere Bauaufsichtsbehörde, an die er den Antrag richtete, dem für die Umsetzung verantwortlichen Immobilienbetrieb der Stadt gemacht hat, um den Brandschutz zu gewährleisten. Bei dieser Einrichtung handelt es sich um einen Eigenbetrieb der Stadt. Er hat keine eigene Rechtspersönlichkeit; seine Tätigkeit ist vielmehr der Stadtverwaltung zuzurechnen.

Für den Eigenbetrieb einer Stadtverwaltung gilt das Akteneinsichts- und Informationszugangsgesetz ebenso wie für die unmittelbare Stadtverwaltung selbst. Die Vorschrift, nach der Informationen öffentlicher Stellen, die dem Anwendungsbereich des Gesetzes nicht unterliegen, nur mit deren Zustimmung herauszugeben sind, kommt deshalb überhaupt nicht zur Anwendung. Als Teil der Stadtverwaltung kann sich ein Eigenbetrieb auch nicht auf die Ausnahmetatbestände zum Schutz überwiegender privater Interessen – wie beispielsweise auf schutzwürdige Unternehmensdaten – berufen.

Wir haben die Stadt darauf hingewiesen, dass es nicht zulässig ist, die Gewährung des Informationszugangs von der Zustimmung ihres eigenen Immobilienbetriebes abhängig zu machen. Dem Einsichtsantrag hat sie vollständig entsprochen.

Eigenbetriebe sind der kommunalen Verwaltung zuzurechnen. Für sie gilt das Akteneinsichts- und Informationszugangsgesetz ebenso wie für die Verwaltung selbst. Eine Zustimmung ist hierfür nicht erforderlich.

5 Tierversuche – ein streng geschütztes Unternehmensgeheimnis

Tierversuche werfen ethische Fragen auf, die stets persönliche und gesellschaftliche Grundwerte berühren. Umso wichtiger müsste es sein, erfahren zu können, welche Regelungen behördliche Genehmigungen für die einzelnen Versuchsprojekte treffen. Antragsteller stoßen hier allerdings schnell an die Grenzen der Informationsfreiheit.

Nachdem ein Antragsteller ein Einsichtsbegehren an eine Behörde richtete, welche die Tierversuche durch ein privatrechtliches Unternehmen genehmigt hatte, erkundigte diese sich beim Unternehmer nach dessen Einverständnis mit der Einsichtnahme. Der Betroffene verweigerte die Zustimmung. Daraufhin signalisierte die Verwaltung dem Antragsteller, dass sie beabsichtige, seinen Antrag abzulehnen. Der Antragsteller hielt jedoch an seinem Begehren fest und erhielt schließlich einen formalen Ablehnungsbescheid. In seiner Eingabe an uns machte er unter anderem geltend, dass es nicht darauf ankomme, dass der Unternehmer einer Akteneinsicht widerspricht. Vielmehr müsse zwischen dem Geheimhaltungswunsch des Betroffenen und dem öffentlichen Einsichtsinteresse abgewogen werden.

Nach unserer Auffassung hat die Behörde im Ergebnis jedoch rechtmäßig entschieden. Bei der in Rede stehenden Genehmigung handelt es sich – unabhängig von der Frage, wie relevant ihr Inhalt für die gesellschaftliche Diskussion ist – um ein unternehmensbezogenes Datum. Das Akteneinsichts- und Informationszugangsgesetz sieht vor, dass die Herausgabe der Informationen unterbleibt, soweit ansonsten eine Tatsache offenbart würde, „die nur einem eng begrenzten Personenkreis bekannt ist, zu einem bestimmten Geschäftsbetrieb in Beziehung steht und die nach dem Willen des Unternehmens geheim zu halten ist oder an deren Geheimhaltung das Unternehmen ein schutzwürdiges Interesse hat.“ Entscheidend an dieser Formulierung ist, dass der letzte Aspekt, also eine objektives Geheimhaltungsinteresse des Unternehmens, nicht zwingend vorliegen muss. Dies wird durch das Wörtchen „oder“ (anstelle von „und“) deutlich. In der Praxis bedeutet dieser Wortlaut, dass ein Unternehmensdatum, das alle übrigen Voraussetzungen erfüllt, nicht herausgegeben werden darf. Unternehmensdaten werden durch das Akteneinsichts- und Informationszugangsgesetz somit noch stärker geschützt als personenbezogene Daten. Es kommt auch nicht darauf an, ob es sich um wettbewerbsrelevante Betriebs- und Geschäftsgeheimnisse handelt.

Die Behörde war also an die verweigerte Zustimmung des Unternehmens gebunden und musste den Antrag ablehnen. Eine Interessenabwägung sieht das Akteneinsichts- und Informationszugangsgesetz in einem solchen Fall nicht vor.

Ein – zumindest teilweise – anderes Ergebnis wäre bei einer Prüfung auf der Grundlage des Umweltinformationsgesetzes zu erwarten gewesen. Dieses schützt nämlich ausschließlich Betriebs- und Geschäftsgeheimnisse – und zwar nur, soweit das öffentliche Interesse an der Bekanntgabe nicht überwiegt. Es geht dem Akteneinsichts- und Informationszugangsgesetz vor, wenn es um Umweltinformationen geht. Trotz der scheinbaren Nähe von Umweltschutz und Tierschutz kann die Genehmigung von Tierversuchen nur insoweit als Umweltinformation gewertet werden, wie beispielsweise Tiere

der freien Natur entnommen werden oder die Versuche konkrete Auswirkungen auf die Umwelt haben können (z. B. geruchsintensive Haltung). Da dies aber nicht relevant war und es sich folglich nicht um Umweltinformationen handelte, war das Umweltinformationsgesetz nicht anzuwenden.

Das Akteneinsichts- und Informationszugangsgesetz sieht einen unverhältnismäßig strengen Schutz unternehmensbezogener Daten vor. Diese müssen selbst dann geheim gehalten werden, wenn ihre Herausgabe den wettbewerbsrechtlichen Schutz von Betriebs- und Geschäftsgeheimnissen gar nicht berühren würde.

6 Genehmigung für die Landung von Wasserflugzeugen

Eine Bürgerinitiative interessierte sich für die Genehmigungsunterlagen eines Sonderlandeplatzes für Wasserflugzeuge auf einem See. Zwar wurde ihr Antrag von der zuständigen Behörde nicht abgelehnt. Deren Bedingungen stellten aber unnötige Hürden dar.

Auf elektronischem Wege wandte sich die Bürgerinitiative zunächst mit der schlichten Anfrage an die zuständige Landesbehörde, ob ein Antrag für die Errichtung eines Sonderlandeplatzes für Wasserflugzeuge vorliege. Die Verwaltung wertete dies als Antrag auf Informationszugang nach dem Akteneinsichts- und Informationszugangsgesetz. Bevor sie den Antrag bearbeitete, teilte sie dem Antragsteller mit, dass eine Gebühr zwischen 0 und 100 Euro festzusetzen sei. Außerdem verlangte sie, den Antrag schriftlich oder per Fernkopie zu stellen. Der Antragsteller, der als Sprecher der Bürgerinitiative auftrat, sollte zudem eine Vertretungsbefugnis nachweisen. Daraufhin wandte dieser sich mit der Bitte um eine rechtliche Bewertung der behördlichen Forderungen an uns.

Bei der Genehmigung für einen Sonderlandeplatz für Wasserflugzeuge handelt es sich – zumindest in weiten Teilen – um Informationen über die Umwelt. Ihre Offenlegung ist daher auf der Grundlage des Umweltinformationsgesetzes zu prüfen. Die entsprechende Gebührenordnung sieht vor, dass sowohl die Einsichtnahme vor Ort als auch einfache Auskünfte gebührenfrei sind. Für die Antragstellung existieren keine Formvorschriften. Auch der Vertretungsbefugnis einer Bürgerinitiative bedarf es nicht.

Selbst für den Fall, dass als Rechtsgrundlage das Akteneinsichts- und Informationszugangsgesetz zum Tragen gekommen wäre, hätte die Behörde solche Bedingungen nicht stellen dürfen:

Zwar sieht die Akteneinsichts- und Informationszugangsgebührenordnung für die Erteilung einer Auskunft einen Gebührenrahmen von 0 bis 100 Euro vor, allerdings hätte die Akten führende Stelle die Gebührenhöhe enger eingrenzen müssen. Angesichts der überschaubaren Anfrage, die womöglich mit einem einfachen „Ja“ oder „Nein“ hätte beantwortet werden können, ist nämlich nicht davon auszugehen gewesen, dass der angekündigte Gebührenrahmen auch nur annähernd ausgeschöpft werden würde. Im Gegenteil war eher zu vermuten, dass eine Bagatellgrenze, die aus Wirtschaftlichkeitsgründen den Gebührenverzicht nahe legt, gar nicht erst überschritten wird. Die unrealistische Gebührenankündigung war schon deshalb unzulässig, weil sie auf den Antragsteller abschreckend hätte wirken können.

Die Behörde verlangte einen schriftlichen Antrag, weil ihr E-Mail-Zugang nicht für die Übermittlung elektronischer Dokumente eröffnet sei. Das formale Kriterium der „Schriftlichkeit“ ist bei einer elektronischen Antragstellung im herkömmlichen Verwaltungsverfahren nur erfüllt, wenn eine qualifizierte digitale Signatur verwendet wird. Da diese technische Möglichkeit nicht jedermann zur Verfügung steht, wurde im Jahre 2003 das Recht auf eine „elektronische“ Antragstellung – per einfacher E-Mail – im Akteneinsichts- und Informationszugangsgesetz ergänzt. Sie sollte die Kontaktaufnahme mit der Verwaltung erleichtern und unnötige Hindernisse beim Informationszugang vermeiden. Selbstverständlich bedeutet dies nicht, dass der Antragsteller sich nicht zu identifizieren braucht. Schließlich benötigt die öffentliche Stelle eine zustellfähige postalische Adresse für ihre Entscheidung und kann einen anonymen Antrag nicht bearbeiten.

Die Regelung des Akteneinsichts- und Informationszugangsgesetzes, nach der Anträge auf Akteneinsicht nur durch den Vorstand bzw. einen Bevollmächtigten gestellt werden können, bezweckt, dass die Behörde für ihren Bescheid eine Ansprechperson hat. Nur in Zweifelsfällen kann die Behörde sich eine Vertretungsbefugnis vorlegen lassen. Diese Vorschrift kann jedoch lediglich auf Vereine oder Verbände angewandt werden. Nur diese verfügen über eine formale Struktur, die es ermöglicht, eine solche Befugnis überhaupt auszustellen. Im Gegensatz dazu sind Bürgerinitiativen durch eine lockere Organisationsform gekennzeichnet. Ein Verwaltungsakt richtet sich daher nicht an sie, sondern an eines ihrer Mitglieder, das sich allenfalls bereit erklären muss, für die Folgen eines Antrags auf Akteneinsicht (z. B. Kostenerhebung) einzustehen.

Im vorliegenden Fall waren weder ein Zweifel an der Identität oder Anschrift des Antragstellers, noch an seiner Funktion in der Bürgerinitiative zu erkennen. Die Behörde hat im Ergebnis unsere Hinweise aufgegriffen und den Informationszugang zügig und kostenfrei gewährt.

Die Ankündigung von Gebühren für die Akteneinsicht kann in unzulässiger Weise von der Antragstellung abschrecken, wenn lediglich der allgemeine Höchstbetrag genannt wird. Für die Antragstellung genügt eine einfache E-Mail ohne elektronische Signatur. Bürgerinitiativen können keine Vertretungsbefugnisse ausstellen. Es reicht aus, wenn sie eine verantwortliche Ansprechperson benennen, die sich bereit erklärt, die rechtlichen und finanziellen Folgen des Einsichtsantrags zu tragen.

Teil C

Die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1 Die Dienststelle

Die Skandale der Jahre 2008 und 2009 wegen mangelnden Datenschutzes haben das Bewusstsein der Bürgerinnen und Bürger für den Schutz ihrer Persönlichkeitssphäre spürbar verstärkt. Diese Entwicklung hat sich auch auf die Arbeit meiner Dienststelle ausgewirkt – nicht zuletzt in Form gestiegener Zahlen von Beratungsersuchen und Bürgerbeschwerden.

Von Seiten der öffentlichen Stellen wurden nicht nur immer mehr, sondern vor allem immer komplexere Verfahren zur Datenverarbeitung eingeführt. Nicht selten handelte es sich dabei um Projekte mit mehreren Stellen, deren datenschutzrechtliche Verantwortung zu klären war: Neuland für viele Beteiligte. Meine Mitarbeiterinnen und Mitarbeiter haben die Einführung solcher Projekte oft über einen langen Zeitraum begleitet.

Ein Schwerpunkt nicht nur unserer Beratungstätigkeit, sondern auch unserer Prüfungen waren Verfahren des E-Government – vor allem auf kommunaler Ebene. Aus den Ergebnissen wurde deutlich, wie eng Fragen der IT-Sicherheit mit jenen des Datenschutzes zusammenhängen. Um mir einen Überblick über den Stand der Umsetzung des Brandenburgischen Datenschutzgesetzes in der Kommunalverwaltung des Landes zu verschaffen, habe ich eine Umfrage in allen Kommunen durchgeführt. Die Auswertung dient meinem Ziel, Unterstützungsleistungen wie Beratungen oder Schulungen künftig so bedarfsgerecht wie möglich anbieten zu können.

Die Stärkung der Medienkompetenz von Kindern und Jugendlichen ist mir ein weiteres wichtiges Anliegen. Unsere gemeinsam mit dem Ministerium des Innern entwickelten Bausteine zur Verwendung in den Schulen sollen Schülerinnen und Schüler für den Umgang mit ihren Persönlichkeitsrechten im Alltag sensibilisieren. Zwar registrierten wir im Berichtszeitraum eine stetig zunehmende Nachfrage danach, doch sind unsere Kapazitäten begrenzt: Weder eine professionelle Weiterentwicklung der Bausteine noch die dringend notwendige Fortbildung der Lehrkräfte in punkto Medienkompetenz kann personell von meiner Dienststelle allein geleistet werden. Ich beabsichtige aber auch weiterhin, insbesondere die Lehrerfortbildung zu nutzen, um so an den

Schulen Multiplikatoren für die Vermittlung eines bewussten Umgangs mit personenbezogenen Daten z. B. im Internet zu gewinnen.

Die auf dem Gebiet der Informationsfreiheit festzustellende Zersplitterung der Rechtsgrundlagen wirkt sich vor allem durch das Nebeneinander von Akteneinsichts- und Informationszugangsgesetz und des Umweltinformationsgesetz aus. In der Praxis entstehen daraus nach meiner Erfahrung große Unsicherheiten in der Umsetzung der Gesetze. Ich habe mich deshalb entschlossen, dies als Thema für das mittlerweile schon traditionelle Internationale Symposium im Juni 2009 zu wählen. Durch ein Zusammenspiel engagierter Kooperationspartner, kompetenter Referenten sowie eines interessierten Publikums ist es dem Symposium gelungen, kritische Anregungen zur Weiterentwicklung des Informationsfreiheitsrechts in Brandenburg zu geben. Ich freue mich bereits darauf, diese erfolgreiche Veranstaltungsreihe im Jahre 2011 fortzusetzen.

Die personelle Situation in meiner Dienststelle hat sich im Berichtszeitraum wesentlich verändert. Meinen Stellvertreter und Leiter des Bereichs Technik und Organisation habe ich im Frühjahr 2008 in den Ruhestand verabschiedet und seine Aufgabe als stellvertretender Landesbeauftragter an den langjährigen Leiter des Bereichs Recht und Verwaltung übertragen. Im Ergebnis einer Ausschreibung übernahm ein erfahrener Mitarbeiter der Dienststelle die Bereichsleitung Technik und Organisation. Darüber hinaus konnten zwei freie Stellen mit einer neuen Mitarbeiterin und einem neuen Mitarbeiter qualifiziert besetzt werden.

Ein Mitarbeiter der Dienststelle hat sich für ein Jahr in eine Bundesbehörde abordnen lassen. Während seiner Abwesenheit wurde er kompetent vertreten. Zudem konnte ich eine engagierte Mitarbeiterin gewinnen, die befristet Teilzeitvertretungen übernommen hat. Den infolge dieser Veränderungen zeitweise nicht besetzten Arbeitsgebieten haben sich sämtliche meiner Mitarbeiterinnen und Mitarbeiter in beiden Jahren mit großem Einsatz angenommen – dafür möchte ich ihnen an dieser Stelle ausdrücklich danken.

2 Zusammenarbeit mit dem Landtag

Der Ausschuss für Inneres des Landtags Brandenburg hat über den 14. Tätigkeitsbericht 2006/2007 mehrfach beraten und dabei die von mir festgestellten Mängel in den Mittelpunkt gestellt. Im Ergebnis legte er dem Landtag Empfehlungen[109] zur Verbesserung des Datenschutzes und der

[109] Landtag Brandenburg, Drucksache 4/6891

Informationsfreiheit vor, die dieser am 19. November 2008 in einem Beschluss annahm.[110] Der Landtag forderte die Landesregierung auf, mir innerhalb von sechs Monaten die IT-Sicherheitskonzepte für den Verfassungsschutz und für das Projekt Neues Finanzmanagement sowie zeitnah jene der Landesministerien vorzulegen. Außerdem sollte die Landesregierung ein Ausführungsgesetz zur Regelung des Datenschutzaudits nach § 11c Brandenburgisches Datenschutzgesetz erarbeiten und im Akteneinsichts- und Informationszugangsgesetz ein ausdrückliches Recht auf die Herausgabe von Fotokopien vorsehen.

Den Aufforderungen und Empfehlungen des Landtags ist die Landesregierung im Berichtszeitraum nur unzureichend nachgekommen: Bei der Sicherheitsdokumentation besteht in den Landesministerien Nachbesserungsbedarf, ein Gesetzentwurf zur Regelung des Auditierungsverfahrens wurde nicht vorgelegt und auch zu einer informationszugangsfreundlichen Regelung des Umgangs mit Fotokopien im Rahmen der Akteneinsicht ist es nicht gekommen.

Während des Berichtszeitraums haben mich mehrere Ausschüsse des Landtages als Sachverständige zu datenschutzrechtlichen Fragen eingeladen: Am 16. Januar 2008 habe ich im Rahmen einer öffentlichen Anhörung des Ausschusses für Arbeit, Soziales, Gesundheit und Familie zur Neuregelung des Öffentlichen Gesundheitsdienstes Stellung genommen. Auf Einladung des Ausschusses für Inneres konnte ich am 2. Oktober 2008 meine Sicht auf die Zusammenlegung der Datenschutzaufsicht über den öffentlichen und nicht öffentlichen Bereich darlegen. Schließlich hatte ich vor demselben Gremium am 6. November 2008 Gelegenheit, meine Position zum Datenschutz im Zuge der Änderung des Brandenburgischen Polizeigesetzes in einer öffentlichen Anhörung zur Diskussion zu stellen.

Der Landtag Brandenburg hat meine Anliegen zum Datenschutz und zur Informationsfreiheit in der abgelaufenen Legislaturperiode unterstützt und die Möglichkeit für Verbesserungen durch meine Einbeziehung im Rahmen der Gesetzgebung wahrgenommen. Ich freue mich auf die Fortsetzung dieser Zusammenarbeit in der laufenden Legislaturperiode.

[110] Landtag Brandenburg, Drucksache 4/6891-B

3 Kooperation mit den behördlichen Datenschutzbeauftragten

Unsere jährliche Beratung mit den behördlichen Datenschutzbeauftragten der Landkreise, kreisfreien Städte und größeren kreisangehörigen Gemeinden haben wir im Jahr 2008 in den Räumen meiner Dienststelle durchgeführt. Fragen zur IT-Sicherheit sowie zur Verarbeitung der Geoinformationen standen dabei im Vordergrund. Der Erfahrungsaustausch erstreckte sich auch auf den Einsatz von Dokumentenmanagementsystemen und auf die Verarbeitung von Personaldaten in der kommunalen Verwaltung.

Die Veranstaltung wird von allen Beteiligten stets gern angenommen. Leider stoßen die räumlichen, vor allem aber die personellen Kapazitäten angesichts des zur Vorbereitung und Organisation erforderlichen Aufwands auf Grenzen. Im Jahr 2009 waren meine Mitarbeiterinnen und Mitarbeiter durch ihre übrige Beratungs- und Kontrolltätigkeit derart ausgelastet, dass das Treffen nicht stattfinden konnte.

Ich halte den Austausch mit den behördlichen Datenschutzbeauftragten weiterhin für eine sinnvolle Unterstützung des Datenschutzes in der Kommunalverwaltung und beabsichtige, die Beratungstreffen auch künftig anzubieten.

4 Zusammenarbeit mit anderen Datenschutzbehörden

Im Berichtszeitraum fanden regelmäßig Kooperationsgespräche mit der Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich, die dem Ministerium des Innern zugeordnet ist, statt. Ein immer wiederkehrendes Thema der Gespräche war der Datenschutz im Gesundheitswesen. Aufgrund der unterschiedlichen Zuständigkeiten für die medizinischen Einrichtungen in privater und öffentlicher Trägerschaft befassen sich beide Aufsichtsbehörden mit zahlreichen Fragen dieses Rechtsgebiets, beispielsweise Datensicherheit und Archivierung in Kliniken. Das mit der Unterstützung der Aufsichtsbehörde erstellte Projekt „Datenschutz für Schüler und Lehrer“ haben wir anlässlich des Europäischen Datenschutztages im Januar 2008 öffentlich vorgestellt und mit Schülern diskutiert.

Auch der regelmäßige Austausch mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit wurde fortgesetzt. Zu einem großen Erfolg hat sich der gemeinsam erarbeitete Ratgeber zu Hartz IV entwickelt. Er wurde mehrfach überarbeitet und um aktuelle Informationen zur neuesten Recht-

sprechung sowie zu anderen datenschutzrechtlichen Entwicklungen ergänzt. Die nächste Überarbeitung des Ratgebers ist bereits in Angriff genommen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte im Jahr 2008 unter dem Vorsitz des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Frühjahr in Berlin und im Herbst in Bonn. Turnusgemäß wechselte der Vorsitz der Konferenz im Jahr 2009 zum Berliner Beauftragten für Datenschutz und Informationsfreiheit. Ein Blick auf die hohe Anzahl von Entschließungen in beiden Jahren macht deutlich, dass die Zahl der aktuellen Themen ständig steigt. Der Text der Entschließungen ist als Anlage 3 Bestandteil dieses Tätigkeitsberichts.

Vor dem Hintergrund der Bundestagswahl im Herbst 2009 mahnte die Konferenz auch eine Modernisierung des Datenschutzrechts an. Um dieses Anliegen angemessen begleiten zu können, hat sie im Frühjahr 2009 in Berlin die Einrichtung der Arbeitsgruppe „Modernisierung des Datenschutzrechts“ beschlossen, die sich mit den Anforderungen an ein modernes Datenschutzgesetz befasst. Erste Ergebnisse sollen auf der Datenschutzkonferenz im Frühjahr 2010 in Stuttgart vorgestellt werden.

5 Arbeitskreis Medien

Um sich über die länderübergreifenden datenschutzrechtlichen Fragen in diesem Bereich auszutauschen, treffen sich Fachreferenten der Datenschutzbeauftragten des Bundes und der Länder im Arbeitskreis Medien und Telekommunikation unter dem Vorsitz der Landesbeauftragten für den Datenschutz und das Recht auf Akteneinsicht des Landes Brandenburg zweimal im Jahr in Potsdam.

Im Berichtszeitraum befasste sich der Arbeitskreis sowohl mit den gesetzlichen und technischen Entwicklungen im Bereich der Telekommunikation, der Telemedien und des Rundfunkrechts als auch mit Einzelfragen in der öffentlichen Verwaltung. Zu verschiedenen Themen konnte der Arbeitskreis hochkompetente Fachreferenten gewinnen, so beispielsweise zum Datenschutz in sozialen Netzwerken, der Vorratsdatenspeicherung in der elektronischen Kommunikation und dem „neuen Grundrecht“ auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Weitere Themenschwerpunkte im Arbeitskreis waren der Einsatz von Voice over IP und Cloud Computing in der Verwaltung sowie die datenschutzkonforme Gestaltung von Bewertungsportalen. Auch das Verfahren der Gebühreneinzugszentrale (GEZ) zur Befreiung von den Rundfunkgebühren war Gegenstand der Beratung.

An den Sitzungen nimmt auch ein Vertreter des Arbeitskreises der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten teil. Seit 2009 wurde die Landesbeauftragte auch als Vertreterin des Arbeitskreises Medien in den zweimal jährlich stattfindenden Arbeitskreis der Rundfunkdatenschutzbeauftragten eingeladen. Die Teilnahme dient der besseren gegenseitigen Information in Fragen des Medienrechts und soll fortgesetzt werden.

6 Informationsfreiheitsbeauftragte

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland tagte in den Jahren 2008 und 2009 insgesamt viermal.

Im ersten Halbjahr 2008 führte der Landesbeauftragte des Saarlandes, Roland Lorenz, den Vorsitz. In dieser Zeit forderte die Konferenz in einer Entschließung zu Transparenz in der Finanzverwaltung diese auf, die Informationsfreiheitsgesetze anzuwenden und in ihren nachgeordneten Bereichen durchzusetzen. Außerdem wandte sie sich in einer weiteren Entschließung gegen die Vorschläge der Europäischen Kommission, den Zugang zu den Dokumenten europäischer Institutionen einzuschränken. Unter Vorsitz des Landesbeauftragten für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, Karsten Neumann, forderte die Konferenz die Bundesregierung in der zweiten Jahreshälfte 2008 auf, die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich zu unterzeichnen und zu ratifizieren, damit dieser erste völkerrechtlich verbindliche Vertrag zur Informationsfreiheit in Kraft treten kann.

Während in Sachsen-Anhalt das Informationszugangsgesetz erst im Jahr 2008 in Kraft getreten war, hatte die Freie und Hansestadt Hamburg das bestehende Informationsfreiheitsgesetz im Jahr 2009 um die Aufgabe eines Landesbeauftragten für die Informationsfreiheit erweitert. Den Vorsitz der Konferenz teilten sich im Jahr 2009 dementsprechend zwei neue Mitglieder: Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt, Dr. Harald von Bose, im ersten und der Landesbeauftragte für Datenschutz und Informationsfreiheit Hamburg, Prof. Dr. Johannes Caspar, im zweiten Halbjahr.

Die Informationsfreiheitsbeauftragten forderten im Jahr 2009 vom Deutschen Bundestag, keine weitere Einschränkung der Transparenz bei Finanzaufsichtsbehörden zuzulassen. Das Parlament hatte nämlich über eine Initiative des Bundesrates zu entscheiden, die Bundesfinanzbehörden dem Anwendungsbereich des Rechts auf Informationszugang zu entziehen. In einer weiteren Entschließung mahnten sie an, den Informationszugang für Bürgerinnen und Bürger zu verbessern und verlangten mehr Transparenz durch

gesetzlichen Schutz von Whistleblowern, d. h. Beschäftigten, die Missstände aufdecken und Gefahr laufen, dadurch ihren Arbeitsplatz zu verlieren. Anlässlich der Ankündigung der neuen Bundesregierung, die Ansprüche der Verbraucherinnen und Verbraucher auf Information in einem einheitlichen Gesetz zur Regelung der Informationsansprüche zusammenzufassen, empfahl die Konferenz, die Zersplitterung der Rechtsgrundlagen durch die anstehende Überarbeitung zu beenden und für transparente, handhabbare Vorschriften einzutreten.

Die Entschließungen zeigen deutlich, dass Transparenz keine Selbstverständlichkeit ist und sowohl in der Rechtsetzung als auch in der Praxis der Informationsfreiheit noch deutlicher Verbesserungsbedarf besteht.

Der Text der Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland ist als Anlage 4 Bestandteil dieses Tätigkeitsberichts.

7 Öffentlichkeitsarbeit

7.1 Internationales Symposium zum Umweltinformationszugang

Am 18. und 19. Juni 2009 veranstaltete die Landesbeauftragte bereits zum sechsten Mal ein Internationales Symposium in Potsdam. Schwerpunkt war der Zugang zu Umweltinformationen. Sowohl die große Nachfrage der mehr als einhundert Teilnehmer als auch die intensiven Gespräche und Diskussionen während der Veranstaltung zeigten, dass gerade Vertreter aus den Kommunal- und Landesverwaltungen diesem Thema eine große Bedeutung für ihre tägliche Praxis beimessen. Bei der Bearbeitung eines Antrags auf Akteneinsicht müssen sie schließlich entscheiden, ob es sich um einen Fall des Akteneinsichts- und Informationszugangsgesetzes oder des Umweltinformationsgesetzes des Landes Brandenburg handelt – mit weit reichenden Unterschieden in den Rechtsfolgen.

Elf Präsentationen analysierten die europarechtlichen Grundlagen des Umweltinformationsrechts und richteten den Blick auf die Praxis in einzelnen Staaten. Die Nutzung der Informationsrechte durch Umweltverbände, die Bedeutung der Rechtsprechung sowie unterschiedliche rechtliche und institutionelle Ausgestaltungen von Informationsrechten wurden vorgestellt. Die Veranstaltung befasste sich auch mit den Veröffentlichungspflichten und deren technischer Umsetzung durch Umweltinformationssysteme. Experten aus Brandenburg, der Bundesrepublik, der Europäischen Union und ihren

Mitgliedsstaaten boten Einblicke in aktuelle Projekte und diskutierten die Rolle der Transparenz im Umweltschutz.

Das Internationale Symposium wurde gemeinsam mit der Alcatel-Lucent Stiftung für Kommunikationsforschung, der Deutschen Gesellschaft für Recht und Informatik sowie dem Unabhängigen Institut für Umweltfragen organisiert. Gefördert wurde das Symposium durch die Deutsche Bundesstiftung Umwelt. Insbesondere durch die erstmalige Zusammenarbeit mit den beiden letztgenannten Einrichtungen gelang es, neue Zielgruppen für das Anliegen der Informationsfreiheit anzusprechen. Die Vorträge sind auf der Website der Landesbeauftragten sowie als gedruckte Broschüre veröffentlicht.

7.2 Veranstaltungen der Landesbeauftragten

Nach diversen Skandalen wegen mangelnden Datenschutzes registrierte die Landesbeauftragte auf ihren Veranstaltungen in der Öffentlichkeit einen stetig steigenden Informationsbedarf.

Dies zeigte sich bereits im Juni 2008 auf dem Tag der offenen Tür des Abgeordnetenhauses von Berlin. Die Landesbeauftragte teilte sich dort einen Informationsstand mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit. Im September 2008 gestaltete die Landesbeauftragte mit ihren Mitarbeitern auf dem zweitägigen Brandenburg-Tag in Königs Wusterhausen ein Informationszelt rund um die Themen Datenschutz und Informationsfreiheit – wiederum unter Beteiligung ihres Berliner Kollegen. Sehr zahlreich nahmen sowohl Brandenburger als auch Berliner die Gelegenheit zu persönlichen Gesprächen wahr. Durch die Kooperation konnten stets konkrete Antworten zur Situation in beiden Ländern gegeben werden. Die Besucher erhielten Hinweise, welche Rechte sie insbesondere im Umgang mit den Behörden haben, um ihre Persönlichkeitssphäre zu schützen oder um öffentliche Informationen zu erhalten. Auch konkrete Beschwerden wurden erörtert. Im Mittelpunkt der Präsentationen der Landesbeauftragten stand ein Jubiläum: Mit dem Akteneinsichts- und Informationszugangsgesetz trat zehn Jahre zuvor erstmals in der Bundesrepublik ein Informationsfreiheitsgesetz in Kraft.

Im Mai 2008 führte die Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht gemeinsam mit dem Landesamt für Bergbau, Geologie und Rohstoffe, dem Landesamt für Mess- und Eichwesen Berlin-Brandenburg und dem Landeslabor Brandenburg einen Tag der offenen Tür im Fachbehördenzentrum am Stahnsdorfer Damm in Kleinmachnow – dem Dienstsitz der beteiligten Stellen – durch.

Eine Präsentation zur elektronischen Verarbeitung biometrischer Merkmale (Gesichtserkennung und Fingerabdrücke) stellte den Schwerpunkt des Informationsstandes der Landesbeauftragten im Juli 2009 auf dem Tag der offenen Tür des Landtages und der Landesregierung in Potsdam dar. Weiterhin führte die Landesbeauftragte persönliche Beratungen durch und bot zahlreiche Publikationen zum Mitnehmen an.

Auf Initiative des Europarats findet jährlich am 28. Januar der Europäische Datenschutztag statt, um in Europa das Bewusstsein für den Datenschutz zu fördern. Der zweite Europäische Datenschutztag 2008 wurde in der Bundesrepublik dezentral in den einzelnen Bundesländern begangen. Die Landesbeauftragte führte hierzu mehrere Veranstaltungen in brandenburgischen Schulen durch.

Der dritte Europäische Datenschutztag im Jahre 2009 wurde mit einer – auch von der Landesbeauftragten unterstützten – zentralen Diskussionsveranstaltung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder begangen. Thema war der Arbeitnehmerdatenschutz: „Die ideale Angestellte, der genormte Arbeitnehmer. Wie viel darf mein Arbeitgeber über mich wissen?“ Die Veranstaltung fand im Abgeordnetenhaus von Berlin statt.

7.3 Bürgersprechstunden

Nach der positiven Resonanz auf die zwei Jahre zuvor begonnenen Bürgersprechstunden entschied sich die Landesbeauftragte, diese im Berichtszeitraum fortzuführen. Um den Bürgerinnen und Bürgern einen unkomplizierten persönlichen Kontakt vor Ort zu ermöglichen, boten sie und ihre Mitarbeiter in den Räumen einiger Verwaltungen von Landkreisen und kreisfreien Städten jeweils eintägige Sprechstunden an. Wenn der Informationsstand im Eingangsbereich der Behörden nicht der richtige Ort für ein Gespräch war, bestand stets auch die Möglichkeit einer vertraulichen Beratung in einem separaten Raum.

Themenschwerpunkte vor Ort waren die Datenübermittlung auf dem Gebiet der Jugendhilfe, der Schutz von Personaldaten sowie ein datenschutzgerechter Umgang mit den neuen Medien. Insbesondere in den so genannten Optionskommunen, d. h. in jenen Landkreisen, die sich entschieden haben, die Betreuung von Hartz-IV-Empfängern in eigener Trägerschaft durchzuführen, stießen der Datenschutz bei der Grundsicherung für Arbeitssuchende sowie Fragen zur Zulässigkeit von Datenerhebung im Rahmen der Beantragung von Sozialleistungen auf großes Interesse. Informationen zu den Grenzen der Videoüberwachung sowie der Datenverarbeitung durch die Gebühreneinzugszentrale (GEZ) waren ebenso gefragt wie Hinweise zu den Einsichts-

rechten auf der Grundlage des Akteneinsichts- und Informationsfreiheitsgesetzes beziehungsweise des Umweltinformationsgesetzes.

Zwar nahmen in erster Linie Bürgerinnen und Bürger die Angebote der Landesbeauftragten wahr, doch nutzten auch Beschäftigte der Verwaltungen die Möglichkeit, Fragen zu stellen oder auch Beratungsgespräche zu führen. Sicherheitsaspekte der Informationstechnik in der öffentlichen Verwaltung standen dabei im Vordergrund: Wie ist mit mobilen Datenträgern umzugehen? Was genau muss eine öffentliche Stelle tun, wenn sie eine Risikoanalyse erstellt? Welchen Anforderungen muss ein Sicherheitskonzept genügen?

Im Jahre 2008 fanden die Bürgersprechstunden in Belzig (Potsdam-Mittelmark), Herzberg (Elbe-Elster), Eberswalde (Barnim), Rathenow (Havelland) und Oranienburg (Oberhavel) statt; im Jahr darauf in Cottbus, Lübben (Dahme-Spreewald) sowie in Brandenburg an der Havel. Ohne die freundliche Unterstützung der Landräte, der behördlichen Datenschutzbeauftragten sowie der Beschäftigten der Kreisverwaltungen wären diese Veranstaltungen nicht möglich gewesen – ihnen gilt unser herzlicher Dank.

7.4 Fortbildungsangebote

Wie schon in den vergangenen Jahren haben auch im Berichtszeitraum Mitarbeiterinnen und Mitarbeiter unserer Behörde eine ganze Reihe von Fortbildungsveranstaltungen zu unterschiedlichen Themen des Datenschutzes, der IT-Sicherheit sowie der Informationsfreiheit durchgeführt oder wesentlich inhaltlich gestaltet. In allen drei Bereichen zeigte sich eine große Nachfrage, die sich in der Anzahl der Veranstaltungen bzw. der Teilnehmer manifestierte. Im Mittelpunkt des Interesses standen neben der Vermittlung von rechtlichen und technisch-organisatorischen Grundlagen insbesondere die Auslegung und Anwendung von Rechtsvorschriften in der Praxis des täglichen Verwaltungshandelns sowie die Information über aktuelle Entwicklungen.

Die Themen der einzelnen Fortbildungsveranstaltungen sind in der folgenden Aufzählung zusammengefasst:

- Datenschutzrecht: Allgemeine Einführung in das Datenschutzrecht, Datenschutz in Kommunalverwaltungen, Datenschutz bei Personalvertretungen, Datenschutzgerechter Umgang mit Sozialdaten im Bereich des SGB II, Betreuungsrecht

- Technisch-organisatorischer Datenschutz, IT-Sicherheit: Datenschutz und Datensicherheit, Datenschutzmanagement, Erstellung von IT-Sicherheitskonzepten, IT-Grundschutz, Einführung von IT-Sicherheitsmanagement-

prozessen in der Kommunalverwaltung, Internet: Kriminalität und Sicherheit, Internet: Technische Risiken, Angriffsszenarien und Schutzmaßnahmen

- Informationsfreiheit: Einführung in das Akteneinsichts- und Informationszugangsgesetz, Informationszugang in Bauaufsichtsbehörden, Informationsfreiheit und Umweltinformationsrecht.

Wir wünschen uns, dass zukünftig auch Vertreter der Führungsebenen von öffentlichen Einrichtungen die Fortbildungsangebote unserer Behörde verstärkt nutzen. Datenschutz- und IT-Sicherheitsmanagement sind zunächst einmal Leitungsaufgaben. Erforderlich sind ein kontinuierliches, aktives Handeln sowie ein systematisches Vorgehen bei der Gestaltung der zugehörigen Prozesse. Nicht zuletzt unsere Umfrage im Bereich der brandenburgischen Kommunalverwaltung hat gezeigt, dass z. T. noch erhebliche Lücken und eine fehlende Sensibilität der Verantwortlichen zu verzeichnen sind.

7.5 Neue Publikationen der Landesbeauftragten

Anlässlich des zehnjährigen Bestehens des Akteneinsichts- und Informationszugangsgesetzes hat die Landesbeauftragte Vertreter der Zeit, in der das Gesetz diskutiert und auf den Weg gebracht wurde und die maßgeblich an seiner Entstehung beteiligt waren, Politiker der aktuell im Landtag vertretenen Parteien, Vertreter der Exekutive, Wissenschaftler, Journalisten und auch Bürger gebeten, ihre Sicht auf das Gesetz zu formulieren. Die Beiträge aus den verschiedenen Blickwinkeln wurden in der im März 2008 herausgegebenen Festschrift „Zehn Jahre Akteneinsichts- und Informationszugangsgesetz in Brandenburg“ durch Auszüge aus den Tätigkeitsberichten der Landesbeauftragten zum Akteneinsichts- und Informationszugangsgesetz ergänzt. Sie spiegeln typische Probleme sowie die Entwicklung des Gesetzes in den zehn Jahren wider.

Nach der amtlichen Neufassung des Brandenburgischen Datenschutzgesetzes im Mai 2008 wurde die bereits bestehende Broschüre im Rahmen der Reihe „Brandenburgisches Informationsgesetzbuch“ überarbeitet. In derselben Reihe wurden die einschlägigen Normen des ebenfalls im Berichtszeitraum in Kraft getretenen Verbraucherinformationsrechts neu aufgenommen. Nachdem sämtliche Ausgaben des Akteneinsichts- und Informationszugangsgesetzes sowie des Umweltinformationsrechts vergriffen waren, hat die Landesbeauftragte beide Publikationen neu aufgelegt. Zwar wurde das Bundesdatenschutzgesetz im Jahre 2009 nach diversen Skandalen wegen unzureichenden Datenschutzes in wesentlichen Punkten geändert. Die entsprechende Broschüre kann jedoch erst im Jahr 2010 in überarbeiteter Form herausgegeben werden, da die letzten Änderungen erst dann in Kraft treten.

Der gemeinsam mit dem Berliner Beauftragten für Datenschutz und Informationsfreiheit herausgegebene Ratgeber zu den datenschutzrechtlichen Gesichtspunkten von Hartz IV stößt sowohl bei Bürgerinnen und Bürgern als auch bei Behörden auf große Resonanz. Unter anderem geht es darin um die Frage, welche persönlichen Daten im Rahmen der Beantragung des Arbeitslosengeldes II beantwortet werden müssen. Dies ist auch für öffentliche Stellen, die entsprechende Fragebögen konzipieren, von Bedeutung. Aufgrund neuer gesetzlicher Regelungen haben sich auch die Befugnisse der zuständigen Behörden geändert. So besteht nunmehr die Möglichkeit, über das Bundeszentralamt für Steuern die Kontenstammdaten der Leistungsempfänger bei deren Kreditinstituten zu erheben. In der Praxis führt dies zu erheblicher Verunsicherung. Dies haben wir zum Anlass genommen, den Ratgeber entsprechend zu überarbeiten.

Insbesondere für Verwaltungen, die Anträge auf Informationszugang bearbeiten, sind die Anwendungshinweise der Landesbeauftragten zum Akteneinsichts- und Informationszugangsgesetz vorgesehen. Sie sind kein Kommentar zum Gesetz, sondern eine Zusammenstellung unserer in konkreten Fällen vertretenen Rechtsauffassung. Die Fortentwicklung des Informationsfreiheitsrechts und die Umsetzung dieser relativ neuen Rechte machten die Überarbeitung und Ergänzung der Anwendungshinweise erforderlich. Der neu aufgelegte Ratgeber steht seit Dezember 2009 wieder zur Verfügung. Er enthält auch für Antragsteller, die Einzelheiten zu ihren Informationsansprüchen erfahren möchten, wichtige Hinweise.

Im Nachgang zum Internationalen Symposium „Zugang zu Umweltinformationen – Informationsfreiheit für den Umweltschutz?“, das am 18./19. Juni 2009 in Potsdam stattfand, gab die Landesbeauftragte einen Tagungsband mit den Beiträgen der Referentinnen und Referenten heraus. Die Dokumentation ist als sechster Band in der Reihe „Potsdamer Materialien zu Akteneinsicht und Informationszugang“ erschienen.

Die genannten Publikationen können in gedruckter Form kostenlos bei der Landesbeauftragten bezogen werden. Sie stehen auch in elektronischer Form auf ihrer Website zur Verfügung.

Im Zusammenhang mit den Kontakten der Landesbeauftragten zu ihren internationalen Kolleginnen und Kollegen wurde mehrfach die Nachfrage nach einer englischen Übersetzung der wichtigsten Regelungen auf dem Gebiet des Datenschutzes und der Informationsfreiheit deutlich. Die Landesbeauftragte ließ daher das neu gefasste Brandenburgische Datenschutzgesetz ins Englische übersetzten.

Die Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet wurde vom Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Berichtszeitraum überarbeitet. Sie soll den für den Betrieb und die Konzeption von Netzen der öffentlichen Verwaltung Verantwortlichen deutlich machen, mit welchen Risiken für die Sicherheit der „internen“ Netze bei einem Anschluss an das Internet zu rechnen ist und wie diese Risiken begrenzt werden können.

Der Arbeitskreis Technik stellte im Berichtszeitraum drei weitere Handreichungen zur Verfügung: Die kurze Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ stellt heraus, dass personenbezogene Daten vor der Freigabe eines Systems ebenso schutzbedürftig sind wie nach dessen Freigabe. Dies ist in allen Phasen eines Projekts, insbesondere während des Testens, zu berücksichtigen. Die Orientierungshilfe „Protokollierung“ enthält grundlegende Empfehlungen für die praktische Ausgestaltung des Protokollierungsverfahrens für Daten verarbeitende Stellen. Zwar sehen die Datenschutzgesetze eine Pflicht zur Protokollierung vor, bieten jedoch kaum konkrete Vorgaben, um diese umzusetzen. Die Möglichkeiten und Grenzen des Einsatzes biometrischer Verfahren bei der Authentisierung thematisiert die dritte neue Orientierungshilfe.

Sowohl die englische Übersetzung des Brandenburgischen Datenschutzgesetzes als auch die Orientierungshilfen liegen ausschließlich in elektronischer Form vor und können von der Website der Landesbeauftragten heruntergeladen werden.

1 Auszug aus dem Geschäftsverteilungsplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Stand: 31. Dezember 2009

Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht	Frau Hartge
Stellvertreter	Herr Dr. Jendro
Sekretariat	Frau Objartel App. 10

Bereich Recht und Verwaltung

Bereichsleiter	Herr Dr. Jendro App. 34

Arbeitsgebiete:
- Rechtliche Grundsatzfragen
- Europaangelegenheiten
- Wissenschaft, Forschung und Kultur
- Landesrechnungshof
- Landtag, Staatskanzlei
- Rechtsfragen der elektronischen Verwaltung (E-Government)
- Beauftragter des Haushalts
- Ausbildung von Referendaren

Arbeitsgebiete: Frau Schraut, App. 41
- Polizei, Verfassungsschutz
- Verkehrsordnungswidrigkeiten
- Ausländer, Asylverfahren
- Staatsanwaltschaften
- Presse- und Öffentlichkeitsarbeit

Arbeitsgebiete:	Frau Burghardt
- Infrastruktur und Landwirtschaft	App. 45
- Umwelt und Verbraucherschutz	
- Personaldaten allgemein	
- Beratung behördlicher Datenschutzbeauftragter	

Arbeitsgebiete:	Herr Müller
- Akteneinsicht und Informationszugang	App. 20
- Redaktion von Veröffentlichungen	
- Koordination des Internetangebots	
- Presse- und Öffentlichkeitsarbeit	

Arbeitsgebiete:	Frau Peschenz
- Bildung, Jugend und Sport	App. 22

Arbeitsgebiete:	Frau Bultmann
- Gesundheit	App. 44
- Gesundheitsdaten allgemein	
- Familie	
- Justiz (außer Staatsanwaltschaften)	

Arbeitsgebiete:	Frau Oehme
- Arbeit und Soziales	App. 66
- Sozialdaten allgemein	
- Telekommunikation und Medien	

Arbeitsgebiete:	Herr Hoff
- Wirtschaft	App. 36
- Finanzen	

Arbeitsgebiete:	Frau Schnorr
- Kommunales	App. 40
- Inneres	
- Zweckverbände	

Arbeitsgebiete:	Frau Berndt
- Personal- und Verwaltungsangelegenheiten	App. 12
- Büroleitungsaufgaben	
- Haushaltsangelegenheiten	
- Beschaffungen	

Arbeitsgebiete: - Bibliothek - Schreibdienst - Informationsmaterialien	Frau Schäfer App. 43
Arbeitsgebiete: - Schreibdienst - Mitarbeit bei der Öffentlichkeitsarbeit - Pflege des Internetangebots	Frau Abel App. 42

Bereich Technik und Organisation

Bereichsleiter	Herr Dr. Reinke App. 31
Arbeitsgebiete: - Technisch/organisatorische Grundsatzfragen - komplexe IT-Verfahren - Technikfolgenabschätzung - Personalinformationssysteme - Dokumentenmanagementsysteme	
Arbeitsgebiete: - kryptographische Verfahren - elektronische Signaturen - Chipkartentechnologien - Kommunikationsnetze - Verzeichnisdienste - zentraler IT-Dienstleister, Landesverwaltungsnetz	Herr Müller App.32
Arbeitsgebiete - Risikoanalysen und Sicherheitskonzepte - Auditierung - Videoüberwachung - TK-Anlagen, VoIP - Protokollierung - Medien	Herr Budszus App. 35

Arbeitsgebiete: - Datenbanksysteme - Geoinformationssysteme - biometrische Verfahren - Einsatz von RFID - elektronische Akteneinsicht	Herr Vangermain App. 30
Arbeitsgebiete: - Statistik - Umgang mit Datenträgern - Langzeitarchivierung - Gebäude- und Raumsicherung	Herr Thiele App. 33
Arbeitsgebiete: - Computerkriminalität - elektronische Zahlverfahren - Einsatz von Laptops und mobilen Endgeräten - Wartung und Fernwartung	Frau Michaelis App. 71
Gleichstellungsbeauftragte	Frau Berndt App. 12
Personalrat	Frau Burghardt App. 45
Behördlicher Datenschutzbeauftragter	Herr Budszus App. 35

2 Aktenplan der Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Problemkreis	Bezeichnung
002	Akteneinsichts- und Informationszugangsgesetz
003	Arbeit
008	Ausländer
009	Bau-/Wohnungswesen
010	Landesregierung
024	Landtag/Parteien
027	Bildung/Kultur/Wissenschaft
028	BRD/Bund/Bundesländer
034	Allgemeines Datenschutzrecht
046	Zusammenarbeit Bundesbeauftragter für den Datenschutz/ Landesbeauftragte für den Datenschutz
054	Dateienregister LDA
056	Internationale Datenschutzangelegenheiten
061	Finanzen
062	Ernährung/Landwirtschaft/Forsten
066	Gesundheitswesen
078	Familie/Frauen/Jugend
082	Justiz
086	Kommunalrecht
089	Interne Verwaltung LDA
100	Öffentlichkeitsarbeit LDA
104	Inneres
108	Personaldatenverarbeitung
110	Polizei
128	Sozialwesen
132	Statistik
135	Technik
136	Medien/Telekommunikation/Post
138	Umwelt/Raumordnung/Stadtentwicklung
146	Verfassungsschutz
147	Verkehr
154	Wirtschaft/Technologie
163	Nicht öffentlicher Datenschutz
180	Personalräte
999	Sonstiges

3 Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

3.1 78. Konferenz vom 8. bis 9. Oktober 2009 in Berlin

3.1.1 Datenschutzdefizite in Europa auch nach Stockholmer Programm

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

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

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

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

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

- Abschluss von Übereinkommen mit Drittstaaten nur unter der Voraussetzung, dass die zwingenden Datenschutzgrundsätze dort beachtet werden.

- Ein unabhängiges datenschutzrechtliches Beratungs- und Kontrollorgan für alle Bereiche der polizeilichen und justiziellen Zusammenarbeit der EU-Mitgliedstaaten.

- Die Evaluation der vielen auf EU-Ebene beschlossenen sicherheitspolitischen Vorhaben im Hinblick auf ihre Effektivität, den Umfang der mit ihnen verbundenen Grundrechtseingriffe sowie mögliche Überschneidungen der Maßnahmen untereinander, bevor weitere Rechtsakte verabschiedet werden.

- Die Verbesserung von Transparenz und demokratischer Kontrolle bei der Rechtsetzung im Bereich der polizeilichen und justiziellen Zusammenarbeit auf europäischer Ebene, ungeachtet der Annahme des Vertrages von Lissabon.

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

3.1.2 Aktueller Handlungsbedarf beim Datenschutz – Förderung der Datenschutzkultur

Zunehmende Überwachung und die ausufernde Verknüpfung von Daten in Staat und Wirtschaft gefährden unser aller Persönlichkeitsrecht. Zusätzliche Herausforderungen ergeben sich aus der technologischen Entwicklung und der Sorglosigkeit der Bürgerinnen und Bürger.

Das aus den 70er Jahren des vorigen Jahrhunderts stammende Datenschutzrecht stellt längst keinen wirksamen Schutz mehr dar. Dies gilt ungeachtet der punktuellen Anpassungen, die das Bundesdatenschutzgesetz seither erfahren hat.

Zu Beginn der neuen Legislaturperiode des Deutschen Bundestags fordert die Konferenz der Datenschutzbeauftragten des Bundes und der Länder eine Generalrevision des Datenschutzrechts, einschließlich der jüngsten Novellierung zum Adresshandel.

Die Konferenz hält es insbesondere für erforderlich:

- Das Datenschutzrecht an die Herausforderungen neuer Technologien anzupassen und dabei z. B. die Rechte der Betroffenen bei der Nutzung des Internets, insbesondere auf Löschung ihrer Daten, zu verbessern;

- Die Integrität und Vertraulichkeit informationstechnischer Systeme zu gewährleisten;

- ein Beschäftigtendatenschutzgesetz zu erlassen und dabei vor allem die Überwachung am Arbeitsplatz effektiv zu begrenzen;

- die Vorratsdatenspeicherung und Online-Durchsuchung zurückzunehmen;

- die übrigen in den letzten Jahren verschärften Einschränkungen der Grundrechte durch Sicherheitsgesetze des Bundes und der Länder kritisch zu überprüfen;

- auf europäischer und internationaler Ebene auf hohe datenschutzrechtliche Grundstandards hinzuwirken und z. B. den verdachtslosen Zugriff auf Fluggast- und Bankdaten zurückzuweisen;

- im Fall der Einführung der elektronischen Gesundheitskarte die Betroffenenrechte umfassend zu realisieren;

- die Videoüberwachung in Staat und Gesellschaft einzuschränken;

- den Schutz der Meldedaten zu verbessern;

- ein praktikables Datenschutzaudit zu schaffen;

- die Datenschutzaufsichtsbehörden so auszugestalten, dass sie ihre Kontroll- und Beratungsaufgaben unabhängig und effektiv wahrnehmen können.

Datenschutz kann jedoch nicht nur verordnet, er muss auch gelebt werden. Dies setzt eine Datenschutzkultur in Staat, Wirtschaft und Gesellschaft voraus, die gepflegt und weiterentwickelt werden muss.

Die Konferenz spricht sich deshalb dafür aus, den Datenschutz auch als Bildungsaufgabe zu verstehen. Sie fordert Staat, Wirtschaft und Gesellschaft auf, ihre entsprechenden Bildungsanstrengungen zu verstärken. Ziel muss es sein, die Fähigkeit und Bereitschaft der Bürgerinnen und Bürger, insbesondere von Kindern und Jugendlichen, zu fördern, verantwortungsvoll mit ihren eigenen Daten und respektvoll mit den Daten anderer Menschen umzugehen.

3.1.3 Krankenhausinformationssysteme datenschutzgerecht gestalten!

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

Das Datenschutzrecht und die ärztliche Schweigepflicht gebieten, dass ein Zugriff auf die Daten von Kranken grundsätzlich nur denjenigen Krankenhausbeschäftigten möglich sein darf, die diese Kranken behandeln oder die Behandlung verwaltungsmäßig abwickeln.

Die Konferenz der Datenschutzbeauftragten fordert daher die datenschutzkonforme Gestaltung der internen Abläufe und der Erteilung von Zugriffsrechten in der Informationstechnik von Krankenhäusern.

Darüber hinaus fordert die Konferenz, dass Patienten nachvollziehen können, wer auf ihre Daten tatsächlich zugegriffen hat. Das ist Teil des Menschenrechts auf Achtung des Privatlebens nach Art. 8 der Europäischen Menschenrechtskonvention, wie der Europäische Gerichtshof für Menschenrechte klargestellt hat. Durch Protokollierung ist zu gewährleisten, dass eine nachträgliche Überprüfung der Zugriffe auf ihre Zulässigkeit möglich ist. Die Systeme müssen behandlungs- und patientenbezogen den technischen Zugriff gemäß den rechtlichen Befugnissen ermöglichen.

Die Krankenhäuser sind in der Pflicht, datenschutzgerechte Systeme einzusetzen. Die Software-Hersteller sind gehalten, entsprechende Systeme anzubieten.

3.1.4 Staatsvertrag zum IT-Planungsrat – Datenschutz darf nicht auf der Strecke bleiben

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die informationstechnische Kooperation von Bundes- und Landesbehörden zunehmend die Verarbeitung von personenbezogenen Daten betrifft, die durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen sind, etwa durch wirksame Verschlüsselungsverfahren.

Das Bundesverfassungsgericht hat die besondere Bedeutung der informationellen Selbstbestimmung und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme für den Schutz des Persönlichkeitsrechts hervorgehoben. Der in einem Staatsvertrag vorgesehene IT-Planungsrat muss diesen Vorgaben bei der Festlegung verbindlicher Interoperabilitäts- und IT-Sicherheitsstandards für die Datenverarbeitung Rechnung tragen. Für Entscheidungen in grundrechtssensiblen Fragestellungen muss auch der IT-Planungsrat die Zuständigkeit der Parlamente in Bund und Ländern berücksichtigen.

Die im Staatsvertrag vorgesehene vorrangige Verwendung bestehender Marktstandards darf nicht dazu führen, dass Verfahren ohne angemessenen Datenschutz beschlossen werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, dass der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit an den Sitzungen des IT-Planungsrats teilnehmen soll. Sie hält es für geboten, auch die Landesdatenschutzbeauftragten einzubeziehen.

3.1.5 „Reality-TV“ – keine Mitwirkung staatlicher Stellen bei der Bloßstellung von Menschen

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

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

Wird das Fernsehen durch zielgerichtete behördliche Unterstützung in die Lage versetzt, personenbezogene Filmaufnahmen anzufertigen, ist dies

rechtlich als Datenübermittlung an private Dritte zu werten. Für einen solchen massiven Eingriff in das Datenschutzgrundrecht der Betroffenen gibt es keine Rechtsgrundlage. Der Staat, der die Betroffenen zur Duldung bestimmter Eingriffsmaßnahmen zwingen kann, ist grundsätzlich nicht befugt, Dritten die Teilnahme daran zu ermöglichen. Auch das Vorliegen einer wirksamen vorherigen Einwilligung der Betroffenen wird regelmäßig zweifelhaft sein. Für eine solche Einwilligung ist es insbesondere notwendig, die betroffene Person rechtzeitig über Umfang, Dauer und Verwendungszwecke der Aufnahmen aufzuklären und auf die Freiwilligkeit seiner Einwilligung hinzuweisen. Angesichts der Überraschungssituation sowie der mit dem staatlichen Eingriff nicht selten verbundenen Einschüchterung ist hier eine besonders sorgfältige Prüfung geboten.

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

3.1.6 Kein Ausverkauf von europäischen Finanzdaten an die USA!

Für Zwecke der Terrorismusbekämpfung verhandeln die USA gegenwärtig mit der Europäischen Union über den Zugriff auf Daten über Finanztransaktionen, die auf SWIFT-Servern in Europa gespeichert werden, selbst wenn sie keinerlei Bezug zu den Vereinigten Staaten aufweisen. Besonders kritisch sieht es die Konferenz der Datenschutzbeauftragten des Bundes und der Länder, dass US-Behörden Zugriffsmöglichkeiten auf Transaktionsdaten anstreben, auch wenn gegen die Betroffenen kein hinreichend konkreter Verdacht besteht, dass sie an Terroraktivitäten oder an deren Unterstützung mitwirken oder beteiligt waren. Ein derartiges Abkommen würde US-Behörden Befugnisse einräumen, die in Deutschland den Sicherheitsbehörden von Verfassungs wegen verwehrt sind.

Ein derartiger weit reichender Eingriff in das Recht auf informationelle Selbstbestimmung weit im Vorfeld des strafrechtlichen Anfangsverdachtes wäre datenschutzrechtlich nicht zu rechtfertigen. Dies wäre auch im Hinblick auf den Vertrauensschutz europäischer Wirtschaftsunternehmen höchst fragwürdig. Der Datentransfer wäre auch deshalb bedenklich, weil die datenschutzrechtlichen Garantien in den USA deutlich hinter den entsprechenden Anforderungen in der Europäischen Union zurückbleiben. Insbesondere besteht dort keine unabhängige Datenschutzkontrolle; Personen ohne ständigen Wohnsitz in den USA haben kein Recht auf gerichtliche Überprüfung der Verwendung ihrer Daten durch US-Behörden.

Im Übrigen bestehen bereits an der Notwendigkeit eines so weit reichenden Zugriffs ausländischer Behörden auf in Europa gespeicherte Daten erhebli-

che Zweifel. So können Strafverfolgungsbehörden im Rahmen der Rechtshilfe schon heute einzelfallbezogen personenbezogene Daten zur Aufklärung von Terrorismusverdachtsfällen übermitteln.

Schließlich ist zu befürchten, dass eine derartige Regelung über den Zugriff auf SWIFT-Daten Präzedenzwirkung entfalten würde. Zum einen könnten die Vereinigten Staaten mit derselben Begründung Zugriff auf andere in Europa gespeicherte sensible Datenbestände verlangen, etwa die Vorratsdaten der Telekommunikation. Zum anderen wäre es schwer nachvollziehbar, warum die Europäische Union den USA einen so weitgehenden Zugriff auf in Europa gespeicherte Daten einräumt, entsprechende Forderungen anderer Drittstaaten aber zurückweisen sollte.

Die Konferenz erwartet von der Bundesregierung, dass sie die besonders sensiblen Bankdaten der Bürgerinnen und Bürger wirksam schützt und einem Abkommen nicht zustimmt, das eine Datenübermittlung weit unterhalb der Schwelle des strafrechtlichen Anfangsverdachts erlaubt und keine angemessenen datenschutzrechtlichen Standards festlegt.

3.2 Entschließung zwischen der 77. und 78. Konferenz 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 Bürgerinnnen und Bürgern und Verwaltung eine rechtlich gesicherte Kommunikation ermöglichen. Insbesondere sind über das Bürgerportal förmliche Zustellungen mit den entsprechenden Rechtsfolgen beabsichtigt. Dies darf nur auf Basis einer sicheren Anmeldung erfolgen. Die nach der Gesetzesbegründung ebenfalls mögliche unsichere Anmeldung mit Passwort wird abgelehnt.

- Der Nachweis der Absenderin oder des Absenders soll lediglich durch Anmeldung am Bürgerportal erfolgen. Das ermöglicht Angriffe durch Schadsoftware auf dem Rechner der Nutzenden. So könnten Zugangsdaten beschafft und widerrechtlich dazu verwendet werden, De-Mails zu versenden, empfangene De-Mails zu unterdrücken, zu verzögern und zu verändern oder unberechtigt auf Daten im De-Safe zuzugreifen. Deshalb sind zusätzliche Sicherungsmaßnahmen vorzusehen.

- Die Möglichkeit, eine pseudonyme Bürgerportaladresse zu nutzen, muss – entgegen der Stellungnahme des Bundesrates vom 3.4.2009 – erhalten bleiben. Denn die pseudonyme Nutzung ermöglicht gerade einen sinnvollen Kompromiss zwischen hinreichender Identifizierbarkeit im Rechtsverkehr und Datenschutz für die Nutzerinnen und Nutzer.

- Die Nutzerinnen und Nutzer müssen bei der Eröffnung des Bürgerportalkontos auf mögliche Rechtsfolgen – etwa zur verbindlichen Kommunikation mit staatlichen Stellen – hingewiesen werden. Die Aufklärungs- und Informationspflichten müssen im Gesetzestext klarer als bislang geschehen gefasst werden. Gleiches gilt für die Feststellung von Identitätsdaten und der Aufdeckung von Pseudonymen.

- Eine Benachteiligung von Bürgerinnen und Bürgern, die über kein Bürgerportalkonto verfügen, muss ausgeschlossen werden. Auch dürfen Bürgerportale nicht dazu führen, dass staatliche Stellen dazu übergehen, bei jeder Inanspruchnahme einer E-Government-Anwendung eine persönliche Identifizierung zu verlangen, selbst wenn dies für die konkrete Dienstleistung nicht erforderlich ist.

- Der Entwurf sieht vor, dass grundsätzliche Fragen der technischen Ausgestaltung der Bürgerportale und der darüber angebotenen Dienste in einer Rechtsverordnung geregelt werden sollen. Dies widerspricht der Rahmenkonzeption des Art. 80 GG und dient auch sonst nicht der Normenklarheit des Gesetzes. Zumindest die grundsätzlichen technisch-organisatorischen Anforderungen an die Eröffnung des Kontos, den Postfach- und Versanddienst, den Speicherplatz, den Identitätsbescheinigungsdienst und das Akkreditierungsverfahren sollten in das Gesetz selbst aufgenommen werden.

- Der Entwurf des Bürgerportalgesetzes sieht jetzt auch vor, dass nicht nur die Datenerhebung, sondern auch die Verarbeitung und Nutzung der erhobenen Daten durch den akkreditierten Dienstanbieter an eine enge Zweckbestimmung gebunden ist. Allerdings ist der pauschale Verweis auf die Regelungen des Bundesdatenschutzgesetzes, des Telemediengesetzes und des Telekommunikationsgesetzes in diesem Zusammenhang zu weitgehend, da so für die Diensteanbieter die Möglichkeit eröffnet wird, die personenbezogenen Daten für Werbung oder Marktforschungszwecke zu nutzen. Die Bürgerinnen und Bürger müssen jedoch sicher sein können, dass ihre Daten ausschließlich zur Teilnahme am Bürgerportal genutzt werden.

3.3 77. Konferenz vom 26. bis 27. März 2009 in Berlin

3.3.1 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.

3.3.2 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.

3.3.3 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 zu-

lässig. 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.

3.3.4 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 der 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.

3.4 Entschließung zwischen der 76. und 77. Konferenz 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.

3.5 76. Konferenz vom 6. bis 7. November 2008 in Bonn

3.5.1 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.

3.5.2 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 Finanz-

verwaltung durch das hierfür geeignete Verfahren der qualifizierten elektronischen Signatur abzusichern.

3.5.3 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.

3.5.4 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 aufgrund 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.

3.5.5 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.

3.5.6 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 er-

heblich 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.

3.5.7 Datenschutzgerechter Zugang zu Geoinformationen

Die Einführung einer einheitlichen Geodateninfrastruktur und die Veröffentlichung der staatlichen Daten eröffnen ein großes Potenzial 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 aufgrund 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.

3.5.8 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.

3.5.9 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 justiziel-

len 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.

3.5.10 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.

3.6 Entschließung zwischen der 75. und 76. Konferenz vom 16. September 2008

Entschlossenes Handeln ist das Gebot der Stunde

Zu den Überlegungen, welche Konsequenzen aus den jüngsten Datenschutzskandalen zu ziehen sind, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder heute folgende Entschließung gefasst:

„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 Gesetz-

geber 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."

3.7 75. Konferenz vom 3. bis 4. April 2008 in Berlin

3.7.1 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 „Daten-

schutz 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.

3.7.2 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.

3.7.3 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.

3.7.4 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 deutschamerikanische 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 Datenübermitt-

lungsbefugnisse 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.

3.7.5 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[111], 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 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.

3.7.6 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

[111] RL 2004/82 EG vom 29.4.2004 Amtsbl. L 261 (2004) S. 24 ff., Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die Beförderten zu übermitteln

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.

3.7.7 Vorgaben des Bundesverfassungsgerichts bei der Online-Durchsuchung beachten

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

2. Ein solches Grundrecht nimmt auch den Staat in die Verantwortung, sich aktiv für die Vertraulichkeit und Integrität informationstechnischer Systeme einzusetzen. Das Bundesverfassungsgericht verpflichtet den Staat, im Zeitalter der elektronischen Kommunikation Vertraulichkeit zu gewährleisten. Nunmehr ist der Gesetzgeber gehalten, diesen Auftrag konsequent umzusetzen. Dazu müssen die Regelungen, welche die Bürgerinnen und Bürger vor einer „elektronischen Ausforschung“ schützen sollen, gemäß den Vorgaben des Gerichts insbesondere im Hinblick auf technische Entwicklungen verbessert werden. Hiermit würde auch ein wesentlicher Beitrag geleistet, Vertrauen in die Sicherheit von E-Government und E-Commerce-Verfahren herzustellen.

3. Die Konferenz unterstützt die Aussagen des Gerichts zum technischen Selbstschutz der Betroffenen. Ihre Möglichkeiten, sich gegen einen unzulässigen Datenzugriff zu schützen, etwa durch den Einsatz von Verschlüsselungsprogrammen, dürfen nicht unterlaufen oder eingeschränkt werden.

4. Die Konferenz begrüßt außerdem, dass das Bundesverfassungsgericht das neue Datenschutzgrundrecht mit besonders hohen verfassungsrechtlichen Hürden vor staatlichen Eingriffen schützt. Sie fordert die Gesetzgeber in Bund und Ländern auf, diese Eingriffsvoraussetzungen zu respektieren. Die Konferenz spricht sich in diesem Zusammenhang gegen Online-Durchsuchungen durch die Nachrichtendienste aus.

5. Das Bundesverfassungsgericht hat den Gesetzgeber erneut verpflichtet, den unantastbaren Kernbereich privater Lebensgestaltung auch bei Eingriffen in informationstechnische Systeme zu gewährleisten. Unvermeidbar erhobene kernbereichsrelevante Inhalte sind unverzüglich zu löschen. Eine Weitergabe oder Verwertung dieser Inhalte ist auszuschließen.

6. Auch wenn Online-Durchsuchungen innerhalb der durch das Bundesverfassungsgericht festgelegten Grenzen verfassungsgemäß sind, fordert die Konferenz die Gesetzgeber auf, die Erforderlichkeit von Online-Durchsuchungsbefugnissen kritisch zu hinterfragen. Sie müssen sich die Frage stellen, ob sie den Sicherheitsbehörden entsprechende Möglichkeiten an die Hand geben wollen. Die Konferenz bezweifelt, dass dieser weiteren Einbuße an Freiheit ein adäquater Gewinn an Sicherheit gegenüber steht.

7. Sollten gleichwohl Online-Durchsuchungen gesetzlich zugelassen werden, sind nicht nur die vom Bundesverfassungsgericht aufgestellten verfassungsrechtlichen Hürden zu beachten. Die Konferenz hält für diesen Fall zusätzliche gesetzliche Regelungen für erforderlich. Zu ihnen gehören vor allem folgende Punkte:

   - Soweit mit der Vorbereitung und Durchführung von Online-Durchsuchungen der Schutzbereich von Art. 13 GG (Unverletzlichkeit der Wohnung) betroffen ist, bedarf es dafür jedenfalls einer besonderen Rechtsgrundlage.

   - Der vom Bundesverfassungsgericht geforderte Richtervorbehalt ist bei Online-Durchsuchungen mindestens so auszugestalten wie bei der akustischen Wohnraumüberwachung. Ergänzend zu einer richterlichen Vorabkontrolle ist eine begleitende Kontrolle durch eine unabhängige Einrichtung vorzuschreiben.

   - Gesetzliche Regelungen, welche Online-Durchsuchungen zulassen, sollten befristet werden und eine wissenschaftliche Evaluation der dabei gewonnenen Erkenntnisse und Erfahrungen anordnen.

   - Informationstechnische Systeme, die von zeugnisverweigerungsberechtigten Berufsgruppen genutzt werden, sind von heimlichen Online-Durchsuchungen auszunehmen.

   - Für die Durchführung von „Quellen-Telekommunikationsüberwachungen“, die mit der Infiltration von IT-Systemen einhergehen, sind die gleichen Schutzvorkehrungen zu treffen wie für die Online-Durchsuchung selbst.

8. Schließlich sind die Gesetzgeber in Bund und Ländern aufgrund der Ausstrahlungswirkung der Entscheidung des Bundesverfassungsgerichts gehalten, die sicherheitsbehördlichen Eingriffsbefugnisse in Bezug auf informationstechnische Systeme, z. B. bei der Überwachung der Telekommu-

nikation im Internet sowie der Beschlagnahme und Durchsuchung von Speichermedien, grundrechtskonform einzuschränken.

3.7.8 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 Aufga-

be 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.

4 Entschließungen der Konferenz der Informationsfreiheitsbeauftragten in Deutschland

4.1 19. Sitzung am 16. Dezember 2009 in Hamburg

„Regelungen zum Informationszugang der Bürgerinnen und Bürger vereinheitlichen!“

Die Konferenz der Informationsfreiheitsbeauftragten des Bundes und der Länder begrüßt die Ankündigung in der Koalitionsvereinbarung der neuen Bundesregierung, die Ansprüche der Verbraucherinnen und Verbraucher auf Information in einem einheitlichen Gesetz zur Regelung der Informationsansprüche der Bürgerinnen und Bürger zusammenzufassen.

Die Ansprüche auf Einsicht in Verwaltungsakten und auf Zugang zu sonstigen Informationen öffentlicher Stellen sind derzeit auf eine Vielzahl von Einzelvorschriften verteilt: Sie finden sich insbesondere im Informationsfreiheitsgesetz, im Umweltinformationsgesetz und im Verbraucherinformationsgesetz. Dabei werden vergleichbare Sachverhalte unterschiedlich geregelt, etwa die Voraussetzungen für den Informationszugang, die Fristen zur Beantwortung von Anfragen, die Gebühren, welche für den Informationszugang zu entrichten sind, und die Rechte auf Anrufung der Informationsfreiheitsbeauftragten. Diese Zersplitterung erschwert die Wahrnehmung der Rechte der Bürgerinnen und Bürger und trägt zu Unsicherheiten bei der Rechtsanwendung durch die Behörden bei.

Bei der anstehenden Überarbeitung sollten die Vorschriften so gestaltet werden, dass ein Höchstmaß an Transparenz und Bürgerfreundlichkeit erreicht wird. Die vielfältigen gesetzlichen Ausnahmetatbestände, wegen derer ein Informationszugang verweigert werden kann, gehören auf den Prüfstand.

4.2 18. Sitzung am 23./24. Juni 2009 in Magdeburg

4.2.1 „Mehr Transparenz durch gesetzlichen Schutz von Whistleblowern“

Beschäftigte, die Missstände und Rechtsverstöße in Behörden oder Unternehmen aufdecken (Whistleblower), sorgen dort für mehr Transparenz. Beispiele wie die Aufdeckung der sog. Gammelfleischskandale, der heimlichen Überwachung von Mitarbeiterinnen und Mitarbeitern, der Ausspähung von Telefonverbindungsdaten und der übermäßigen Erfassung von Gesundheitsdaten belegen das. Nur weil Beschäftigte betriebsinterne Vorgänge offenbarten, gelangten die Rechtsverstöße überhaupt ans Licht.

Das öffentliche Interesse an der Offenlegung von Missständen muss mit den zivil- und arbeitsrechtlichen Loyalitätspflichten der Beschäftigten gegenüber den Arbeitgeberinnen und Arbeitgebern in einen angemessenen Ausgleich gebracht werden. Transparenz kann nur erreicht und gefördert werden, wenn die Hinweisgeberinnen und Hinweisgeber keine Repressalien durch Arbeitgeberinnen und Arbeitgeber und die Kollegenschaft befürchten müssen.

Die Konferenz der Informationsfreiheitsbeauftragten fordert den Deutschen Bundestag auf, für mehr Informationsfreiheit einzutreten, indem endlich der Schutz von Whistleblowern gesetzlich festgeschrieben wird. Beschäftigte sollen keine arbeitsrechtlichen Konsequenzen befürchten müssen, nur weil sie Rechtsverstöße im Arbeitsumfeld anzeigen. Die Konferenz bedauert, dass ein erster Schritt hierzu, nämlich mit einem neuen § 612a BGB den Informantenschutz für Beschäftigte durch ein Anzeigerecht zu regeln, nicht weiterverfolgt wurde.

Der Gesetzgeber ist auch gehalten, den Transparenzgedanken und die datenschutzrechtlichen Belange der meldenden sowie der gemeldeten Person in ein ausgewogenes Verhältnis zu bringen. Hierfür hält die Konferenz folgende Erwägungen für maßgeblich:

- Zur Wahrung der schutzwürdigen Belange der Beteiligten sind verbindliche Verfahrensregeln in Behörden und Unternehmen unerlässlich.

- Whistleblowern muss die vertrauliche Behandlung des Hinweises zugesagt werden können.

- Auch die Rechte der belasteten Person, z. B. auf Benachrichtigung, Auskunft über sowie Berichtigung und Löschung von Daten, müssen berücksichtigt werden.

- Zum Schutz der Vertraulichkeit können Beschwerden an unabhängige ggf. externe Stellen (Ombudsleute) geschickt werden, die sie nur anonymisiert weitergeben dürfen.

4.2.2 „Informationszugang für Bürgerinnen und Bürger verbessern!“

Die Anwendung der Informationsfreiheitsgesetze in Bund und Ländern hat bewiesen: Der freie Zugang von Bürgerinnen und Bürgern zu Informationen öffentlicher Stellen ist auch in Deutschland fester Bestandteil der Demokratie. Seit 1998 haben nun schon elf Länder und der Bund ein allgemeines Informationsfreiheitsgesetz erlassen. Umweltinformationsgesetze und das Verbraucherinformationsgesetz ergänzen und erweitern den freien Zugang zu Informationen in spezifischen Bereichen.

In einer Vielzahl von Fällen haben die Bürgerinnen und Bürger Zugang zu amtlichen Informationen erhalten. Die Erfahrungen zeigen aber auch, dass sie immer wieder auf unnötige Hindernisse stoßen, wenn sie ihre Informationsrechte geltend machen wollen. So ist es für alle Beteiligten, auch für die Behörden, immer wieder schwer zu bestimmen, welches Informationszugangsrecht gilt. Zudem mindern teilweise ausufernde Ablehnungsgründe die Erfolgsaussichten von Zugangsanträgen.

Die Informationsfreiheitsbeauftragten halten es deshalb zugunsten einer größeren Transparenz des Verwaltungshandelns für geboten,

- einen unkomplizierten und umfassenden Zugang zu amtlichen Informationen zu ermöglichen
- Ausnahmen vom Informationszugang auf das unabdingbar notwendige Maß zu beschränken
- den Informationszugang grundsätzlich kostenfrei zu gewähren
- die Verfahren zur Rechtsdurchsetzung des Informationsanspruchs zu beschleunigen
- Veröffentlichungspflichten als zweite Säule des Informationszugangs im Sinne einer aktiven Informationspolitik zu stärken.

Die Konferenz der Informationsfreiheitsbeauftragten Deutschlands sieht darüber hinaus die Notwendigkeit, die Bewertung des Informationsfreiheitsgesetzes des Bundes auf unabhängiger wissenschaftlicher Grundlage anzugehen.

4.3 Entschließung zwischen der 17. und 18. Sitzung vom 26. Januar 2009

„Keine weitere Einschränkung der Transparenz bei Finanzaufsichtsbehörden“

Der Bundesrat hat im Zuge seiner Beratung des Zahlungsdiensteumsetzungsgesetzes (BT-Drs. 16/11613) vorgeschlagen, das Informationsfreiheitsgesetz des Bundes noch weiter einzuschränken: Ausgerechnet gegenüber Bundesbehörden der Finanz-, Wertpapier- und Versicherungsaufsicht soll es künftig kein Recht auf Informationszugang mehr geben. Die Entscheidung liegt jetzt beim Deutschen Bundestag.

Die Informationsfreiheitsbeauftragten in Deutschland lehnen die Schaffung einer solchen pauschalen Ausnahme entschieden ab. Es kann nicht sein, dass gerade bei den Aufsichtsbehörden, deren Tätigkeit durch die aktuelle Finanz- und Bankenkrise in die öffentliche Kritik geraten ist, die Transparenz noch weiter eingeschränkt wird. Das Vertrauen der Öffentlichkeit in die staatlichen Kontrollinstanzen sollte durch mehr Offenheit wiederhergestellt und nicht durch Einschränkung der Informationsfreiheit noch weiter erschüttert werden.

Informationen, die in diesem Bereich tatsächlich geheimhaltungsbedürftig sind, werden bereits heute durch das Informationsfreiheitsgesetz ausreichend geschützt. So müssen solche Informationen nicht offen gelegt werden, deren Bekanntwerden im jeweiligen Einzelfall nachteilige Auswirkungen auf die Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden haben kann; ohnehin sind Betriebs- und Geschäftsgeheimnisse sowie personenbezogene Daten geschützt. Damit besteht schon gegenwärtig im Bereich der Finanzaufsicht nur eine begrenzte Transparenz. Auch die Gerichte entwickeln hier differenzierte und sachgerechte Kriterien für die Anwendung der gesetzlichen Geheimhaltungsgründe. Diese von der Rechtsprechung eingeleitete Gesetzesauslegung nun durch eine Gesetzesänderung korrigieren zu wollen und den Zugang zu Informationen der Finanzaufsichtsbehörden gänzlich auszuschließen, widerspricht Sinn und Zweck des Informationsfreiheitsgesetzes und den berechtigten Auskunftsinteressen der Bürgerinnen und Bürger. Durch die vorgeschlagene Gesetzesänderung würde sogar der Zugang zu Informationen über solche Unternehmen ausgeschlossen, die kontinuierlich gegen schwerwiegende Straftatbestände verstoßen.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland appelliert an den Deutschen Bundestag, eine solche Einschränkung des Informationsfreiheitsgesetzes nicht zu beschließen.

4.4 17. Sitzung am 3./4. Dezember 2008 in Schwerin

„Die neue Konvention des Europarats zur Informationsfreiheit so bald wie möglich unterzeichnen und ratifizieren!“

Der Ministerausschuss des Europarats hat am 27. November 2008 den Entwurf einer Konvention über den Zugang zu amtlichen Dokumenten beschlossen. Mit ihrem Inkrafttreten wird die Konvention alle Vertragsstaaten verpflichten, jedem Menschen ein allgemeines Recht auf gebührenfreien Zugang zu Behördeninformationen einzuräumen, ohne dass dies begründet werden muss.

Es ist zu begrüßen, dass damit erstmals weltweit ein völkerrechtlich verbindlicher Vertrag zur Informationsfreiheit auf den Weg gebracht worden ist.

Jetzt ist die Bundesregierung aufgefordert, die Konvention so bald wie möglich zu unterzeichnen und dem Bundestag zur Ratifikation zuzuleiten, damit die Konvention schnell in Kraft treten kann. Die wenigen verbleibenden Bundesländer, die noch immer keine Informationsfreiheitsgesetze verabschiedet haben, müssen ihre Haltung jetzt dringend revidieren, damit die Bundesrepublik nicht zum Schlusslicht unter den Mitgliedstaaten des Europarats wird.

4.5 Entschließung zwischen der 16. und 17. Sitzung vom 30. Juni 2008

„Die Europäische Union braucht nicht weniger, sondern mehr Transparenz“

Mit der Verordnung 1049/2001 ist erstmals allen Unionsbürgerinnen und -bürgern der freie Zugang zu Dokumenten der Europäischen Union eröffnet worden. Die Verordnung hat unmittelbare Wirkung in allen Mitgliedstaaten, sodass auch deutsche Behörden, bei denen solche Dokumente vorliegen, sie beachten müssen.

Die Europäische Kommission hat nun allerdings Vorschläge vorgelegt, die – neben marginalen Verbesserungen – zu einer drastischen Einschränkung des Zugangs zu europäischen Dokumenten führen würden. Sie plant, den Zugang zu Dokumenten der EU-Institutionen künftig nur noch dann zu gestatten, wenn sie entweder bereits einem bestimmten Empfängerkreis übermittelt oder „registriert“ worden sind. Damit hätten die europäischen Behörden es selbst in der Hand, zu bestimmen, welche Dokumente sie herausgeben. Darüber hinaus sollen Informationen, die die EU-Institutionen von außen im Rahmen laufender Verfahren erhalten, auch nach deren Abschluss selbst dann unter Verschluss gehalten werden können, wenn an ihrer Offenlegung ein überwiegendes öffentliches Interesse besteht. Schließlich sollen die EU-Institutionen Dokumente geheim halten dürfen, die sie zur Vorbereitung von Entscheidungen nur einem bestimmten Kreis extern Beratender zugänglich gemacht haben.

Die Informationsfreiheitsbeauftragten in Deutschland sehen die Gefahr, dass bei einer Annahme dieser Vorschläge eine massive Einschränkung der gebotenen Transparenz des Handelns europäischer Institutionen die Folge wäre. Sie teilen die Kritik, die der Europäische Bürgerbeauftragte in seiner Stellungnahme gegenüber dem Ausschuss für Bürgerrechte, Justiz und Inneres des Europäischen Parlaments am 2. Juni 2008 geübt hat (Presseerklärung deutsch:

http://ombudsman.europa.eu/release/de/2008-06-02.htm.
Text der Stellungnahme nur englisch:
http://www.ombudsman.europa.eu/letters/en/20080526-1.htm).
Die deutschen Informationsfreiheitsbeauftragten fordern deshalb das Europäische Parlament und den Rat auf, den Vorschlägen der Kommission nicht zu folgen und stattdessen das Transparenzniveau bei den Institutionen der Europäischen Union spürbar zu erhöhen.

4.6 16. Sitzung am 11. Juni 2008 in Saarbrücken

„Transparenz in der Finanzverwaltung“

Die Informationsfreiheitsgesetze nehmen die Finanzverwaltung nicht von ihrem Anwendungsbereich aus. Deshalb gilt auch hier: Die grundsätzliche Offenheit der amtlichen Informationen gilt, sofern nicht eine in diesen Gesetzen geregelte Ausnahme (z. B. das Steuergeheimnis) greift.

In der Vergangenheit haben verschiedene Finanzbehörden häufig einen Anspruch der Bürgerinnen und Bürger auf Einsicht in eigene Steuerunterlagen sowie Verwaltungsvorgänge in das Behördenermessen gestellt. Der Bundesgesetzgeber habe mit dem Erlass der Abgabenordnung das steuerliche Verfahren abschließend geregelt und dort durch „absichtsvolles Unterlassen“ bewusst auf eine Regelung verzichtet. Nachdem das Bundesverfassungsgericht mit seinem Beschluss vom 10. März 2008 (1 BvR 2388/03) den Anspruch auf Informationen aus der eigenen Steuerakte für verfassungsrechtlich geboten erklärt hat, ist diese Argumentation nicht mehr länger haltbar.

Nichts anderes kann für die Anwendung der Informationsfreiheitsgesetze gelten, die jedem Menschen einen Anspruch auf Zugang zu den bei öffentlichen Stellen vorhandenen Informationen sichern. Der Zugang zur Information und die Transparenz behördlicher Entscheidungen ist eine wichtige Voraussetzung für die effektive Wahrnehmung von Bürgerrechten.

Die Konferenz der Informationsfreiheitsbeauftragten in Deutschland fordert die Finanzverwaltungen des Bundes und der Länder auf, die Informationsfreiheitsgesetze anzuwenden und in ihren nachgeordneten Bereichen durchzusetzen.

5 Übersicht aller Orientierungshilfen der Datenschutzbeauftragten

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat folgende Orientierungshilfen und Handreichungen erarbeitet. Auf der Website der Landesbeauftragten[112] können die einzelnen Dokumente heruntergeladen werden.

- Orientierungshilfe „Protokollierung“ (November 2009)
- Orientierungshilfe „Datenschutz und Datensicherheit in Projekten: Projekt- und Produktivbetrieb“ (November 2009)
- Orientierungshilfe „Biometrische Authentisierung – Möglichkeiten und Grenzen“ (November 2009)
- Orientierungshilfe „Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“ (November 2008)
- Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz (September 2007)
- Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ (Dezember 2006)
- Orientierungshilfe „Datenschutz bei Dokumentenmanagementsystemen“ (März 2006)
- Handlungsempfehlungen „Datenschutz bei technikunterstützten Verfahren der Personal- und Haushaltsbewirtschaftung“ (März 2006)
- Orientierungshilfe „Datenschutz in drahtlosen Netzen“ (September 2005)
- Handreichung „Die Virtuelle Poststelle im datenschutzgerechten Einsatz“ (November 2004)
- Orientierungshilfe „Datensicherheit bei USB-Geräten“ (November 2004)
- Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“ (2004)
- Orientierungshilfe zum Einsatz kryptografischer Verfahren (September 2003)

[112] siehe http://www.lda.brandenburg.de → Informationsmaterial

- Orientierungshilfe „Datenschutz bei Windows XP Professional“ (2003)
- Handreichung „Datenschutzgerechtes E-Government“ (November 2002)
- Empfehlungen zum Datenschutz bei Windows 2000 (2002)
- Orientierungshilfe „Datenschutzrechtliche Aspekte beim Einsatz von Verzeichnisdiensten“ (August 2000)
- Arbeitspapier „Datenschutzrechtliche Technologien in der Telekommunikation“ (Oktober 1997)
- Orientierungshilfe „Anforderungen zur informationstechnischen Sicherheit bei Chipkarten“ (Dezember 1996)

6 Abkürzungsverzeichnis

Abl.	=	Amtsblatt
Abs.	=	Absatz
ADV	=	Automatische Datenverarbeitung
AES	=	Advanced Encryption Standard
AFIG	=	Agrar- und Fischereifonds-Informationengesetz
AFIVO	=	Agrar- und Fischereifonds-Informationen-Verordnung
AO	=	Abgabenordnung
APC	=	Arbeitsplatzcomputer
Art.	=	Artikel
AsylbLG	=	Asylbewerberleistungsgesetz
AsylVfG	=	Asylverfahrensgesetz
AufenthG	=	Aufenthaltsgesetz
Az.	=	Aktenzeichen
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgDolmG	=	Brandenburgisches Dolmetschergesetz
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgKHEG	=	Brandenburgisches Krankenhausentwicklungsgesetz
BbgMeldG	=	Brandenburgisches Meldegesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgUVollzG	=	Brandenburgisches Untersuchungshaftvollzugsgesetz
BDSG	=	Bundesdatenschutzgesetz
BES	=	BlackBerry Enterprise Server
BGBl.	=	Bundesgesetzblatt
BKA	=	Bundeskriminalamt
BMF	=	Bundesministerium der Finanzen
BR-Drs.	=	Bundesratsdrucksache
BSI	=	Bundesamt für Sicherheit in der Informationstechnik
BSI-Gesetz	=	Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes
BT-Drs.	=	Bundestagsdrucksache
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
bzw.	=	beziehungsweise
CCC	=	Customer Competence Center
CERT BB	=	Computer Emergency Response Team Brandenburg
ComVor	=	Polizeiliches Vorgangsbearbeitungssystem
CSA	=	Cloud Security Alliance
3DES	=	Triple Data Encryption Standard
d. h.	=	das heißt
DMS/VBS	=	Dokumentmanagement- und Vorgangsbearbeitungssystem
DNA	=	Desoxyribonuclein Acid (Desoxyribonukleinsäure)

DV	=	Datenverarbeitung
EAP	=	Einheitliche Ansprechpartner
eBAnz.	=	Elektronischer Bundesanzeiger
EC	=	electronic cash
EFF	=	Europäischer Fischereifonds
EG	=	Europäische Gemeinschaft
EGFL	=	Europäischer Garantiefonds für die Landwirtschaft
EL.DOK BB	=	Elektronisches Dokumentmanagement- und Vorgangsbearbeitungssystem Land Brandenburg
ELENA	=	Verfahren des elektronischen Entgeltnachweises
ELER	=	Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums
endg.	=	endgültig
etc.	=	et cetera
EU	=	Europäische Union
EURODAC	=	Europäisches daktyloskopisches System
EUROJUST	=	Einheit für justizielle Zusammenarbeit der Europäischen Union
EUROPOL	=	Europäisches Polizeiamt
e. V.	=	eingetragener Verein
EWR	=	Europäischer Wirtschaftsraum
FIDIS	=	Future of Identity in the Information Society
ff.	=	fortfolgende
Fraunhofer SIT	=	Fraunhofer-Institut für Sichere Informationstechnologie
GAC	=	Google Analytics Code
GebOMLUV	=	Gebührenordnung des Ministeriums für Ländliche Entwicklung, Umwelt und Verbraucherschutz
gem.	=	gemäß
GEZ	=	Gebühreneinzugszentrale
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GSM	=	Global System for Mobile Communication
GVBl.	=	Gesetz- und Verordnungsblatt
HKR	=	Haushalts-, Kassen- und Rechnungswesen
IDM	=	Implementierung eines Identitätsmanagementsystems
i. d. R.	=	in der Regel
IMI	=	Internal Market Information System
INPOL	=	Polizeiliches Informationssystem
INSPIRE	=	Infrastructure for Spatial Information in the European Community
IT	=	Informationstechnik
Kfz	=	Kraftfahrzeug
LAN	=	Lokal Area Network
LBG	=	Landesbeamtengesetz

LDS	=	Landesbetrieb für Datenverarbeitung und Statistik
LVN	=	Landesverwaltungsnetz
MBJS	=	Ministerium für Bildung, Jugend und Sport
MESTA	=	Mehrländer-Staatsanwaltschaft-Automation
NFM	=	Neues Finanzmanagement
Nr.	=	Nummer
OSCI	=	Online Services Computer Interface
OWiG	=	Ordnungswidrigkeitengesetz
PaßG	=	Passgesetz
PC	=	Personal Computer
PDA	=	Personal Digital Assistant
PERIS	=	Personalinformationssystem
PersVG	=	Personalvertretungsgesetz für das Land Brandenburg
Pkt.	=	Punkt
PNR	=	Passenger Name Record
POLAS	=	Polizeiliches Auskunftssystem
PRIME	=	Privacy and Identity Management for Europe
RIM	=	Research in Motion
RIM NOC	=	RIM Network Operating Center
RIO	=	Ressort Information Officer
SeSamBB	=	Security and Safety made in Berlin-Brandenburg e. V.
SfFV	=	SprachfestFörderverordnung
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB II	=	Zweites Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
S/MIME	=	Secure/Multipurpose Internet Mail Extensions
SNC	=	Secure Network Communication
SSL	=	Secure Socket Layer
Steuer-ID	=	Steuer-Identifikationsnummer
StPO	=	Strafprozessordnung
StVG	=	Straßenverkehrsgesetz
SWIFT	=	Society for Worldwide Interbank Financial Telecommunication
TKG	=	Telekommunikationsgesetz
TMG	=	Telemediengesetz
TUIV-AG	=	Kommunale Arbeitsgemeinschaft Technikunterstützte Informationsverarbeitung im Land Brandenburg
TV	=	Television
u. a.	=	unter anderem
UMTS	=	Universal Mobile Telecommunications System
USA	=	United States of America (Vereinigte Staaten von Amerika)
US	=	United States
USB	=	Universal Serial Bus

usw.	=	und so weiter
u. U.	=	unter Umständen
vgl.	=	vergleiche
VIG	=	Verbraucherinformationsgesetz
VIS	=	Europäisches Visa-Informationssystem
VZR	=	Verkehrszentralregister
z. B.	=	zum Beispiel
ZIT-BB	=	Brandenburgischer IT-Dienstleister
z. T.	=	zum Teil

7 Stichwortverzeichnis

Abgabenordnung 29, 115
Abgeordneter 139
Abhören
  unbemerktes 108
Abwassergebühren 96
Adressmittlungsverfahren 130
Agrar- und Fischereifonds-Informationen-Gesetz 142
Agrarsubventionen 141
Akte
  elektronische 83
Akteneinsicht 100
Akteneinsichts- und Informationszugangsgebührenordnung 154
Aktenführung 116
Ambulanz
  forensische 104
Antragstellung
  elektronische 154
Arbeitgeber 111
Arbeitskreis Medien 160
Arbeitslosengeld II 110, 112
Arbeitsvertrag 112
Arzt 100, 111, 114, 123, 128, 129
Asylbewerberleistungsgesetz 66
Auskunft 100, 109
Authentifizierung 108, 122
Authentisierung 43, 47
Babybegrüßungsdienst 130
Bauamt
  virtuelles 48
Bauangelegenheiten 48, 49
Berufsgeheimnis 100
Betreuungscontrolling 124, 126
Betriebs- und Geschäftsgeheimnis 143, 147, 149, 152
Bewährungshelfer 104
Bewerbung 111
Bewertungsportal 22, 25
Bezahlplattform 45
Binnenmarktinformationssystem 121
BlackBerry 37
Blacklist 45
Bonitätsprüfung 45

Brandenburgisches Gesundheitsdienstgesetz 30, 123, 127, 128
Brandenburgisches Psychisch-Kranken-Gesetz 30
Brandenburgisches Schulgesetz 105, 107, 124
Brandenburgisches Statistikgesetz 106
Bundesagentur für Arbeit 115
Bundesamt für Sicherheit in der Informationstechnik 54, 66
Bundesanstalt für Landwirtschaft und Ernährung 142
Bundesverfassungsgericht 52
Bundeszentralamt für Steuern 115
Bürgerinitiative 154
Cloud Computing 33
Cookie 36
Datenabgleich 125, 128
Datenbank
  zentrale 119
Datengeheimnis 42
Datenlöschung 132
Datenschutzerklärung 37
Datenschutzverordnung Schulwesen 105
Datensparsamkeit 123
Datentrennungsgebot 47
Datenverarbeitung im Auftrag 37, 81
Dienstanweisung 130
Dienstleistungsportal der Landesverwaltung 121
Dienstleistungsrichtlinie
  europäische 120
Dienstvereinbarung 108
Direktionsrecht 93
Dokumentation
  medizinische 111
Dokumentationspflicht 115
Dolmetscher 98, 99
Dolmetscher- und Übersetzerverzeichnis 98
E-Government 43, 48
Eigenbetrieb 151
Einheitlicher Ansprechpartner 121
Einkommen 112
Einladungs- und Rückmeldewesen 127, 128
Einverständnis/Einwilligung 23, 24, 25, 44, 46, 49, 114, 125, 130, 132
EL.DOK BB 83
Elektronischer Entgeltnachweis 119
E-Mail und Internet
  am Arbeitsplatz 93
E-Mail-Push-Dienst 37

Empfangsbereich 112
Ende-zu-Ende-Verschlüsselung 86, 136
Entschließung 52
ePass-Verfahren 70
E-Payment 45, 48
Ereignisspeicher 108
Erforderlichkeit 96, 124
Ersterhebungsgrundsatz 112, 113
Fahrverbot 62
Fernmeldegeheimnis 53
Fernwartung/Fernzugriff 41
Finanzverwaltung 29
Fingerabdruck 71
Förderschule 108
Fraunhofer SIT 38
Freiwilligkeit 124, 127
Früherkennungsuntersuchung 127, 128
Führungsaufsichtsstelle 104
G 10-Kommission 66
Gebühren (Akteneinsicht) 154
Gegensprechanlage 108
Gehaltsbescheinigung 119
Gericht 99, 104
Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes 54
Gesundheitsamt 124, 126, 127, 129, 130
Gesundheitsdaten 93, 100, 111, 126, 128
Gesundheitsdienst 30
Google Analytics 36
Google Apps 35
Google-Cache 73
Grid Computing 34
Grundsicherung für Arbeitsuchende 110
Hartz-IV 110, 111, 112, 113
Hausbesuch 126, 127, 130
Haushalts-, Kassen- und Rechnungswesen 133, 135
Heimarbeitsplatzcomputer 40
Identitätsmanagement 46, 48
Informantendaten 27
Internet 26
Internetsperren 53
IP-Adresse 36
IP-Telefonie 85
IT-Grundschutzkatalog 66
IT-Sicherheitskonzept 65, 76, 130

IT-Sicherheitsmanagement 19, 78
JobCenter 115
Jugendamt 30, 104, 109, 123, 125, 127, 130
Justizvollzugsanstalt 104
Kinder- und Jugendgesundheitsdienstverordnung 123
Kindergarten 124, 125
Kinderpornografie 53
Kinderschutz 123, 126, 130
Kindertagesstätten 107, 125
Kontendatenabruf 115
Kontoauszug 110
Krankenhaus 122
Krankenkasse 132
Kundendaten 112
Landesbeamtengesetz 86
Landesgesundheitsamt 128
Landesmelderegister 69
Landwirtschaft 141
Laufzeitumgebung 32
Lebensmittel- und Futtermittelgesetzbuch 145
Lehrerrat 108
Medienkompetenz 21, 27
Mehrbedarf für kostenaufwändige Ernährung 110
Mehrländer-Staatsanwaltschafts-Automation MESTA 56
Meinungsfreiheit 25
Meldewesen 69, 125, 128, 130
Mobiler Bürgerservice 97
Mobilfunk 37
Netzwerk
  soziales 21, 52
Netzwerk „Gesunde Kinder“ 124
Neues Finanzmanagement 133, 135, 137
Notruf 108
Nutzungsrecht 24
Ordnungswidrigkeit 29
Organisationsplan 95
Parlamentarische Kontrollkommission 66
Personalakte
  automatisierte 87
Personalinformationssystem 89
Personalrat 88
Personalvertretungsgesetz 108
Persönlichkeitsrecht 21, 24, 25
Polizeiliches Auskunftssystem POLAS 56

Polizeiliches Vorgangsbearbeitungssystems ComVor 57
Portal 122
Privatsphäre 55
Projekt 21
Projekt „Datenschutz für Schüler und Lehrer“ 21
Prosoz 116
Protokollierung 94, 109, 113
Pseudonym 37
Recht am eigenen Bild 22
Reihenuntersuchung 124
Reisepass 70
Remote Access 41
Rundfunkgebühr 50
SAP R/3-System 133, 135
SAP-Leitstelle 137
Schule 23, 107
Schülerdatei
  automatisierte 105
Schülerlaufbahnstatistik 105
Schulstatistik 105
Schweigepflicht
  ärztliche 30, 100, 111, 114, 124, 126, 129
Schwerbehindertenausweis 114
Selbstständige 112
Serverkonsolidierung 32
Serviceportal 43
Signatur
  qualifizierte elektronische 49
Single-Sign-On 46
Smartphone 37
Sozialauswahl 92
Sozialbehörde 30, 127
Sozialdaten 111, 113, 132
Sozialdatenschutz 114
Sozialgeheimnis 112, 113, 114
Sperrliste 54
Spick mich 25
Sprachförderung 107
Sprachstandsfeststellung 107
Statistikstelle 106
Steuerpflichtige 29
Strafgesetzbuch 30
Straftat 55
Subventionsempfänger 142

Tagespflege 109, 125
Telearbeit 39
Telefax 128
Telekommunikationsüberwachung 51
Telemediengesetz 44, 46, 49, 55
Tierversuch 151
Tracking Tool 35
Transparenzinitiative 141
Übersetzer 98, 99
Umweltinformationen 162
Umweltinformationsgesetz 146, 149, 152, 153
Umweltinformationsrichtlinie 147
Unternehmensdaten 143, 147, 149, 151, 152
Untersuchungsgefangener 100
Untersuchungshaftvollzugsgesetz 99
Urheberrecht 22, 23, 24
USB-Schnittstelle 117
Verbraucherinformationsgesetz 145
Verfahrensverzeichnis 105
Verfassungsbeschwerdeverfahren 52
Verhaltens- und Leistungskontrolle 94
Verkehrszentralregister 63
Vermieter 111
Veröffentlichung 23, 24, 99, 106
Veröffentlichung von Mitarbeiterdaten 94
Verschlüsselung 46
Vertretungsbefugnis 153
Verwaltungsverfahrensrecht 146
Vier-Augen-Prinzip 138
Virtualisierung 34
Voice over IP 85
Volkszählung 75
Vorratsdatenspeicherung 51
Wartung 41, 42
Web Tracking 37
Weingesetz 145
Whistleblower 31
Zensus 75
Zentralisierung von IT-Strukturen 82
Zugangserschwerungsgesetz 53
Zuverlässigkeitsprüfung 59